Introducción a las Redes Companion Guide (CCNAv7) En Español

Aprenda de forma inmediata conceptos de redes, tecnologías, protocolos y dispositivos con el plan de estudios en línea.

Autorizado por NetTel
https://www.nettelperu.net

Objetivos

Enumerados al comienzo de cada capítuloAl final de cada capítulo hay un resumen. Sirve como ayuda para el estudio.

Cobertura temática

* Notas que señalan hechos interesantes. Ahorran tiempo y cuestiones importantes de seguridad.
* Resumen: Proporciona una sinopsis del capítulo y sirve como ayuda para el estudio.
* Práctica: laboratorios, y actividades de Packet Tracer

Lectura

Prácticas

Videos y animaciones

Luis González

Un curso de formación, un examen

Obtener la certificación CCNA es el primer paso en la preparación para una carrera en tecnologías de TI. Para obtener la certificación CCNA, aprueba un examen que cubre una amplia gama de fundamentos para las carreras de TI, basado en las últimas tecnologías de redes, habilidades de desarrollo de software y roles laborales.
CCNA le brinda la base que necesita para llevar su carrera en cualquier dirección.

Prerrequisitos

No existen requisitos previos formales para la certificación CCNA, pero debe tener una comprensión de los temas del examen antes de realizar el examen.
Los candidatos de CCNA a menudo también tienen:

- Uno o más años de experiencia implementando y administrando soluciones de Cisco
- Conocimiento del direccionamiento IP básico
- Una buena comprensión de los fundamentos de la red.

A quién está dirigido

A los estudiantes de CCNA de NetTel.

Agradecimientos

A NetTel por brindar la oportunidad de realizar este curso.
A mi bruja personal (casi esposa jaja) por aguantar que me acueste tarde estudiando (sí, estudiando).

Sobre este documento

Este documento está realizado sobre la base del contenido de la plataforma Netacad de Cisco. Se adjuntan screenshot de las imágenes, videos y hasta de los test realizados en todos los capítulos, tanto en idioma Inglés como español.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Indíce

Tabla de contenido

INTRODUCCIÓN A LAS REDES 31
NETWORKING ACADEMY CCNAV7 31
NETWORKING ACADEMY CCNAV7 31

CAPÍTULO 1_REDES HOY 32

INTRODUCCIÓN 32

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 32
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 32

LAS REDES AFECTAN NUESTRAS VIDAS 33

LAS REDES NOS CONECTAN 33
VIDEO - LA EXPERIENCIA DE APRENDIZAJE EN CISCO NETWORKING ACADEMY 33
NO HAY LÍMITES 34

COMPONENTES DE LA RED 35

ROLES DE HOST 35
ENTRE PARES 36
DISPOSITIVOS FINALES 37
DISPOSITIVOS INTERMEDIARIOS 39
MEDIOS DE RED 40
VERIFIQUE SU COMPRENSIÓN: COMPONENTES DE RED 41
REPRESENTACIONES DE RED 43
DIAGRAMAS DE TOPOLOGÍA 44
VERIFIQUE SU COMPRENSIÓN: REPRESENTACIONES DE RED Y TOPOLOGÍAS 47

TIPOS COMUNES DE REDES 48

REDES DE MUCHOS TAMAÑOS 48
LAN Y WAN 51
EL INTERNET 54
INTRANETS Y EXTRANETS 55
VERIFIQUE SU COMPRENSIÓN: TIPOS DE REDES COMUNES 56

CONEXIONES A INTERNET 58

TECNOLOGÍAS DE ACCESO A INTERNET 58
CONEXIONES A INTERNET DOMÉSTICAS Y DE OFICINAS PEQUEÑAS 58
CONEXIONES A INTERNET EMPRESARIALES 59
LA RED CONVERGENTE 61
VIDEO: DESCARGUE E INSTALE PACKET TRACER 62
VÍDEO - INTRODUCCIÓN A CISCO PACKET TRACER 63
PACKET TRACER: REPRESENTACIÓN DE LA RED 64

REDES CONFIABLES 64

ARQUITECTURA DE RED 64
TOLERANCIA A FALLAS 65
ESCALABILIDAD 66
CALIDAD DE SERVICIO 67
SEGURIDAD DE LA RED 68
VERIFIQUE SU COMPRENSIÓN - REDES CONFIABLES 69

TENDENCIAS DE RED 71

TENDENCIAS RECIENTES 71
TRAIGA SU PROPIO DISPOSITIVO (BYOD) 72
COLABORACIÓN EN LÍNEA 73
COMUNICACIONES DE VIDEO 73
VÍDEO - CISCO WEBEX PARA HUDDLES 74
COMPUTACIÓN EN LA NUBE 74
TIPOS DE NUBES 75
TENDENCIAS TECNOLÓGICAS EN EL HOGAR 76
REDES POWERLINE 78
BANDA ANCHA INALÁMBRICA 79
VERIFIQUE SU COMPRENSIÓN - TENDENCIAS DE RED 80

SEGURIDAD DE LA RED 82

AMENAZAS DE SEGURIDAD 82
SOLUCIONES DE SEGURIDAD 83
VERIFIQUE SU COMPRENSIÓN - SEGURIDAD DE RED 85

EL PROFESIONAL DE TI 86

CCNA 86

EMPLEOS DE REDES 87
LABORATORIO - INVESTIGUE LAS OPORTUNIDADES DE TRABAJO EN REDES Y TI 87

MÓDULO DE PRÁCTICA Y PRUEBA 88

¿QUÉ APRENDÍ EN ESTE MÓDULO? 88
PRUEBA DEL MÓDULO - REDES EN LA ACTUALIDAD 91

CAPÍTULO 2_CONFIGURACIÓN BÁSICA DE SWITCHES Y TERMINALES 95

INTRODUCCIÓN 95

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 95
¿QUÉ APRENDERÁ EN ESTE MÓDULO? 96

ACCESO A CISCO IOS 96

SISTEMAS OPERATIVOS 97
GUI 98
PROPÓSITO DEL OS 99
EJEMPLO DE DESCARGA DE SOFTWARE DE CISCO 100
MÉTODOS DE ACCESO 100
PROGRAMAS DE EMULACIÓN DE TERMINAL 101
VERIFIQUE SU COMPRENSIÓN - ACCESO CISCO IOS 103

NAVEGACIÓN IOS 106

MODOS DE COMANDO PRINCIPAL 106
MODO DE CONFIGURACIÓN Y MODOS DE SUBCONFIGURACIÓN 107
VIDEO - IOS CLI MODOS DE COMANDO PRINCIPAL 108
NAVEGACIÓN ENTRE LOS MODOS DE IOS 108
VIDEO - NAVEGACIÓN ENTRE LOS MODOS DE IOS 109
UNA NOTA SOBRE LAS ACTIVIDADES DEL VERIFICADOR DE SINTAXIS 110
COMPROBADOR DE SINTAXIS - NAVEGAR ENTRE LOS MODOS IOS 110
COMPRUEBE SU COMPRENSIÓN - NAVEGACIÓN DEL IOS 112

LA ESTRUCTURA DE LOS COMANDOS 115

ESTRUCTURA BÁSICA DE COMANDOS DE IOS 115
COMPROBACIÓN DE LA SINTAXIS DEL COMANDO DE IOS 116
FUNCIONES DE AYUDA DE IOS 117
VIDEO - AYUDA SENSIBLE AL CONTEXTO Y VERIFICACIÓN DE SINTAXIS DE COMANDOS 118

TECLAS DE ACCESO RÁPIDO Y MÉTODOS ABREVIADOS 118
VIDEO - TECLAS DE ACCESO RÁPIDO Y MÉTODOS ABREVIADOS 120
PACKET TRACER - NAVEGA POR EL IOS 121
LABORATORIO: NAVEGUE POR EL IOS MEDIANTE TERA TERM PARA LA CONECTIVIDAD DE LA CONSOLA 121

CONFIGURACIÓN BÁSICA DE DISPOSITIVOS 122

NOMBRES DE LOS DISPOSITIVOS 122
PAUTAS DE LA CONTRASEÑA 124
CONFIGURACIÓN DE CONTRASEÑAS 124
ENCRIPTACIÓN DE LAS CONTRASEÑAS 126
MENSAJES DE AVISO 126
VIDEO - PROTEGER EL ACCESO ADMINISTRATIVO A UN SWITCH 127
COMPROBADOR DE SINTAXIS - CONFIGURACIÓN BÁSICA DE DISPOSITIVOS 128
COMPRUEBE SU COMPRENSIÓN - CONFIGURACIÓN BÁSICA DEL DISPOSITIVO 129

GUARDAR LAS CONFIGURACIONES 132

ARCHIVOS DE CONFIGURACIÓN 132
MODIFICACIÓN DE LA CONFIGURACIÓN EN EJECUCIÓN 133
VIDEO - MODIFICACIÓN DE LA CONFIGURACIÓN EN EJECUCIÓN 134
CAPTURA DE CONFIGURACIÓN A UN ARCHIVO DE TEXTO 135
PACKET TRACER - CONFIGURE AJUSTES INICIALES DEL SWITCH 137

PUERTOS Y DIRECCIONES 137

DIRECCIONES IP 137
INTERFACES Y PUERTOS 140
COMPRUEBE SU COMPRENSIÓN - PUERTOS Y DIRECCIONES 141

CONFIGURAR DIRECCIONAMIENTO IP 143

CONFIGURACIÓN MANUAL DE DIRECCIÓN IP PARA DISPOSITIVOS FINALES 143
CONFIGURACIÓN AUTOMÁTICA DE DIRECCIONES IP PARA DISPOSITIVOS FINALES 145
COMPROBADOR DE SINTAXIS - VERIFICAR LA CONFIGURACIÓN IP DE WINDOWS PC 146
CONFIGURACIÓN DE INTERFAZ VIRTUAL DE SWITCH 147
VERIFICADOR DE SINTAXIS: CONFIGURACIÓN DE UNA INTERFAZ VIRTUAL DE SWITCH 148
PACKET TRACER: IMPLEMENTACIÓN DE CONECTIVIDAD BÁSICA 148

VERIFICAR LA CONECTIVIDAD 148

ACTIVIDAD DE VÍDEO - PRUEBA LA ASIGNACIÓN DE INTERFAZ 149
VIDEO - PRUEBA DE CONECTIVIDAD DE EXTREMO A EXTREMO 149

MODULE PRACTICE AND QUIZ 150

PACKET TRACER — CONFIGURACIÓN BÁSICA DEL SWITCH Y DEL DISPOSITIVO FINAL 150
LAB - CONFIGURACIÓN BÁSICA DE SWITCH Y DISPOSITIVO FINAL 151
¿QUÉ APRENDIÓ EN ESTE MÓDULO? 151
PRUEBA DEL MÓDULO - CONFIGURACIÓN BÁSICA DEL SWITCH Y EL DISPOSITIVO FINAL 152

CAPÍTULO 3_PROTOCOLOS Y MODELOS 160

INTRODUCCIÓN 160

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 160
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 161
ACTIVIDAD DE CLASE: DISEÑO DE UN SISTEMA DE COMUNICACIONES 162

LAS REGLAS 162

VÍDEO - DISPOSITIVOS EN UNA BURBUJA 162
FUNDAMENTOS DE LA COMUNICACIÓN 163
PROTOCOLOS DE COMUNICACIÓN 163
ESTABLECIMIENTO DE REGLAS 165
REQUISITOS DE PROTOCOLO DE RED 165
CODIFICACIÓN DE LOS MENSAJES 166
FORMATO Y ENCAPSULAMIENTO DEL MENSAJE 167
TAMAÑO DEL MENSAJE 169
SINCRONIZACIÓN DEL MENSAJE 171
OPCIONES DE ENTREGA DEL MENSAJE 171
UNA NOTA SOBRE EL ICONO DE NODO 175
VERIFIQUE SU COMPRENSIÓN- LAS REGLAS 176

PROTOCOLOS 179

DESCRIPCIÓN GENERAL DEL PROTOCOLO DE RED 179
FUNCIONES DE PROTOCOLO DE RED 180
INTERACCIÓN DE PROTOCOLOS 181
VERIFIQUE SU COMPRESIÓN: PROTOCOLOS 183

SUITES DE PROTOCOLOS 186

CONJUNTOS DE PROTOCOLOS DE RED 186
EVOLUCIÓN DE LOS CONJUNTOS DE PROTOCOLOS 187
EJEMPLO DE PROTOCOLO TCP/IP 189
CONJUNTO DE TCP/IP 189
PROCESO DE COMUNICACIÓN TCP/IP 193
VERIFIQUE SU COMPRESIÓN: - PROTOCOLOS 197

ORGANIZACIONES ESTÁNDARES 201

ESTÁNDARES ABIERTOS 201
ESTÁNDARES DE INTERNET 202
ORGANIZACIONES DE ESTÁNDARES PARA COMUNICACIONES Y ELECTRÓNICA 205
LABORATORIO: INVESTIGACIÓN DE ESTÁNDARES DE REDES 205
COMPRUEBE SU COMPRENSIÓN - ORGANIZACIONES DE ESTÁNDARES 206

MODELOS DE REFERENCIA 209

BENEFICIOS DEL USO DE UN MODELO EN CAPAS 209
EL MODELO DE REFERENCIA OSI 211
MODELO DE PROTOCOLO TCP/IP 212
COMPARACIÓN DEL MODELO OSI Y EL MODELO TCP/IP 213
PACKET TRACER: INVESTIGACIÓN DE LOS MODELOS TCP/IP Y OSI EN ACCIÓN 215

ENCAPSULAMIENTO DE DATOS 216

SEGMENTACIÓN DEL MENSAJE 216
SECUENCIACIÓN 218
UNIDADES DE DATOS DE PROTOCOLO 219
EJEMPLO DE ENCAPSULAMIENTO 221
EJEMPLO DE DESENCAPSULAMIENTO 222
VERIFIQUE SU COMPRENSIÓN: PROTECCIÓN DE DATOS 223

ACCESO A LOS DATOS 225

DIRECCIONES 225
DIRECCIÓN LÓGICA DE CAPA 3 226
DISPOSITIVOS EN LA MISMA RED 228
FUNCIÓN DE LAS DIRECCIONES DE LA CAPA DE ENLACE DE DATOS: LA MISMA RED IP 229
DISPOSITIVOS EN UNA RED REMOTA 230
FUNCIÓN DE LAS DIRECCIONES DE LA CAPA DE RED 230
ROL DE ACCESO A DATOS DE LAS DIRECCIONES DE CAPA DE VÍNCULO DE DATOS: DIFERENTES REDES IP 232
DIRECCIONES DE ENLACE DE DATOS 233

PRÁCTICA DE LABORATORIO: INSTALACIÓN DE WIRESHARK 237
PRÁCTICA DE LABORATORIO: USO DE WIRESHARK PARA VER EL TRÁFICO DE LA RED 237
PONGA A PRUEBA SU CONOCIMIENTO: ACCESO DE DATOS 238

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 242

¿QUÉ APRENDERÉ EN ESTE MÓDULO? 242
MÓDULO QUIZ - PROTOCOLOS Y MODELOS 245

CAPÍTULO 4_CAPA FÍSICA 254

INTRODUCCIÓN 254

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 254
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 254

PROPÓSITO DE LA CAPA FÍSICA 255

LA CONEXIÓN FÍSICA 255
ROUTER INALÁMBRICO 256
CONEXIÓN POR CABLE AL ROUTER INALÁMBRICO 256
CONEXIÓN POR CABLE CON UNA NIC ETHERNET 257
LA CAPA FÍSICA 257
COMPRUEBE SU COMPRENSIÓN - PROPÓSITO DE LA CAPA FÍSICA 258

CARACTERÍSTICAS DE LA CAPA FÍSICA 260

ESTÁNDARES DE LA CAPA FÍSICA 261
COMPONENTES FÍSICOS 262
CODIFICACIÓN 263
SEÑALIZACIÓN 264
ANCHO DE BANDA 266
TERMINOLOGÍA DEL ANCHO DE BANDA 266
VERIFIQUE SU COMPRENSIÓN - CARACTERÍSTICAS DE LA CAPA FÍSICA 268

CABLEADO DE COBRE 271

CARACTERÍSTICAS DEL CABLEADO DE COBRE 271
TIPOS DE CABLEADO DE COBRE 273
PAR TRENZADO NO BLINDADO (UTP) 274
PAR TRENZADO BLINDADO (STP) 275
CABLE COAXIAL 276

COMPRUEBE SU COMPRENSIÓN - CABLEADO DE COBRE 277

CABLEADO UTP 279

PROPIEDADES DEL CABLEADO UTP 279
CONECTORES Y ESTÁNDARES DE CABLEADO UTP 280
CABLE UTP MAL TERMINADO 283
CABLE UTP CORRECTAMENTE TERMINADO 283
CABLES UTP DIRECTOS Y CRUZADOS 283
TIPOS DE CABLES Y ESTÁNDARES 285
ACTIVIDAD - PINOUTS DE CABLE 285

CABLEADO DE FIBRA ÓPTICA 287

PROPIEDADES DEL CABLEADO DE FIBRA ÓPTICA 287
TIPOS DE MEDIOS DE FIBRA 288
USO DEL CABLEADO DE FIBRA ÓPTICA 289
CONECTORES DE FIBRA ÓPTICA 290
CABLES DE CONEXIÓN DE FIBRA 292
FIBRA VERSUS COBRE 295
COMPRUEBE SU COMPRENSIÓN - CABLEADO DE FIBRA ÓPTICA 296

MEDIOS INALÁMBRICOS 298

PROPIEDADES DE LOS MEDIOS INALÁMBRICOS 298
TIPOS DE MEDIOS INALÁMBRICOS 299
LAN INALÁMBRICA 300
CISCO MERAKI MX64W 301
COMPRUEBE SU COMPRENSIÓN — MEDIOS INALÁMBRICOS 301
PACKET TRACER - CONECTE UNA LAN CABLEADA E INALÁMBRICA 303
LAB - VER INFORMACIÓN DE NIC CABLEADA E INALÁMBRICA 304

MÓDULO DE PRÁCTICA Y PRUEBA 304

PACKET TRACER - CONECTAR LA CAPA FÍSICA 304
¿QUÉ APRENDIÓ EN ESTE MÓDULO? 305
PRUEBA DEL MÓDULO: LA CAPA FÍSICA 307

CAPÍTULO 5_ SISTEMAS NUMÉRICOS 316

INTRODUCCIÓN 316

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 316
¿QUÉ APRENDERÁ EN ESTE MÓDULO? 316

SISTEMA DE NUMERACIÓN BINARIA 317

DIRECCIONES BINARIAS E IPV4 317
VIDEO - CONVERSIÓN ENTRE SISTEMAS DE NUMERACIÓN BINARIOS Y DECIMALES 319
NOTACIÓN DE POSICIÓN BINARIA 320
VERIFIQUE SU COMPRENSIÓN - SISTEMA DE NÚMEROS BINARIOS 321
CONVERTIR BINARIO A DECIMAL 323
ACTIVIDAD - CONVERSIÓN DE SISTEMA BINARIO A DECIMAL 325
CONVERSIÓN DE SISTEMA DECIMAL A BINARIO 326
EJEMPLO DE CONVERSIÓN DE SISTEMA DECIMAL A BINARIO 331
ACTIVIDAD - CONVERSIONES DE DECIMAL A BINARIO 338
ACTIVIDAD: JUEGO BINARIO 338
DIRECCIONES IPV4 339

SISTEMA NUMÉRICO HEXADECIMAL 340

VIDEO - CONVERSIÓN ENTRE SISTEMAS DE NUMERACIÓN HEXADECIMALES Y DECIMALES 343
CONVERSIONES DECIMALES A HEXADECIMALES 343
CONVERSIÓN HEXADECIMAL A DECIMAL 344
COMPRUEBE SU COMPRENSIÓN - SISTEMA DE NÚMEROS HEXADECIMALES 344

MÓDULO DE PRÁCTICA Y PRUEBA 345

¿QUÉ APRENDIÓ EN ESTE MÓDULO? 345
PRUEBA DE MÓDULO - SISTEMAS NUMÉRICOS 346

CAPÍTULO 6_CAPA DE ENLACE DE DATOS 353

INTRODUCCIÓN 353

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 353
¿QUÉ APRENDERÁ EN ESTE MÓDULO? 354

PROPÓSITO DE LA CAPA DE ENLACE DE DATOS 354

LA CAPA DE ENLACE DE DATOS 354
SUBCAPAS DE ENLACE DE DATOS IEEE 802 LAN/MAN 356
PROVISIÓN DE ACCESO A LOS MEDIOS 358
ESTÁNDARES DE LA CAPA DE ENLACE DE DATOS 359

LOGOTIPOS DE LA ORGANIZACIÓN DE INGENIERÍA 360
COMPRUEBE SU COMPRENSIÓN - PROPÓSITO DE LA CAPA DE ENLACE DE DATOS 360

TOPOLOGÍAS 364

TOPOLOGÍAS FÍSICA Y LÓGICA 364
TOPOLOGÍA FÍSICA 366
TOPOLOGÍA LÓGICA 367
TOPOLOGÍAS DE WAN 367
TOPOLOGÍA WAN DE PUNTO A PUNTO 369
TOPOLOGÍAS DE LAN 370
TOPOLOGÍAS FÍSICAS 371
COMUNICACIÓN DÚPLEX COMPLETO Y SEMIDÚPLEX 372
MÉTODOS DE CONTROL DE ACCESO 373
ACCESO POR CONTENCIÓN: CSMA/CD 375
ACCESO POR CONTENCIÓN: CSMA/CA 377
COMPRUEBE SU COMPRENSIÓN - TOPOLOGÍAS 378

TRAMA DE ENLACE DE DATOS 381

LA TRAMA 382
CAMPOS DE TRAMA 383
DIRECCIONES DE CAPA 2 384
TRAMAS LAN Y WAN 387
COMPRUEBE SU COMPRENSIÓN — TRAMA DE ENLACE DE DATOS 389

MÓDULO DE PRÁCTICA Y PRUEBA 391

¿QUÉ APRENDERÉ EN ESTE MÓDULO? 391
PRUEBA DEL MÓDULO — CAPA DE ENLACE DE DATOS 393

CAPÍTULO 7_SWITCHING ETHERNET 402

INTRODUCCIÓN 402

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 402
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 403

TRAMAS DE ETHERNET 403

ENCAPSULAMIENTO DE ETHERNET 403
ETHERNET Y EL MODELO OSI 404

SUBCAPAS DE ENLACE DE DATOS 404
SUBCAPA MAC 406
CAMPOS DE TRAMA DE ETHERNET 407
DETALLE DE CAMPOS DE TRAMA DE ETHERNET 408
COMPRUEBE SU COMPRENSIÓN - ETHERNET SWITCHING 410
LAB - UTILIZAR WIRESHARK PARA EXAMINAR TRAMAS DE ETHERNET 414

DIRECCIÓN MAC DE ETHERNET 414

DIRECCIÓN MAC Y HEXADECIMAL 414
EQUIVALENTES DECIMALES Y BINARIOS A LOS VALORES HEXADECIMALES DEL 0 AL F 415
EQUIVALENTES DECIMALES, BINARIOS Y HEXADECIMALES SELECCIONADOS 416
DIRECCIÓN MAC DE ETHERNET 417
PROCESAMIENTO DE TRAMAS 418
DIRECCIÓN MAC DE UNICAST 421
DIRECCIÓN MAC BROADCAST 423
DIRECCIÓN MAC DE MULTICAST 424
LAB - VER LAS DIRECCIONES MAC DEL DISPOSITIVO DE RED 426

TABLA DE DIRECCIONES MAC 427

FUNDAMENTOS DE SWITCHES 427

SWITCH, APRENDIENDO Y REENVIANDO 428
FILTRADO DE TRAMAS 430
VIDEO: TABLAS DE DIRECCIONES MAC EN SWITCHES CONECTADOS 432
VIDEO - ENVÍO DE UNA TRAMA AL GATEWAY PREDETERMINADO 433
ACTIVIDAD: ¡EL SWITCH! 434
LAB - VISUALIZACIÓN DE LA TABLA DE DIRECCIONES MAC DEL SWITCH 435

VELOCIDADES Y MÉTODOS DE REENVÍO DEL SWITCH 436

MÉTODOS DE REENVÍO DE TRAMAS DE LOS SWITCHES CISCO 436
SWITCHING POR MÉTODO DE CORTE 438
ALMACENAMIENTO EN BÚFER DE MEMORIA EN LOS SWITCHES 439
MÉTODO DE ALMACENAMIENTO EN BÚFER DE MEMORIA 439
CONFIGURACIÓN DE DÚPLEX Y VELOCIDAD 440
AUTO-MDIX (MDIX AUTOMÁTICO) 442
COMPRUEBE SU COMPRENSIÓN — CAMBIAR VELOCIDADES Y MÉTODOS DE REENVÍO 443

MÓDULO DE PRÁCTICA Y PRUEBA 446

¿QUÉ APRENDIÓ EN ESTE MÓDULO? 446
PRUEBA DE MÓDULO- ETHERNET SWITCHING 447

CAPÍTULO 8_CAPA DE RED 456

INTRODUCCIÓN 456

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 456
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 456

CARACTERÍSTICAS DE LA CAPA DE RED 457

LA CAPA DE RED 457
PROTOCOLOS DE CAPA DE RED 457
ENCAPSULACIÓN IP 460
CARACTERÍSTICAS DE IP 461
SIN CONEXIÓN 461
SERVICIO MÍNIMO 462
INDEPENDIENTE DE LOS MEDIOS 463
VERIFIQUE SU COMPRENSIÓN - CARACTERÍSTICAS DE IP 465

PAQUETE IPV4 467

ENCABEZADO DE PAQUETES IPV4 467
CAMPOS DE ENCABEZADO DE PAQUETE IPV4 468
CAMPOS DEL ENCABEZADO DE PAQUETES IPV4 468
VIDEO: EJEMPLOS DE ENCABEZADOS IPV4 EN WIRESHARK 470
VERIFIQUE SU COMPRENSIÓN - PAQUETE IPV4 470

PAQUETE IPV6 473

LIMITACIONES DE IPV4 473
INFORMACIÓN GENERAL SOBRE IPV6 473
COMPARACIÓN DEL ESPACIO DE DIRECCIONES IPV4 E IPV6 474
CAMPOS DE ENCABEZADO DE PAQUETE IPV4 EN EL ENCABEZADO DE PAQUETE IPV6 475
ENCABEZADO DE PAQUETES IPV4 476
ENCABEZADO DE PAQUETES IPV6 477
ENCABEZADO DE PAQUETES IPV6 477
CAMPOS DEL ENCABEZADO DE PAQUETES IPV6 478
VIDEO: EJEMPLOS DE ENCABEZADOS IPV6 EN WIRESHARK 479
VERIFIQUE SU COMPRENSIÓN - PAQUETE IPV6 479

¿CÓMO ARMA LAS RUTAS EL HOST? 482

LA DECISIÓN DE REENVÍO DE HOST 482
GATEWAY PREDETERMINADO 484
UN HOST ENRUTA A LA PUERTA DE ENLACE PREDETERMINADA 484
TABLAS DE ENRUTAMIENTO DE HOST 485
TABLA DE ENRUTAMIENTO IPV4 PARA LA PC1 486
COMPRUEBE SU COMPRENSIÓN - CÓMO ENRUTA UN HOST 486

INTRODUCCIÓN AL ENRUTAMIENTO 489

DECISIÓN DE ENVÍO DE PAQUETES DEL ROUTER 489
TABLA DE ENRUTAMIENTO IP DEL ROUTER 490
ENRUTAMIENTO ESTÁTICO 491
ENRUTAMIENTO DINÁMICO 493
VIDEO- TABLAS DE ENRUTAMIENTO DE ROUTER IPV4 495
INTRODUCCIÓN A UNA TABLA DE ENRUTAMIENTO IPV4 496
VERIFIQUE SU COMPRENSIÓN - INTRODUCCIÓN AL ENRUTAMIENTO 498

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 501

¿QUÉ APRENDERÉ EN ESTE MÓDULO? 501
MÓDULO QUIZ - CAPA DE RED 503

CAPÍTULO 9_RESOLUCIÓN DE DIRECCIONES 511

INTRODUCCIÓN 511

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 511
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 512

MAC E IP 512

DESTINO EN LA MISMA RED 512
DESTINO EN UNA RED REMOTA 513
PACKET TRACER: IDENTIFICACIÓN DE DIRECCIONES MAC Y DIRECCIONES IP 516
VERIFIQUE SU COMPRENSIÓN: MAC E IP 517

ARP 519

DESCRIPCIÓN GENERAL DE ARP 519
FUNCIONES DEL ARP 520

VIDEO - SOLICITUD DE ARP 523
VÍDEO - FUNCIONAMIENTO DE ARP - RESPUESTA DE ARP 524
VIDEO - ROL ARP EN COMUNICACIONES REMOTAS 526
ELIMINACIÓN DE ENTRADAS DE UNA TABLA ARP 526
TABLAS ARP EN DISPOSITIVOS DE RED 527
PROBLEMAS DE ARP: BROADCASTS ARP Y ARP SPOOFING 528
PACKET TRACER: EXAMINAR LA TABLA ARP 530
VERIFIQUE SU COMPRENSIÓN - ARP 530

DETECCIÓN DE VECINOS IPV6 534

VIDEO - DETECCIÓN DE VECINOS IPV6 534
MENSAJES DE DESCUBRIMIENTO DE VECINOS IPV6 534
DESCUBRIMIENTO DE VECINOS IPV6: RESOLUCIÓN DE DIRECCIONES 535
PACKET TRACER - DETECCIÓN DE VECINOS IPV6 537
COMPRUEBE SU COMPRENSIÓN - DETECCIÓN DE VECINOS 537

MÓDULO DE PRÁCTICA Y PRUEBA 539

¿QUÉ APRENDIÓ EN ESTE MÓDULO? 539
PRUEBA DE MÓDULO - RESOLUCIÓN DE DIRECCIONES 540

CAPÍTULO 10_CONFIGURACIÓN BÁSICA DE UN ROUTER 548

INTRODUCCIÓN 549

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 549
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 549

CONFIGURACIÓN DE LOS PARÁMETROS INICIALES DEL ROUTER 550

PASOS BÁSICOS EN LA CONFIGURACIÓN DE UN ROUTER 550
CONFIGURACIÓN BÁSICA DE UN ROUTER 551
COMPROBADOR DE SINTAXIS - CONFIGURAR LOS AJUSTES INICIALES DEL ENRUTADOR 552
PACKET TRACER: CONFIGURACIÓN INICIAL DEL ROUTER 554

CONFIGURACIÓN DE INTERFACES 554

CONFIGURAR INTERFACES DE ROUTERS 554
EJEMPLO DE CONFIGURACIÓN DE INTERFACES DE ROUTERS 555
VERIFICACIÓN DE CONFIGURACIÓN DE INTERFAZ 556
CONFIGURACIÓN COMANDOS DE VERIFICACIÓN 557

COMPROBADOR DE SINTAXIS - CONFIGURAR INTERFACES. 562

CONFIGURACIÓN DEL GATEWAY PREDETERMINADO 563

GATEWAY PREDETERMINADO PARA UN HOST 563
GATEWAY PREDETERMINADO PARA UN SWITCH 565
COMPROBADOR DE SINTAXIS - CONFIGURAR LA PUERTA DE ENLACE PREDETERMINADA 567
PACKET TRACER: CONEXIÓN DE UN ROUTER A UNA LAN 567
PACKET TRACER: SOLUCIÓN DE PROBLEMAS DEL GATEWAY PREDETERMINADO 567

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 568

VIDEO - DIFERENCIAS DE DISPOSITIVOS DE RED: PARTE 1 568
VIDEO - DIFERENCIAS DE DISPOSITIVOS DE RED: PARTE 2 569
PACKET TRACER - CONFIGURACIÓN BÁSICA DEL DISPOSITIVO 569
LABORATORIO: ARMAR UNA RED CON UN SWITCH Y UN ROUTER 570
¿QUÉ APRENDÍ EN ESTE MÓDULO? 570
PRUEBA DEL MÓDULO: CONFIGURACIÓN BÁSICA DE UN ROUTER. 571

CAPÍTULO 11_ DIRECCIONAMIENTO IPV4 579

INTRODUCCIÓN 579

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 579
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 579

ESTRUCTURA DE LA DIRECCIÓN IPV4 580

PORCIONES DE RED Y DE HOST 580
LA MÁSCARA DE SUBRED 581
CONFIGURACIÓN IPV4 EN UN EQUIPO CON WINDOWS 581
MÁSCARA DE SUBRED 582
LA LONGITUD DE PREFIJO 583
COMPARACIÓN DE LA MÁSCARA DE SUBRED Y LA LONGITUD DE PREFIJO 584
DETERMINACIÓN DE LA RED: LÓGICA AND 584
VIDEO - DIRECCIONES DE RED, HOST Y BROADCAST 586
DIRECCIONES DE RED, DE HOST Y DE DIFUSIÓN 586
DIRECCIONES DE RED, DE HOST Y DE DIFUSIÓN 588
ACTIVIDAD: USO DE LA OPERACIÓN AND PARA DETERMINAR LA DIRECCIÓN DE RED 589
COMPRUEBE SU COMPRENSIÓN - ESTRUCTURA DE DIRECCIONES IPV4 590

IPV4 UNICAST, BROADCAST, Y MULTICAST 593

UNIDIFUSIÓN 593
TRANSMISIÓN DE UNICAST 594
DIRECCIÓN 594
TRANSMISIÓN DE DIFUSIÓN LIMITADA 595
MULTIDIFUSIÓN 596
ACTIVIDAD: UNIDIFUSIÓN, DIFUSIÓN Y MULTIDIFUSIÓN? 597

TIPOS DE DIRECCIONES IPV4 598

DIRECCIONES IPV4 PÚBLICAS Y PRIVADAS 598
ESTOS SON LOS BLOQUES DE DIRECCIONES PRIVADAS 599
ENRUTAMIENTO EN INTERNET 599
TRADUCCIÓN DE DIRECCIONES DE RED (NAT), PARA UTILIZAR DIRECCIONES IP PRIVADAS .. 600
ACTIVIDAD: ADMITIR O BLOQUEAR DIRECCIONES IPV4 601
DIRECCIONES IPV4 DE USO ESPECIAL 602
PING A LA INTERFAZ DE BUCLE INVERTIDO 603
DIRECCIONAMIENTO CON CLASE ANTIGUA 603
RESUMEN DE ASIGNACIÓN DE DIRECCIONES CON DISTINCIÓN DE CLASES 604
ASIGNACIÓN DE DIRECCIONES IP 605
REGISTROS REGIONALES DE INTERNET 605
ACTIVIDAD: DIRECCIONES IPV4 PÚBLICAS O PRIVADAS 606
VERIFIQUE SU COMPRENSIÓN - TIPOS DE DIRECCIONES IPV4 607

SEGMENTACIÓN DE LA RED 609

DOMINIOS DE DIFUSIÓN Y SEGMENTACIÓN 609
PROBLEMAS CON LOS DOMINIOS DE DIFUSIÓN GRANDES 611
RAZONES PARA SEGMENTAR REDES 612
VERIFIQUE SU COMPRENSIÓN - SEGMENTACIÓN DE RED 615

DIVISIÓN DE SUBREDES DE UNA RED IPV4 616

DIVISIÓN EN SUBREDES EN EL LÍMITE DEL OCTETO 616
MÁSCARAS DE SUBRED EN LÍMITES DE OCTETO 617
RED DE SUBREDES 10.0.0.0/8 USANDO UN /16 618
RED DE SUBREDES 10.0.0.0/8 MEDIANTE UN PREFIJO /24 618
SUBRED DENTRO DE UN LÍMITE DE OCTETO 619
SUBRED A / 24 RED 619
VÍDEO: LA MÁSCARA DE SUBRED 619
VIDEO - SUBRED CON EL NÚMERO MÁGICO 620
PACKET TRACER - SUBRED UNA RED IPV4 621

SUBRED UNA BARRA DIAGONAL 16 Y UN PREFIJO DE BARRA DIAGONAL 8 621

CREAR SUBREDES CON UN PREFIJO SLASH 16 ..... **621**
SUBRED A / 16 RED 622
CREE 100 SUBREDES CON UN PREFIJO SLASH 16 ..... **622**
CANTIDAD DE SUBREDES CREADAS 623
RED 172.16.0.0/23 624
RESULTADO: SUBREDES DE /23 625
INTERVALO DE DIRECCIONES PARA LA SUBRED 172.16.0.0/23 626
CREE 1000 SUBREDES CON UN PREFIJO SLASH 8 ..... **626**
CANTIDAD DE SUBREDES CREADAS 627
RED 10.0.0.0/18 627
SUBREDES /18 RESULTANTES 628
INTERVALO DE DIRECCIONES PARA LA SUBRED 10.0.0.0/18 629
VIDEO: SUBRED EN VARIOS OCTETOS **629**
ACTIVIDAD: CÁLCULO DE MÁSCARA DE SUBRED **630**
PRÁCTICA DE LABORATORIO: CÁLCULO DE SUBREDES IPV4 ..... **631**

DIVISIÓN EN SUBREDES PARA CUMPLIR CON REQUISITOS **631**

ESPACIO DE DIRECCIONES IPV4 PRIVADO DE SUBRED FRENTE AL ESPACIO PÚBLICO **631**
ESPACIO DE DIRECCIONES IPV4 PÚBLICO Y PRIVADO 632
RED DE SUBREDES 10.0.0.0/8 USANDO UN /16 632
RED DE SUBREDES 10.0.0.0/8 USANDO UN /24 633
MINIMIZAR LAS DIRECCIONES IPV4 DE HOST NO UTILIZADAS Y MAXIMIZAR LAS SUBREDES. **634**
DIVISIÓN DE UNA RED /24 EN SUBREDES 635
EJEMPLO: SUBREDES IPV4 EFICIENTES **635**
DIRECCIÓN DE RED 636
TOPOLOGÍA CORPORATIVA CON CINCO SITIOS 636
ESQUEMA DE SUBREDES 637
ASIGNACIONES DE SUBRED A CADA SITIO E ISP 638
ACTIVIDAD: DETERMINAR LA CANTIDAD DE BITS QUE SE DEBEN TOMAR PRESTADOS **638**
PACKET TRACER: DIVISIÓN EN SUBREDES, SITUACIÓN **639**

VLSM **639**

VÍDEO - ASPECTOS BÁSICOS DE VLSM **639**
VIDEO: EJEMPLO DE VLSM **640**
CONSERVACIÓN DE DIRECCIONES IPV4 ..... **641**
ESQUEMA DE SUBREDES BÁSICO 642
DIRECCIONES SIN UTILIZAR EN SUBREDES WAN 644
VLSM **644**
ESQUEMA BÁSICO DE SUBREDES 646
ESQUEMA DE DIVISIÓN EN SUBREDES DE VLSM 647
ASIGNACIÓN DE DIRECCIONES DE TOPOLOGÍA VLSM **649**

ACTIVIDAD - VLSM PRACTICE 650
192.168.5.0/24 | TABLA 1 - PRIMER CÁLCULO DE SUBREDES 651
192.168.5.0/24 | TABLA 2 - CÁLCULO DE VLSM 652

DISEÑO ESTRUCTURADO 653

PLANIFICACIÓN DE DIRECCIONES DE RED IPV4 653
ASIGNACIÓN DE DIRECCIONES DE DISPOSITIVO 654
PACKET TRACER - PRÁCTICA DE DISEÑO E IMPLEMENTACIÓN DE VLSM 654

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 655

"PACKET TRACER: DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE DIRECCIONAMIENTO VLSM" 655
PRÁCTICA DE LABORATORIO: DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE DIRECCIONAMIENTO VLSM 655
¿QUÉ APRENDÍ EN ESTE MÓDULO? 656
MÓDULO QUIZ - DIRECCIONAMIENTO IPV4 659

CAPÍTULO 12_ASIGNACIÓN DE DIRECCIONES IPV6 668

INTRODUCCIÓN 668

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 668
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 668

PROBLEMAS CON IPV4 669

NECESIDAD DE UTILIZAR IPV6 669
FECHAS DE AGOTAMIENTO DE LAS DIRECCIONES IPV4 DE RIR 670
COEXISTENCIA DE IPV4 E IPV6 671
VERIFIQUE SU COMPRENSIÓN - PROBLEMAS DE IPV4 673

DIRECCIONAMIENTO DINÁMICO PARA LAS GUAS DE IPV6 675

FORMATOS DE DIRECCIONAMIENTO IPV6 675
SEGMENTOS O HEXETOS DE 16 BITS 675
REGLA 1: OMITIR LOS CEROS INICIALES 676
OMISIÓN DE CEROS INICIALES 677
REGLA 2 - DOBLE COLON 677
OMITIR 0 A LA IZQUIERDA Y TODOS LOS 0 SEGMENTOS 679
ACTIVIDAD: REPRESENTACIÓN DE DIRECCIÓN IPV6 679

TIPOS DE DIRECCIONES IPV6 681

UNIDIFUSIÓN, MULTIDIFUSIÓN, DIFUSIÓN ILIMITADA 681
LONGITUD DE PREFIJO IPV6 681
LONGITUD DE PREFIJO IPV6 682
TIPOS DE DIRECCIONES DE UNIDIFUSIÓN IPV6 682
UNA NOTA SOBRE LA DIRECCIÓN LOCAL ÚNICA 683
IPV6 GUA 684
DIRECCIÓN IPV6 CON UN PREFIJO DE ENRUTAMIENTO GLOBAL /48 Y UN PREFIJO /64 685
ESTRUCTURA IPV6 GUA 685
IPV6 LLA 687
COMUNICACIONES DE ENLACE LOCAL DE IPV6 687
VERIFIQUE SU COMPRENSIÓN - TIPOS DE DIRECCIÓN IPV6 688

CONFIGURACIÓN ESTÁTICA DE GUA Y LLA 691

CONFIGURACIÓN DE GUA ESTÁTICA EN UN ROUTER 691
TOPOLOGÍA DE EJEMPLO 692
CONFIGURACIÓN DE IPV6 GUA EN EL ROUTER R1 693
CONFIGURACIÓN DE GUA ESTÁTICA EN UN HOST DE WINDOWS 693
CONFIGURACIÓN ESTÁTICA DE UNA DIRECCIÓN DE UNIDIFUSIÓN LOCAL DE ENLACE 694
COMPROBADOR DE SINTAXIS: CONFIGURACIÓN ESTÁTICA GUA Y LLA 696

DIRECCIONAMIENTO DINÁMICO PARA GUA IPV6 698

MENSAJES RS Y RA 698
MENSAJES DE RS Y RA DE ICMPV6 698
MÉTODO 1: SLAAC 699
MÉTODO 2: SLAAC Y DHCPV6 SIN ESTADO 700
MÉTODO 3: DHCPV6 CON ESTADO 702
PROCESO EUI-64 VERSUS GENERADO ALEATORIAMENTE 703
CREACIÓN DINÁMICA DE UN ID DE INTERFAZ 704
PROCESO EUI-64 704
ID DE INTERFAZ GENERADA MEDIANTE EUI-64 706
ID DE INTERFAZ GENERADAS ALEATORIAMENTE 706
ID DE INTERFAZ DE 64 BITS GENERADA ALEATORIAMENTE 706
COMPRUEBE SU COMPRENSIÓN - DIRECCIONAMIENTO DINÁMICO PARA GUA IPV6 707

DIRECCIONAMIENTO DINÁMICO PARA LAS LLAS IPV6 710

LLA DINÁMICOS 710
LLA DINÁMICOS EN WINDOWS 710
ID DE INTERFAZ GENERADA MEDIANTE EUI-64 711

ID DE INTERFAZ DE 64 BITS GENERADA ALEATORIAMENTE 711
LLA DINÁMICOS EN ENRUTADORES CISCO 711
IPV6 LLA CON EUI-64 EN EL ROUTER R1 712
VERIFIQUE LA CONFIGURACIÓN DE LA DIRECCIÓN IPV6 712
COMPROBADOR DE SINTAXIS: VERIFICAR LA CONFIGURACIÓN DE LA DIRECCIÓN IPV6 715
PACKET TRACER: CONFIGURACIÓN DE DIRECCIONAMIENTO IPV6 716

DIRECCIONES IPV6 DE MULTIDIFUSIÓN 717

DIRECCIONES IPV6 DE MULTIDIFUSIÓN ASIGNADAS 717
DIRECCIONES DE MULTIDIFUSIÓN IPV6 BIEN CONOCIDAS 717
DIRECCIONES IPV6 DE MULTIDIFUSIÓN DE NODO SOLICITADO 718
LABORATORIO: IDENTIFICACIÓN DE DIRECCIONES IPV6 719

DIVISIÓN DE SUBREDES DE UNA RED IPV6 720

SUBRED CON LA ID DE SUBRED 720
GUA CON UN ID DE SUBRED DE 16 BITS 721
EJEMPLO DE SUBRED IPV6 721
SUBREDIZACIÓN CON UNA ID DE SUBRED DE 16 BITS 722
ASIGNACIÓN DE SUBREDES IPV6 722
TOPOLOGÍA DE EJEMPLO 723
ENRUTADOR CONFIGURADO CON SUBREDES IPV6 724
CONFIGURACIÓN DE DIRECCIONES IPV6 EN EL ENRUTADOR R1 724
COMPRUEBE SU COMPRENSIÓN - SUBRED UNA RED IPV6 725

12.8 – PRÁCTICA DEL MÓDULO Y CUESTIONARIO 728

PACKET TRACER: IMPLEMENTE UN ESQUEMA DE DIRECCIONAMIENTO IPV6 SUBRED 728
LAB – CONFIGURACIÓN DE DIRECCIONES IPV6 EN DISPOSITIVOS DE RED 728
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 728
MÓDULO QUIZ - DIRECCIÓN IPV6 731

CAPÍTULO 13_ICMP 740

INTRODUCCIÓN 740

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 740
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 740

MENSAJES ICMP 741

MENSAJES ICMPV4 E ICMPV6 741
ACCESIBILIDAD AL HOST 741
DESTINO O SERVICIO INACCESIBLE 742
TIEMPO EXCEDIDO 743
MENSAJES ICMPV6 743
VERIFIQUE SU COMPRENSIÓN - MENSAJES ICMP 746

PRUEBAS DE PING Y TRACEROUTE 748

PING: PRUEBA DE CONECTIVIDAD 748
HACER PING AL LOOPBACK 749
HACER PING AL GATEWAY PREDETERMINADO 750
HACER PING A UN HOST REMOTO 751
TRACEROUTE: PRUEBA EL CAMINO 752
PACKET TRACER: VERIFICAR EL DIRECCIONAMIENTO IPV4 E IPV6 754
PACKET TRACER: UTILICE PING Y TRACEROUTE PARA PROBAR LA CONECTIVIDAD DE RED . 754

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 754

PACKET TRACER - UTILICE ICMP PARA PROBAR Y CORREGIR LA CONECTIVIDAD DE RED ... 754
LAB - USE PING Y TRACEROUTE PARA PROBAR LA CONECTIVIDAD DE RED. 755
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 755
PRUEBA DE MÓDULO - ICMP 756

CAPÍTULO 14_CAPA DE TRANSPORTE 766

INTRODUCCIÓN 766

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 766
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 766

TRANSPORTE DE DATOS 767

FUNCIÓN DE LA CAPA DE TRANSPORTE 767
TAREAS DE LA CAPA DE TRANSPORTE 768
PROTOCOLOS DE CAPA DE TRANSPORTE 773
PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP) 774
PROTOCOLO DE DATAGRAMAS DE USUARIO (UDP) 782
PROTOCOLO DE LA CAPA DE TRANSPORTE CORRECTO PARA LA APLICACIÓN ADECUADA 784
COMPRUEBE SU COMPRENSIÓN - TRANSPORTE DE DATOS 786

DESCRIPCIÓN GENERAL DE TCP 788

CARACTERÍSTICAS DE TCP **788**
ENCABEZADO TCP **789**
CAMPOS DE ENCABEZADO TCP **789**
APLICACIONES QUE UTILIZAN TCP **790**
VERIFIQUE SU COMPRENSIÓN - DESCRIPCIÓN GENERAL DE TCP **791**

VISIÓN GENERAL DE UDP **793**

CARACTERÍSTICAS DE UDP **793**
ENCABEZADO UDP **793**
CAMPOS DE ENCABEZADO UDP **794**
APLICACIONES QUE UTILIZAN UDP **794**
VERIFIQUE SU COMPRENSIÓN - DESCRIPCIÓN GENERAL DE UDP **796**

NÚMEROS DE PUERTO **798**

COMUNICACIONES MÚLTIPLES SEPARADAS **798**
PARES DE ENCHUFES **799**
GRUPOS DE NÚMEROS DE PUERTO **801**
NÚMEROS DE PUERTO CONOCIDOS 802
EL COMANDO NETSTAT **802**
VERIFIQUE SU COMPRENSIÓN - NÚMEROS DE PUERTO **803**

PROCESO DE COMUNICACIÓN TCP **805**

PROCESOS DEL SERVIDOR TCP **805**
ESTABLECIMIENTO DE CONEXIONES TCP **809**
TERMINACIÓN DE SESIÓN **811**
ANÁLISIS DEL ENLACE DE TRES VÍAS DE TCP **813**
CAMPO DE BITS DE CONTROL 814
VÍDEO: PROTOCOLO DE ENLACE TCP DE 3 VÍAS **814**
COMPRUEBE SU COMPRENSIÓN - PROCESO DE COMUNICACIÓN TCP **815**

CONFIABILIDAD Y CONTROL DE FLUJO **817**

FIABILIDAD DE TCP: ENTREGA GARANTIZADA Y ORDENADA **817**
LOS SEGMENTOS TCP SE VUELVEN A ORDENAR EN EL DESTINOSEGME 818
LA FIGURA MUESTRA QUE, AUNQUE LOS SEGMENTOS PUEDEN TOMAR DIFERENTES RUTAS Y LLEGAR FUERA DE SERVICIO EN EL DESTINO, TCP TIENE LA CAPACIDAD DE REORDENAR LOS SEGMENTOS. 819
VIDEO: CONFIABILIDAD DE TCP: NÚMEROS DE SECUENCIA Y ACUSES DE RECIBO **819**
FIABILIDAD DE TCP: PÉRDIDA Y RETRANSMISIÓN DE DATOS **819**
VIDEO: CONFIABILIDAD DE TCP: PÉRDIDA Y RETRANSMISIÓN DE DATOS **821**
CONTROL DE FLUJO DE TCP: TAMAÑO DE LA VENTANA Y RECONOCIMIENTOS **822**

EJEMPLO DE TAMAÑO DE VENTANA DE TCP 823
CONTROL DE FLUJO TCP - TAMAÑO MÁXIMO DE SEGMENTO (MSS) 824
CONTROL DE FLUJO DE TCP: PREVENCIÓN DE CONGESTIONES 826
CONTROL DE CONGESTIÓN DE TCP 826
COMPRUEBE SU COMPRENSIÓN - FIABILIDAD Y CONTROL DE FLUJO 827

COMUNICACIÓN UDP 830

COMPARACIÓN DE BAJA SOBRECARGA Y CONFIABILIDAD DE UDP 830
REENSAMBLAJE DE DATAGRAMAS DE UDP 830
UDP: SIN CONEXIÓN Y POCO CONFIABLE 831
PROCESOS Y SOLICITUDES DEL SERVIDOR UDP 831
SERVIDOR UDP A LA ESCUCHA DE SOLICITUDES 832
PROCESOS DE CLIENTE UDP 832
COMPRUEBE SU COMPRENSIÓN - COMUNICACIÓN UDP 836

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 838

PACKET TRACER: COMUNICACIONES DE TCP Y UDP 838
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 839
MÓDULO QUIZ - CAPA DE TRANSPORTE 841

CAPÍTULO 15_CAPA DE APLICACIÓN 849

INTRODUCCIÓN 849

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 849
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 849

APLICACIÓN, PRESENTACIÓN Y SESIÓN 850

CAPA DE APLICACIÓN 850
CAPA DE PRESENTACIÓN Y SESIÓN 851
PROTOCOLOS DE CAPA DE APLICACIÓN DE TCP/IP 853
COMPRUEBE SU COMPRENSIÓN - APLICACIÓN, SESIÓN, PRESENTACIÓN 855

PUNTO A PUNTO 859

MODELO CLIENTE-SERVIDOR 859
REDES ENTRE PARES 860
PEER-TO-PEER APPLICATIONS 861
APLICACIONES P2P COMUNES 862

VERIFIQUE SU COMPRENSIÓN CLIENTE A SERVIDOR 863

PROTOCOLOS WEB Y DE CORREO ELECTRÓNICO 866

PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO Y LENGUAJE DE MARCADO DE HIPERTEXTO 866
HTTP Y HTTPS 869
PROTOCOLOS DE CORREO ELECTRÓNICO 870
SMTP, POP E IMAP 871
VERIFIQUE SU COMPRENSIÓN: WEB Y PROTOCOLOS DE CORREO ELECTRÓNICO 872

SERVICIOS DE DIRECCIONAMIENTO IP 876

SERVICIO DE NOMBRES DE DOMINIOS 876
FORMATO DE MENSAJE DNS 880
JERARQUÍA DNS 880
EL COMANDO NSLOOKUP 882
PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST 884
FUNCIONAMIENTO DE DHCP 886
LABORATORIO: OBSERVAR LA RESOLUCIÓN DE NOMBRES DNS 887
COMPRUEBE SU COMPRENSIÓN — SERVICIOS DE DIRECCIONAMIENTO IP 888

SERVICIOS DE INTERCAMBIO DE ARCHIVOS 891

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS 891
BLOQUE DE MENSAJES DEL SERVIDOR 892
VERIFIQUE SUS CONOCIMIENTOS: SERVICIOS DE COMPATIR ARCHIVOS 894

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 897

¿QUÉ APRENDERÉ EN ESTE MÓDULO? 897
MÓDULO QUIZ - CAPA DE APLICACIÓN 899

CAPÍTULO 16_FUNDAMENTOS DE SEGURIDAD DE LA RED 907

INTRODUCCIÓN 907

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 907
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 908

VULNERABILIDADES Y AMENAZAS A LA SEGURIDAD 908

TIPOS DE AMENAZAS **908**
TIPOS DE VULNERABILIDADES **910**
VULNERABILIDADES TECNOLÓGICAS 911
VULNERABILIDADES DE CONFIGURACIÓN 912
VULNERABILIDADES DE POLÍTICA 912
SEGURIDAD FÍSICA **912**
PLANIFIQUE LA SEGURIDAD FÍSICA PARA LIMITAR EL DAÑO AL EQUIPO 913
VERIFIQUE SU COMPRENSIÓN - AMENAZAS Y VULNERABILIDADES DE SEGURIDAD **914**

ATAQUES DE RED **918**

TIPOS DE MALWARE **918**
ATAQUES DE RECONOCIMIENTO **920**
ATAQUES CON ACCESO **925**
ATAQUES DE DENEGACIÓN DE SERVICIO **929**
VERIFIQUE SU COMPRENSIÓN: ATAQUES DE RED **933**
LABORATORIO - INVESTIGACIÓN DE AMENAZAS DE SEGURIDAD DE RED **937**

MITIGACIONES DE ATAQUE A LA RED **938**

ENFOQUE DE DEFENSA EN PROFUNDIDAD **938**
MANTENER COPIAS DE SEGURIDAD **939**
ACTUALIZACIÓN, ACTUALIZACIÓN Y REVISIÓN **940**
AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD AAA **941**
FIREWALLS **942**
FUNCIONAMIENTO DEL FIREWALL 943
TOPOLOGÍA DE FIREWALL CON DMZ 944
TIPOS DE FIREWALLS **944**
SEGURIDAD DE TERMINALES **945**
VERIFIQUE SU COMPRENSIÓN - MITIGACIÓN DE ATAQUES DE RED **945**

SEGURIDAD DE LOS DISPOSITIVOS **948**

CISCO AUTOSECURE **948**
CONTRASEÑAS **949**
CONTRASEÑAS DÉBILES 949
CONTRASEÑAS SEGURAS 950
SEGURIDAD ADICIONAL DE CONTRASEÑAS **950**
HABILITACIÓN DE SSH **951**
INHABILITACIÓN DE SERVICIOS NO UTILIZADOS **952**
PACKET TRACER - CONFIGURE CONTRASEÑAS SEGURAS Y SSH **953**
LABORATORIO: CONFIGURAR DISPOSITIVOS DE RED CON SSH **954**

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 954

PACKET TRACER - DISPOSITIVOS DE RED SEGUROS 954
LABORATORIO: DISPOSITIVOS DE RED SEGUROS 954
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 955
PRUEBA DEL MÓDULO - FUNDAMENTOS DE SEGURIDAD DE RED 956

CAPÍTULO 17_CREAR UNA RED PEQUEÑA 967

INTRODUCCIÓN 967

¿POR QUÉ DEBERÍA TOMAR ESTE MÓDULO? 967
¿QUÉ APRENDERÉ EN ESTE MÓDULO? 967

DISPOSITIVOS DE UNA RED PEQUEÑA 968

TOPOLOGÍAS DE REDES PEQUEÑAS 968
SELECCIÓN DE DISPOSITIVOS PARA REDES PEQUEÑAS. 969
ASIGNACIÓN DE DIRECCIONES IP PARA REDES PEQUEÑAS. 970
REDUNDANCIA EN REDES PEQUEÑAS 973
ADMINISTRACIÓN DEL TRÁFICO 974
COMPRUEBE SU COMPRENSIÓN — DISPOSITIVOS EN UNA RED PEQUEÑA 975

PROTOCOLOS Y APLICACIONES DE REDES PEQUEÑAS 978

APLICACIONES COMUNES 978
PROTOCOLOS COMUNES 979
APLICACIONES DE VOZ Y VÍDEO 982
COMPRUEBE SU COMPRENSIÓN — APLICACIONES Y PROTOCOLOS EN REDES PEQUEÑAS 983

ESCALAR HACIA REDES MÁS GRANDES 985

CRECIMIENTO DE LAS REDES PEQUEÑAS 985
ANÁLISIS DE PROTOCOLOS 986
UTILIZACIÓN DE LA RED POR PARTE DE LOS EMPLEADOS 987
VERIFIQUE SU COMPRENSIÓN — CRECIMIENTO HACIA REDES MÁS GRANDES 988

VERIFICAR LA CONECTIVIDAD 991

VERIFICAR LA CONECTIVIDAD CON PING 991
INDICADORES DE PING IOS 993
PING EXTENDIDO 993

VERIFICAR LA CONECTIVIDAD CON TRACEROUTE 995
COMANDO TRACE DE WINDOWS Y CISCO IOS 995
TRACEROUTE EXTENDIDO 997
LÍNEA BASE DE RED 999
PRÁCTICA DE LABORATORIO: PRUEBA DE LA LATENCIA DE RED CON LOS COMANDOS PING Y TRACEROUTE 1000

COMANDOS DE HOST Y DE IOS 1001

CONFIGURACIÓN DE IP EN UN HOST WINDOWS 1001
CONFIGURACIÓN DE IP EN UN HOST LINUX 1003
CONFIGURACIÓN DE IP EN UN HOST MACOS 1005
EL COMANDO ARP 1006
REPASO DE COMANDOS SHOW COMUNES 1007
EL COMANDO SHOW CDP NEIGHBORS 1014
EL COMANDO SHOW IP INTERFACE BRIEF 1015
VIDEO: EL COMANDO SHOW VERSION 1016
PACKET TRACER - INTERPRETAR LA SALIDA DEL COMANDO SHOW 1017

METODOLOGÍAS PARA LA SOLUCIÓN DE PROBLEMAS 1017

ENFOQUES BÁSICOS PARA LA SOLUCIÓN DE PROBLEMAS 1017
¿SOLUCIONAR O ESCALAR? 1019
COMANDO DEBUG 1019
EL MONITOR TERMINAL DE COMANDOS 1021
VERIFIQUE SU COMPRENSIÓN: METODOLOGÍAS DE SOLUCIÓN DE PROBLEMAS 1022

ESCENARIOS DE RESOLUCIÓN DE PROBLEMAS 1025

PROBLEMAS DE FUNCIONAMIENTO DÚPLEX Y DISCORDANCIA 1025
PROBLEMAS DE ASIGNACIÓN DE DIRECCIONES IP EN DISPOSITIVOS IOS 1027
PROBLEMAS DE ASIGNACIÓN DE DIRECCIONES IP EN TERMINALES 1027
PROBLEMAS CON LA PUERTA DE ENLACE PREDETERMINADA 1028
SOLUCIÓN DE PROBLEMAS DE DNS 1030
LAB - SOLUCIONE PROBLEMAS DE CONECTIVIDAD 1032
PACKET TRACER - SOLUCIONAR PROBLEMAS DE CONECTIVIDAD 1032

PRÁCTICA DEL MÓDULO Y CUESTIONARIO 1032

LAB – DISEÑAR Y CONSTRUIR UNA RED DE EMPRESA PEQUEÑA 1032
PACKET TRACER: DESAFÍO DE INTEGRACIÓN DE HABILIDADES 1033
PACKET TRACER: DESAFÍO DE RESOLUCIÓN DE PROBLEMAS 1033
¿QUÉ APRENDÍ EN ESTE MÓDULO? 1033

MÓDULO QUIZ — CONSTRUIR UNA RED PEQUEÑA 1036
ANEXO GRÁFICO 1045

(Esta página intencionalmente está en blanco)

Introducción a las Redes
Networking Academy CCNAv7

¡Bienvenido! al primer curso del currículo CCNAV7 de Cisco Networking Academy, Introducción a las Redes (ITN). Este es el primero de los tres cursos que están alineados con el examen de certificación CCNA. ITN contiene 17 módulos, cada uno con una serie de temas.

En Introducción a las Redes, obtendrá una comprensión básica de la forma en que operan las redes. Aprenderá acerca de los componentes de red y sus funciones, así como cómo se estructura una red y las arquitecturas utilizadas para crear redes, incluyendo Internet.

Pero ITN se trata de algo más que de aprender conceptos de redes. Al final de este curso, podrá crear redes de área local (LAN), configurar configuraciones básicas en enrutadores y conmutadores e implementar el protocolo de Internet (IP).

Networking Academy CCNAv7

En ITN, todos los conceptos que aprendas y habilidades que desarrolles se utilizarán en el resto del currículo del CCNA. ¡Ahora es el momento de sobrecargar su carrera profesional en redes y dejar que Cisco Networking Academy lo ayude a alcanzar su objetivo!

Capítulo 1_Redes hoy

Introducción

1.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Redes en la actualidad!

¡Felicitaciones! Este módulo lo inicia en su camino hacia una carrera exitosa en Tecnología de la Información al brindarle una comprensión fundamental de la creación, operación y mantenimiento de redes. Como ventaja, puede sumergirse en simulaciones de red usando Packet Tracer. ¡Le prometemos que realmente lo disfrutará!

1.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Las redes en la actualidad

Objetivos del módulo: Explique los avances en las tecnologías de red modernas.

Título del tema	Objetivo del tema
Las redes afectan nuestras vidas	Explique la forma en que las redes afectan nuestra vida diaria.
Componentes de la red	Explique la forma en que se utilizan los dispositivos host y de red.
Topologías y representaciones de red	Explique las representaciones de la red y cómo se usan en la red. topologías
Tipos comunes de redes	Compare las características de los tipos comunes de redes.
Conexiones a Internet	Explique la forma en que las LAN y las WAN se interconectan a Internet.
Redes confiables	Describa los cuatro requisitos básicos de una red confiable.
Tendencias de red	Explique cómo tendencias como BYOD, colaboración en línea, video y nube la informática está cambiando la forma en que interactuamos.
Seguridad de la red	Identifique algunas amenazas y soluciones de seguridad básicas para todas las redes.

Título del tema	Objetivo del tema
El profesional de TI	Explique las oportunidades de empleo en el campo de las redes.

Las redes en la actualidad / Las redes afectan nuestras vidas

Las redes afectan nuestras vidas

1.1.1

Las redes nos conectan

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está justo después de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua, los alimentos y un lugar para vivir.

En el mundo actual, estamos conectados como nunca antes gracias al uso de redes. Las personas que tienen alguna idea pueden comunicarse de manera instantánea con otras personas para hacer esas ideas realidad. Las noticias y los descubrimientos se conocen en todo el mundo en cuestión de segundos. Incluso, las personas pueden conectarse y jugar con amigos que estén del otro lado del océano y en otros continentes.

1.1.2

Video - La experiencia de aprendizaje en Cisco Networking Academy

Los cambiadores del mundo no nacen. Se hacen. Desde 1997, Cisco Networking Academy ha estado trabajando hacia un único objetivo: la educación y el desarrollo de habilidades de la próxima generación de talentos necesarios para la economía digital.

Haga clic en Jugar para ver cómo Cisco Networking Academy para aprender cómo usamos la tecnología para hacer del mundo un lugar mejor.

1.1.3

No hay límites

Los avances en tecnologías de red son, quizá, los agentes de cambio más significativos en el mundo actual. Gracias a estos avances, podemos crear un mundo en el que las fronteras nacionales, las distancias geográficas y las limitaciones físicas se vuelven menos importantes y se convierten en obstáculos cada vez más fáciles de sortear.

Internet cambió la manera en la que se producen las interacciones sociales, comerciales, políticas y personales. La naturaleza inmediata de las comunicaciones en Internet alienta la formación de comunidades mundiales. Estas comunidades permiten una interacción social que no depende de la ubicación ni de la zona horaria.

La creación de comunidades en línea para el intercambio de ideas e información tiene el potencial de aumentar las oportunidades de productividad en todo el planeta.

La creación de la nube nos permite almacenar documentos e imágenes y acceder a ellos en cualquier lugar y en cualquier momento. Así que ya sea que estemos en un tren, en un parque o en la cima de una montaña, podemos acceder sin problemas a nuestros datos y aplicaciones desde cualquier dispositivo.

1. Las redes en la actualidad / Componentes de la red

Componentes de la red

1.2.1

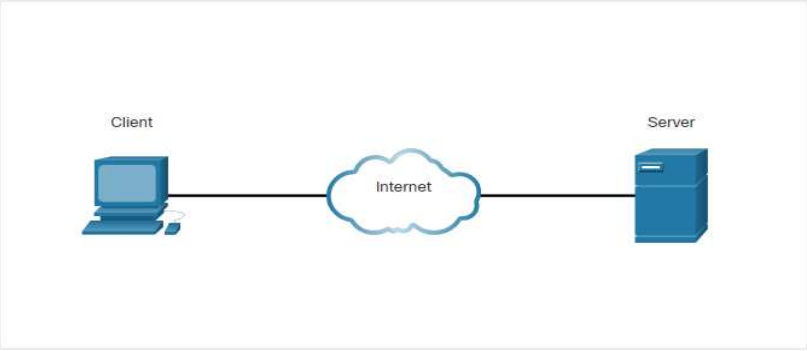
Roles de host

Si desea formar parte de una comunidad en línea global, su computadora, tableta o teléfono inteligente primero deben estar conectados a una red. Esa red debe estar conectada a Internet. En este tema se describen las partes de una red. ¡Vea si reconoce estos componentes en su propia red de hogar o escuela!

Todas las computadoras que están conectadas a una red y participan directamente en la comunicación de la red se clasifican como hosts. Los hosts se pueden llamar dispositivos finales. Algunos hosts también se llaman clientes. Sin embargo, el término hosts se refiere específicamente a los dispositivos de la red a los que se asigna un número para fines de comunicación. Este número identifica el host dentro de una red determinada. Este número se denomina dirección de protocolo de Internet (IP). Una dirección IP identifica el host y la red a la que está conectado el host.

Los servidores son computadoras con software que les permite proporcionar información, como correo electrónico o páginas web, a otros dispositivos finales de la red. Cada servicio requiere un software de servidor independiente. Por ejemplo, para proporcionar servicios web a la red, un servidor requiere un software de servidor web. Una computadora con software de servidor puede proporcionar servicios simultáneamente a muchos clientes diferentes.

Como se mencionó anteriormente, los clientes son un tipo de host. Los clientes disponen de software para solicitar y mostrar la información obtenida del servidor, como se muestra en la figura.



Una máquina cliente y un servidor conectado a través de una nube que simboliza Internet

Un navegador web, como Chrome o Firefox, es un ejemplo de software de cliente. Una única PC también puede ejecutar varios tipos de software de cliente. Por ejemplo, un usuario puede consultar el correo electrónico y ver una página web mientras envía mensajes instantáneos y escucha una transmisión de audio. La tabla enumera tres tipos comunes de software de servidor.

Tipo	Descripción
Correo electrónico	El servidor de correo electrónico ejecuta el software del servidor de correo electrónico. Los clientes usan cliente de correo software, como Microsoft Outlook, para acceder al correo electrónico en el servidor.
Web	El servidor web ejecuta software de servidor web. Los clientes utilizan software de navegador, como Windows Internet Explorer, para acceder a páginas web en el servidor.
Archivo	El servidor de archivos almacena archivos de usuario y empresariales en una ubicación central. Los dispositivos cliente acceden a estos archivos con software cliente como Explorador de archivos de Windows

1.2.2

Entre pares

El software de cliente y servidor generalmente se ejecuta en computadoras separadas, pero también es posible usar una computadora para ambos roles al mismo tiempo. En pequeñas empresas y hogares, muchas PC funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares.

La imagen es una pequeña red entre pares, con una impresora a la izquierda, conectada a un par para compartir impresiones en el medio, conectada a un par para compartir archivos a la derecha. Debajo de la topología hay una lista de las ventajas y desventajas de las redes entre pares. Las ventajas de las redes entre pares: fácil de configurar, menos complejo, de menor costo porque es posible que no se requieran dispositivos de red y servidores dedicados, y se pueden usar para tareas simples como transferir archivos y compartir impresoras. Las desventajas de las redes entre pares: sin una administración centralizada, no tan segura ni escalable, todos los dispositivos pueden actuar como clientes y servidores, lo que puede ralentizar su rendimiento.

Las ventajas de las redes entre pares:

- Fácil de configurar
- Menos complejo
- Menor costo porque es posible que no se necesiten dispositivos de red ni servidores dedicados.
- Se pueden utilizar para tareas sencillas como transferir archivos y compartir impresoras

Las desventajas de las redes entre pares:

- La administración no está centralizada
- No son tan seguras
- No son escalables
- Todos los dispositivos pueden funcionar como clientes y como servidores, lo que puede lentificar el rendimiento
- finales. Para distinguir un dispositivo final de otro, cada dispositivo final de una red tiene una dirección. Cuando un dispositivo final inicia la comunicación, utiliza la dirección del dispositivo final de destino para especificar dónde entregar el mensaje.

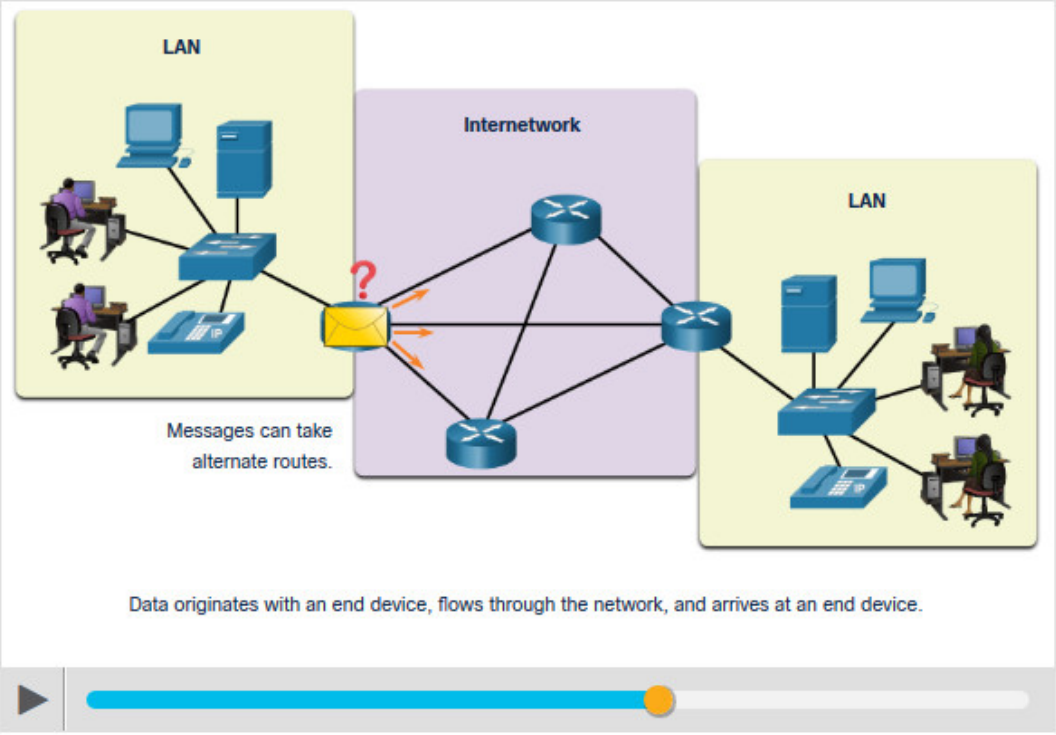
1.2.3

Dispositivos finales

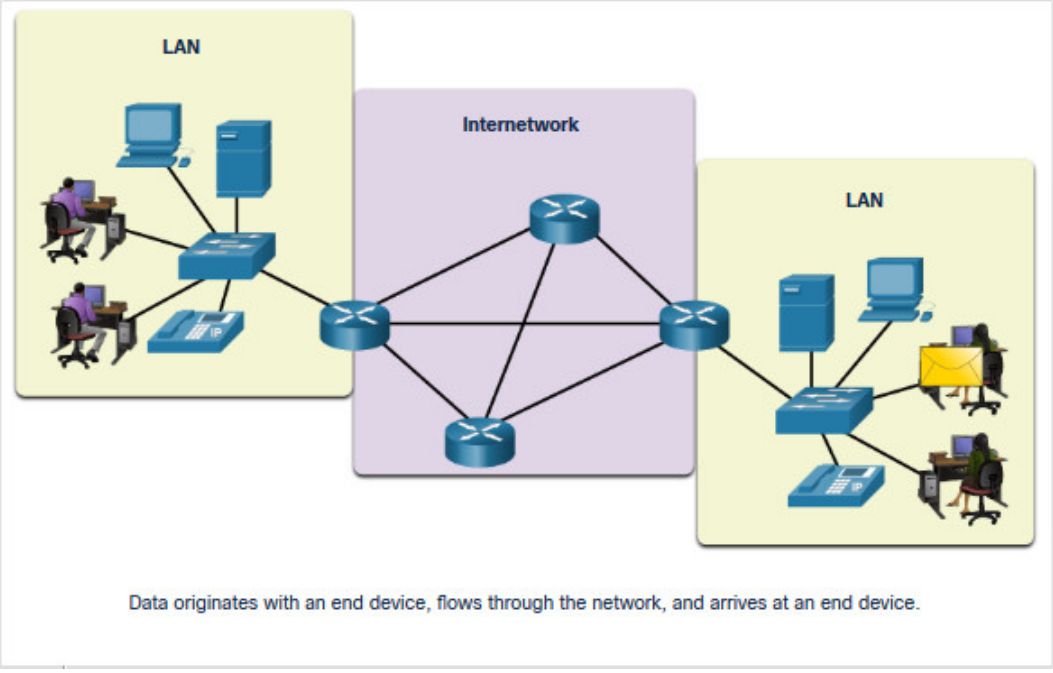
Los dispositivos de red con los que las personas están más familiarizadas se denominan dispositivos saje.

Un terminal es el origen o el destino de un mensaje transmitido a través de la red.

Haga clic en el botón Reproducir de la figura para ver una animación del flujo de datos por una red.



La topología de red física muestra una LAN con dos usuarios un teléfono IP, un PC y un servidor, conectados a un switch. Un vínculo físico conecta el switch LAN a un router perimetral que se acerca a la LAN y a una red internetwork. El Internetwork consta de cuatro routers conectados en una topología de malla completa. Un router perimetral borda la interconexión y una segunda LAN que también consta de dos usuarios, un teléfono IP, un PC y un servidor. Cuando se inicia la animación, un mensaje se origina en uno de los usuarios de la primera LAN y viaja desde el usuario, al switch y al router perimetral que borda la red internetwork. En Internetwork, el mensaje se enruta a través del otro router de bordes que se conecta con la segunda LAN. El mensaje se reenvía a la segunda LAN, a través del switch y al usuario final de destino. El texto debajo del gráfico se lee: los datos se originan con un dispositivo final, fluyen a través de la red y llegan al dispositivo final.



Los datos se originan con un dispositivo final, fluyen por la red y llegan a un dispositivo final.

1.2.4

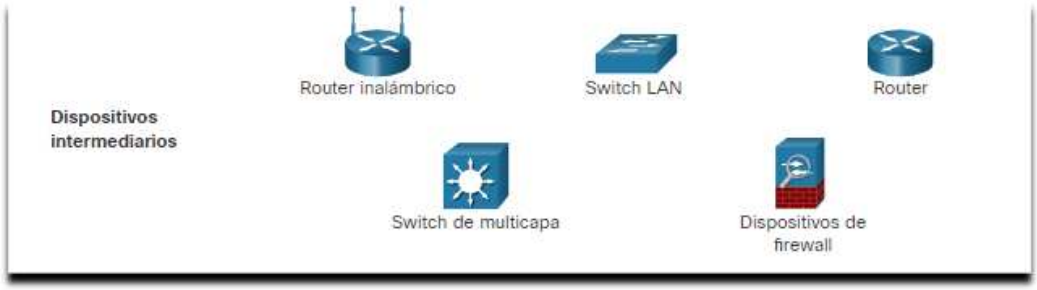
Dispositivos intermediarios

Los dispositivos intermedios conectan los dispositivos finales individuales a la red. Pueden conectar múltiples redes individuales para formar una red interna. Los dispositivos intermedios proporcionan conectividad y garantizan el flujo de datos en toda la red.

Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red. En la figura, se muestran algunos ejemplos de los dispositivos intermediarios más comunes y una lista de funciones.

La imagen muestra símbolos de cinco dispositivos intermediarios comunes y describe algunas de sus funciones. En la parte superior hay un router inalámbrico, un switch LAN y un router. A continuación, se muestra un conmutador multicapa y un dispositivo de firewall. Los dispositivo de red intermediarios realizan algunas de las siguientes funciones o todas ellas: regenerar y retransmitir señales de datos, mantener información sobre qué rutas existen a través de la red y de la interconexión de redes, notificar a otros dispositivos los errores y las fallas de comunicación, dirigir datos por rutas alternativas cuando existen fallas en un enlace, clasificar y direccionar mensajes según las prioridades, y permitir o denegar el flujo de datos en función de la configuración de seguridad. Nota: No se muestra un concentrador Ethernet. Un hub de Ethernet también se conoce como repetidor multipuerto. Los repetidores

regeneran y retransmiten las señales de comunicación. Observe que todos los dispositivos intermedios realizan la función de repetidor.



Un dispositivo de red intermediario puede admitir algunas de estas funciones o todas ellas:

- Regenerar y retransmitir señales de comunicación
- Conservar información acerca de las rutas que existen a través de la red y de internetwork
- Notificar a otros dispositivos los errores y las fallas de comunicación
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace
- Clasificar y dirigir mensajes de acuerdo a las prioridades
- Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad

Nota: No se muestra un concentrador Ethernet. Un hub de Ethernet también se conoce como repetidor multipuerto. Los repetidores regeneran y retransmiten las señales de comunicación. Observe que todos los dispositivos intermedios realizan la función de repetidor.

1.2.5

Medios de red

La comunicación se transmite a través de una red en los medios. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar dispositivos, como se muestra en la figura:

- **Hilos metálicos dentro de cables** - Los datos se codifican en impulsos eléctricos.
- **Fibras de vidrio o plástico (cable de fibra óptica)** - Los datos se codifican como pulsos de luz. Transmisión* **inalámbrica** - Los datos se codifican a través de la modulación de frecuencias específicas de ondas electromagnéticas.

Hay tres imágenes de medios de red comunes seguidos de criterios que se deben utilizar al elegir medios de red. La imagen superior muestra cables y conectores de par trenzado utilizados con medios de cobre. La imagen media es un cable de fibra óptica de múltiples hilos y conectores de fibra óptica. La imagen inferior muestra dispositivos inalámbricos,

incluyendo un router y una cámara. Criterios a considerar al elegir los medios de red: ¿Cuál es la distancia máxima que los medios pueden transportar con éxito una señal? ¿Cuál es el entorno en el que se instalarán los medios? ¿Cuál es la cantidad de datos y a qué velocidad deben transmitirse? ¿Cuál es el costo del medio y de la instalación?

Cobre / Fibra óptica / Tecnología inalámbrica

Criterios a considerar al elegir los medios de red:

- ¿Cuál es la distancia máxima en la que el medio puede transportar una señal exitosamente?
- ¿Cuál es el entorno en el que se instalarán los medios?
- ¿Cuál es la cantidad de datos y a qué velocidad deben transmitirse?
- ¿Cuál es el costo del medio y de la instalación?

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni tampoco son adecuados para los mismos propósitos.

1.2.6

Verifique su comprensión: Componentes de red

Check your understanding of network components by choosing the BEST answer to the following questions.

Correct

You have successfully identified the correct answers.

1. Hosts are all computers connected to a network that participate directly in network communication.
2. Fiber-optic cable is the media is being used to transmit the data when data is encoded as pulses of light.
3. Routers and switches are intermediary devices.

You got 3 out of 3 questions correct.

1. Which of the following is the name for all computers connected to a network that participate directly in network communication?

You got it!

- servers
- intermediary devices
- (•) hosts
- media

2. When data is encoded as pulses of light, which media is being used to transmit the data?

You got it!

- wireless
- (•) Fiber-optic cable
- copper cable

3. Which two devices are intermediary devices? (Choose two)

You got it!

- hosts
- [x] routers
- servers
- [x] switches

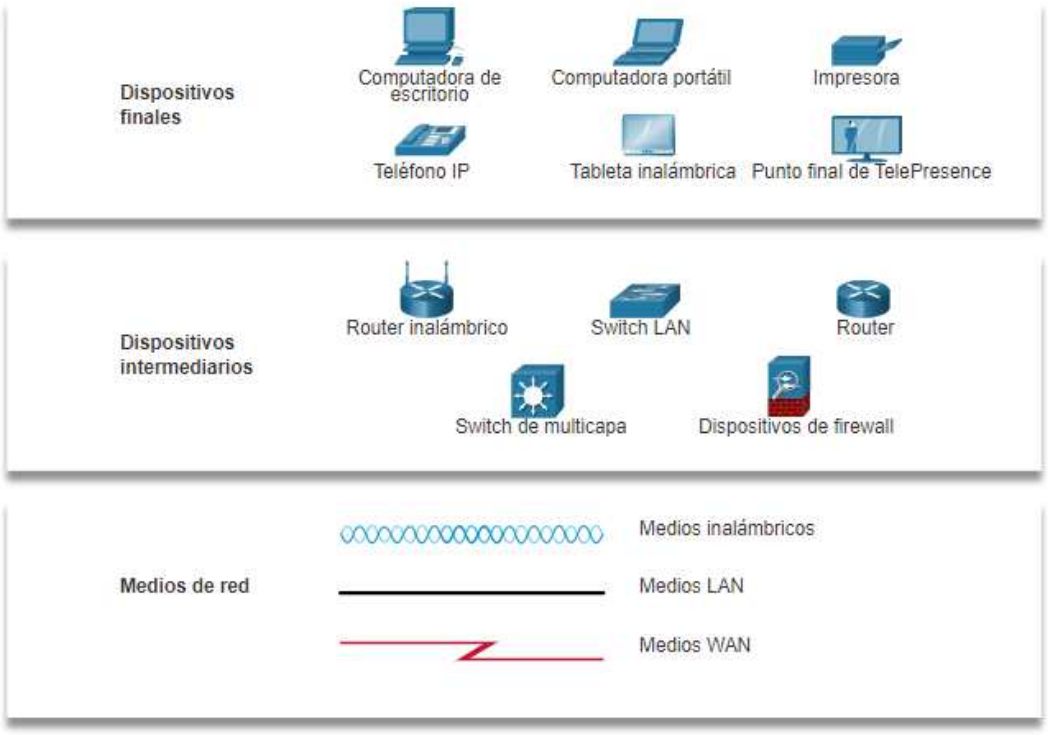
Representaciones de red y Topologías

1.3.1

Representaciones de red

Los arquitectos y administradores de redes deben poder mostrar el aspecto que tendrán sus redes. Necesitan poder ver fácilmente qué componentes se conectan a otros componentes, dónde se ubicarán y cómo se conectarán. Los diagramas de redes a menudo usan símbolos, como los que se muestran en la figura, para representar los diferentes dispositivos y conexiones que forman una red.

La imagen muestra los símbolos utilizados en los diagramas de red. En la parte superior se encuentran los siguientes dispositivos finales: computadora de escritorio, computadora portátil, impresora, teléfono IP, mesa inalámbrica y punto final de Tele Presencia. En el medio están los siguientes dispositivos intermediarios: router inalámbrico, switch LAN, router, switch multicapa y dispositivo firewall. En la parte inferior se encuentran los siguientes medios de red: ondas azules que representan medios inalámbricos, una línea negra sólida que representa medios LAN y un perno de iluminación rojo que representa medios WAN.



Un diagrama proporciona una manera fácil de comprender cómo se conectan los dispositivos en una red grande. Este tipo de representación de una red se denomina diagrama de topología. La capacidad de reconocer las representaciones lógicas de los componentes físicos de red es fundamental para poder visualizar la organización y el funcionamiento de una red.

Además de estas representaciones, se utiliza una terminología especializada para describir cómo cada uno de estos dispositivos y medios se conectan entre sí:

- **Tarjeta de interfaz de red (NIC)** - Una NIC conecta físicamente el dispositivo final a la red.
- **Puerto físico** -Un conector o conexión en un dispositivo de red donde se conectan los medios a un terminal u otro dispositivo de red.
- **Interfaz** - Puertos especializados en un dispositivo de red que se conecta a redes individuales. Debido a que los routers conectan redes, los puertos en un router se denominan interfaces de red.

Nota: A menudo, los términos puerto e interfaz se usan indistintamente.

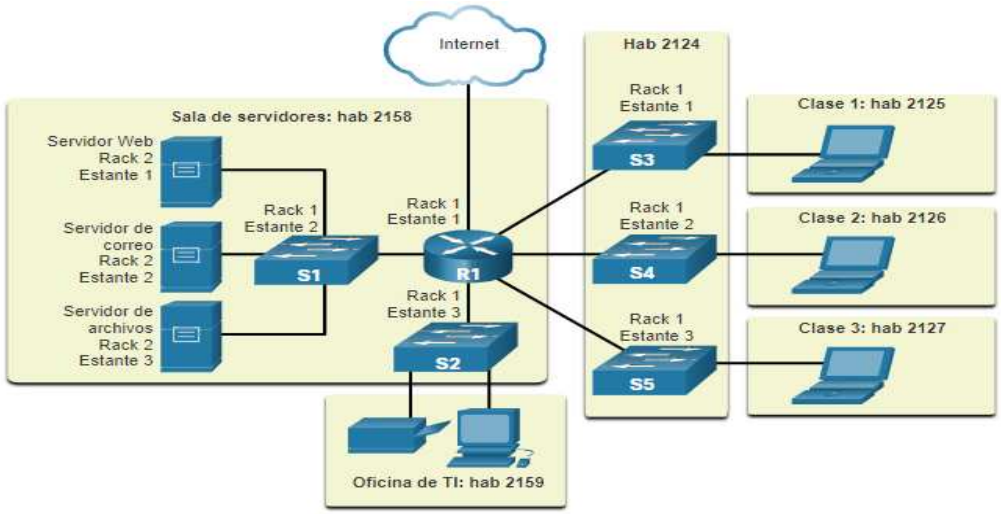
1.3.2

Diagramas de topología

Los diagramas de topología son documentación obligatoria para cualquier persona que trabaje con una red. Estos diagramas proporcionan un mapa visual que muestra cómo está conectada la red. Hay dos tipos de diagramas de topología, físicos y lógicos.

Diagramas de topología física

Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación del cable, como se muestra en la figura. Puede ver que las habitaciones en las que se encuentran estos dispositivos están etiquetadas en esta topología física.



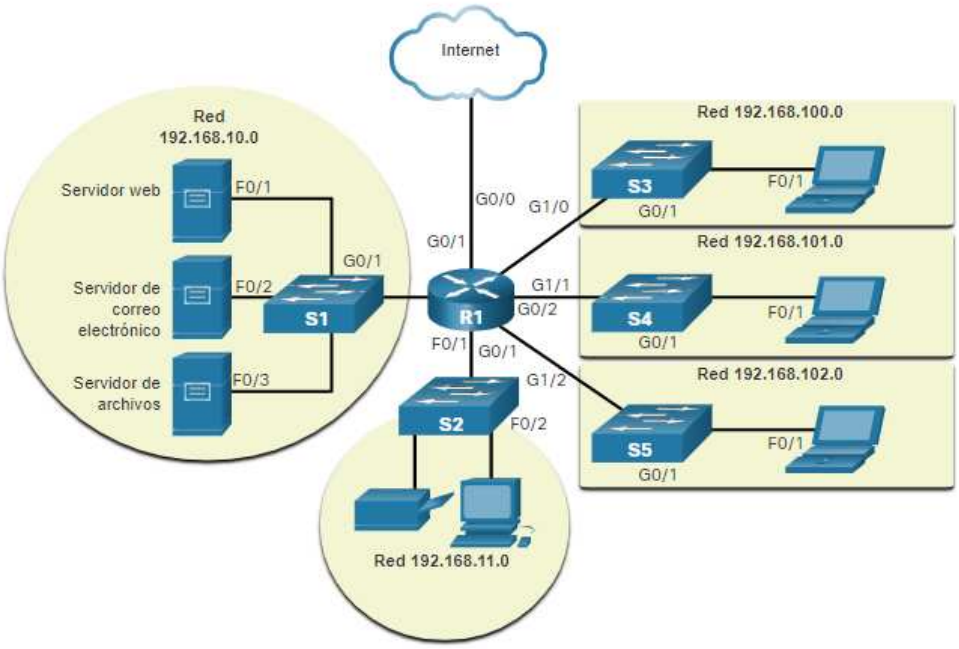
La topología de red física muestra seis salas, cada una resaltada en un cuadro amarillo claro, con varios dispositivos de red y cableado. En el lado izquierdo está la sala de servidores etiquetada como sala 2158. Contiene un router etiquetado R1 montado en el estante 1, estante 1 con seis conexiones de cable. Un cable en la parte superior se conecta a una nube etiquetada como Internet. Un cable a la izquierda se conecta a un switch con la etiqueta S1 montado en el rack 1, estante 2. S1 está conectado a tres servidores: un servidor web montado en el rack 2 estante 1, un servidor de correo electrónico montado en el rack 2 estante 2 y un servidor de archivos montado en el rack 2 estante 3. Un cable conectado a la parte inferior de R1 se conecta a un switch marcado S2 montado en el rack 1 estante 3. S2 tiene dos conexiones que conducen a una impresora y una PC en la oficina de TI etiquetada como habitación 2159. R1 tiene tres cables a la derecha conectados a tres switches ubicados en la habitación 2124. El switch superior está etiquetado S3 y montado en el rack 1 estante 1. El switch del medio tiene la etiqueta S4 y está montado en el rack 1, estante 2. El switch inferior tiene la etiqueta S5 y está montado en el rack 1, estante 3. S3 tiene un cable a la izquierda conectado a una computadora portátil en una habitación llamada clase 1 habitación 2125. S4 tiene un cable a la izquierda conectado a una computadora portátil en una habitación llamada clase 2 habitación 2126. S5 tiene un cable a la izquierda conectado a una computadora portátil en una habitación llamada clase 3 habitación 2127.

Diagramas de topología lógica

Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red, como se muestra en la figura. Puede ver qué dispositivos finales están conectados a qué dispositivos intermediarios y qué medios se están utilizando.

La topología de red lógica muestra dispositivos, etiquetas de puerto y el esquema de direccionamiento de red. En el centro de la imagen hay un router con la etiqueta R1. Un puerto etiquetado G0/0 se conecta a una nube en la parte superior con la etiqueta Internet. Un puerto etiquetado G0/1 se conecta a la izquierda a un switch etiquetado S1 en el puerto G0/1.

S1 está conectado a tres servidores. S1 y los servidores se resaltan en un círculo amarillo claro con la red 192.168.10.0 escrita en la parte superior. El puerto F0/1 en S1 se conecta a un servidor web. El puerto F0/2 en S1 se conecta a un servidor web. El puerto F0 / 3 en S1 se conecta a un servidor de archivos. El puerto F0/1 en R1 se conecta en la parte inferior a un switch etiquetado S2. S2 se conecta a una impresora y una PC, todos los cuales se resaltan en un círculo amarillo claro con la red 192.168.11.0 escrita en la parte inferior. A la izquierda de R1 hay tres conexiones adicionales, cada una de las cuales se conecta a un switch en el puerto G0/1 que luego se conecta a un portátil en el puerto F0/1. Cada switch y computadora portátil se resaltan en amarillo y se muestra la dirección de red. El puerto G0/0 de R1 se conecta en la parte superior a un switch etiquetado S3 en la red 192.168.100.0. El puerto G1/1 de R1 se conecta en el medio a un switch etiquetado S4 en la red 192.169.101.0. El puerto G1/2 en R1 se conecta en la parte inferior a un switch etiquetado S5 en la red 192.168.102.0.



Las topologías que se muestran en los diagramas físicos y lógicos son adecuadas para su nivel de comprensión en este punto del curso. Utilice Internet para buscar “diagramas de topología de red” y ver algunos ejemplos más complejos. Si agrega la palabra "Cisco" a su frase de búsqueda, encontrará muchas topologías que usan íconos similares a los que ha visto en estas figuras.

1.3.3

Verifique su comprensión: Representaciones de Red y Topologías

Compruebe su comprensión de las representaciones y topologías de red eligiendo la mejor respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. A NIC is a specialized port on a networking device that connects to individual networks.
2. An interface physically connects the end device to the network.
3. The logical topology lets you see which end devices are connected to which intermediary devices and what media is being used.
4. The physical topology lets you see the actual location of intermediary devices and cable installation.

You got 4 out of 4 questions correct.

1. Which connection physically connects the end device to the network?

You got it!

- Port
- (•) NIC
- Interface

2. Which connections are specialized ports on a networking device that connect to individual networks?

You got it!

- Port
- NIC
- (•) Interface

3. Which type of network topology lets you see which end devices are connected to which intermediary devices and what media is being used?

You got it!

- Physical topology
- (•) Logical topology

4. Which type of network topology lets you see the actual location of intermediary devices and cable installation?

You got it!

- (•) Physical topology
- Logical topology

Tipos comunes de redes

1.4.1

Redes de muchos tamaños

Ahora que está familiarizado con los componentes que componen las redes y sus representaciones en topologías físicas y lógicas, está listo para aprender acerca de los diferentes tipos de redes.

Hay redes de todo tamaño. Pueden ir desde redes simples, compuestas por dos PC, hasta redes que conectan millones de dispositivos.

Las redes domésticas sencillas le permiten compartir recursos, como impresoras, documentos, imágenes y música, entre unos pocos dispositivos finales locales.

Las redes de oficinas pequeñas y oficinas domésticas (SOHO) permiten a las personas trabajar desde casa o desde una oficina remota. Muchos trabajadores independientes utilizan este tipo de redes para anunciar y vender productos, pedir suministros y comunicarse con los clientes.

Las empresas y las grandes organizaciones usan redes para proporcionar consolidación, almacenamiento y acceso a la información en los servidores de red. Las redes proporcionan correo electrónico, mensajería instantánea y colaboración entre empleados. Muchas organizaciones usan la conexión de su red a Internet para proporcionar productos y servicios a los clientes.

Internet es la red más extensa que existe. De hecho, el término Internet significa “red de redes”. Es una colección de redes privadas y públicas interconectadas.

En pequeñas empresas y hogares, muchas PC funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares.

Haga clic en cada botón para obtener más información.

Redes domésticas pequeñas | Redes domésticas/de oficinas pequeñas | Redes medianas a grandes | Redes mundiales

Small Home Networks

Las redes domésticas pequeñas conectan algunas computadoras entre sí y a Internet.

Small home networks connect a few computers to each other and to the internet.

Redes domésticas pequeñas | Redes domésticas/de oficinas pequeñas | Redes medianas a grandes | Redes mundiales

Small Office and Home Office Networks

La red SOHO permite que las computadoras en una oficina hogareña o remota se conecten a una red corporativa o accedan a recursos compartidos centralizados.

The SOHO network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources.

Redes domésticas pequeñas | Redes domésticas/de oficinas pequeñas | Redes medianas a grandes | Redes mundiales

Medium to Large Networks

Las redes medianas a grandes, como las que se utilizan en corporaciones y escuelas, pueden tener muchas ubicaciones con cientos o miles de hosts interconectados.

Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts.

Redes domésticas pequeñas | Redes domésticas/de oficinas pequeñas | Redes medianas a grandes | Redes mundiales

World Wide Networks

Internet es una red de redes que conecta cientos de millones de computadoras en todo el mundo.

The internet is a network of networks that connects hundreds of millions of computers world-wide.

1.4.2

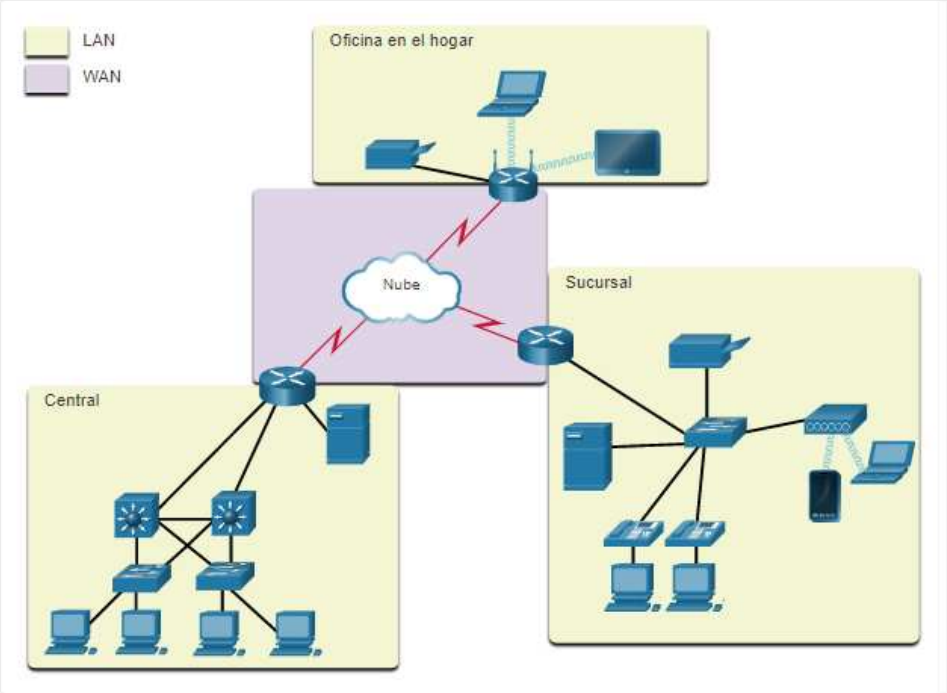
LAN y WAN

Las infraestructuras de red pueden variar en gran medida en términos de:

- El tamaño del área que abarcan.
- La cantidad de usuarios conectados.
- La cantidad y los tipos de servicios disponibles.
- El área de responsabilidad

Los dos tipos más comunes de infraestructuras de red son las redes de área local (LAN) y las redes de área amplia (WAN). Una LAN es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña. Normalmente, una LAN se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas. Una WAN es una infraestructura de red que proporciona acceso a otras redes en un área geográfica amplia, que generalmente es propiedad y está administrada por una corporación más grande o un proveedor de servicios de telecomunicaciones. La figura muestra las LAN conectadas a una WAN.

La topología de red muestra tres LAN conectadas a través de un vínculo WAN en el centro. Una leyenda muestra que las LAN se resaltan en amarillo y las WAN en morado claro. La WAN se encuentra en el centro del diagrama. Contiene un símbolo de nube etiquetado nube con conexiones WAN rojas a tres routers. Cada router se encuentra en parte en la WAN y en parte en una LAN. En la parte inferior izquierda se encuentra la LAN central. Contiene un servidor, dos switches multicapa, dos switches LAN y cuatro PC. En la parte inferior derecha está la sucursal LAN. Contiene un switch, un servidor, una impresora, dos teléfonos IP conectados cada uno a un PC y un punto de acceso inalámbrico con conexiones inalámbricas a un ordenador portátil y un teléfono inteligente. En la parte superior derecha se encuentra la LAN de la oficina en casa. Contiene un router inalámbrico con una conexión por cable a una impresora y conexiones inalámbricas a una computadora portátil y un monitor.

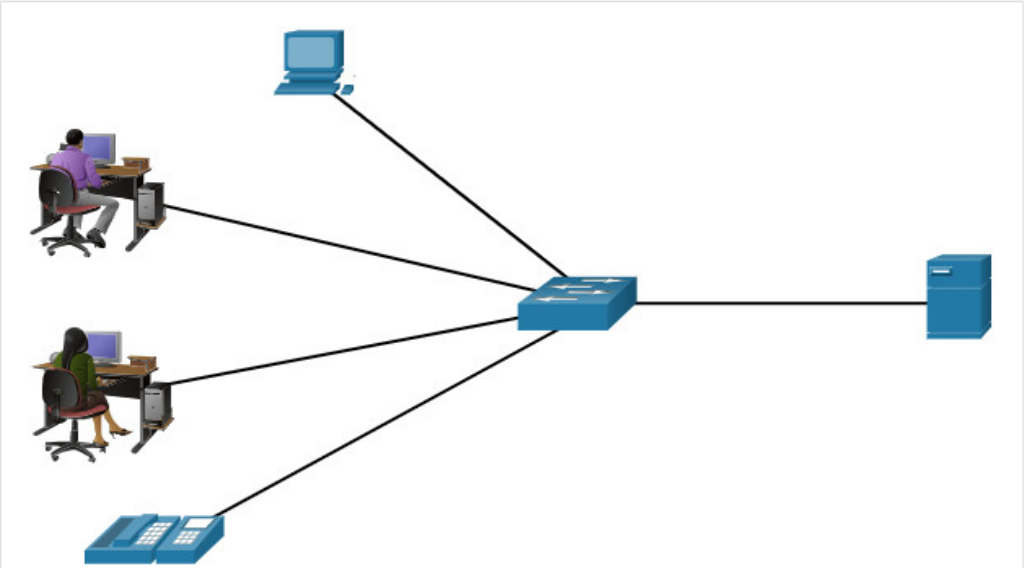


LANs

Una LAN es una infraestructura de la red que abarca un área geográfica pequeña. Las LANs tienen características específicas:

- Las LANs interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.
- Por lo general, la administración de las LAN está a cargo de una única organización o persona. El control administrativo se aplica a nivel de red y rige las políticas de seguridad y control de acceso.
- Las LANs proporcionan ancho de banda de alta velocidad a dispositivos finales internos y dispositivos intermedios, como se muestra en la figura.

El diagrama es una ilustración de una LAN. En el centro del diagrama hay un switch. Hay cuatro conexiones Ethernet en el switch. En la parte superior izquierda hay una conexión a un PC. Debajo de eso hay una conexión a la computadora en el escritorio de un trabajador. Debajo de eso hay otra conexión a la computadora en el escritorio de un trabajador. En la parte inferior izquierda hay una conexión a un teléfono IP. A la derecha del switch hay una conexión a un servidor. El texto debajo de la figura dice: una red que sirve una casa, un edificio pequeño o un campus pequeño se considera una LAN.



Una red que sirve a una casa, un edificio pequeño o un campus pequeño se considera una LAN.

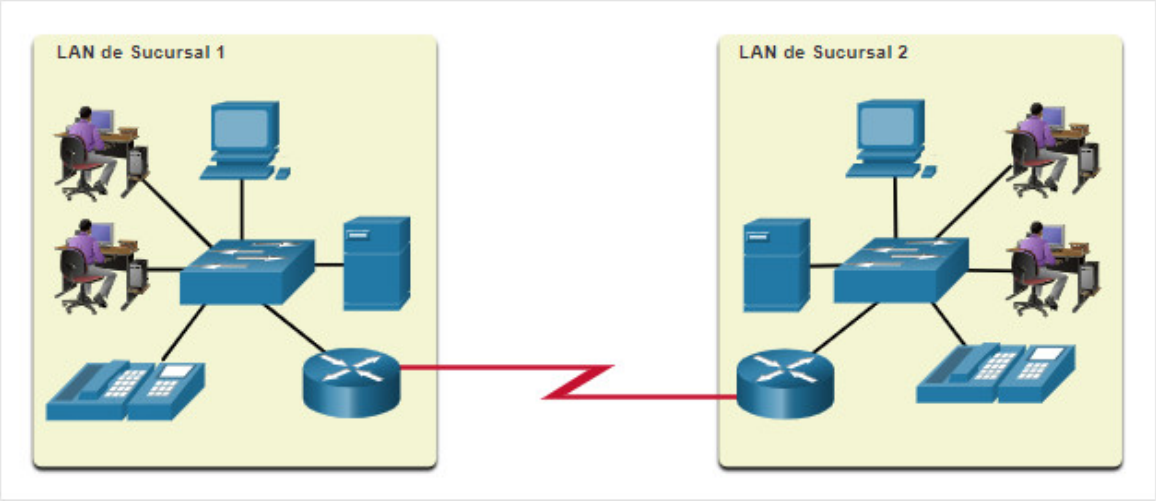
WANs

La figura muestra una WAN que interconecta dos LAN. Una WAN es una infraestructura de la red que abarca un área geográfica extensa. Las WAN generalmente son administradas por proveedores de servicios (SP) o proveedores de servicios de Internet (ISP).

Las WANs tienen características específicas:

- Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes.
- Por lo general, la administración de las WAN está a cargo de varios proveedores de servicios.
- Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN.

En la figura, se muestran dos sucursales LAN conectadas por un enlace WAN. Ambas LAN se resaltan en una caja amarilla clara y constan de un conmutador central conectado a tres PC, un teléfono IP, un servidor y un enrutador. Los dos routers están conectados a través de un enlace WAN rojo. A la izquierda está la LAN de la sucursal 1 y a la derecha la LAN de la sucursal 2.

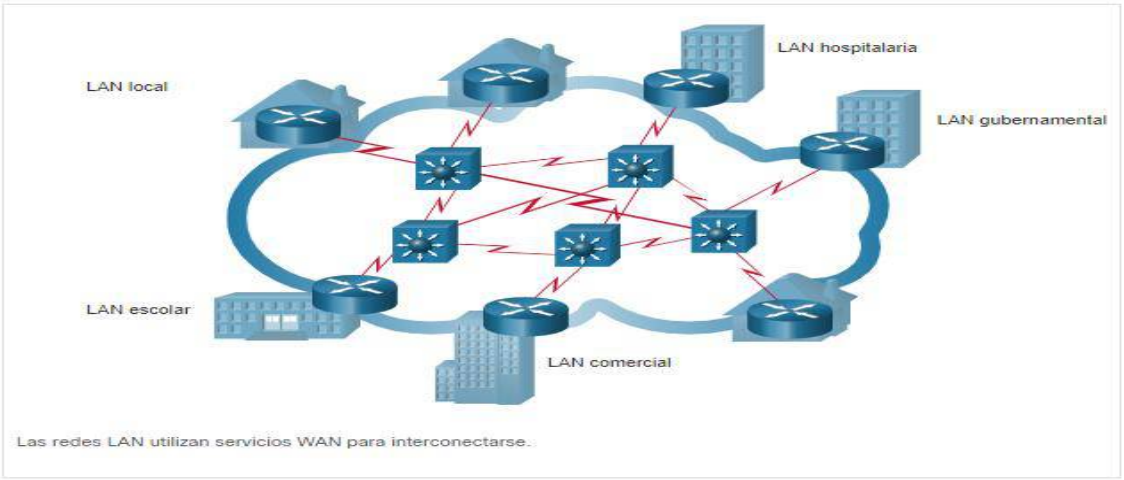


1.4.3

El Internet

Internet es una colección global de redes interconectadas (internetwork o internet para abreviar). En la figura se muestra una forma de ver a la Internet como una colección de LAN y WAN interconectadas.

Cinco switches multicapa con enlaces redundantes se muestran dentro de una nube grande. Alrededor del borde de la nube hay siete routers conectados a varias LAN. Hay una LAN de hospital, una LAN de escuela, una LAN de negocios, una LAN del gobierno y tres LAN domésticas. El texto en la parte inferior dice que las LAN usan los servicios WAN para interconectarse.



Algunos de los ejemplos de LAN están conectados entre sí a través de una conexión WAN. Las WAN están conectadas entre sí. Las líneas de conexión WAN rojas representan todas las variedades de formas en las que conectamos las redes. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions (not shown).

Internet no pertenece a una persona o un grupo. Garantizar una comunicación efectiva en esta infraestructura heterogénea requiere la aplicación de estándares y tecnologías uniformes, y comúnmente reconocidas, así como también la cooperación de muchas agencias de administración de redes. Hay organizaciones que se desarrollaron para ayudar a mantener la estructura y la estandarización de los protocolos y procesos de Internet. Entre estas organizaciones, se encuentran el Grupo de trabajo de ingeniería de Internet (IETF), la Corporación de Internet para la Asignación de Nombres y Números (ICANN) y el Consejo de Arquitectura de Internet (IAB), entre muchas otras.

1.4.4

Intranets y Extranets

Hay otros dos términos que son similares al término internet: intranet y extranet.

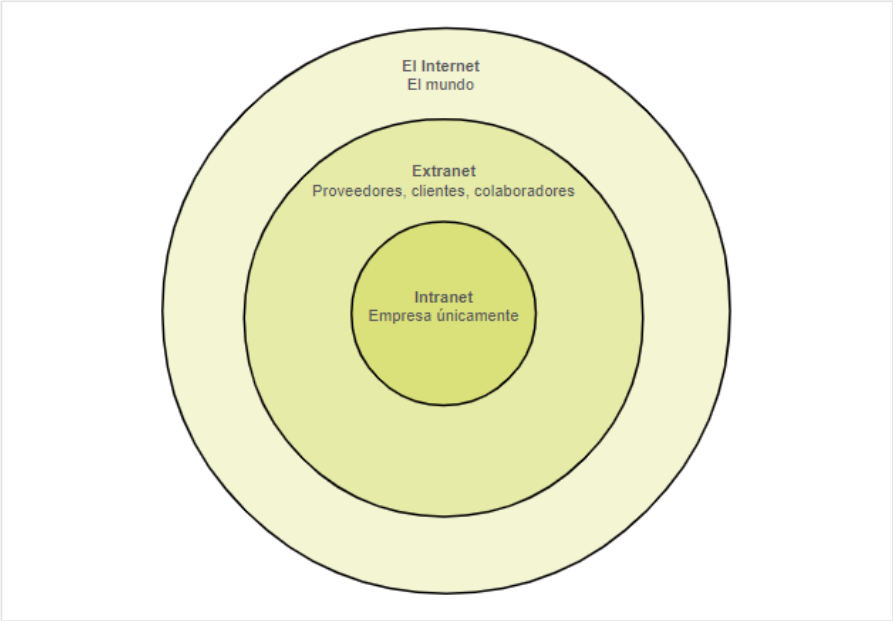
El término intranet se utiliza para referirse a la conexión privada de LAN y WAN que pertenecen a una organización. Una intranet está diseñada para que solo puedan acceder a ella los miembros y empleados de la organización, u otras personas autorizadas.

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa. Aquí hay algunos ejemplos de extranets:

- Una empresa que proporciona acceso a proveedores y contratistas externos.
- Un hospital que proporciona un sistema de reservas a los médicos para que puedan hacer citas para sus pacientes.
- Una secretaría de educación local que proporciona información sobre presupuesto y personal a las escuelas del distrito.

La figura ilustra los niveles de acceso que los diferentes grupos tienen a una intranet de la empresa, a una extranet de la empresa y a Internet.

Un círculo central tiene la etiqueta Intranet y sólo tiene acceso de empresa. Alrededor que hay otro círculo etiquetado Extranet y es accesible por proveedores, clientes y colaboradores. Alrededor de eso hay otro círculo etiquetado Internet y es accesible por el mundo.



1.4.5

Verifique su comprensión: Tipos de Redes Comunes

Verifique su comprensión de los tipos comunes de redes eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. A LAN provides access to users and end devices in a small geographical area.
2. An extranet provides secure and safe access to individuals who work for a different organization but require access to the organization's data.
3. A WAN provides access to other networks over a large geographical area.

You got 3 out of 3 questions correct.

1. Which network infrastructure provides access to users and end devices in a small geographical area, which is typically a network in a department in an enterprise, a home, or small business?

You got it!

- Extranet
- Intranet
- (•) LAN
- WAN

2. Which network infrastructure might an organization use to provide secure and safe access to individuals who work for a different organization but require access to the organization's data?

You got it!

- (•) Extranet
- Intranet
- LAN
- WAN

3. Which network infrastructure provides access to other networks over a large geographical area, which is often owned and managed by a telecommunications service provider?

You got it!

- Extranet
- Intranet
- LAN
- (•) WAN

Conexiones a Internet

1.5.1

Tecnologías de acceso a Internet

Por lo tanto, ahora tiene una comprensión básica de lo que forma una red y los diferentes tipos de redes. Pero, ¿cómo se conecta realmente a los usuarios y organizaciones a Internet? Como habrás adivinado, hay muchas maneras diferentes de hacer esto.

Los usuarios domésticos, los trabajadores remotos y las oficinas pequeñas generalmente requieren una conexión a un ISP para acceder a Internet. Las opciones de conexión varían mucho entre los ISP y las ubicaciones geográficas. Sin embargo, las opciones más utilizadas incluyen banda ancha por cable, banda ancha por línea de suscriptor digital (DSL), redes WAN inalámbricas y servicios móviles.

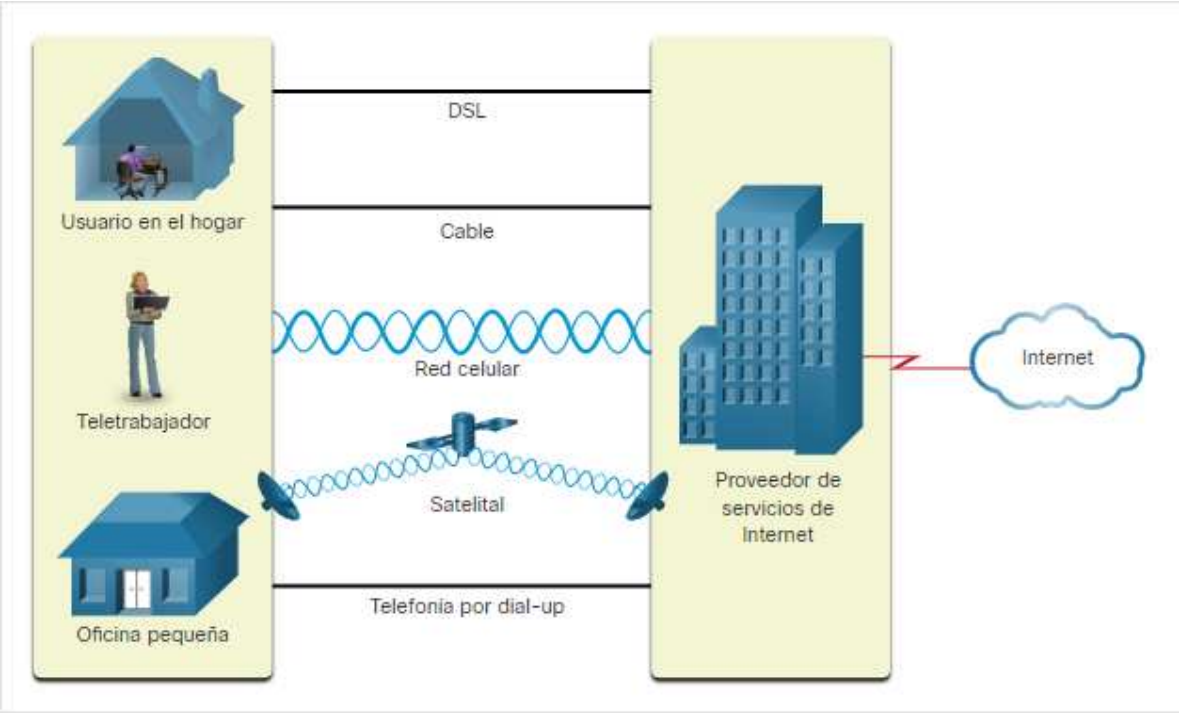
Las organizaciones generalmente necesitan acceso a otros sitios corporativos, así como a Internet. Para admitir servicios empresariales, como telefonía IP, videoconferencias y el almacenamiento en centros de datos, se requieren conexiones rápidas. Los ISPs ofrecen interconexiones de clase empresarial. Los servicios de nivel empresarial más comunes son DSL empresarial, líneas arrendadas y red Metro Ethernet.

1.5.2

Conexiones a Internet domésticas y de oficinas pequeñas

En la figura, se muestran opciones de conexión comunes para los usuarios de oficinas pequeñas y oficinas en el hogar, que incluyen las siguientes:

opciones de conexión comunes para usuarios de oficinas pequeñas y oficinas domésticas



- **Cable** - Típicamente ofrecido por los proveedores de servicios de televisión por cable, la señal de datos de Internet se transmite en el mismo cable que ofrece la televisión por cable. Proporciona un gran ancho de banda, alta disponibilidad y una conexión a Internet siempre activa.
- **DSL** - Las líneas de suscriptor digital también proporcionan un gran ancho de banda, alta disponibilidad y una conexión permanente a Internet. DSL se transporta por la línea de teléfono. En general los usuarios de oficinas en el hogar o pequeñas se conectan mediante una línea de suscriptor digital asimétrica (ADSL), esto implica que la velocidad de descarga es mayor que la velocidad de carga.
- **Celular** - El acceso a internet celular utiliza una red de telefonía celular para conectarse. En cualquier lugar donde tenga cobertura de telefonía móvil, puede tener acceso a Internet. El rendimiento está limitado por las capacidades del teléfono y la torre celular a la que está conectado.
- **Satelital** - La disponibilidad de acceso a internet satelital es un beneficio en aquellas áreas que de otra manera no tendrían conectividad a internet. Las antenas parabólicas requieren una línea de vista despejada al satélite.
- **Telefonía por Dial-up** - Es una opción de bajo costo que funciona con cualquier línea telefónica y un módem. El ancho de banda que proporciona una conexión por módem, conexión por dial-up es bajo y, por lo general, no es suficiente para trasferencias de datos masivas, si bien es útil para acceso móvil durante viajes.

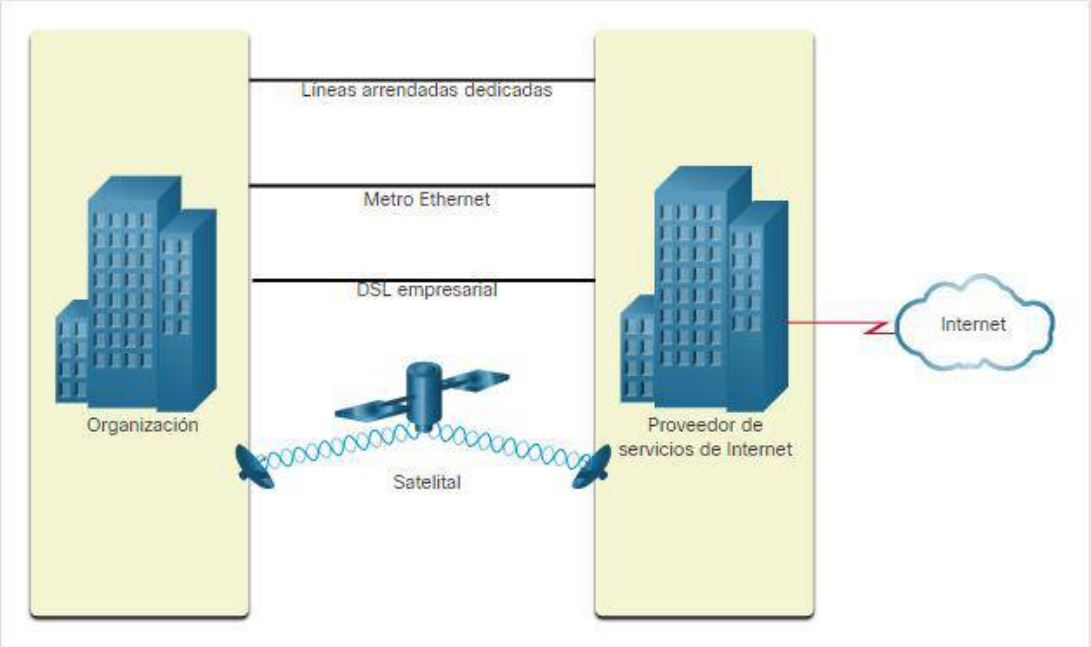
La oferta de opciones de conexión varía según la ubicación geográfica y la disponibilidad de proveedores de servicios.1.5.3

Conexiones a Internet empresariales

Las opciones de conexión corporativas difieren de las opciones que tienen los usuarios domésticos. Es posible que las empresas requieran un ancho de banda mayor y dedicado, además de servicios administrados. Las opciones de conexión disponibles varían según el tipo de proveedores de servicios que haya en las cercanías.

La figura ilustra las opciones de conexión comunes para las empresas.

opciones de conexión comunes para empresas



- **Líneas arrendadas dedicadas** - Las líneas arrendadas son circuitos reservados dentro de la red del proveedor de servicios que conectan oficinas separadas geográficamente para redes privadas de voz y / o datos. Los circuitos se alquilan a una tasa mensual o anual.
- **Metro Ethernet** - Esto a veces se conoce como Ethernet WAN. En este módulo, nos referiremos a él como Metro Ethernet. Metro ethernet extiende la tecnología de acceso LAN a la WAN. Ethernet es una tecnología LAN que analizará en un capítulo más adelante.
- **DSL empresarial** - El servicio de DSL empresarial está disponible en diversos formatos. Una opción muy utilizada es la línea de suscriptor digital simétrica (SDSL), que es similar a la versión de DSL para el consumidor, pero proporciona las mismas velocidades de subida y descarga.
- **Satelital** - El servicio satelital puede proporcionar una conexión cuando una solución por cable no está disponible.

Las opciones de conexión varían según la ubicación geográfica y la disponibilidad del proveedor de servicios.

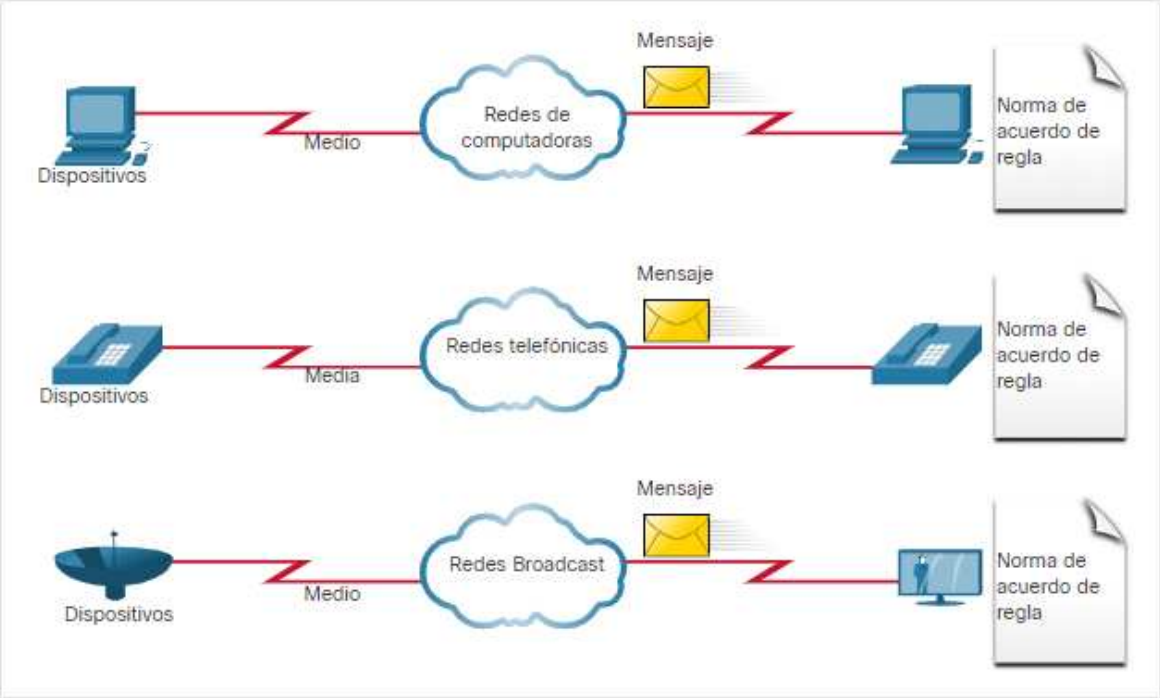
1.5.4

La red convergente

Redes separadas tradicionales

Piense en una escuela construida hace cuarenta años. En ese entonces, las aulas contaban con conexiones por cable para la red de datos, la red telefónica y la red de vídeo para los televisores. Estas redes separadas no pueden comunicarse entre sí. Cada red utilizaba tecnologías diferentes para transportar la señal de comunicación. Cada red tenía su propio conjunto de reglas y estándares para asegurar una comunicación satisfactoria. Múltiples servicios se ejecutaron en múltiples redes.

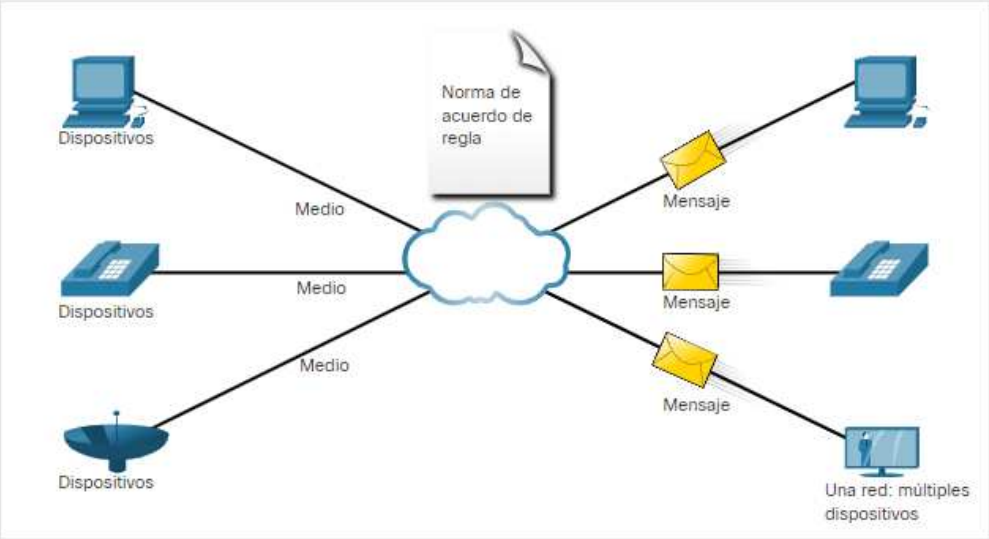
Computadoras separadas, teléfonos y redes de difusión



Redes convergentes

Hoy, las redes separadas de datos, telefonía y vídeo están convergiendo. A diferencia de las redes dedicadas, las redes convergentes pueden transmitir datos, voz y vídeo entre muchos tipos diferentes de dispositivos en la misma infraestructura de red. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación. Las redes de datos convergentes transportan servicios múltiples en una red.

Las redes de datos convergentes transportan servicios múltiples en una red.



1.5.5

Video: descargue e instale Packet Tracer

Este video le mostrará cómo descargar e instalar Packet Tracer. Utilizará Packet Tracer para simular la creación y prueba de redes en su equipo. Packet Tracer es un programa de software flexible y divertido que te dará la oportunidad de usar las representaciones de red y teorías que acabas de aprender a construir modelos de red y explorar LAN y WAN relativamente complejas.

Por lo general, los estudiantes usan Packet Tracer para lo siguiente:

- Preparase para un examen de certificación.
- Practicar lo aprendido en los cursos de redes.
- Refinar sus habilidades para una entrevista laboral.
- Examinar el impacto de agregar nuevas tecnologías a los diseños de red existentes.
- Desarrollar sus habilidades para realizar trabajos en Internet de las cosas.
- Competir en desafíos globales de diseño (consulte 2017 PT 7 Desafío de diseño en Facebook).

Packet Tracer es una herramienta esencial de aprendizaje que se utiliza en muchos cursos de Cisco Networking Academy.

Para obtener e instalar Cisco Packet Tracer siga estos pasos:

Paso 1. Iniciar sesión en la página de "I'm Learning" de Cisco Networking Academy.

Paso 2. Seleccione Recursos.

Paso 3. Seleccione Descargar Packet Tracer.

Paso 4. Seleccione la versión de Packet Tracer que necesita.

Paso 5. Guarde el archivo en la computadora.

Paso 6. Inicie el programa de instalación de Packet Tracer.

Haga clic en Reproducir en el video para realizar un recorrido detallado del proceso de descarga e instalación de Packet Tracer.

1.5.6

Vídeo - Introducción a Cisco Packet Tracer

Packet Tracer es una herramienta que permite simular redes reales. Proporciona tres menús principales:

- Puede agregar dispositivos y conectarlos a través de cables o inalámbricos.
- Puede seleccionar, eliminar, inspeccionar, etiquetar y agrupar componentes dentro de la red.
- Puede administrar su red abriendo una red existente o de muestra, guardando la red actual y modificando su perfil de usuario o preferencias.

Si ha utilizado algún programa, como un procesador de textos o una hoja de cálculo, ya está familiarizado con los comandos del menú Archivo ubicados en la barra de menús superior. Los comandos Abrir, Guardar, Guardar como y Salir funcionan como lo harían con cualquier programa, pero hay dos comandos especiales para Packet Tracer.

El comando Open Samples mostrará un directorio de ejemplos preconstruidos de características y configuraciones de varios dispositivos de red e Internet de las cosas incluidos en Packet Tracer.

El comando Salir y cerrar sesión eliminará la información de registro de esta copia de Packet Tracer y requerirá que el siguiente usuario de esta copia de Packet Tracer realice el procedimiento de inicio de sesión de nuevo.

Haga clic en Reproducir en el vídeo para aprender a utilizar los menús y a crear su primera red Packet Tracer. animación del flujo de datos por una red.

1.5.7

Packet Tracer: Representación de la red

En esta actividad, explorará la forma en que Packet Tracer sirve como herramienta de creación de modelos para representaciones de red.

Representación de la red

Representación de la red

Las redes en la actualidad / Redes confiables

Redes confiables

1.6.1

Arquitectura de red

¿Alguna vez ha estado ocupado trabajando en línea, sólo para tener «Internet se cae»? Como ya sabes, Internet no se cayó, acabas de perder tu conexión con él. Es muy frustrante. Con tantas personas en el mundo que dependen del acceso a la red para trabajar y aprender, es imperativo que las redes sean confiables. En este contexto, la fiabilidad significa más que su conexión a Internet. Este tema se centra en los cuatro aspectos de la fiabilidad de la red.

La función de la red cambió de una red únicamente de datos a un sistema que permite conectar personas, dispositivos e información en un entorno de red convergente y con gran variedad de medios. Para que las redes funcionen eficazmente y crezcan en este tipo de entorno, se deben crear sobre la base de una arquitectura de red estándar.

Las redes también admiten una amplia gama de aplicaciones y servicios. Deben operar sobre muchos tipos diferentes de cables y dispositivos, que conforman la infraestructura física. En

este contexto, el término arquitectura de red, se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red.

A medida que las redes evolucionan, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para cumplir con las expectativas del usuario:

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

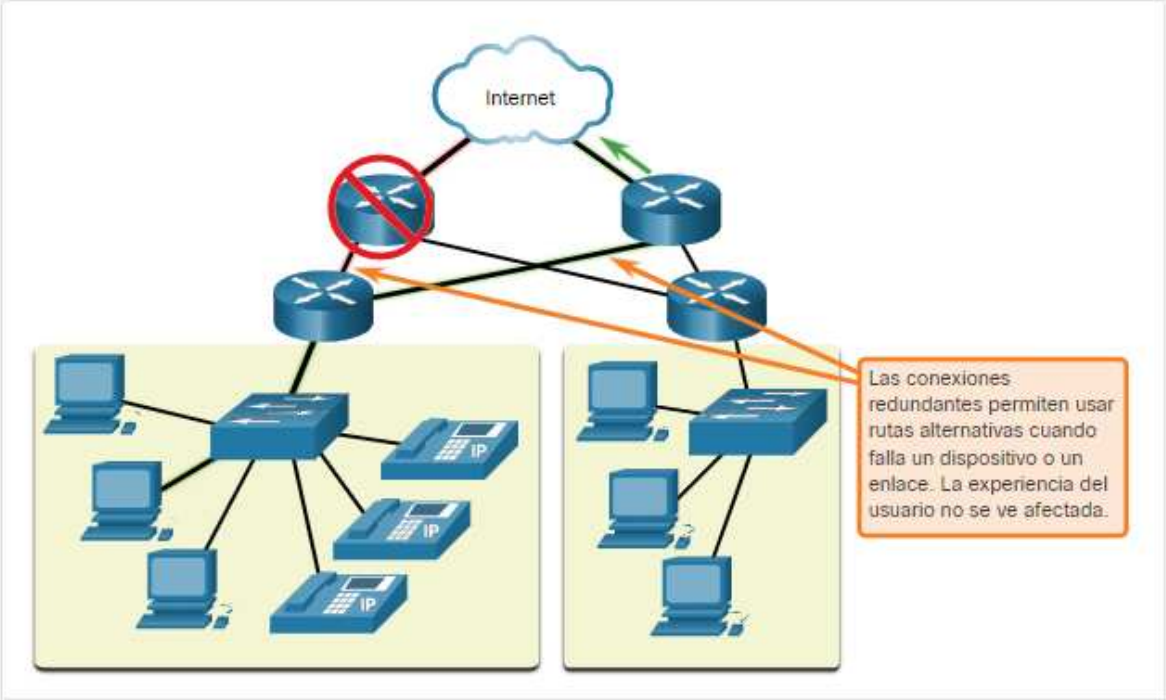
1.6.2

Tolerancia a fallas

Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla. Está construido para permitir una recuperación rápida cuando se produce una falla de este tipo. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia.

La implementación de una red de packet-switched es una forma en que las redes confiables proporcionan redundancia. La conmutación de paquetes divide el tráfico en paquetes que se enrutan a través de una red compartida. Un solo mensaje, como un correo electrónico o una transmisión de vídeo, se divide en múltiples bloques de mensajes, llamados paquetes. Cada paquete tiene la información de dirección necesaria del origen y el destino del mensaje. Los routers dentro de la red cambian los paquetes según la condición de la red en ese momento. Esto significa que todos los paquetes en un mismo mensaje pueden tomar distintas rutas para llegar a destino. En la figura, el usuario no se da cuenta y no se ve afectado por el cambio dinámico de rutas que hace el router cuando falla un enlace.

La topología de red consta de cuatro routers con vínculos redundantes. En la parte superior del diagrama se encuentra la nube de Internet con dos conexiones en la parte inferior, cada una que conduce a un router. Debajo de estos routers hay una conexión a otro router. Cada router inferior se conecta de nuevo a ambos routers que se conectan a Internet. El router en la parte inferior izquierda está conectado a un switch con tres escritorios y tres teléfonos IP. El router en la parte inferior derecha está conectado a un switch con tres escritorios. El router superior izquierdo tiene un círculo rojo con una línea diagonal. El router superior derecho tiene una flecha verde que conduce a Internet. Un cuadro de texto dice: las conexiones redundantes permiten rutas alternativas si falla un dispositivo; la presencia del usuario no se ve afectada.

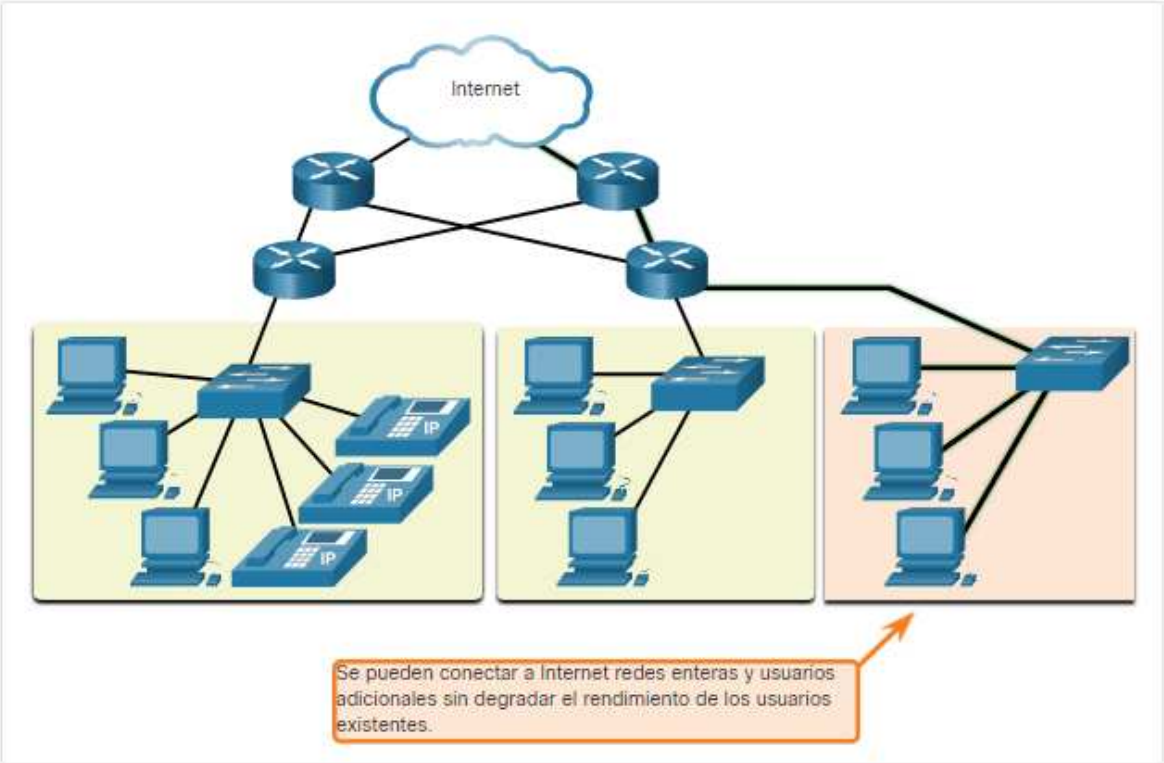


1.6.3

Escalabilidad

Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Lo hace sin degradar el rendimiento de los servicios a los que están accediendo los usuarios existentes. En la figura, se muestra cómo puede agregarse una red nueva a una red existente con facilidad. Además, las redes son escalables porque los diseñadores siguen los estándares y protocolos aceptados. Esto permite a los proveedores de software y hardware centrarse en mejorar los productos y servicios sin tener que diseñar un nuevo conjunto de reglas para operar dentro de la red.

La topología de red consta de cuatro routers con enlaces redundantes, incluidas dos conexiones a la nube de Internet. Hay tres LAN, una de las cuales se ha agregado recientemente. Se lee un cuadro de texto: se pueden conectar a Internet usuarios adicionales y redes enteras sin degradar el rendimiento de los usuarios existentes.



1.6.4

Calidad de servicio

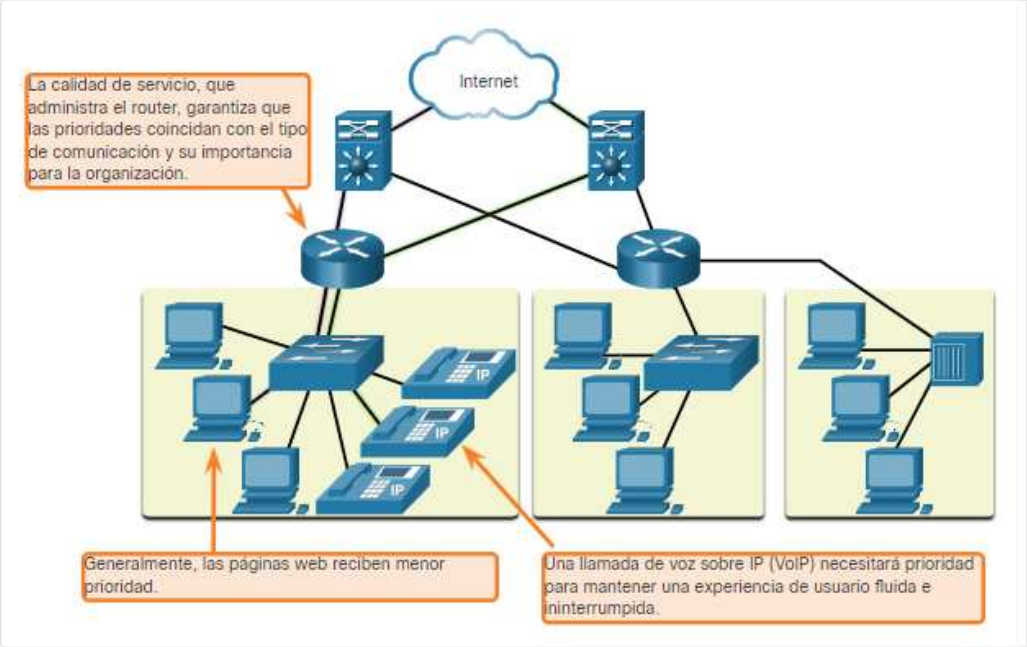
La calidad de servicio (QoS) es un requisito cada vez más importante para las redes hoy en día. Las nuevas aplicaciones disponibles para los usuarios en internetworks, como las transmisiones de voz y de vídeo en vivo generan expectativas más altas sobre la calidad de los servicios que se proporcionan. ¿Alguna vez intentó mirar un vídeo con interrupciones y pausas constantes? A medida que el contenido de datos, voz y vídeo sigue convergiendo en la misma red, QoS se convierte en un mecanismo principal para administrar la congestión y garantizar el envío confiable de contenido a todos los usuarios.

La congestión se produce cuando la demanda de ancho de banda excede la cantidad disponible. El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps). Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red.

Cuando el volumen de tráfico es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos. En la figura, un usuario solicita una página web y otro está realizando una

llamada telefónica. Con una política de QoS, el router puede administrar el flujo de datos y el tráfico de voz, dando prioridad a las comunicaciones de voz si la red se congestiona.

Topología de red con PC y teléfonos IP conectados a un switch que está conectado a un router que administra la calidad del servicio priorizando el tráfico.



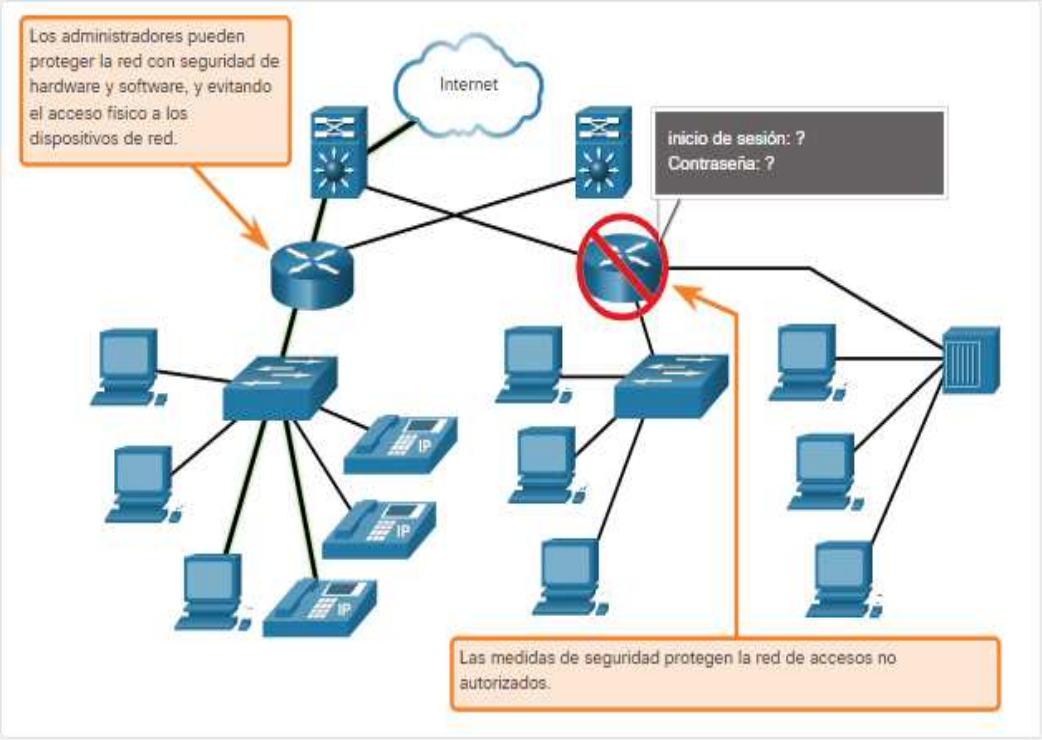
1.6.5

Seguridad de la red

La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad de la infraestructura de red y seguridad de la información.

Asegurar la infraestructura de red incluye asegurar físicamente los dispositivos que proporcionan conectividad de red y evitar el acceso no autorizado al software de administración que reside en ellos, como se muestra en la figura.

Topología de red con PC y teléfonos IP conectados a un switch que está conectado a un router que puede proteger la red con seguridad de software y hardware e impedir el acceso físico a los dispositivos de red.



Los administradores de red también deben proteger la información contenida en los paquetes que se transmiten a través de la red y la información almacenada en los dispositivos conectados a la red. Para alcanzar los objetivos de seguridad de la red, hay tres requisitos principales

- **Confidencialidad** - La confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados pueden acceder a los datos y leerlos.
- **Integridad** - Integridad de datos significa tener la seguridad de que la información no se va a alterar en la transmisión, del origen al destino.
- **Disponibilidad** - Significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados.

1.6.6

Verifique su comprensión - Redes confiables

Verifique su comprensión de redes confiables eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. Scalability happens when designers follow accepted standards and protocols.
2. Confidentiality, integrity, and availability are requirements of security.
3. QoS means that a router will manage the flow of data and voice traffic, giving priority to voice communications.
4. Redundancy is an example a fault-tolerant network architecture.

You got 4 out of 4 questions correct.

1. When designers follow accepted standards and protocols, which of the four basic characteristics of network architecture is achieved?

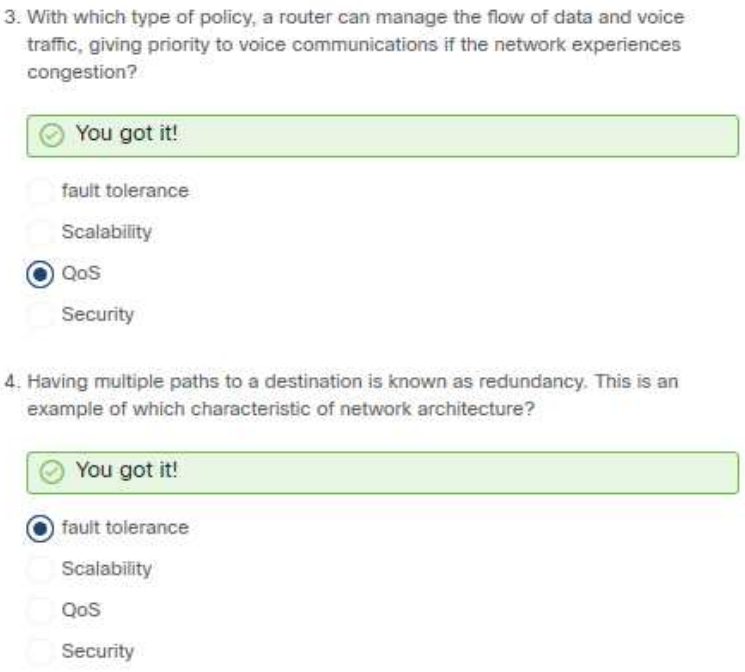
You got it!

- fault tolerance
- (•) Scalability
- QoS
- Security

2. Confidentiality, integrity, and availability are requirements of which of the four basic characteristics of network architecture?

You got it!

- fault tolerance
- Scalability
- QoS
- (•) Security



Las redes en la actualidad / Tendencias de red

Tendencias de red

1.7.1

Tendencias recientes

Ahora sabe mucho sobre las redes, de qué están hechas, cómo nos conectan y qué se necesita para mantenerlas confiables. Pero las redes, como todo lo demás, continúan cambiando. Hay algunas tendencias en la creación de redes que usted, como estudiante de NetaCAD, debería conocer.

A medida que se lanzan al mercado nuevas tecnologías y dispositivos para usuarios finales, las empresas y los consumidores deben continuar adaptándose a este entorno en constante evolución. Existen varias tendencias de redes que afectan a organizaciones y consumidores:

- Traiga su propio dispositivo (BYOD)
- Colaboración en línea
- Comunicaciones de video
- Computación en la nube

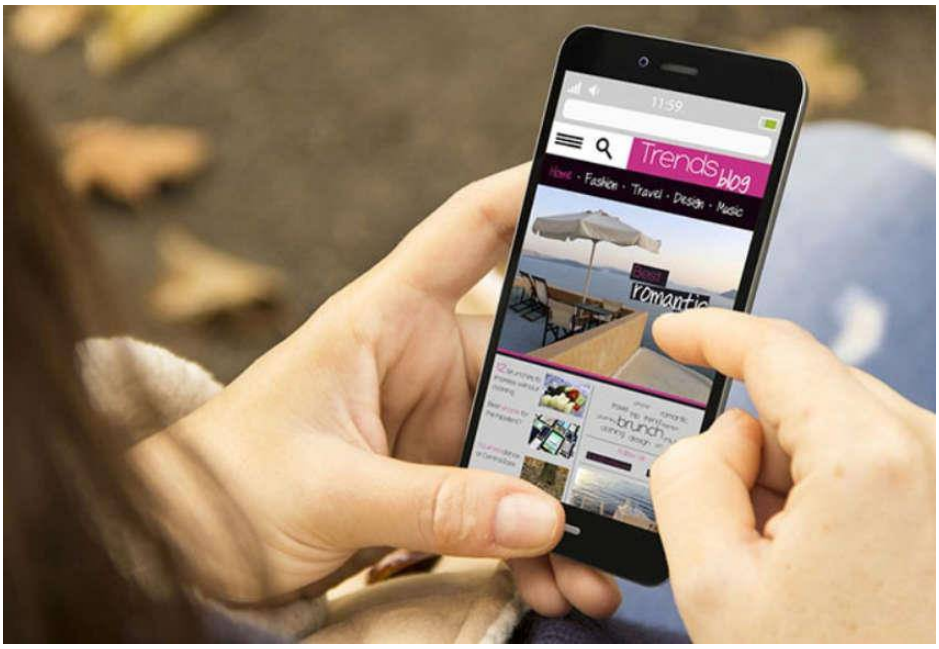
1.7.2

Traiga su propio dispositivo (BYOD)

El concepto de cualquier dispositivo, para cualquier contenido, de cualquier manera, es una tendencia global importante que requiere cambios significativos en la forma en que usamos los dispositivos y los conectamos de manera segura a las redes. Esto se llama Traiga su propio dispositivo (BYOD).

BYOD permite a los usuarios finales la libertad de usar herramientas personales para acceder a la información y comunicarse a través de una red de negocios o campus. Con el crecimiento de los dispositivos de consumo y la caída relacionada en el costo, los empleados y estudiantes pueden tener dispositivos avanzados de computación y redes para uso personal. Estos incluyen computadoras portátiles, tabletas, teléfonos inteligentes y lectores electrónicos. Estos pueden ser comprados por la compañía o la escuela, comprados por el individuo, o ambos.

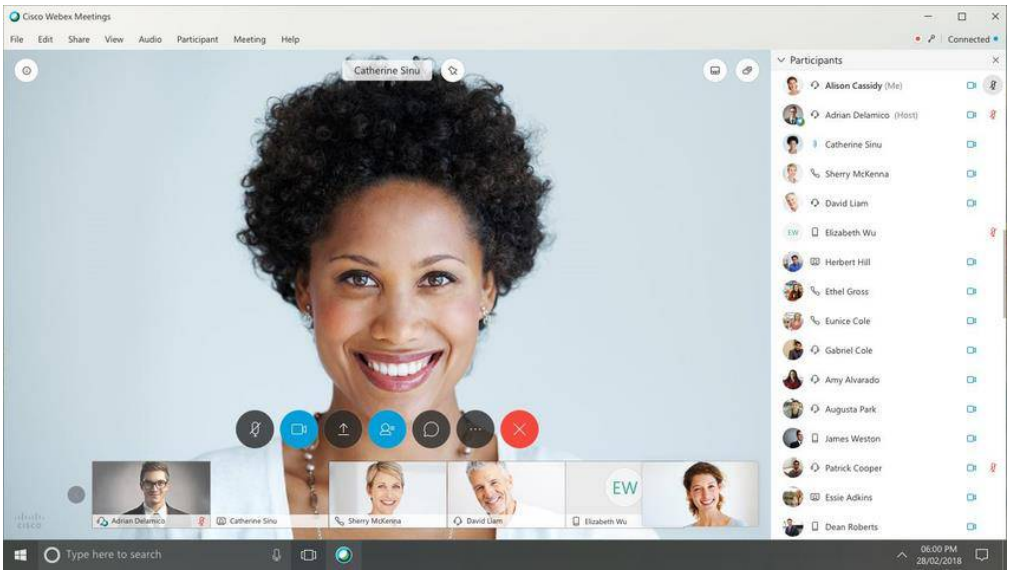
BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar.



1.7.3

Colaboración en línea

Las personas quieren conectarse a la red no solo para acceder a aplicaciones de datos, sino también para colaborar entre sí. La colaboración se define como “el acto de trabajar con otras personas en un proyecto conjunto”. Las herramientas de colaboración, como Cisco Webex que se muestra en la figura, brindan a los empleados, estudiantes, profesores, clientes y asociados una forma de conectarse, interactuar y lograr sus objetivos de forma inmediata.



La Colaboración es una prioridad crítica y estratégica que las organizaciones están utilizando para seguir siendo competitivas. La colaboración también es una prioridad en la educación. Los estudiantes necesitan colaborar para ayudarse mutuamente con el aprendizaje, para desarrollar las habilidades de trabajo en equipo que se utilizan en la fuerza laboral y para trabajar juntos en proyectos en equipo.

Cisco Webex Teams es una herramienta de colaboración multifuncional que le permite enviar mensajes instantáneos a una o más personas, publicar imágenes y publicar vídeos y enlaces. Cada equipo 'espacio' mantiene un historial de todo lo que se publica allí.

1.7.4

Comunicaciones de video

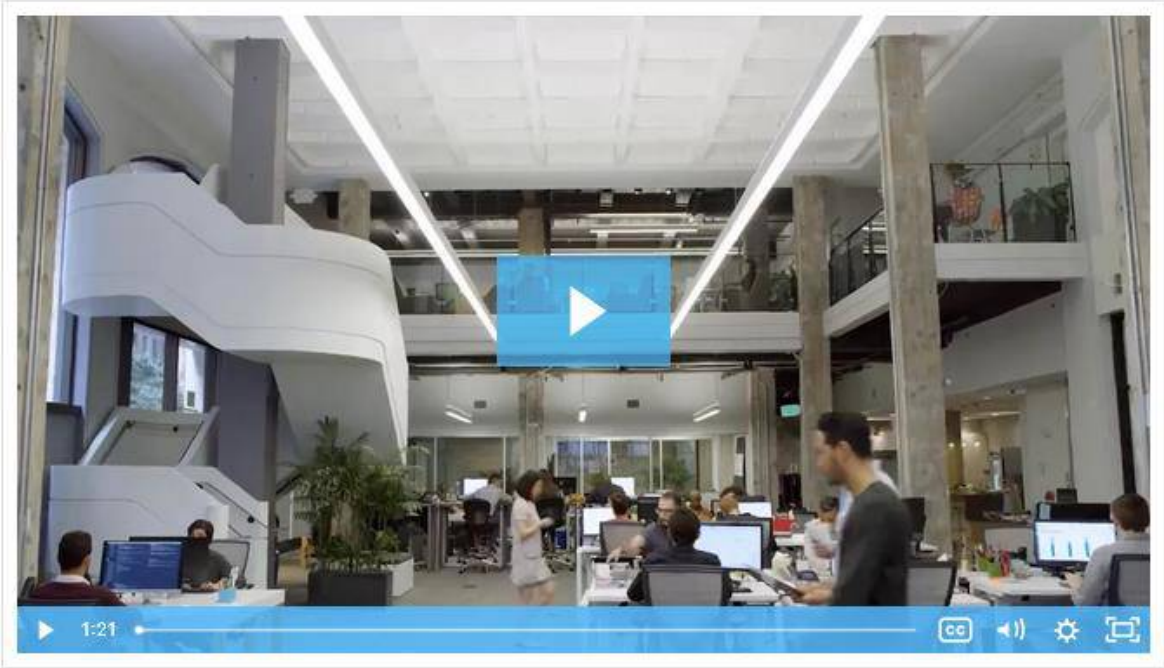
Otra faceta de las redes que es crítica para el esfuerzo de comunicación y colaboración es el video. El video se usa para comunicaciones, colaboración y entretenimiento. Las video llamadas se realizan desde y hacia cualquier persona con conexión a Internet, independientemente de dónde se encuentren.

La videoconferencia es una herramienta poderosa para comunicarse con otros, tanto local como globalmente. A medida que las organizaciones se extienden más allá de los límites geográficos y culturales, el vídeo se convierte en un requisito crítico para una colaboración eficaz.

1.7.5

Vídeo - Cisco Webex para Huddles

Haga clic en Reproducir en la figura para ver cómo se incorpora Cisco Webex en la vida cotidiana y los negocios.



1.7.6

Computación en la nube

La informática en la nube es una de las formas en que accedemos y almacenamos datos. La computación en la nube nos permite almacenar archivos personales, incluso hacer copias de seguridad de una unidad completa en servidores a través de Internet. Se puede acceder a aplicaciones como procesamiento de texto y edición de fotos usando la nube.

Para las empresas, la computación en la nube amplía las capacidades de TI sin requerir inversión en nueva infraestructura, capacitación de personal nuevo o licencias de software nuevo. Estos servicios están disponibles a petición y se proporcionan de forma económica a cualquier dispositivo en cualquier lugar del mundo, sin comprometer la seguridad ni el funcionamiento.

La computación en la nube es posible gracias a los centros de datos. Los centros de datos son instalaciones utilizadas para alojar sistemas informáticos y componentes asociados. Un centro de datos puede ocupar una habitación de un edificio, uno o más pisos o un edificio completo del tamaño de un almacén. Por lo general, la creación y el mantenimiento de centros de datos son muy costosos. Por esta razón, solo las grandes organizaciones utilizan centros de datos privados creados para alojar sus datos y proporcionar servicios a los usuarios. Las organizaciones más pequeñas que no pueden mantener su propio centro de datos privado pueden reducir el costo total de propiedad mediante el arrendamiento de servicios de servidor y almacenamiento a una organización de centro de datos más grande en la nube.

Por motivos de seguridad, fiabilidad y tolerancia a fallos, los proveedores de nube suelen almacenar datos en centros de datos distribuidos. En lugar de almacenar todos los datos de una persona u organización en un centro de datos, se almacenan en varios centros de datos en diferentes ubicaciones.

Existen cuatro tipos principales de nubes: nubes públicas, nubes privadas, nubes híbridas y nubes comunitarias, como se muestra en la tabla.

Tipos de nubes

Cloud Type	Description
Public clouds	Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the internet to provide services.
Private clouds	Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as a government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
Hybrid clouds	A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a distinct object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.

Community clouds	A community cloud is created for exclusive use by specific entities or organizations. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality. Community clouds are used by multiple organizations that have similar needs and concerns. Community clouds are similar to a public cloud environment, but with set levels of security, privacy, and even regulatory compliance of a private cloud.

Tipo de nube	Descripción
Nubes públicas	Se realizan aplicaciones y servicios basados en la nube ofrecidos en una nube pública disponible para la población en general. Los servicios pueden ser gratuitos o se ofrecen en un modelo de pago por uso, como pagar por el almacenamiento en línea. El público la nube utiliza Internet para proporcionar servicios.
Nubes privadas	Las aplicaciones y servicios basados en la nube que se ofrecen en una nube privada son diseñada para una organización o una entidad específica, como el gobierno. A la nube privada se puede configurar utilizando la red, aunque esto puede ser costoso de construir y mantener. Una privada nube también puede ser administrada por una organización externa con acceso estricto seguridad.
Nubes híbridas	Una nube híbrida se compone de dos o más nubes (por ejemplo: parte privada, parte pública), donde cada parte sigue siendo un objeto distinto, pero ambos son conectados usando una única arquitectura. Individuos en una nube híbrida sería capaz de tener grados de acceso a diversos servicios basados en derechos de acceso.
Nubes comunitarias	Una nube comunitaria se crea para la utilización exclusiva de entidades u organizaciones. Las diferencias entre nubes públicas y las comunitarias son las necesidades funcionales que han sido personalizadas para la comunidad. Por ejemplo, las organizaciones de servicios de salud deben cumplir las políticas y leyes (por ejemplo, la HIPAA) que requieren una autenticación y una confidencialidad especiales. Las nubes comunitarias son utilizadas por múltiples organizaciones que tienen necesidades e inquietudes similares. Las nubes comunitarias son similares a un entorno de nube pública, pero con el establecimiento de niveles de seguridad, la privacidad e incluso el cumplimiento reglamentario de una nube privada.

1.7.7

Tendencias tecnológicas en el hogar

Las tendencias de las redes no solo afectan la forma en que nos comunicamos en el trabajo y en la escuela, sino que también cambian muchos aspectos del hogar. Las nuevas tendencias del hogar incluyen la “tecnología del hogar inteligente”.

La tecnología inteligente para el hogar se integra en los electrodomésticos de todos los días, que luego pueden conectarse con otros dispositivos para hacer que los electrodomésticos sean más "inteligentes" o automatizados. Por ejemplo, puede preparar la comida y colocarla en el horno para cocinar antes de salir de la casa por el día. Usted programa su horno inteligente para la comida que desea que cocine. También estaría conectado a su "calendario de eventos" para poder determinar a qué hora debería estar disponible para comer y ajustar las horas de inicio y la duración de la cocción en consecuencia. Incluso podría ajustar el tiempo y la temperatura de cocción sobre la base de los cambios en su agenda. Además, una conexión de teléfono inteligente o tableta le permite conectarse directamente al horno para realizar los ajustes que desee. Cuando la comida está lista, el horno envía un mensaje de alerta a usted (o a alguien que especifique) de que la comida está terminada y se calienta.

La tecnología de hogar inteligente se está desarrollando actualmente para todas las habitaciones dentro de una casa. La tecnología inteligente para el hogar se volverá más común a medida que se expandan las redes domésticas y la tecnología de Internet de alta velocidad.

Una representación de la tecnología del hogar inteligente que muestra una nube con flechas que apuntan a una casa, un coche y un teléfono inteligente. El texto en la parte inferior dice: El teléfono inteligente se actualiza desde la nube con el estado de los dispositivos de casa inteligente y el coche inteligente; el usuario puede utilizar el teléfono inteligente para interactuar con el hogar inteligente y el coche inteligente.

Nube

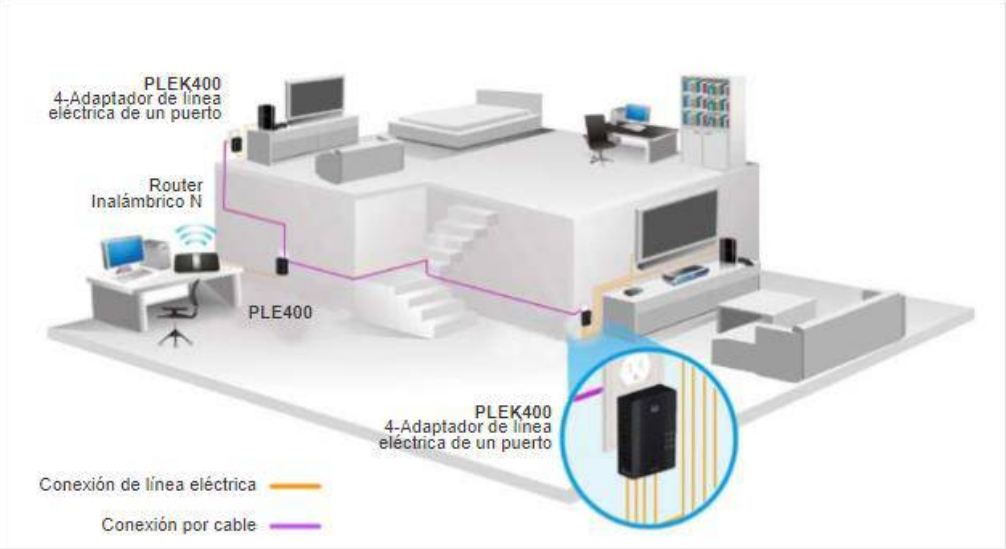
El teléfono inteligente se actualiza desde la nube con el estado de los dispositivos de hogar inteligente y el automóvil inteligente. El usuario puede utilizar el teléfono inteligente para interactuar con la casa inteligente y el coche inteligente.

1.7.8

Redes powerline

Las redes Powerline para redes domésticas utilizan el cableado eléctrico existente para conectar dispositivos, como se muestra en la figura.

Plano de planta abierto de un hogar que utiliza la red powerline para una red doméstica. Hay tres adaptadores de línea eléctrica PLEK400 de 4 puertos conectados a tres tomas eléctricas diferentes, todos conectados a través de conexiones cableadas. Cada adaptador tiene al menos una conexión de línea eléctrica a un dispositivo en red, incluidos equipos de sobremesa y televisores.



Mediante un adaptador estándar de línea eléctrica, los dispositivos pueden conectarse a la LAN donde haya un tomacorriente. No es necesario instalar cables de datos, y se utiliza poca o ninguna electricidad adicional. Mediante el uso de los mismos cables que transmiten electricidad, la red de línea de alimentación envía información mediante el envío de datos en ciertas frecuencias.

La red Powerline es especialmente útil cuando los puntos de acceso inalámbrico no pueden llegar a todos los dispositivos en el hogar. La red Powerline no es un sustituto del cableado dedicado en redes de datos. Sin embargo, es una alternativa cuando los cables de red de datos o las comunicaciones inalámbricas no son posibles o efectivas.

1.7.9

Banda ancha inalámbrica

En muchas áreas donde el cable y el DSL no están disponibles, es posible que la conexión inalámbrica se utilice para conectarse a Internet.

Proveedor de servicios de Internet inalámbrico

El proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado o una zona activa mediante tecnologías inalámbricas similares a las que se encuentran en las redes de área local inalámbrica (WLAN). Los WISP se encuentran con mayor frecuencia en entornos rurales donde los servicios de cable o DSL no están disponibles.

Aunque se puede instalar una torre de transmisión separada para la antena, típicamente la antena está unida a una estructura elevada existente, como una torre de agua o una torre de radio. Se instala una pequeña antena en el techo del suscriptor, al alcance del transmisor del WISP. La unidad de acceso del suscriptor se conecta a la red conectada por cable dentro del hogar. Desde la perspectiva del usuario doméstico, la configuración no es muy diferente de la de DSL o el servicio de cable. La diferencia principal es que la conexión del hogar al ISP es inalámbrica, en lugar de establecerse mediante un cable físico.

Servicio de banda ancha inalámbrica

Otra solución inalámbrica para los hogares y las pequeñas empresas es la banda ancha inalámbrica, como se muestra en la figura.

Esta solución utiliza la misma tecnología celular que un teléfono inteligente. Se instala una antena fuera del hogar, que proporciona conectividad inalámbrica o por cable a los dispositivos en el hogar. En muchas zonas, la banda ancha inalámbrica doméstica compite directamente con los servicios de DSL y cable.

1.7.10

Verifique su comprensión - Tendencias de red

Verifique su comprensión de las tendencias de la red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. Video communications is a good conferencing tool to use with others who are located elsewhere in your city, or even in another country.
2. BYOD feature describes using personal tools to access information and communicate across a business or campus network.
3. Cloud computing contains options such as Public, Private, Custom and Hybrid.
4. Powerline is being used when connecting a device to the network using an electrical outlet.
5. Wireless broadband uses the same cellular technology as a smart phone.

You got 5 out of 5 questions correct.

1. Which feature is a good conferencing tool to use with others who are located elsewhere in your city, or even in another country?

You got it!

- BYOD
- (•) Video communications
- Cloud computing

2. Which feature describes using personal tools to access information and communicate across a business or campus network?

You got it!

- (•) BYOD
- Video communications
- Cloud computing

3. Which feature contains options such as Public, Private, Custom and Hybrid?

You got it!

- BYOD
- Video communications
- (•) Cloud computing

4. Which feature is being used when connecting a device to the network using an electrical outlet?

You got it!

- Smart home technology
- (•) Powerline
- Wireless broadband

5. Which feature uses the same cellular technology as a smart phone?

You got it!

- Smart home technology
- Powerline
- (•) Wireless broadband

Las redes en la actualidad / Seguridad de la red

Seguridad de la red

1.8.1

Amenazas de seguridad

Sin duda, ha escuchado o leído noticias sobre la violación de la red de una empresa, lo que brinda a los atacantes acceso a la información personal de miles de clientes. Por esta razón, la seguridad de la red siempre va a ser una prioridad de los administradores.

La seguridad de la red es una parte integral de la red informática, independientemente de si la red está en un hogar con una sola conexión a Internet o es una corporación con miles de usuarios. La seguridad de la red debe tener en cuenta el entorno, así como las herramientas y requisitos de la red. Debe ser capaz de proteger los datos al tiempo que permite la calidad de servicio que los usuarios esperan de la red.

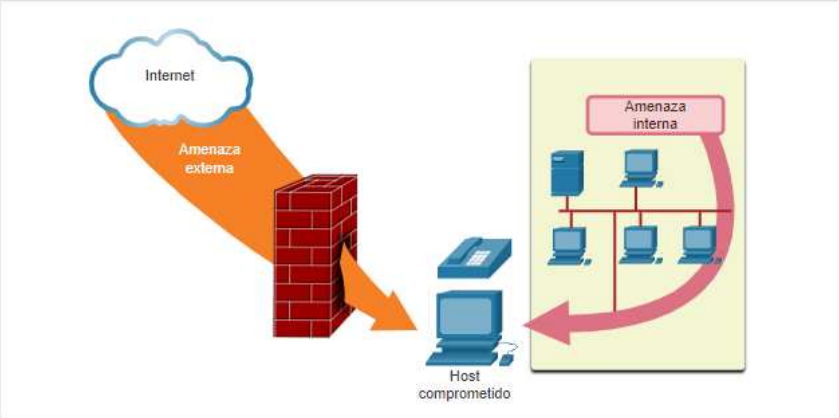
Asegurar una red implica protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar las amenazas. Los vectores de amenazas pueden ser externos o internos. Muchas amenazas de seguridad de redes externas se originan hoy en Internet.

Existen varias amenazas externas comunes a las redes:

- **Virus, gusanos y caballos de Troya** - Estos contienen software malicioso o código que se ejecuta en un dispositivo de usuario.
- **Spyware y adware** \ - Estos son tipos de software que se instalan en el dispositivo de un usuario. El software recopila en secreto información sobre el usuario.
- **Ataques de día cero** - También llamados ataques de hora cero, se producen el primer día que se conoce una vulnerabilidad
- **Amenazas de Atacantes**: una persona malintencionada ataca dispositivos de usuario o recursos de red.
- **Ataques por denegación de servicio** - Estos ataques ralentizan o bloquean las aplicaciones y procesos en un dispositivo de red.
- **Intercepción y robo de datos** - Este ataque captura información privada de la red de una organización.
- **Robo de identidad** - Este ataque roba las credenciales de inicio de sesión de un usuario para acceder a datos privados.

También es importante tener en cuenta las amenazas internas. Se llevaron a cabo numerosos estudios que muestran que las violaciones de datos más comunes suceden a causa de los usuarios internos de la red. Esto se puede atribuir a dispositivos perdidos o robados o al mal uso accidental por parte de los empleados, y dentro del entorno comercial, incluso a empleados maliciosos. Con las estrategias de BYOD en desarrollo, los datos corporativos son mucho más vulnerables. Por lo tanto, al desarrollar una política de seguridad, es

importante abordar las amenazas de seguridad internas y externas, como se muestra en la figura.



Dos flechas que conducen a un host comprometido; una procedente de la nube de Internet pasando por un firewall, la otra procedente de una amenaza interna en la red interna.

1.8.2

Soluciones de seguridad

No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad. Si un componente de seguridad no puede identificar y proteger la red, otros pueden tener éxito.

En general, la implementación de seguridad de las redes domésticas es muy básica. Por lo general, lo implementa en los dispositivos finales, así como en el punto de conexión a Internet, e incluso puede confiar en los servicios contratados por el ISP.

Estos son los componentes básicos de seguridad para una red doméstica o de oficina pequeña:

- **Antivirus y antispyware** - Estas aplicaciones ayudan a proteger los dispositivos finales para que no se infecten con software malicioso.
- **Filtrado de Firewall** - El filtrado de firewall bloquea el acceso no autorizado dentro y fuera de la red. Esto puede incluir un sistema de firewall ejecutado en un host que se implemente para impedir el acceso no autorizado al terminal o un servicio de filtrado básico en el router doméstico para impedir el acceso no autorizado del mundo exterior a la red.

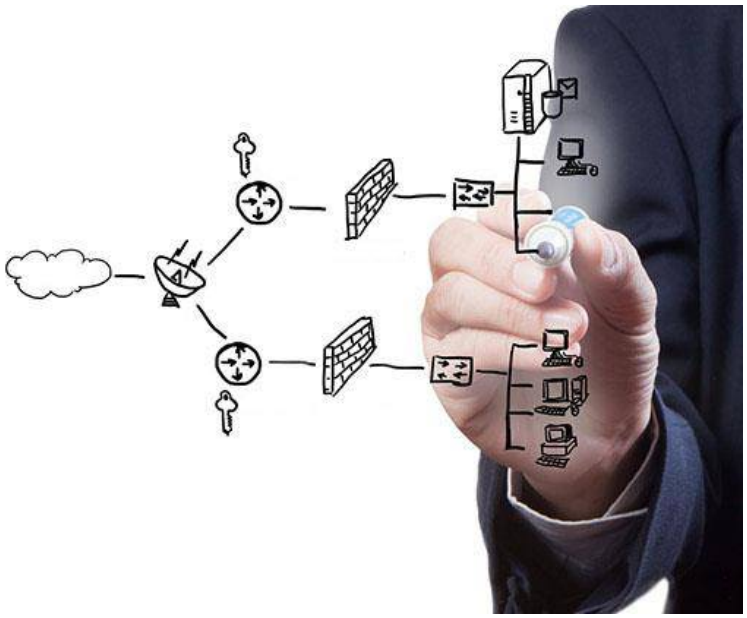
Por otra parte, la implementación de seguridad de la red en redes de las empresas normalmente consiste en la integración de numerosos componentes a la red para controlar y

filtrar el tráfico. Lo ideal es que todos los componentes funcionen juntos, lo que minimiza la necesidad de mantenimiento y aumenta la seguridad. Las redes más grandes y las redes corporativas utilizan filtros antivirus, antispyware y firewall, pero también tienen otros requisitos de seguridad:

- **Sistemas de firewall dedicados** - Estos proporcionan capacidades de firewall más avanzadas que pueden filtrar grandes cantidades de tráfico con más granularidad.
- **Listas de control de acceso (ACL)** - Estos filtran aún más el acceso y el reenvío de tráfico en función de las direcciones IP y las aplicaciones.
- **Sistemas de prevención de intrusiones (IPS)** - Estos identifican amenazas de rápida propagación, como ataques de día cero o de hora cero.
- **Redes Privadas Virtuales (VPN)** - Estos proporcionan acceso seguro a una organización para trabajadores remotos.

Los requisitos de seguridad de la red deben tener en cuenta el entorno, así como las diversas aplicaciones y los requisitos informáticos. Tanto el entorno doméstico como el empresarial deben poder proteger sus datos y, al mismo tiempo, permitir la calidad de servicio que los usuarios esperan de cada tecnología. Además, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, en constante cambio.

El estudio de las amenazas de seguridad de red y de las técnicas de mitigación comienza con una comprensión clara de la infraestructura de switching y routing subyacente utilizada para organizar los servicios de red.



1.8.3

Verifique su comprensión - Seguridad de red

Verifique su comprensión de la seguridad de la red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. A DoS attack slows down or crashes equipment and programs.
2. A VPN creates a secure connection for remote workers.
3. A firewall blocks unauthorized access to your network.
4. A zero-day or zero-hour attack occurs on the first day that a vulnerability becomes known.
5. A virus, worm, or Trojan horse is malicious code running on user devices.

You got 5 out of 5 questions correct.

1. Which attack slows down or crashes equipment and programs?

You got it!

- Firewall
- Virus, worm, or Trojan horse
- Zero-day or Zero-hour
- Virtual Private Network (VPN)
- (•) Denial of Service (DoS)

2. Which option creates a secure connection for remote workers?

You got it!

- Firewall
- Virus, worm, or Trojan horse
- Zero-day or Zero-hour
- (•) Virtual Private Network (VPN)
- Denial of Service (DoS)

3. Which option blocks unauthorized access to your network?

You got it!

- (•) Firewall
- ( ) Virus, worm, or Trojan horse
- ( ) Zero-day or Zero-hour
- ( ) Virtual Private Network (VPN)
- ( ) Denial of Service (DoS)

4. Which option describes a network attack that occurs on the first day that a vulnerability becomes known?

You got it!

- ( ) Firewall
- ( ) Virus, worm, or Trojan horse
- (•) Zero-day or Zero-hour
- ( ) Virtual Private Network (VPN)
- ( ) Denial of Service (DoS)

5. Which option describes malicious code running on user devices?

You got it!

- ( ) Firewall
- (•) Virus, worm, or Trojan horse
- ( ) Zero-day or Zero-hour
- ( ) Virtual Private Network (VPN)
- ( ) Denial of Service (DoS)

Las redes en la actualidad / El profesional de TI

El profesional de TI

1.9.1

CCNA

Como estudiante de NetaCAD, es posible que ya tenga una carrera en TI o que siga preparándose para prepararse para su carrera profesional. En cualquier caso, es bueno conocer las habilidades necesarias para adaptarse a los tipos de trabajos que están disponibles en TI.

La función y las competencias necesarias de los ingenieros de redes están en desarrollo y son más necesarias que nunca. La certificación Cisco Certified Network Associate (CCNA) demuestra que usted tiene conocimiento de las tecnologías fundamentales y asegura que se mantenga relevante con los conjuntos de habilidades necesarios para la adopción de tecnologías de próxima generación.

Un CCNA consolidado y actualizado para ingenieros de redes consta de tres cursos y un examen que cubre los temas fundamentales para todas las tecnologías de red. El nuevo CCNA se enfoca en temas de seguridad y fundamentos de IP junto con programación inalámbrica, virtualización, automatización y red.

Existen nuevas certificaciones DevNet a nivel asociado, especializado y profesional, para validar sus habilidades de desarrollo de software.

Existen opciones de certificación especializadas para validar sus habilidades de acuerdo con su rol e intereses laborales. Esto incluye la certificación Cisco Enterprise Advanced Infrastructure Specialist.

Puede empezar donde quiera. No hay requisitos previos para comenzar a obtener su certificación de nivel asociado, especialista, profesional o experto. Los créditos de educación continua para la recertificación y el desarrollo continuo ya están disponibles para el CCNA.

1.9.2

Empleos de redes

Su certificación CCNA lo preparará para una variedad de puestos de trabajo en el mercado actual. En [www.netacad.com] (http://www.netacad.com) puede hacer clic en el menú Carreras y, a continuación, seleccionar Oportunidades de empleo. Puede encontrar oportunidades de empleo donde vive utilizando el nuevo programa, el Talent Bridge Matching Engine. Busque trabajos con Cisco y con asociados y distribuidores de Cisco que necesiten estudiantes y graduados de Cisco Networking Academy.

También puede buscar empleos de TI usando motores de búsqueda online como Indeed, Glassdoor y Monster. Utilice términos de búsqueda como TI, administrador de red, arquitectos de red y administrador de sistemas informáticos. También puede buscar utilizando el término Cisco CCNA.

1.9.3

Laboratorio - Investigue las oportunidades de trabajo en redes y TI

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Buscar oportunidades laborales
- Parte 2: Reflexionar sobre la investigación

Investigue las oportunidades de trabajo en TI y redes

1. Las redes en la actualidad
2. Módulo de Práctica y Prueba

Módulo de Práctica y Prueba

1.10.1

¿Qué aprendí en este módulo?

Las redes afectan nuestras vidas

En el mundo actual, estamos conectados como nunca antes gracias al uso de redes. Las personas que tienen alguna idea pueden comunicarse de manera instantánea con otras personas para hacer esas ideas realidad. La creación de comunidades en línea para el intercambio de ideas e información tiene el potencial de aumentar las oportunidades de productividad en todo el planeta. La creación de la nube nos permite almacenar documentos e imágenes y acceder a ellos en cualquier lugar y en cualquier momento.

Componentes de red

Todas las computadoras que están conectadas a una red y participan directamente en la comunicación de la red se clasifican como hosts. Los hosts se pueden llamar dispositivos finales. Algunos hosts también se llaman clientes. Muchas computadoras funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares. Un terminal es el origen o el destino de un mensaje transmitido a través de la red. Estos dispositivos conectan los terminales individuales a la red y pueden conectar varias redes individuales para formar una internetwork. Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Representaciones y topología de red

Los diagramas de redes a menudo usan símbolos para representar los diferentes dispositivos y conexiones que forman una red. Un diagrama proporciona una manera fácil de comprender cómo se conectan los dispositivos en una red grande. Este tipo de representación de una red se denomina diagrama de topología. Los diagramas de topología física ilustran la ubicación

física de los dispositivos intermedios y la instalación de cables. Los diagramas de topología lógica ilustran dispositivos, puertos y el esquema de direccionamiento de la red.

Tipos comunes de redes

Las redes domésticas pequeñas conectan algunas computadoras entre sí y a Internet. La red de oficina pequeña / oficina doméstica (SOHO) permite que las computadoras de una oficina doméstica o remota se conecten a una red corporativa o accedan a recursos centralizados y compartidos. Las redes medianas a grandes, como las que se utilizan en corporaciones y escuelas, pueden tener muchas ubicaciones con cientos o miles de hosts interconectados. Internet es una red de redes que conecta cientos de millones de computadoras en todo el mundo. Los dos tipos más comunes de infraestructuras de red son las redes de área local (LAN) y las redes de área amplia (WAN). Una LAN es una infraestructura de la red que abarca un área geográfica pequeña. Una WAN es una infraestructura de la red que abarca un área geográfica extensa. Intranet se refiere a una conexión privada de LAN y WAN que pertenece a una organización. Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa.

Conexiones a Internet

Las conexiones a Internet de SOHO incluyen cable, DSL, celular, satélite y telefonía por Dial-up. Las conexiones a Internet de negocios incluyen Línea dedicada arrendada, Metro Ethernet, Business DSL y Satélite. Las opciones de conexión varían según la ubicación geográfica y la disponibilidad del proveedor de servicios. Las utilizaban diferentes tecnologías, reglas y estándares. Las redes convergentes entregan datos, voz y video entre muchos tipos diferentes de dispositivos a través de la misma infraestructura de red. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación. Packet Tracer es un programa de software flexible que le permite utilizar representaciones de red y teorías para construir modelos de red y explorar LAN y WAN relativamente complejas.

Redes confiables

En este contexto, el término arquitectura de red, se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red. A medida que evolucionan las redes, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para satisfacer las expectativas de los usuarios: tolerancia a fallos, escalabilidad, calidad de servicio (QoS) y seguridad. Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia. Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Las redes son escalables porque los diseñadores siguen los estándares y protocolos aceptados. QoS es un mecanismo principal para gestionar la congestión y garantizar la entrega confiable de contenido a todos los usuarios. Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad

de la infraestructura de red y seguridad de la información. Para alcanzar los objetivos de seguridad de red, existen tres requisitos principales: Confidencialidad, Integridad y Disponibilidad.

Tendencias de red

Existen varias tendencias de redes recientes que afectan a las organizaciones y a los consumidores: Traiga su propio dispositivo (BYOD), colaboración en línea, comunicaciones de video y computación en la nube. BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar. Las herramientas de colaboración, como Cisco WebEx, brindan a los empleados, estudiantes, maestros, clientes y socios una forma de conectarse, interactuar y alcanzar sus objetivos al instante. El video se usa para comunicaciones, colaboración y entretenimiento. Las video llamadas se realizan desde y hacia cualquier persona con conexión a Internet, independientemente de dónde se encuentren. La computación en la nube nos permite almacenar archivos personales, incluso hacer copias de seguridad de una unidad completa en servidores a través de Internet. Se puede acceder a aplicaciones como procesamiento de texto y edición de fotos usando la nube. Existen cuatro tipos principales de nubes: nubes públicas, nubes privadas, nubes híbridas y nubes personalizadas. La tecnología de hogar inteligente se está desarrollando actualmente para todas las habitaciones dentro de una casa. La tecnología inteligente para el hogar se volverá más común a medida que se expandan las redes domésticas y la tecnología de Internet de alta velocidad. Mediante el uso de los mismos cables que transmiten electricidad, la red de línea de alimentación envía información mediante el envío de datos en ciertas frecuencias. El proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado o una zona activa mediante tecnologías inalámbricas similares a las que se encuentran en las redes de área local inalámbrica (WLAN).

Network Security

Existen varias amenazas externas comunes a las redes:

- Virus, gusanos y caballos de Troya
- Spyware y adware
- Ataques de día cero Amenazas de Atacantes*
- Ataques por denegación de servicio
- Intercepción y robo de datos
- Robo de identidad

Estos son los componentes básicos de seguridad para una red doméstica o de oficina pequeña:

- Antivirus y antispyware
- Filtrado de firewall

Las redes más grandes y las redes corporativas utilizan filtros antivirus, antispyware y firewall, pero también tienen otros requisitos de seguridad:

- Sistemas de firewall exclusivos
- Listas de control de acceso (ACL)
- Sistemas de prevención de intrusiones (IPS)
- Redes privadas virtuales (VPN)

El profesional de TI

La certificación Cisco Certified Network Associate (CCNA) demuestra que usted tiene conocimiento de las tecnologías fundamentales y asegura que se mantenga relevante con los conjuntos de habilidades necesarios para la adopción de tecnologías de próxima generación. Su certificación CCNA lo preparará para una variedad de puestos de trabajo en el mercado actual. En www.netacad.com, puede hacer clic en el menú Carreras y, a continuación, seleccionar Oportunidades de empleo. Puede encontrar oportunidades de empleo donde vive utilizando el nuevo programa, el Talent Bridge Matching Engine. Busque trabajos con Cisco y con asociados y distribuidores de Cisco que necesiten estudiantes y graduados de Cisco Networking Academy.

1.10.2

Prueba del módulo - Redes en la actualidad

1. During a routine inspection, a technician discovered that software that was installed on a computer was secretly collecting data about websites that were visited by users of the computer. Which type of threat is affecting this computer?

Topic 1.8.0 - Spyware is software that is installed on a network device and that collects information.

- DoS attack
- identity theft
- (•) spyware
- zero-day attack

2. Which term refers to a network that provides secure access to the corporate offices by suppliers, customers and collaborators?

Topic 1.4.0 - The term Internet refers to the worldwide collection of connected networks. Intranet refers to a private connection of LANs and WANS that belong to an organization and is designed to be accessible to the members of the organization, employees, or others with authorization. Extranets provide secure and safe access to suppliers, customers, and collaborators. Extendednet is not a type of network.

- Internet
- intranet
- (•) extranet
- extendednet

3. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

Topic 1.7.0 - BYOD allows end users to use personal tools to access the corporate network. Allowing this trend can have major impacts on a network, such as security and compatibility with corporate software and devices.

- cloud computing
- online collaboration
- (•) bring your own device
- video conferencing

4. What is an ISP?

Topic 1.5.0 - An ISP, or Internet Service Provider, is an organization that provides access to the Internet for businesses and individuals.

- It is a standards body that develops cabling and wiring standards for networking.
- It is a protocol that establishes how computers within a local network communicate.
- (•) It is an organization that enables individuals and businesses to connect to the Internet.
- It is a networking device that combines the functionality of several different networking devices in one.

5. In which scenario would the use of a WISP be recommended?

Topic 1.7.0 - Wireless Internet Service Providers (WISPs) are typically found in rural areas where DSL or cable access is not available. A dish or antenna on the property of the subscriber connects wirelessly to a WISP transmitter, eliminating the need for physical cabling outside the building.

- an Internet cafe in a city
- (•) a farm in a rural area without wired broadband access
- any home with multiple wireless devices
- an apartment in a building with cable access to the Internet

6. What characteristic of a network enables it to quickly grow to support new users and applications without impacting the performance of the service being delivered to existing users?

Topic 1.6.0 - Networks must be able to quickly grow to support new users and services, without impacting existing users and services. This ability to grow is known as scalability.

- reliability
- (•) scalability
- quality of service
- accessibility

7. A college is building a new dormitory on its campus. Workers are digging in the ground to install a new water pipe for the dormitory. A worker accidentally damages a fiber optic cable that connects two of the existing dormitories to the campus data center. Although the cable has been cut, students in the dormitories only experience a very short interruption of network services. What characteristic of the network is shown here?

Topic 1.6.0 - Fault tolerance is the characteristic of a network which allows it to quickly respond to failures of network devices, media, or services. Quality of service refers to the measures taken to ensure that network traffic requiring higher throughput receives the required network resources. Scalability refers to the ability of the network to grow to accommodate new requirements. Security refers to protecting networks and data from theft, alteration, or destruction. Integrity refers to the completeness of something and is generally not used as a characteristic of networks in the same way as the other terms.

- quality of service (QoS)
- scalability
- security
- (•) fault tolerance
- integrity

8. What are two characteristics of a scalable network? (Choose two.)

Topic 1.6.0 - Scalable networks are networks that can grow without requiring costly replacement of existing network devices. One way to make a network scalable is to buy networking devices that are modular.

- easily overloaded with increased traffic
- [x] grows in size without impacting existing users
- is not as reliable as a small network
- [x] suitable for modular devices that allow for expansion
- offers limited number of applications

9. Which device performs the function of determining the path that messages should take through internetworks?

Topic 1.2.0 - A router is used to determine the path that the messages should take through the network. A firewall is used to filter incoming and outgoing traffic. A DSL modem is used to provide Internet connection for a home or an organization.

- (•) a router
- a firewall
- a web server
- a DSL modem

10. Which two Internet connection options do not require that physical cables be run to the building? (Choose two.)

Topic 1.5.0 - Cellular connectivity requires the use of the cell phone network. Satellite connectivity is often used where physical cabling is not available outside the home or business.

- DSL
- [x] cellular
- [x] satellite
- dialup
- dedicated leased line

11. What type of network must a home user access in order to do online shopping?

Topic 1.5.0 - Home users will go online shopping over the Internet because online vendors are accessed through the Internet. An intranet is basically a local area network for internal use only. An extranet is a network for external partners to access certain resources inside an organization. A home user does not necessarily need a LAN to access the Internet. For example, a PC connects directly to the ISP through a modem.

- an intranet
- (•) the Internet
- an extranet
- a local area network

12. How does BYOD change the way in which businesses implement networks?

Topic 1.7.0 - A BYOD environment requires an organization to accommodate a variety of devices and access methods. Personal devices, which are not under company control, may be involved, so security is critical. Onsite hardware costs will be reduced, allowing a business to focus on delivering collaboration tools and other software to BYOD users.

- BYOD requires organizations to purchase laptops rather than desktops.
- BYOD users are responsible for their own network security, thus reducing the need for organizational security policies.
- BYOD devices are more expensive than devices that are purchased by an organization.
- (•) BYOD provides flexibility in where and how users can access network resources.

13. An employee wants to access the network of the organization remotely, in the safest possible way. What network feature would allow an employee to gain secure remote access to a company network?

Topic 1.8.0 - Virtual private networks (VPN) are used to provide secure access to remote workers.

- ACL
- IPS
- (•) VPN
- BYOD

14. What is the Internet?

Topic 1.5.0 - The Internet provides global connections that enable networked devices (workstations and mobile devices) with different network technologies, such as Ethernet, DSL/cable, and serial connections, to communicate. A private network for an organization with LAN and WAN connections is an intranet.

- It is a network based on Ethernet technology.
- It provides network access for mobile devices.
- (•) It provides connections through interconnected global networks.
- It is a private network for an organization with LAN and WAN connections.

15. What are two functions of end devices on a network? (Choose two.)

Topic 1.2.0 - End devices originate the data that flows through the network. Intermediary devices direct data over alternate paths in the event of link failures and filter the flow of data to enhance security. Network media provide the channel through which network messages travel.

- [x] They originate the data that flows through the network.
- [ ] They direct data over alternate paths in the event of link failures.
- [ ] They filter the flow of data to enhance security.
- [x] They are the interface between humans and the communication network.
- [ ] They provide the channel over which the network message travels.

Capítulo 2_Configuración básica de switches y terminales

Introducción

2.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Configuración básica de switches y dispositivos finales!

Como parte de su carrera profesional en redes, es posible que tenga que configurar una nueva red o mantener y actualizar una existente. En cualquier caso, configurará switches y dispositivos finales para que sean seguros y funcionen de manera eficaz según sus requisitos.

Fuera de la caja, los switches y los dispositivos finales vienen con alguna configuración general. Pero para su red particular, los switches y los dispositivos finales requieren su información e instrucciones específicas. En este módulo, aprenderá a acceder a los dispositivos de red Cisco IOS. Aprenderá los comandos de configuración básicos y los usará

para configurar y verificar un dispositivo Cisco IOS y un dispositivo final con una dirección IP.

Por supuesto, hay mucho más en la administración de la red, pero nada de eso puede suceder sin configurar primero los switches y los dispositivos finales. Comencemos ya mismo.

2.0.2

¿Qué aprenderá en este módulo?

Título del módulo: Configuración básica de switches y terminales

Objetivos del módulo: Implemente la configuración inicial, incluidas contraseñas, dirección IP y parámetros de gateway predeterminados en un switch de red y terminales.

Título del tema	Objetivo del tema
Acceso a Cisco IOS	Explique la forma en que se accede a un dispositivo Cisco IOS para propósitos de configuración.
Navegación IOS	Explique la forma en que se explora Cisco IOS para configurar los dispositivos de red.
La estructura de comandos	Describe la estructura de comandos del software Cisco IOS.
Configuración básica de dispositivos	Configure un dispositivo Cisco IOS usando CLI.
Guardar las configuraciones	Utilice los comandos de IOS para guardar la configuración en ejecución.
Puertos y direcciones	Explique la forma en que se comunican los dispositivos a través de los medios de red.
Configurar direccionamiento IP	Configure un dispositivo host con una dirección IP.
Verificar la conectividad	Verifique la conectividad entre dos terminales.

Configuración básica de switches y terminales / Acceso a Cisco IOS

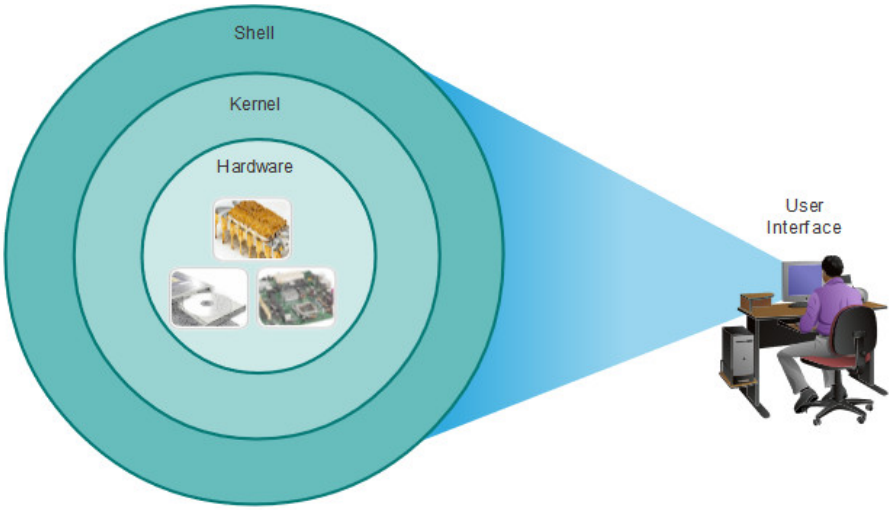
Acceso a Cisco IOS

2.1.1

Sistemas operativos

Todos los dispositivos finales y dispositivos de red requieren un sistema operativo (OS). Como se muestra en la figura, la parte del Sistema Operativo que interactúa directamente con el hardware de la PC se conoce como kernel. La parte que interactúa con las aplicaciones y el usuario se conoce como shell. El usuario puede interactuar con el shell mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica del usuario (GUI).

Hay tres círculos concéntricos que parecen irradiar desde el monitor de una interfaz de usuario etiquetada por computadora. Muestran la relación entre las diferentes partes de un sistema operativo. El círculo interno etiquetado hardware muestra ejemplos de hardware de computadora, el círculo medio se etiqueta kernel y el círculo externo se etiqueta shell. El texto en la parte inferior dice: Shell - La interfaz de usuario que permite a los usuarios solicitar tareas específicas de la computadora. Estas solicitudes se pueden realizar a través de las interfaces CLI o GUI; Kernel - Se comunica entre el hardware y el software de un equipo y administra cómo se utilizan los recursos de hardware para cumplir los requisitos de software; Hardware - La parte física de un equipo, incluida la electrónica subyacente.



- **Shell**: la interfaz de usuario que permite a los usuarios solicitar tareas específicas del equipo. Estas solicitudes se pueden realizar a través de las interfaces CLI o GUI.
- **Kernel** - Establece la comunicación entre el hardware y el software de una computadora y administra el uso de los recursos de hardware para cumplir los requisitos del software
- **Hardware** - La parte física de una computadora, incluida la electrónica subyacente.

Cuando se usa una CLI, el usuario interactúa directamente con el sistema en un entorno basado en texto ingresando comandos en el teclado en un símbolo del sistema, como se muestra en el ejemplo. El sistema ejecuta el comando y, por lo general, proporciona una

respuesta en forma de texto. La CLI necesita muy poca sobrecarga para operar. Sin embargo, exige que el usuario tenga conocimientos de la estructura subyacente que controla el sistema.

```
analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive
[analyst@secOps ~]$
```

2.1.2

GUI

Una GUI como Windows, macOS, Linux KDE, Apple iOS o Android le permite al usuario interactuar con el sistema utilizando un entorno de iconos gráficos, menús y ventanas. The GUI example in the figure is more user-friendly and requires less knowledge of the underlying command structure that controls the system. Por este motivo, muchas personas prefieren los entornos GUI.

Sin embargo, las GUI no siempre pueden proporcionar todas las funcionalidades que hay disponibles en la CLI. Las GUI también pueden fallar, colapsar o simplemente no operar como se les indica. Por eso, se suele acceder a los dispositivos de red mediante una CLI. La CLI consume menos recursos y es muy estable en comparación con una GUI.

La familia de sistemas operativos de red utilizados en muchos dispositivos Cisco se llama Cisco Internetwork Operating System (IOS). Cisco IOS se utiliza en muchos routers y switches de Cisco, independientemente del tipo o tamaño del dispositivo. Cada router o tipo

de switch de dispositivo utiliza una versión diferente de Cisco IOS. Otros sistemas operativos de Cisco incluyen IOS XE, IOS XR y NX-OS.

Nota: El sistema operativo de los routers domésticos generalmente se denomina *firmware*. El método más frecuente para configurar un router doméstico consiste en utilizar un explorador web para acceder a una GUI.

2.1.3

Propósito del OS

Los sistemas operativos de red son similares al sistema operativo de una PC. Mediante una GUI, un sistema operativo de PC permite que el usuario realice lo siguiente:

- Utilice un mouse para hacer selecciones y ejecutar programas.
- Introduzca texto y comandos de texto.
- Vea resultados en un monitor.

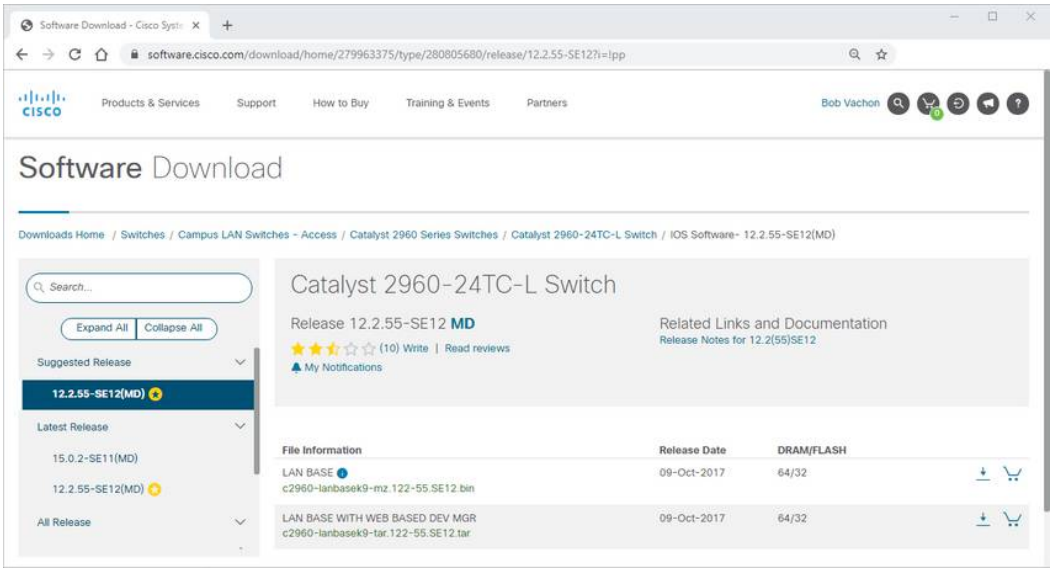
Un sistema operativo basado en CLI como el Cisco IOS en un switch o router, permite que un técnico de red realice lo siguiente:

- Utilice un teclado para ejecutar programas de red basados en la CLI.
- Utilice un teclado para introducir texto y comandos basados en texto.
- Vea resultados en un monitor.

Los dispositivos de red de Cisco ejecutan versiones especiales de Cisco IOS. La versión de IOS depende del tipo de dispositivo que se utilice y de las características necesarias. Si bien todos los dispositivos traen un IOS y un conjunto de características predeterminados, es posible actualizar el conjunto de características o la versión de IOS para obtener capacidades adicionales.

En la figura se muestra una lista de las versiones del software IOS para un switch Cisco Catalyst 2960.

Ejemplo de descarga de software de Cisco



2.1.4

Métodos de acceso

Un switch reenviará el tráfico de forma predeterminada y no necesita configurarse explícitamente para funcionar. Por ejemplo, dos hosts configurados conectados al mismo switch nuevo podrían comunicarse.

Independientemente del comportamiento predeterminado de un switch nuevo, todos los switches deben estar configurados y protegidos.

Method	Description
Console	This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only. The advantage of using a console port is that the device is accessible even if no networking services are configured, such as performing the initial configuration. A computer running terminal emulation software and a special console cable to connect to the device are required for a console connection.
Secure Shell (SSH)	SSH is an in-band and recommended method for remotely establishing a secure CLI connection, through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device, including an active interface configured with an address. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.
Telnet	Telnet is an insecure, in-band method of remotely establishing a CLI session, through a virtual interface, over a network. Unlike SSH, Telnet does not provide a secure, encrypted connection and should only be used in a lab environment. User authentication, passwords, and commands are sent over the network in plaintext. The best practice is to use SSH instead of Telnet. Cisco IOS includes both a Telnet server and Telnet client.

Método	Descripción
Consola	Este es un puerto de administración físico que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de mantenimiento del dispositivo. La ventaja de usar un puerto de consola es que el dispositivo es accesible incluso si no hay servicios de red configurados, como realizar la configuración inicial. Para una conexión de consola se requiere un equipo con software de emulación de terminal y un cable de consola especial para conectarse al dispositivo.
Secure Shell (SSH)	SSH es un método para establecer de manera remota una conexión CLI segura a través de una interfaz virtual por medio de una red. A diferencia de las conexiones de consola, las conexiones SSH requieren servicios de red activos en el dispositivo, incluida una interfaz activa configurada con una dirección. La mayoría de las versiones de Cisco IOS incluyen un servidor SSH y un cliente SSH que pueden utilizarse para establecer sesiones SSH con otros dispositivos.
Telnet	Telnet es un método inseguro para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. A diferencia de SSH, Telnet no proporciona una conexión segura y encriptada y solo debe usarse en un entorno de laboratorio. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto simple. La mejor práctica es usar SSH en lugar de Telnet. Cisco IOS incluye un servidor Telnet y un cliente Telnet.

Nota: Algunos dispositivos, como los routers, también pueden admitir un puerto heredado auxiliar utilizado para establecer una sesión CLI de forma remota a través de una conexión telefónica utilizando un módem. Al igual que la conexión de consola, el puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red.

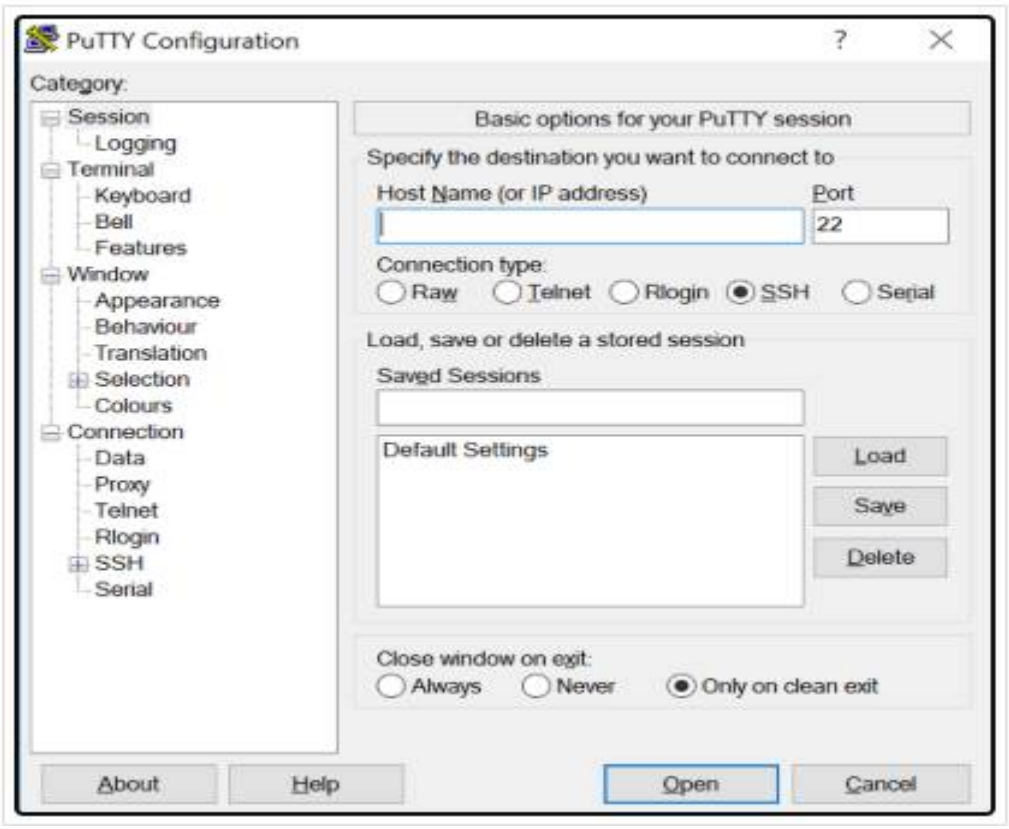
2.1.5

Programas de emulación de terminal

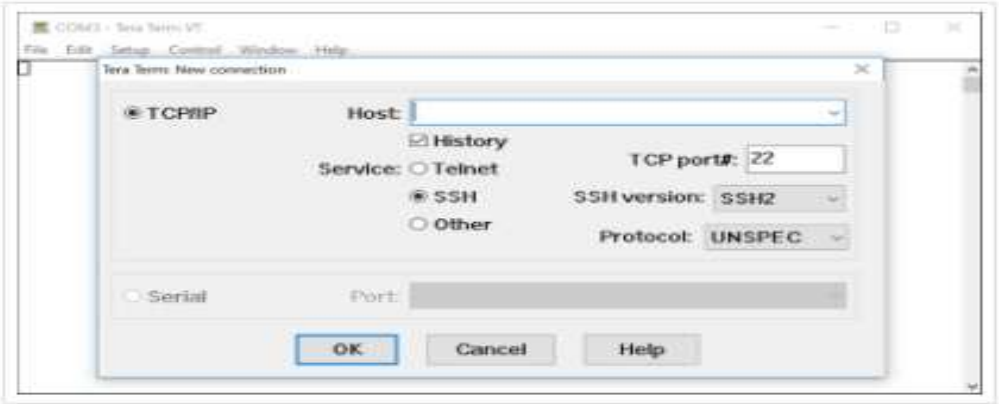
Existen varios programas de emulación de terminal que puede usar para conectarse a un dispositivo de red, ya sea mediante una conexión en serie a través de un puerto de consola o mediante una conexión SSH / Telnet. Estos programas le permiten aumentar la productividad mediante ajustes del tamaño de la ventana, modificaciones de los tamaños de fuente y cambios en los esquemas de colores.

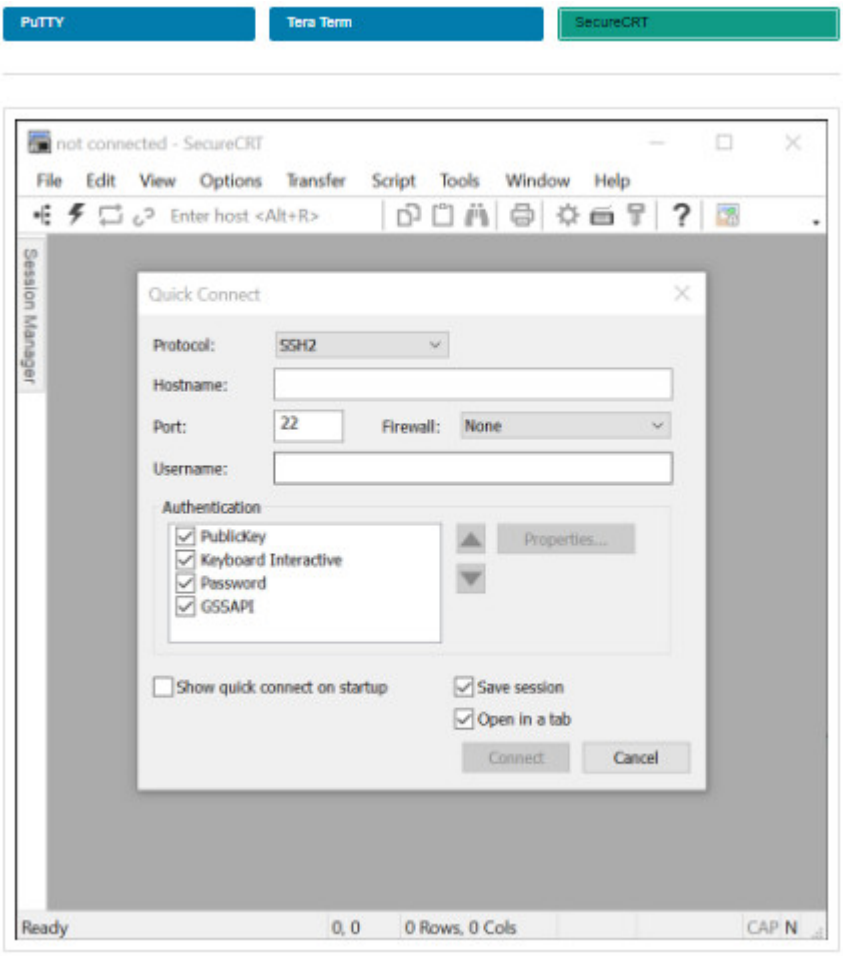
Haga clic en el nombre de cada programa para ver una captura de pantalla de la interfaz.

PuTTY | Tera Term | SecureCRT



PuTTY | Tera Term | SecureCRT





2.1.6

Verifique su comprensión - Acceso Cisco IOS

Verifique su comprensión de Cisco IOS Access eligiendo la MEJOR respuesta a las siguientes preguntas.

Preguntas y respuestas en español e inglés.

1. ¿Qué método de acceso sería más apropiado si estaría en la sala de equipos con un nuevo interruptor que necesita ser configurado?

¡Lo tienes!

- (•) Consola
- ( ) Telnet/SSH
- ( ) Aux

2. ¿Qué método de acceso sería más apropiado si su gerente le diera un cable especial y le dijera qué usar para configurar el interruptor?

¡Lo tienes!

- (•) Consola
- ( ) Telnet/SSH
- ( ) Aux

3. ¿Qué método de acceso sería el acceso en banda más apropiado al IOS a través de una conexión de red?

¡Lo tienes!

- ( ) Consola
- (•) Telnet/SSH
- ( ) Aux

4. ¿Qué método de acceso sería el más apropiado si llama a su gerente para decirle que no puede acceder a su enrutador en otra ciudad a través de Internet y él proporciona la información para acceder al enrutador a través de una conexión telefónica?

¡Lo tienes!

- ( ) Consola
- ( ) Telnet/SSH
- (•) Aux

Correct

You have successfully identified the correct answers.

1. Because a new switch would not have any initial configurations, it could only be configured through the console port.
2. Connecting a computer to a Cisco device through the console port requires a special console cable.
3. Both Telnet and SSH are in-band access methods that require an active network connection to the device.
4. The AUX port on a Cisco device provided out-of-band connections over a telephone line.

You got 4 out of 4 questions correct.

1. Which access method would be most appropriate if you were in the equipment room with a new switch that needs to be configured?

You got it!

- (●) Console
- ( ) Telnet/SSH
- ( ) Aux

2. Which access method would be most appropriate if your manager gave you a special cable and told you to use it to configure the switch?

You got it!

- (●) Console
- ( ) Telnet/SSH
- ( ) Aux

3. Which access method would be the most appropriate in-band access to the IOS over a network connection?

You got it!

- ( ) Console
- (●) Telnet/SSH
- ( ) Aux

4. Which access method would be the most appropriate if you call your manager to tell him you cannot access your router in another city over the internet and he provides you with the information to access the router through a telephone connection?

You got it!

- ( ) Console
- ( ) Telnet/SSH
- (●) Aux

Configuración básica de switches y terminales / Navegación IOS

Navegación IOS

2.2.1

Modos de comando principal

En el tema anterior, aprendió que todos los dispositivos de red configurados un sistema operativo y que pueden configurar mediante la CLI o una GUI. El uso de la CLI puede proporcionar al administrador de red un control y flexibilidad más precisos que el uso de la GUI. En este tema, describa el uso de CLI para navegar por Cisco IOS.

Como característica de seguridad, el software IOS de Cisco divide el acceso de administración en los siguientes dos modos de comando:

- **Modo de ejecución de usuario** - Este tiene capacidades limitadas, pero resulta útil en el caso de algunas operaciones básicas. Permite solo una cantidad limitada de comandos de monitoreo básico, pero no permite la ejecución de ningún comando que pueda cambiar la configuración del dispositivo. El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo>.
- **Modo de ejecución privilegiado** - Para ejecutar comandos de configuración, un administrador de redes debe acceder al modo de ejecución privilegiado. Solo puede ingresar el modo de configuración global y los modos de configuración más altos por medio del modo EXEC con privilegios. El modo EXEC con privilegios se puede reconocer por la petición de entrada que termina con el # símbolo.

La tabla resume los dos modos y muestra las solicitudes CLI predeterminadas de un switch y router Cisco.

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as "view-only" mode.	`Switch>` `Router>`
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC del usuario	El modo permite el acceso a solo un número limitado de comandos básicos de monitoreo. A menudo se le conoce como un modo de "visualización solamente".	`Switch>` `Enrutador>`
Modo EXEC privilegiado	El modo permite el acceso a todos los comandos y funciones. El usuario puede usar cualquier comando de monitoreo y ejecutar la configuración y comandos de administración.	`Switch #` `Router #`

2.2.2

Modo de configuración y modos de subconfiguración

Para configurar el dispositivo, el usuario debe ingresar el modo de configuración global, que normalmente se denomina modo de configuración. global.

Desde el modo de configuración global, se realizan cambios en la configuración de la CLI que afectan la operación del dispositivo en su totalidad. El modo de configuración global se identifica mediante un mensaje que termina (config) # después del nombre del dispositivo, como **Switch (config) #**.

Antes de acceder a otros modos de configuración específicos, acceda al modo de configuración global. Desde el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. Dos modos de subconfiguración comunes incluyen:

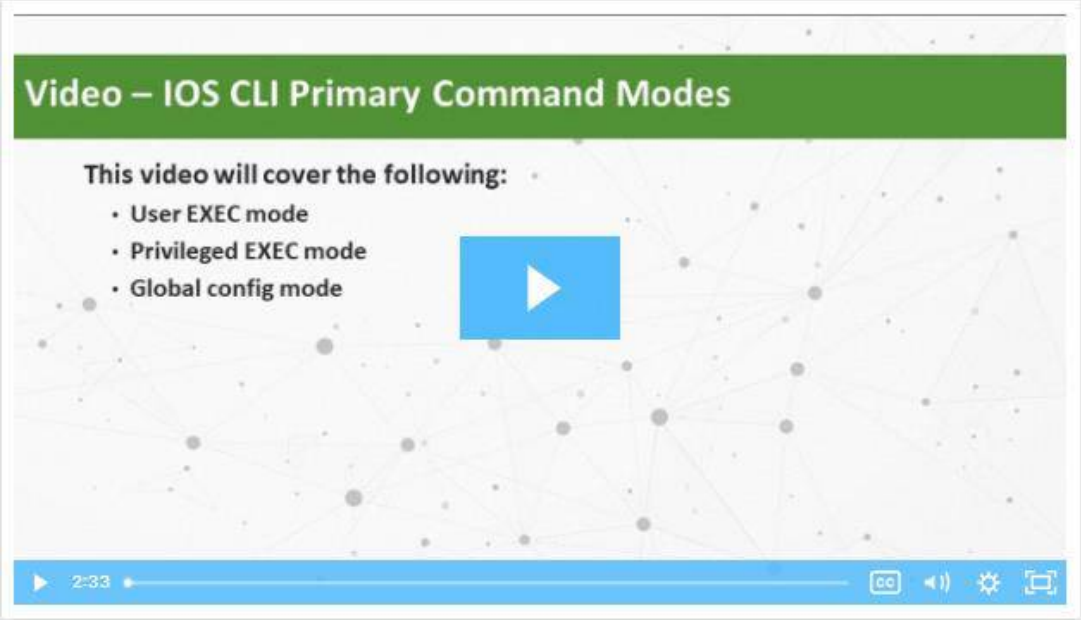
- **Modo de configuración de líneas -** Se utiliza para configurar la consola, SSH, Telnet o el acceso auxiliar.
- **Modo de configuración de interfaz:** se utiliza para configurar un puerto de conmutación o una interfaz de red de enrutador.

Cuando se utiliza la CLI, el modo se identifica mediante la línea de comandos que es exclusiva de ese modo. De manera predeterminada, cada petición de entrada comienza con el nombre del dispositivo. Después del nombre, el resto de la petición de entrada indica el modo. Por ejemplo, el indicador predeterminado para el modo de configuración de línea es **Switch (config-line) #** y el indicador predeterminado para el modo de configuración de la interfaz es **Switch (config-if) #**.

2.2.3

Video - IOS CLI modos de comando principal

Haga clic en el botón Reproducir en la figura para ver una demostración en el video de la navegación entre los modos de IOS.



2.2.4

Navegación entre los modos de IOS

Se utilizan varios comandos para pasar dentro o fuera de los comandos de solicitud de entrada. Para pasar del modo EXEC del usuario al modo EXEC con privilegios, ingrese

el comando de **habilitación**. Use el **deshabilitar** comando del modo EXEC privilegiado para volver al modo EXEC del usuario.

Nota: El modo EXEC con privilegios se suele llamar modo habilitar.

Para entrar y salir del modo de configuración global, use el comando **configure terminal** del modo EXEC privilegiado. Para volver al modo EXEC privilegiado, ingrese el comando del modo **salida** de configuración global.

Existen diversos tipos de modos de subconfiguración. Por ejemplo, para ingresar al modo de subconfiguración de línea, use la **línea de** comando seguida del tipo de línea de administración y el número al que desea acceder. Use el comando **salir** para salir de un modo de subconfiguración y volver al modo de configuración global.

```
Switch(config)# line console 0
Switch(config-line)# exit
Switch(config)#
```

Para pasar de cualquier modo de subconfiguración del modo de configuración global al modo un paso por encima de él en la jerarquía de modos, ingrese el comando de **salida**.

Para pasar de cualquier modo de subconfiguración al modo EXEC privilegiado, ingrese el comando **final** o ingrese la combinación de teclas. **Ctrl + Z**.

```
Switch(config-line)# end
Switch#
```

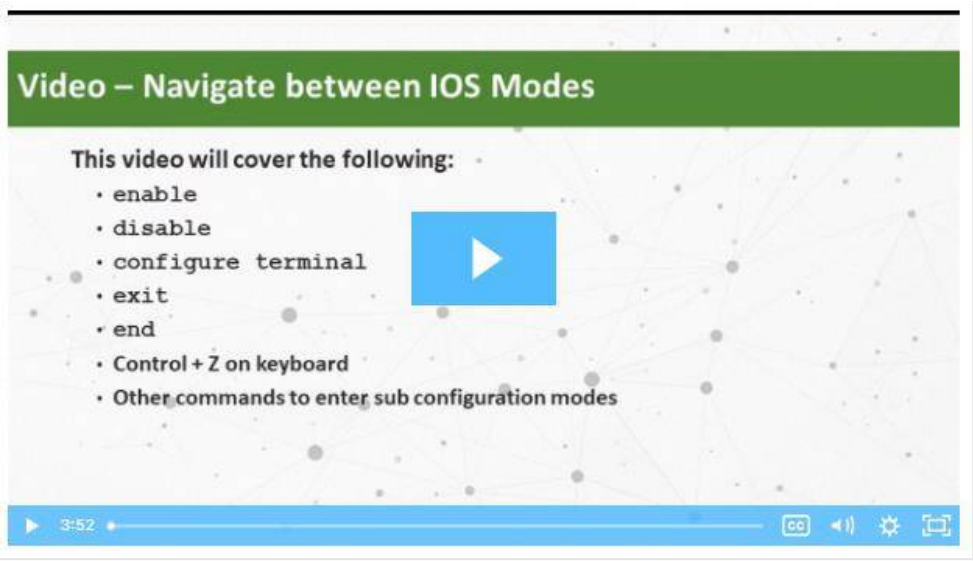
Puede trasladarse directamente desde un modo de subconfiguración a otro. Vea cómo después de seleccionar una interfaz, el comando de petición cambia de **(config-line) #** a **(config-if) #**.

```
Switch(config-line)# interface FastEthernet 0/1
Switch(config-if)#
```

2.2.5

Video - Navegación entre los modos de IOS

Haga clic en el botón Reproducir en la figura para ver una demostración en video de la navegación entre los distintos modos de la CLI de IOS.



2.2.6

Una nota sobre las actividades del verificador de sintaxis

Cuando esté aprendiendo a modificar las configuraciones de los dispositivos, es posible que desee comenzar en un entorno seguro que no sea de producción antes de probarlo en equipos reales. NetaCAD le ofrece diferentes herramientas de simulación para ayudar a desarrollar sus habilidades de configuración y solución de problemas. Debido a que se trata de herramientas de simulación, normalmente no tienen toda la funcionalidad del equipo real. Una de esas herramientas es el Comprobador de sintaxis. En cada Comprobador de sintaxis, vea el conjunto de instrucciones para introducir un conjunto específico de comandos. No puede progresar en el Comprobador de sintaxis a menos que se ingrese el comando exacto y completo como se especifica. Las herramientas de simulación más avanzadas, como Packet Tracer, le permiten introducir comandos abreviados, como lo haría con equipos reales.

2.2.7

Comprobador de sintaxis - Navegar entre los modos IOS

Utilice la actividad Comprobador de sintaxis para navegar entre las líneas de comando del IOS en un interruptor.

Enter privileged EXEC mode using the **enable** command.

Switch>enable

Return to user EXEC mode using the **disable** command.

Switch#disable

Re-enter privileged EXEC mode.

Switch>enable

Enter global configuration mode using the **configure terminal** command.

Switch#configure terminal

Exit global configuration mode and return to privileged EXEC mode using the **exit** command.

Switch(config)#exit

Re-enter global configuration mode.

Switch#configure terminal

Enter line subconfiguration mode for the console port using the **line console 0** command.

Switch(config)#line console 0

Return to global configuration mode using the **exit** command.

Switch(config-line)#exit

Enter VTY line subconfiguration mode using the **line vty 0 15** command.

Switch(config)#line vty 0 15

Return to global configuration mode.

Switch(config-line)#exit

Enter the VLAN 1 interface subconfiguration mode using the **interface vlan 1** command.

Switch(config)#interface vlan 1

From interface configuration mode, switch to line console subconfiguration mode using the **line console 0** global configuration command.

Switch(config-if)#line console 0

Return to privileged EXEC mode using the **end** command.

Switch(config-line)#end

You successfully navigated between the various IOS command line modes.

2.2.8

Compruebe su comprensión - Navegación del IOS

Verifique su comprensión de la navegación IOS eligiendo la MEJOR respuesta a las siguientes preguntas.

1. ¿Qué modo IOS permite el acceso a todos los comandos y funciones?

¡Lo tienes!

- ○ Modo de configuración global
- ○ Modo de subconfiguración de la interfaz.
- ○ modo de subconfiguración de la línea de consola.
- ◉ Modo EXEC privilegiado
- ○ Modo EXEC de usuario

2. ¿En qué modo IOS se encuentra si se muestra el Switch(config)# indicador?

¡Lo tienes!

- ◉ Modo de configuración global
- ○ Modo de subconfiguración de la interfaz.
- ○ modo de subconfiguración de la línea de consola.
- ○ Modo EXEC privilegiado
- ○ Modo EXEC de usuario

3. ¿En qué modo IOS se encuentra si se muestra el simbolo del switch>?

¡Lo tienes!

- ○ Modo de configuración global
- ○ Modo de subconfiguración de la interfaz.
- ○ modo de subconfiguración de la línea de consola.
- ○ Modo EXEC privilegiado
- ◉ Modo EXEC de usuario

4. ¿Qué dos comandos le devolverían al símbolo EXEC privilegiado independientemente del modo de configuración en el que se encuentre? (Escoja dos.)

¡Lo tienes!

- ☑ **CTRL+Z**
- ☐ **deshabilitar**
- ☐ **enable**
- ☑ **end**
- ☐ **exit**

Correct

You have successfully identified the correct answers.

1. The privileged EXEC mode allows access to all commands. Higher levlel commands like global configuration mode and subconfiguration modes can only be reached from the privileged EXEC mode.
2. Global configuration mode is identified by the **(config)#** prompt.
3. The **>** prompt after the device name identifies user EXEC mode.
4. To return from any prompt, all the way down to privileged EXEC mode, type the **end** command or by pressing the **CTRL+Z** keys simultaneously on the keyboard.

You got 4 out of 4 questions correct.

1. Which IOS mode allows access to all commands and features?

You got it!

- Global configuration mode
- Interface subconfiguration mode
- Line console subconfiguration mode
- (•) Privileged EXEC mode
- User EXEC mode

2. Which IOS mode are you in if the Switch(config)# prompt is displayed?

You got it!

- (•) Global configuration mode
- Interface subconfiguration mode
- Line console subconfiguration mode
- Privileged EXEC mode
- User EXEC mode

3. Which IOS mode are you in if the Switch> prompt is displayed?

You got it!

- Global configuration mode
- Interface subconfiguration mode
- Line console subconfiguration mode
- Privileged EXEC mode
- (•) User EXEC mode

4. Which two commands would return you to the privileged EXEC prompt regardless of the configuration mode you are in? (Choose two.)

You got it!

- [x] **CTRL+Z**
- [ ] **disable**
- [ ] **enable**
- [x] **end**
- [ ] **exit**

La estructura de los comandos

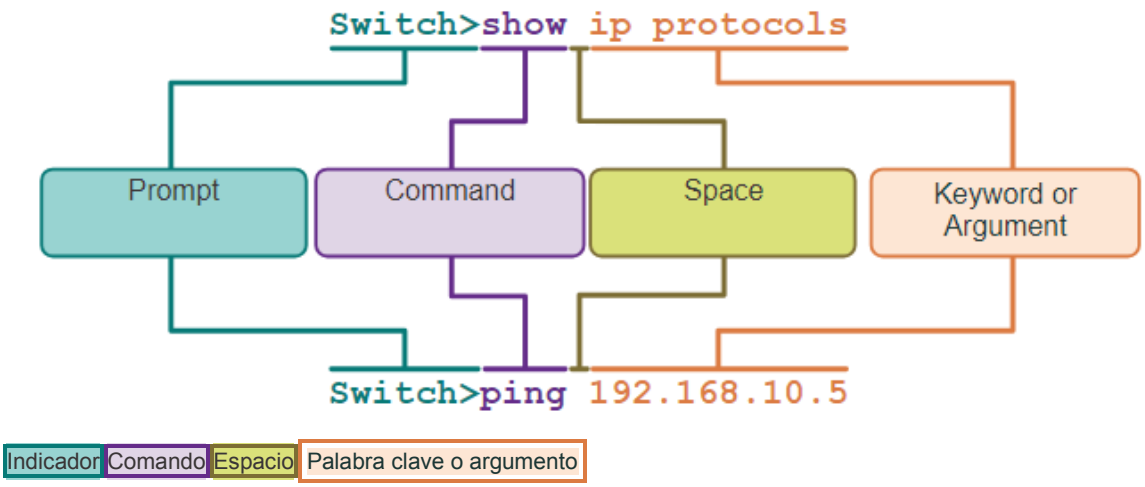
2.3.1

Estructura básica de comandos de IOS

Este tema cubre la estructura básica de los comandos para Cisco IOS. Un administrador de red debe conocer la estructura de comandos básica del IOS para poder usar la CLI para la configuración del dispositivo.

Los dispositivos Cisco IOS admiten muchos comandos. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando, que se muestra en la figura, es el comando seguido de cualquier palabra clave y argumento apropiados.

El diagrama muestra la sintaxis general de un comando switch (que es prompt, command, space y keyword o argument) y proporciona dos ejemplos. En el primer ejemplo, el símbolo del sistema es Switch>, el comando es show, sigue un espacio y la palabra clave es ip protocols. En el segundo ejemplo, el símbolo del sistema es Switch>, el comando es ping, sigue un espacio y el argumento es 192.168.10.5.



- **Keyword** - This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
- **Argumento** - This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5**).

Después de ingresar cada comando completo, incluidas las palabras clave y los argumentos, presione la **Enter** tecla para enviar el comando al intérprete de comandos.

2.3.2

Comprobación de la sintaxis del comando de IOS

Un comando podría requerir uno o más argumentos. Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulte la sintaxis de comandos. La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.

Como se identifica en la tabla, el texto en negrita indica los comandos y las palabras clave que se ingresan como se muestra. El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.

Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que ingresa literalmente como se muestra.
cursiva	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento opcional (palabra clave o argumento).
{x}	Las llaves indican un elemento obligatorio (palabra clave o argumento).
[x {y | z }]	Las llaves y las líneas verticales entre corchetes indican que se requiere dentro de un elemento opcional. Los espacios se utilizan para delinear claramente partes del comando.

Por ejemplo, la sintaxis para utilizar el comando **description** es **description** *string*. El argumento es un valor *string* proporcionado por el usuario. El comando **description**, se usa típicamente para identificar el propósito de una interfaz. Por ejemplo, al ingresar el comando, **description Connects to the main headquarter office switch**, se describe dónde se encuentra el otro dispositivo al final de la conexión.

Los siguientes ejemplos muestran algunas convenciones utilizadas para registrar y usar comandos de IOS:

- **ping** *ip-address* – El commando es **ping** y el argumento definido por el usuario es la *ip-address* del dispositivo destino. Por ejemplo, **ping 10.10.5**.

- **traceroute** *ip-address* – El commando es **traceroute** y el argumento definido por el usuario es la *ip-address* del dispositivo destino. Por ejemplo, **traceroute 192.168.254.254**.

Si un comando es complejo con múltiples argumentos, puede verlo representado así:

```
Switch (config-if) # switchport port-security envejecimiento { estática | tiempo  tiempo | tipo { absoluto
| inactividad }}
```

El comando normalmente se seguirá una descripción detallada del comando y cada argumento.

La referencia de comando de Cisco IOS es la última fuente de información para un comando de IOS en particular.

2.3.3

Funciones de ayuda de IOS

El IOS tiene dos formas de ayuda disponibles: la ayuda contextual y el verificador de sintaxis de comandos.

La ayuda contextual le permite encontrar rápidamente respuestas a estas preguntas:

- ¿Qué comandos están disponibles en cada modo de comando?
- ¿Qué comandos comienzan con caracteres específicos o grupo de caracteres?
- ¿Qué argumentos y palabras clave están disponibles para comandos particulares?

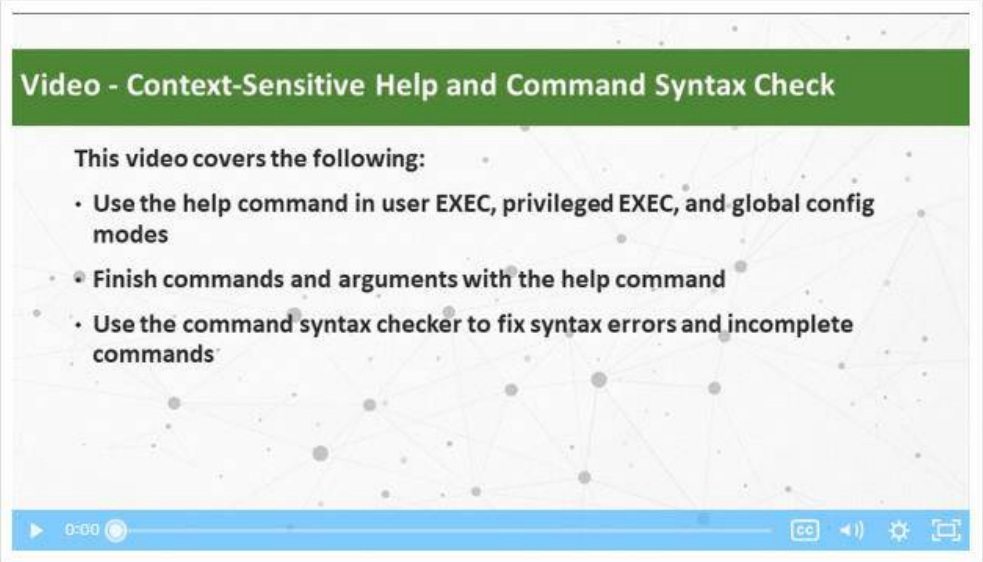
Para acceder a la ayuda contextual, simplemente ingrese un signo de interrogación, en la CLI: **?**

La verificación de la sintaxis del comando comprueba que el usuario haya introducido un comando válido. Cuando se introduce un comando, el intérprete de la línea de comandos analiza al comando de izquierda a derecha. Si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente. Sin embargo, si el intérprete no puede comprender el comando que se ingresa, mostrará un comentario que describe el error del comando.

2.3.4

Video - Ayuda sensible al contexto y verificación de sintaxis de comandos

Haga clic en el botón Reproducir en la figura para ver una demostración en video de la ayuda contextual y la verificación de la sintaxis del comando.



2.3.5

Teclas de acceso rápido y métodos abreviados

La CLI de IOS proporciona teclas de acceso rápido y accesos directos que facilitan la configuración, el monitoreo y la solución de problemas.

Los comandos y las palabras clave pueden acortarse a la cantidad mínima de caracteres que identifica a una selección única. Por ejemplo, el **configure** comando se puede acortar a **conf** porque **configure** es el único comando que comienza con **conf**. Una versión aún más corta **con**, no funcionará porque más de un comando comienza con **con**. Las palabras clave también pueden acortarse.

La tabla muestra las pulsaciones de teclas para mejorar la edición de la línea de comandos.

Pulsación de teclas	Descripción
Tabulación	Completa una entrada de nombre de comando parcial.
Retroceso	Borra el caracter a la izquierda del cursor.
Ctrl+D	Borra el caracter donde está el cursor.
Ctrl+K	Borra todos los caracteres desde el cursor hasta el final de la línea de comandos.
Esc D	Borra todos los caracteres desde el cursor hasta el final de la palabra.
Ctrl+U o **Ctrl+X**	Borra todos los caracteres desde el cursor hasta el comienzo de la línea de comando
Ctrl+W	Borra la palabra a la izquierda del cursor.
Ctrl+A	Desplaza el cursor hacia el principio de la línea.
Flecha izquierda o **Ctrl+B**	Desplaza el cursor un carácter hacia la izquierda.
Esc B	Desplaza el cursor una palabra hacia la izquierda.
Esc F	Desplaza el cursor una palabra hacia la derecha.
Flecha derecha o **Ctrl+F**	Desplaza el cursor un carácter hacia la derecha.
Ctrl+E	Desplaza el cursor hasta el final de la línea de comandos.
Flecha arriba o **Ctrl+P**	Recupera los comandos en el búfer de historial, comenzando con la mayoría comandos recientes
Ctrl+R o **Ctrl+I** o **Ctrl+L**	Vuelve a mostrar el indicador del sistema y la línea de comando después de que se muestra un mensaje de consola recibido.

Nota: Aunque la **Delete** clave normalmente elimina el carácter a la derecha de la solicitud, la estructura del comando IOS no reconoce la tecla Eliminar.

Cuando una salida de comando produce más texto del que se puede mostrar en una ventana de terminal, el IOS mostrará una **"--More--"** solicitud. En la tabla siguiente se describen las pulsaciones de teclas que se pueden utilizar cuando se muestra esta solicitud.

Pulsación de teclas	Descripción
Tecla**Enter**	Muestra la siguiente línea.
Barra espaciadora	Muestra la siguiente pantalla.
Cualquier otra tecla	Termina la cadena que se muestra y vuelve al modo EXEC con privilegios.

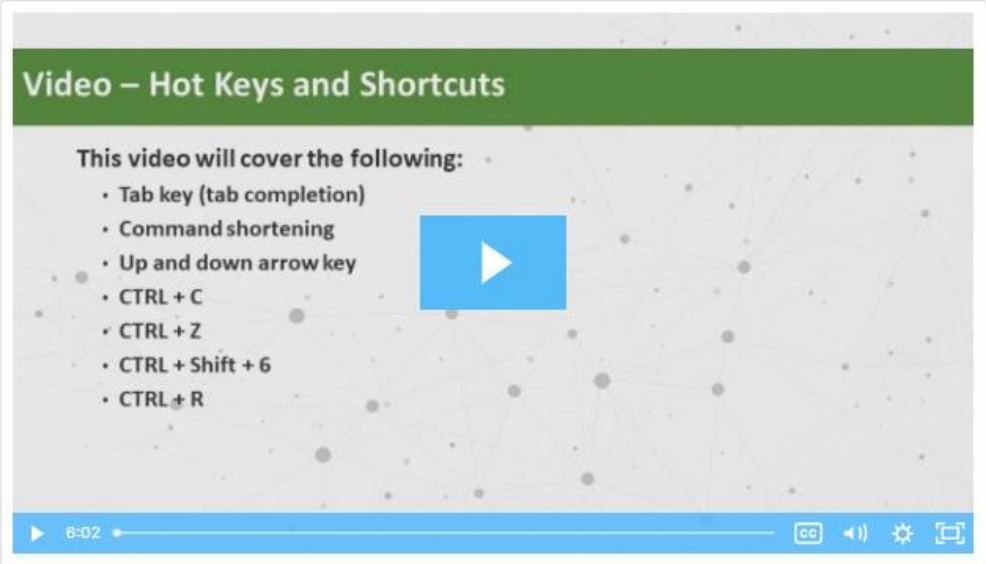
En esta tabla se enumeran los comandos utilizados para salir de una operación.

Pulsación de teclas	Descripción
Ctrl-C	Cuando está en cualquier modo de configuración, finaliza el modo de configuración y regresa al modo EXEC privilegiado. Cuando está en modo de configuración, aborta de nuevo al comando como indicador de comandos.
Ctrl-Z	Cuando está en cualquier modo de configuración, finaliza el modo de configuración y regresa al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de interrupción multipropósito utilizada para anular búsquedas DNS, traceroutes, pings, etc.

2.3.6

Video - Teclas de acceso rápido y métodos abreviados

Haga clic en el botón Reproducir en la figura para ver una demostración en vídeo de las distintas teclas de acceso rápido y métodos abreviados.



2.3.7

Packet Tracer - Navega por el IOS

En esta actividad, practicará las habilidades necesarias para navegar dentro de Cisco IOS, incluidos distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando clock.

Navega por el IOS

Navega por el IOS

2.3.8

Laboratorio: Navegue por el IOS mediante Tera Term para la conectividad de la consola

En este laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Acceso a un switch Cisco a través del puerto serial de consola
- Parte 2: Muestra y configuración de parámetros básicos de los dispositivos
- Parte 3: Acceso a un router Cisco mediante un cable de consola mini-USB (opcional)

Navegue por el IOS mediante Tera Term para la conectividad de la consola

Configuración básica de interruptores y terminales / Configuración básica de dispositivos

Configuración básica de dispositivos

2.4.1

Nombres de los dispositivos

Ha aprendido mucho acerca del IOS de Cisco, la navegación del IOS y la estructura de comandos. ¡Ahora, ya está listo para configurar dispositivos! El primer comando de configuración en cualquier dispositivo debe ser dado un nombre de dispositivo único o nombre de host. De forma predeterminada, a todos los dispositivos se les asigna un nombre predeterminado de fábrica. Por ejemplo, un switch Cisco IOS es «Switch. ««

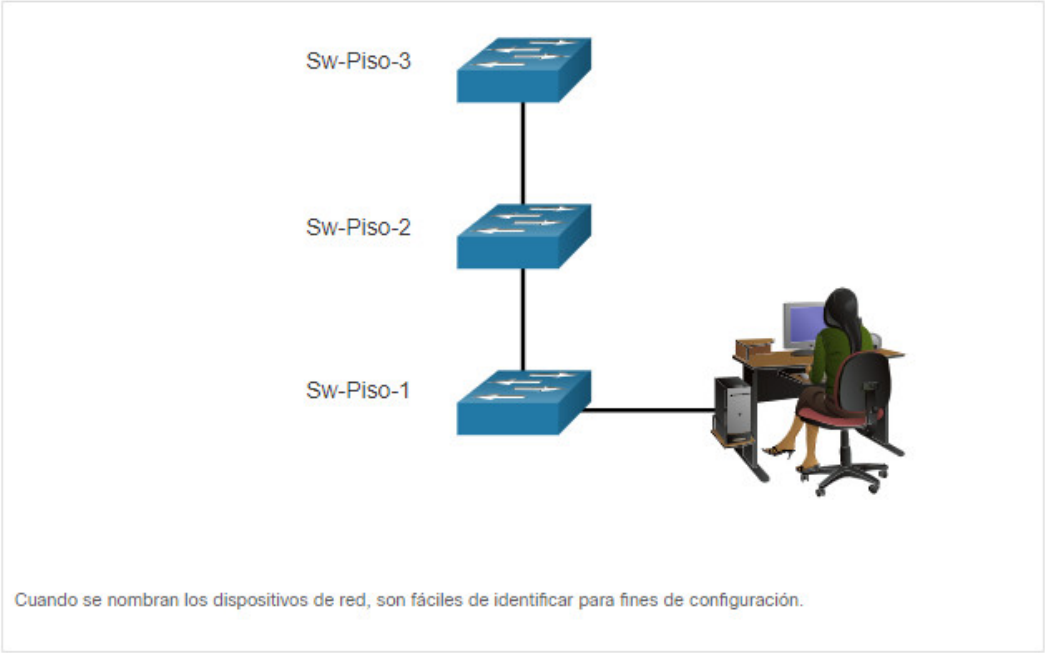
El problema es que, si todos los interruptores de una red se quedaran con sus nombres predeterminados, sería difícil identificar un dispositivo específico. Por ejemplo, ¿cómo sabrías que estás conectado al dispositivo correcto al acceder remotamente a través de SSH? El nombre de host proporciona la confirmación de que está conectado al dispositivo correcto.

El nombre predeterminado debe cambiarse a algo más descriptivo. Al elegir nombres atinadamente, resulta más fácil recordar, identificar e identificar los dispositivos de red. Estas son algunas pautas de nomenclatura importantes para los anfitriones:

- Comenzar con una letra.
- No contener espacios.
- Finalizar con una letra o dígito.
- Utilizar específicamente letras, dígitos y guiones.
- Tener menos de 64 caracteres de longitud.

Una organización debe elegir una convención de nomenclatura que haga que sea fácil e intuitivo identificar un dispositivo específico. Los nombres de host utilizados en el IOS del dispositivo conservan el uso de caracteres en mayúscula y minúscula. Por ejemplo, la figura muestra que tres interruptores, que abarcan tres pisos diferentes, están interconectados en una red. La convención de nomenclatura que se puede incorporar la ubicación y el propósito de cada dispositivo. La documentación de red debe explicar cómo se seleccionará estos nombres para que pueda seguir el mismo criterio en la denominación de los dispositivos adicionales.

El diagrama muestra tres interruptores interconectados que abarcan tres pisos. El switch superior se denomina Sw-Floor-3, el switch central se denomina Sw-Floor-2, y el switch inferior se llama Sw-Floor-1. Un usuario sentado en un equipo host está conectado al switch SW-Floor-1. El texto en la parte inferior lee: cuando se nombran los dispositivos de red, son fáciles de identificar para fines de configuración.



Cuando se ha identificado la convención de nomenclatura, el siguiente paso es usar la CLI para aplicar los nombres a los dispositivos. Como se muestra en el ejemplo, desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando **configure terminal**. Observe el cambio en el comando de petición de entrada.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Desde el modo de configuración global, ingrese el comando **hostname** seguido del nombre del interruptor y presione **Intro**. Observe el cambio en el comando de petición de entrada.

Nota: Para devolver el interruptor al indicador predeterminado, use el comando de configuración global. **sin nombre de host.**

Siempre asegúrese de que la documentación esté actualizada cada vez que se agregue o modifique un dispositivo. Identifique los dispositivos en la documentación por su ubicación, propósito y dirección.

2.4.2

Pautas de la contraseña

El uso de contraseñas debiles o fácilmente adivinadas sigue siendo la mayor preocupación de seguridad de las organizaciones. Los dispositivos de red, incluso los enrutadores inalámbricos hogareños, siempre deben tener contraseñas configuradas para limitar el acceso administrativo.

Cisco IOS puede configurar para utilizar contraseñas en modo jerárquico y permitir diferentes privilegios de acceso al dispositivo de red.

Todos los dispositivos de red deben limitar el acceso administrativo asegurando EXEC privilegiado, EXEC de usuario y acceso Telnet remoto con contraseñas. Además, todas las contraseñas deben estar encriptadas y deben proporcionar notificaciones legales.

Al elegir contraseñas, use contraseñas seguras que no sean fáciles de adivinar. Hay algunos puntos clave a considerar al elegir las contraseñas:

- Utilice contraseñas que tengan más de ocho caracteres de longitud.
- Utilice una combinación de letras mayúsculas y minúsculas, números, caracteres especiales o secuencias numéricas.
- Evite el uso de la misma contraseña para todos los dispositivos.
- No usar palabras comunes porque se adivinan fácilmente.

Buscar una búsqueda en Internet para encontrar un generador de contraseñas. Muchos parámetros establecidos la longitud, el conjunto de caracteres y otros parámetros.

Nota: La mayoría de los laboratorios en este curso usan contraseñas simples como **cisco** o **class**. Estas contraseñas son específicas y fáciles de adivinar, y deben evitarse en un entorno de producción. Estas contraseñas solo se usan por comodidad en el aula o para ilustrar ejemplos de configuración.

2.4.3

Configuración de contraseñas

Cuando se conecta encuentra un dispositivo, se encuentra en modo EXEC de usuario. Este modo está protegido usando la consola.

Para proteger el acceso al modo EXEC del usuario, ingrese el modo de configuración de la consola de línea mediante el comando de configuración global **line console 0**, como se

muestra en el ejemplo. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola. Luego, configure la contraseña de modo EXEC de usuario con el comando **password** *contraseña.* Finalmente, habilite el acceso EXEC de usuario con el comando **login.**

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# end
Sw-Floor-1#
```

El acceso a la consola ahora requiere una contraseña antes de permitir el acceso al modo EXEC del usuario.

Para tener acceso de administrador a todos los comandos del IOS, incluida la configuración de un dispositivo, debe obtener acceso en modo EXEC privilegiado. Es el método de acceso más importante porque proporciona acceso completo al dispositivo.

Para garantizar el acceso privilegiado a EXEC, use el comando **enable secret** *password* global config, como se muestra en el ejemplo.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
SW-Floor-1(config)# exit
Sw-Floor-1#
```

Las líneas de terminal virtual (VTY) permiten el acceso remoto mediante Telnet o SSH al dispositivo. Muchos switches de Cisco admiten hasta 16 líneas VTY que se numeran del 0 al 15.

Para proteger las líneas VTY, ingrese el modo VTY de línea mediante el comando **line vty 0 15** global config. Luego, especifique la contraseña de VTY con el comando **contraseña** *contraseña.* Por último, habilite el acceso a VTY con el comando **login.**

Se muestra un ejemplo de seguridad de las líneas VTY en un switch.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# end
Sw-Floor-1#
```

2.4.4

Encriptación de las contraseñas

Los archivos startup-config y running-config varían la mayoría de las contraseñas en texto simple. Esta es una amenaza de seguridad porque cualquiera puede descubrir las contraseñas si tiene acceso a estos archivos.

Para encriptar todas las contraseñas de texto sin formato, use el comando **service password-encryption** en el modo de configuración global como se muestra en el ejemplo.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

El comando aplica un cifrado débil a todas las contraseñas no encriptadas. Esta encriptación solo se aplica a las contraseñas del archivo de configuración; no a las contraseñas mientras se envían a través de los medios. El propósito de este comando es evitar que los individuos no vean las contraseñas en el archivo de configuración.

Use el comando **show running-config,** para verificar que las contraseñas estén ahora encriptadas.

```
SW-Floor-1(config)# end
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
login
!
!
end
```

2.4.5

Mensajes de aviso

Aunque solicitar contraseñas es una forma de mantener al personal no autorizado fuera de la red, es vital proporcionar un método para declarar que solo el personal autorizado debe intentar acceder al dispositivo. Para hacerlo, agregue un aviso a la salida del dispositivo. Los avisos pueden ser una parte importante en los procesos legales en el caso de una demanda por el ingreso no autorizado a un dispositivo. Algunos sistemas legales no permiten la acusación, y ni siquiera el monitoreo de los usuarios, a menos que haya una notificación visible.

Para crear un mensaje de banner del día en un dispositivo de red, use el comando de configuración global **banner motd #** *el mensaje del día* **#**. El símbolo "#" en la sintaxis del comando se denomina carácter delimitador. Se ingresa antes y después del mensaje. El carácter delimitador puede ser cualquier carácter siempre que no tenga sentido en el mensaje. Por este motivo, a menudo se usan símbolos como "#". Una vez que se ha ejecutado el comando, pulse el aviso en todos los intentos posteriores de acceso al dispositivo hasta que el aviso se elimine.

En el ejemplo siguiente, seleccione los pasos para configurar el mensaje en Sw-Floor-1.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6

Video - Proteger el acceso administrativo a un Switch

En la figura, haga clic en el botón Reproducir para ver una demostración en video acerca de cómo proteger un acceso administrativo a un interruptor.

2.4.7

Comprobador de sintaxis - Configuración básica de dispositivos

Proteger el acceso administrativo a un interruptor

- Asigne un nombre de dispositivo
- Proteger el modo EXEC del usuario
- Proteger el acceso a EXEC privilegiado.
- Proteja el acceso a VTY.
- Cifre todas las contraseñas de texto simple.
- Mostrar un banner de inicio de sesión.

Enter global configuration mode.

```
Switch#configure terminal
```

Name the switch “Sw-Floor-1”.

```
Switch(config)#hostname Sw-Floor-1
```

Secure user EXEC mode access by entering **line console 0**, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
```

Secure privileged EXEC mode access using the password **class.**

```
Sw-Floor-1(config)#enable secret class
```

Secure the VTY lines 0 through 15, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

```
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
```

Encrypt all plaintext passwords.

```
Sw-Floor-1(config)#service password-encryption
```

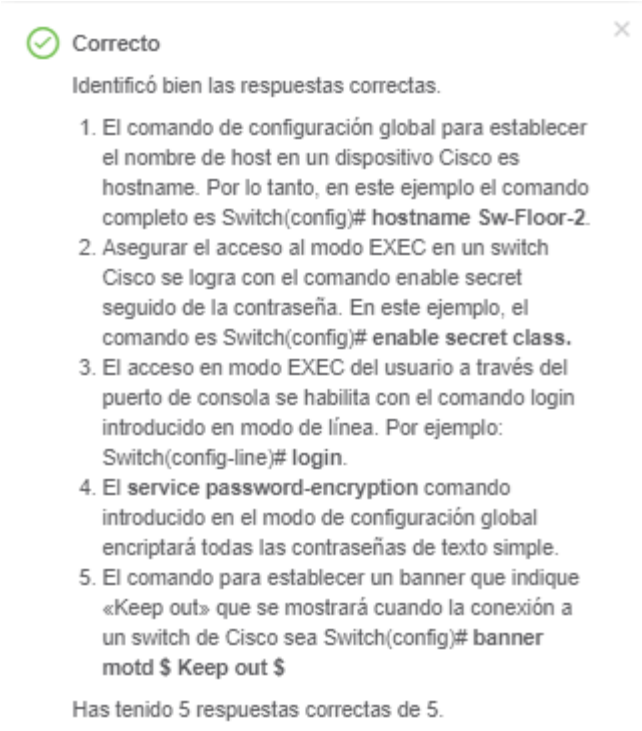
Create a banner message using the "**#**" symbol as the delimiter. The banner should display exactly: **Warning! Authorized access only!**

```
Sw-Floor-1(config)#banner #Warning! Authorized access only! #
You must enter the exact and full command.
Sw-Floor-1(config)#banner motd #Warning! Authorized access only!#
You successfully completed the basic requirements to access and secure a
device.
```

2.4.8

Compruebe su comprensión - Configuración básica del dispositivo

Verifique su comprensión de la configuración básica del dispositivo eligiendo la MEJOR respuesta a las siguientes preguntas.



Correcto

Identificó bien las respuestas correctas.

1. El comando de configuración global para establecer el nombre de host en un dispositivo Cisco es hostname. Por lo tanto, en este ejemplo el comando completo es Switch(config)# **hostname Sw-Floor-2**.
2. Asegurar el acceso al modo EXEC en un switch Cisco se logra con el comando enable secret seguido de la contraseña. En este ejemplo, el comando es Switch(config)# **enable secret class.**
3. El acceso en modo EXEC del usuario a través del puerto de consola se habilita con el comando login introducido en modo de línea. Por ejemplo: Switch(config-line)# **login**.
4. El **service password-encryption** comando introducido en el modo de configuración global encriptará todas las contraseñas de texto simple.
5. El comando para establecer un banner que indique «Keep out» que se mostrará cuando la conexión a un switch de Cisco sea Switch(config)# **banner motd $ Keep out $**

Has tenido 5 respuestas correctas de 5.

1. ¿Cuál es el comando para asignar el nombre «Sw-Floor-2» a un switch?

¡Lo tienes!

- (●) **nombre de host** SW-Floor-2
- ( ) nombre de**host** SW-Floor-2
- ( ) **nombre** SW-Floor-2

2. ¿Cómo se asegura el acceso en modo EXEC privilegiado en un switch?

¡Lo tienes!

- ( ) **habilitar clase**
- ( ) **clasesecreta**
- (●) **enable secret class**
- ( ) **service password-encryption**

3. ¿Qué comando habilita la autenticación de contraseña para el acceso en modo EXEC del usuario en un switch?

¡Lo tienes!

- ( ) **Comando enable secret**
- (●) **Inicio de sesión**
- ( ) **secret**
- ( ) **cifrado de contraseña de servicio**

4. ¿Qué comando encripta todas las contraseñas de texto simple en un switch?

¡Lo tienes!

- ( ) **Comando enable secret**
- ( ) **Inicio de sesión**
- ( ) **secret**
- (●) **cifrado de contraseña de servicio**

5. ¿Cuál es el comando para configurar un banner que se mostrará al conectarse a un switch?

¡Lo tienes!

- ( ) **banner $Mantener fuera $**
- (●) **banner motd $Mantener fuera $**
- ( ) **mostrar $Mantener fuera $**
- ( ) banner de**inicio de sesión $Mantener fuera $**

Correct

You have successfully identified the correct answers.

1. The global configuration command to set the host name on a Cisco device is hostname. So, in this example the full command is Switch(config)# **hostname Sw-Floor-2**.
2. Securing access to the EXEC mode on a Cisco switch is accomplished with the enable secret command followed by the password. In this example the command is Switch(config)# **enable secret class.**
3. User EXEC mode access through the console port is enabled with the login command entered in line mode. For example: Switch(config-line)# **login**.
4. The **service password-encryption** command entered in global configuration mode will encrypt all plaintext passwords.
5. The command to set a banner stating "Keep out" that will be displayed when connection to a Cisco switch is Switch(config)# **banner motd $ Keep out $**

You got 5 out of 5 questions correct.

1. What is the command to assign the name "Sw-Floor-2" to a switch?

You got it!

- (●) **hostname** Sw-Floor-2
- ( ) **host name** Sw-Floor-2
- ( ) **name** Sw-Floor-2

2. How is the privileged EXEC mode access secured on a switch?

You got it!

- ( ) **enable class**
- ( ) **secret class**
- (●) **enable secret class**
- ( ) **service password-encryption**

3. Which command enables password authentication for user EXEC mode access on a switch?

You got it!

- ( ) **enable secret**
- (●) **login**
- ( ) **secret**
- ( ) **service password-encryption**

4. Which command encrypts all plaintext passwords access on a switch?

You got it!

- enable secret
- login
- secret
- service password-encryption

5. Which is the command to configure a banner to be displayed when connecting to a switch?

You got it!

- banner $ Keep out $
- banner motd $ Keep out $
- display $ Keep out $
- login banner $ Keep out $

Configuración básica de switches y terminales / Guardar las configuraciones

Guardar las configuraciones

2.5.1

Archivos de configuración

Ahora sabe cómo realizar la configuración básica en un switch, incluidas las contraseñas y los mensajes de banner. En este tema se mostrará cómo guardar las configuraciones.

Existen dos archivos de sistema que almacenan la configuración de dispositivos.

- **startup-config** - Este es el archivo de configuración guardado que se almacena en NVRAM. Contiene todos los comandos que usará el dispositivo al iniciar o reiniciar. Flash no pierde su contenido cuando el dispositivo está apagado.
- **running-config** - Esto se almacena en la memoria de acceso aleatorio (RAM). Refleja la configuración actual. La modificación de una configuración en ejecución afecta el funcionamiento de un dispositivo Cisco de inmediato. La memoria RAM es volátil. Pierde todo el contenido cuando el dispositivo se apaga o se reinicia.

El comando de modo EXEC **show running-config** privilegiado se utiliza para ver la configuración en ejecución. Como se muestra en el ejemplo, el comando mostrará la configuración completa actualmente almacenada en RAM.

```
Switch# show running-config
Building configuration...
Current configuration : 1351 bytes
!
! Last configuration change at 00:01:20 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

Para ver el archivo de configuración de inicio, use el comando **show startup-config** EXEC privilegiado.

Si se corta la energía al dispositivo o si este se reinicia, se perderán todos los cambios de configuración a menos que se hayan guardado. Para guardar los cambios realizados en la configuración en ejecución en el archivo de configuración de inicio, utilice el comando **copy running-config startup-config** del modo EXEC privilegiado.

2.5.2

Modificación de la configuración en ejecución

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado y la configuración en ejecución aún no se ha guardado, puede restaurar el dispositivo a su configuración anterior. Elimine los comandos modificados individualmente o vuelva a cargar el dispositivo con el comando EXEC **reload** privilegiado para restaurar el startup-config.

La desventaja de usar el **reload** comando para eliminar una configuración en ejecución no guardada es la breve cantidad de tiempo que el dispositivo estará fuera de línea, causando el tiempo de inactividad de la red.

Cuando se inicia una recarga, el IOS detectará que la configuración en ejecución tiene cambios que no se guardaron en la configuración de inicio. Aparecerá una petición de entrada para preguntar si se desean guardar los cambios. Para descartar los cambios, ingrese **n** o **no**.

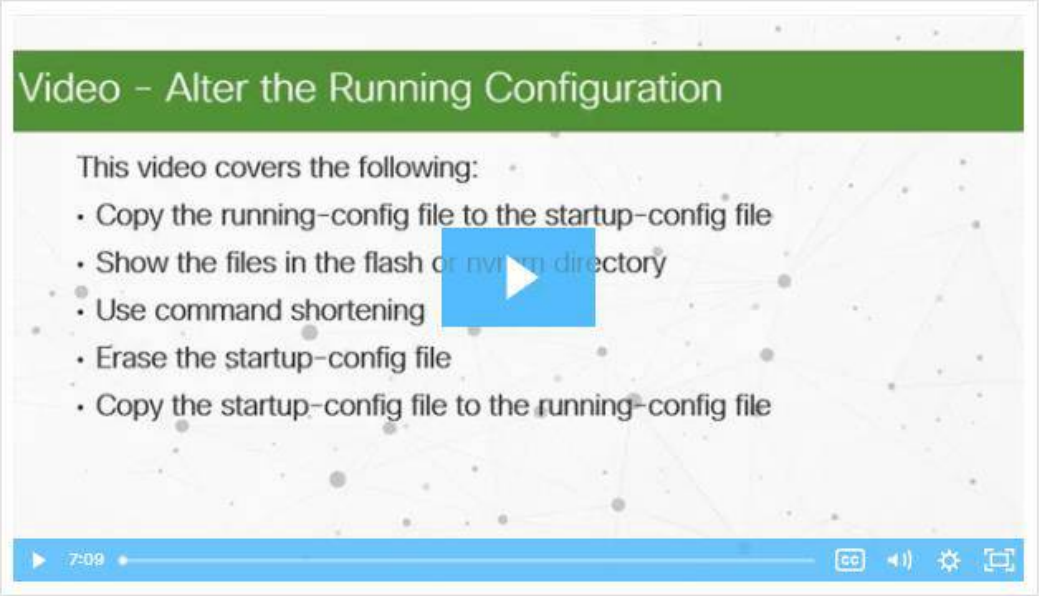
Alternativamente, si los cambios no deseados se guardaron en la configuración de inicio, puede ser necesario borrar todas las configuraciones. Esto requiere borrar la configuración de inicio y reiniciar el dispositivo. La configuración de inicio se elimina mediante el **erase startup-config** comando del modo EXEC privilegiado. Una vez que se emite el comando, el switch le solicita confirmación. Press **Enter** to accept.

Después de eliminar la configuración de inicio de la NVRAM, recargue el dispositivo para eliminar el archivo de configuración actual en ejecución de la memoria RAM. En la recarga, un switch cargará la configuración de inicio predeterminada que se envió originalmente con el dispositivo.

2.5.3

Video - Modificación de la configuración en ejecución

Haga clic en el botón Reproducir en la figura para ver una demostración en vídeo sobre cómo guardar archivos de configuración.



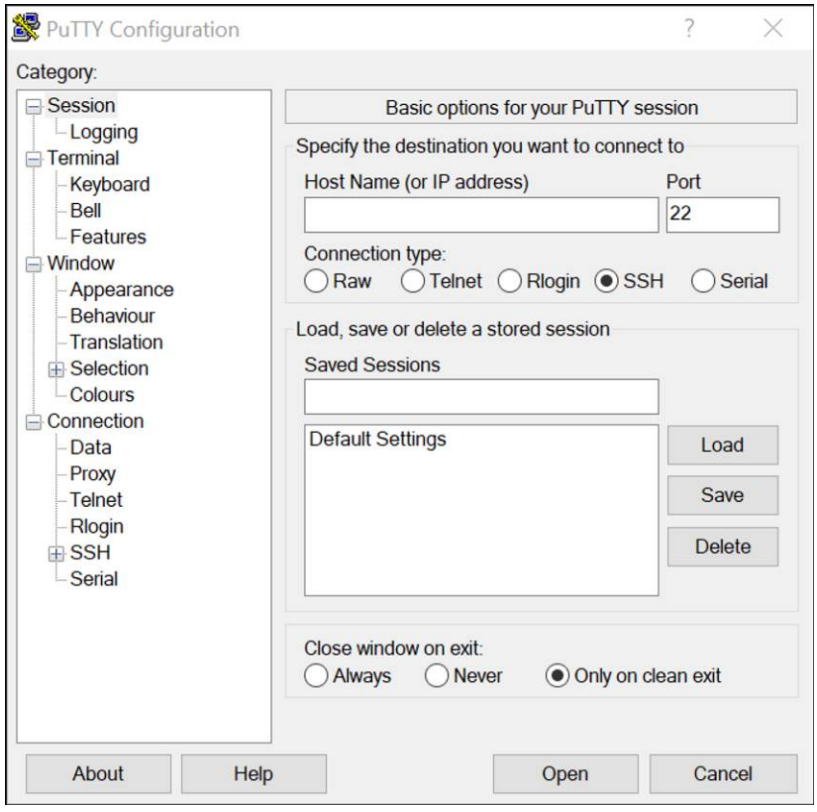
2.5.4

Captura de configuración a un archivo de texto

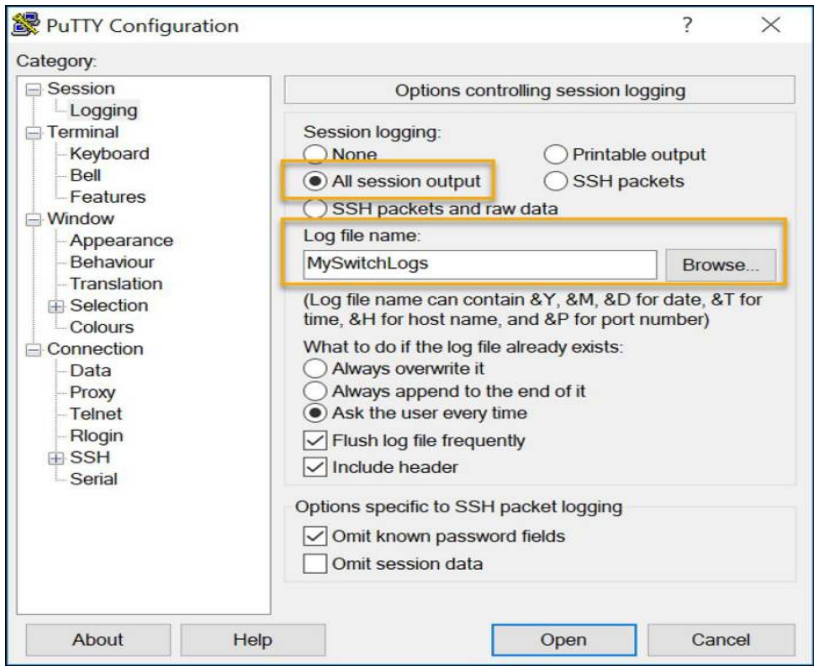
Los archivos de configuración pueden guardarse y archivarse en un documento de texto. Esta secuencia de pasos asegura la disponibilidad de una copia utilizable del archivo de configuración para su modificación o reutilización en otra oportunidad.

Por ejemplo, suponga que se configuró un switch y que la configuración en ejecución se guardó en el dispositivo.

Paso 1. Abra el software de emulación de terminal, como PuTTY o Tera Term, que ya está conectado a un switch.



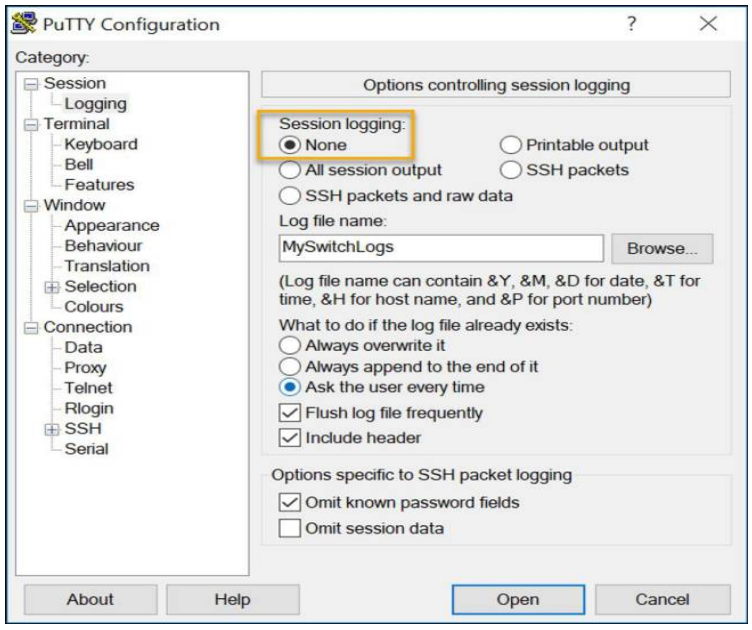
Paso 2. Habilite el inicio de sesión en el software del terminal y asigne un nombre y una ubicación de archivo para guardar el archivo de registro. La figura muestra que **All session output** se capturará en el archivo especificado (es decir, MySwitchLogs).



Paso 3. Ejecute el comando **show running-config,** o el comando **show startup-config** en el símbolo EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.

```
Switch# show running-config
Building configuration...
```

Paso 4. Desactive el inicio de sesión en el software del terminal. La figura muestra cómo deshabilitar el registro seleccionando **None** la opción de registro de sesión.



El archivo de texto creado se puede utilizar como un registro del modo en que se implementa actualmente el dispositivo. El archivo puede requerir edición antes de poder utilizarse para restaurar una configuración guardada a un dispositivo.

Para restaurar un archivo de configuración a un dispositivo:

Paso 1. Ingrese al modo de configuración global en el dispositivo.

Paso 2. Copie y pegue el archivo de texto, en la ventana del terminal, conectada al switch.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Este es un método conveniente para configurar manualmente un dispositivo.

2.5.5

Packet Tracer - Configure ajustes iniciales del switch

En esta actividad, se efectuarán las configuraciones básicas del switch. Protegerá el acceso seguro a la CLI y al puerto de consola con contraseñas encriptadas y de texto simple. También aprenderá cómo configurar mensajes para los usuarios que inician sesión en el switch. Estos avisos también se utilizan para advertir a usuarios no autorizados que el acceso está prohibido.

Configure ajustes iniciales del interruptor

Configure ajustes iniciales del interruptor

Configuración básica de switches y terminales / Puertos y direcciones

Puertos y direcciones

2.6.1

Direcciones IP

¡Felicitaciones, has realizado una configuración básica del dispositivo! Por supuesto, la diversión aún no ha terminado. Si desea que sus dispositivos finales se comuniquen entre sí, debe asegurarse de que cada uno de ellos tiene una dirección IP adecuada y está correctamente conectado. En este tema encontrará información sobre las direcciones IP, los puertos de dispositivos y los medios utilizados para conectar dispositivos.

El uso de direcciones IP es el principal medio para permitir que los dispositivos se ubiquen entre sí y para establecer la comunicación completa en Internet. Cada terminal en una red se debe configurar con direcciones IP. Los ejemplos de dispositivos finales incluyen estos:

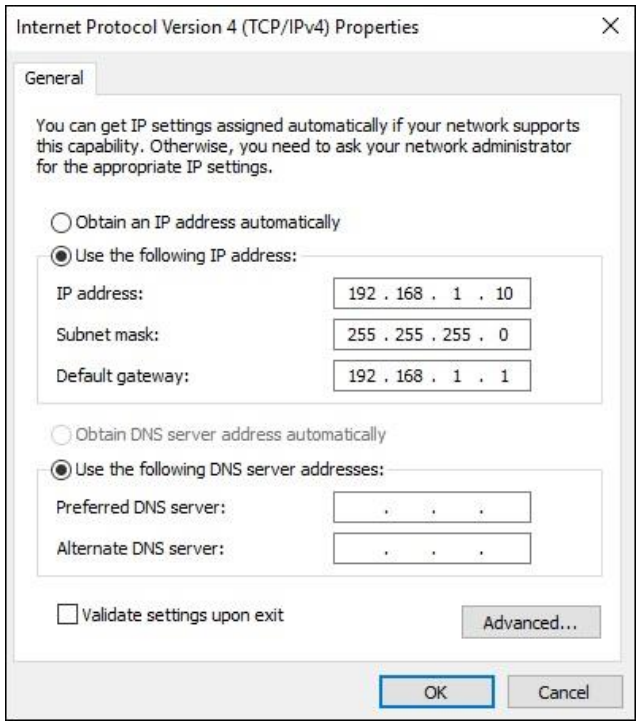
- PC (estaciones de trabajo, PC portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Teléfonos inteligentes
- Dispositivos portátiles móviles (tal como los escáners inalámbricos para códigos de barras)

La estructura de una dirección IPv4 se denomina notación decimal punteada y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red.

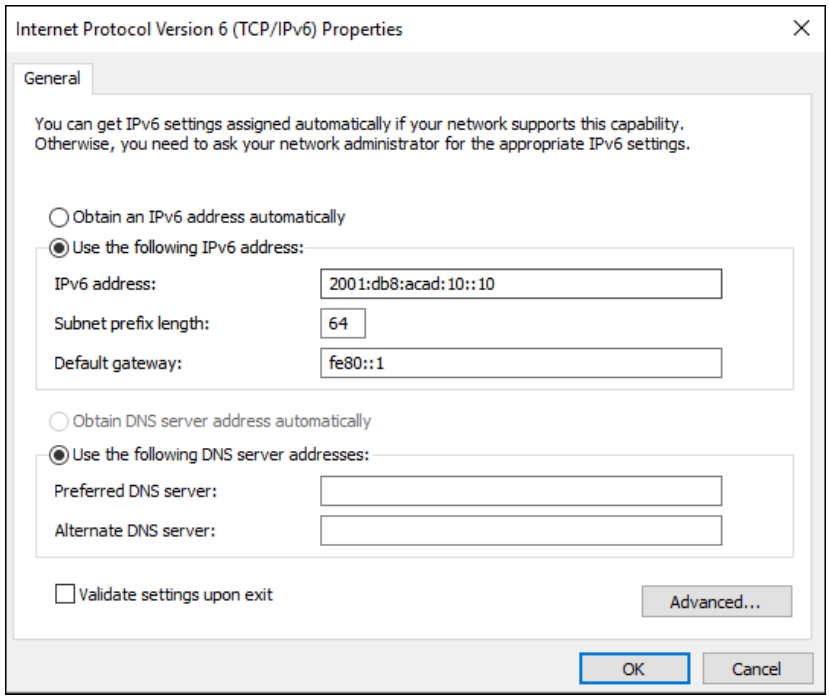
Nota: IP en este curso se refiere a los protocolos IPv4 e IPv6. IPv6 es la versión más reciente de IP y está reemplazando al IPv4 que es más común.

Con la dirección IPv4, también se necesita una máscara de subred. Una máscara de subred IPv4 es un valor de 32 bits que separa la porción de red de la dirección de la porción de host. Junto con la dirección IPv4, la máscara de subred determina a qué subred pertenece el dispositivo.

El ejemplo de la figura muestra la dirección IPv4 (192.168.1.10), la máscara de subred (255.255.255.0) y el gateway predeterminado (192.168.1.1) asignados a un host. La dirección de gateway predeterminado es la dirección IP del router que el host utilizará para acceder a las redes remotas, incluso a Internet.



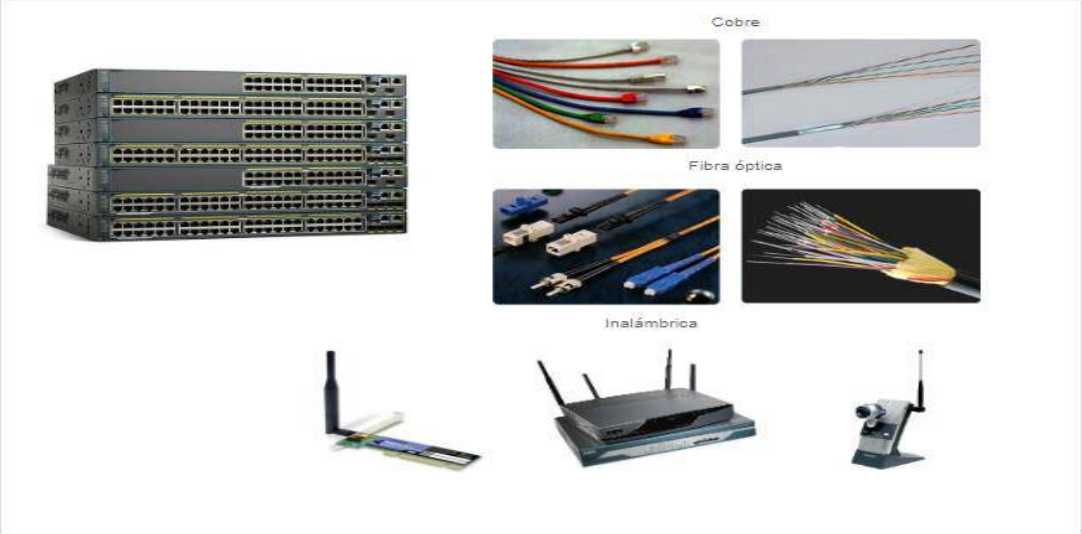
Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Los grupos de cuatro dígitos hexadecimales están separados por dos puntos (:). Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.



2.6.2

Interfaces y puertos

Las comunicaciones de red dependen de las interfaces de los dispositivos para usuarios finales, las interfaces de los dispositivos de red y los cables que las conectan. Cada interfaz física tiene especificaciones o estándares que la definen. Los cables que se conectan a la interfaz deben estar diseñados para cumplir con los estándares físicos de la interfaz. Los tipos de medios de red incluyen los cables de cobre de par trenzado, los cables de fibra óptica, los cables coaxiales o la tecnología inalámbrica, como se muestra en la figura.



Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características. No todos los medios son apropiados para el mismo propósito. Estas son algunas de las diferencias entre varios tipos de medios:

- La distancia a través de la cual los medios pueden transportar una señal correctamente.
- El ambiente en el cual se instalará el medio.
- La cantidad de datos y la velocidad a la que se deben transmitir.
- El costo de los medios y de la instalación.

Cada enlace de Internet no solo requiere un tipo específico de medio de red, sino que también requiere una determinada tecnología de red. Por ejemplo, Ethernet es la tecnología de red de área local (LAN) de uso más frecuente en la actualidad. Hay puertos Ethernet en los dispositivos para usuarios finales, en los dispositivos de switch y en otros dispositivos de red que se pueden conectar físicamente a la red mediante un cable.

Los switches de la capa 2 de Cisco IOS cuentan con puertos físicos para conectar dispositivos. Estos puertos no son compatibles con las direcciones IP de la capa 3. En consecuencia, los switches tienen una o más interfaces virtuales de switch (SVI). Son

interfaces virtuales porque no hay hardware físico en el dispositivo asociado a ellas. Una SVI se crea en el software.

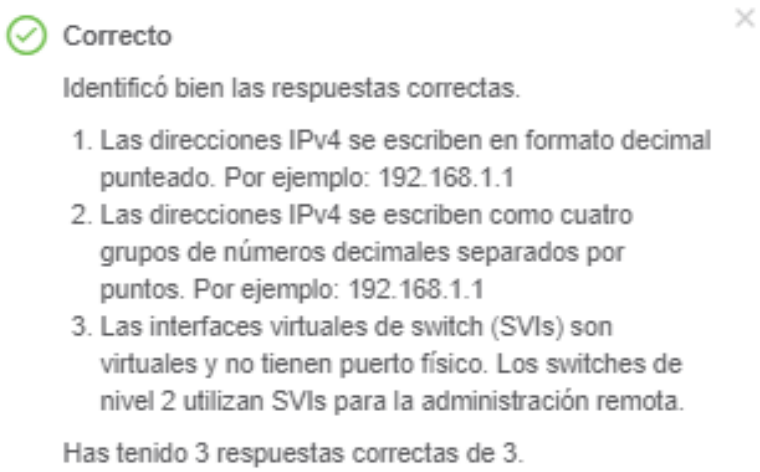
La interfaz virtual le permite administrar de forma remota un switch a través de una red utilizando IPv4 e IPv6. Cada switch viene con una SVI que aparece en la configuración predeterminada, fácil de instalar. La SVI predeterminada es interfaz VLAN1.

Nota: Un switch de capa 2 no necesita una dirección IP. La dirección IP asignada a la SVI se utiliza para acceder al switch de forma remota. No se necesita una dirección IP para que el switch realice estas operaciones.

2.6.3

Compruebe su comprensión - Puertos y direcciones

Verifique su comprensión de los puertos y direcciones eligiendo la MEJOR respuesta a las siguientes preguntas.



1. ¿Cuál es la estructura de una dirección IPv4 llamada?

¡Lo tienes!

- ○ formato binario punteado
- ◉ formato decimal punteado
- ○ formato hexadecimal punteado

2. ¿Cómo se representa una dirección IPv4?

¡Lo tienes!

- ○ cuatro números binarios entre 0 y 1 separados por dos puntos.
- ◉ cuatro números decimales entre 0 y 255 separados por puntos.
- ○ treinta y dos números hexadecimales separados por puntos.
- ○ treinta y dos números hexadecimales separados por puntos.

3. ¿Qué tipo de interfaz no tiene ningún puerto físico asociado?

¡Lo tienes!

- ○ Consola
- ○ Ethernet
- ○ Serial
- ◉ interfaz virtual de switch (SVI)

Correct

You have successfully identified the correct answers.

1. IPv4 addresses are written in dotted-decimal format. For example: 192.168.1.1.
2. IPv4 addresses are written as four groups of decimal numbers separated by periods. For example: 192.168.1.1.
3. Switch virtual interfaces (SVIs) are virtual and have no physical port. Layer 2 switches use SVIs for remote management.

You got 3 out of 3 questions correct.

1. What is the structure of an IPv4 address called?

You got it!

- ○ dotted-binary format
- ◉ dotted-decimal format
- ○ dotted-hexadecimal format

2. How is an IPv4 address represented?

You got it!

- ○ four binary numbers between 0 and 1 separated by colons.
- ◉ four decimal numbers between 0 and 255 separated by periods.
- ○ thirty-two hexadecimal numbers separated by colons.
- ○ thirty-two hexadecimal numbers separated by periods.

3. What type of interface has no physical port associated with it?

You got it!

- ○ console
- ○ Ethernet
- ○ serial
- ◉ switch virtual interface (SVI)

1. Configuración básica de switches y terminales / Configurar direccionamiento IP

Configurar direccionamiento IP

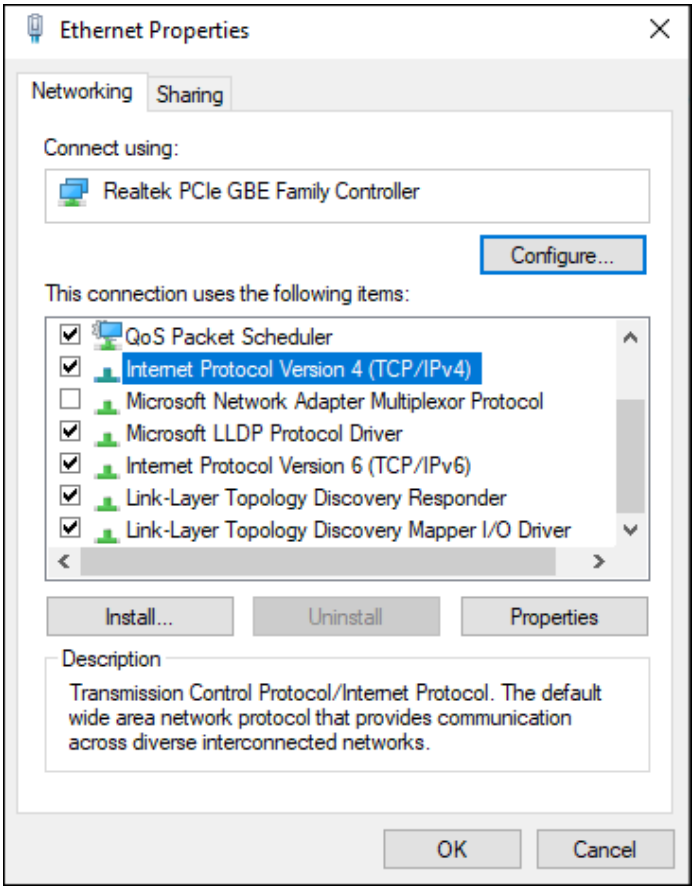
2.7.1

Configuración manual de dirección IP para dispositivos finales

Al igual que necesitas los números de teléfono de tus amigos para enviarles mensajes de texto o llamarlos, los dispositivos finales de tu red necesitan una dirección IP para que puedan comunicarse con otros dispositivos de tu red. En este tema, implementará la conectividad básica configurando el direccionamiento IP en switches y PC.

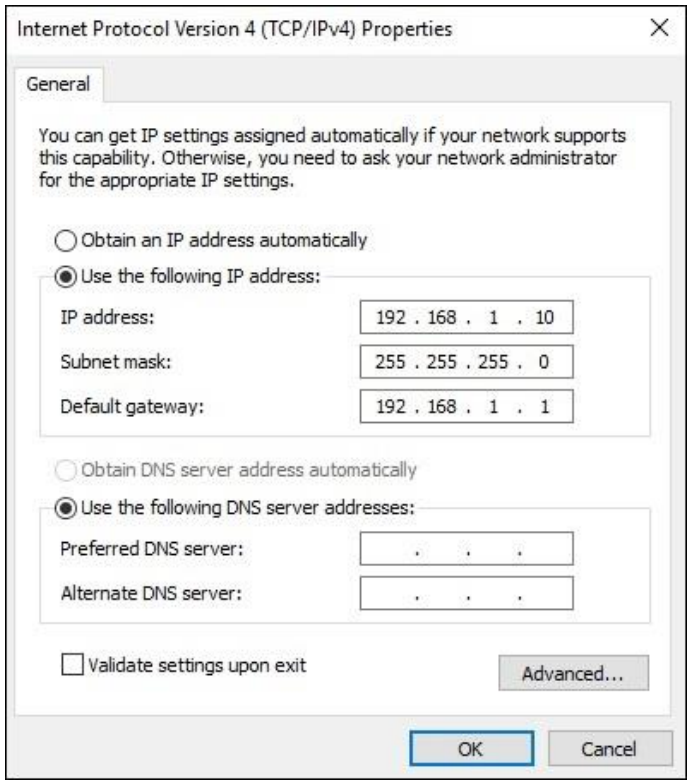
La información de la dirección IPv4 se puede ingresar en los dispositivos finales de forma manual o automática mediante el Protocolo de configuración dinámica de host (DHCP).

Para configurar manualmente una dirección IPv4 en un host de Windows, abra **Control Panel > Network Sharing Center > Change adapter settings** y elija el adaptador. A continuación, haga clic con el botón derecho y seleccione **Properties** para mostrar el **Local Area Connection Properties**, como se muestra en la figura.



Resalte Protocolo de Internet versión 4 (TCP/IPv4) y haga clic **Properties** para abrir la ventana **Internet Protocol Version 4 (TCP/IPv4) Properties**, que se muestra en la figura. Configure la información de la dirección IPv4 y la máscara de subred, y el gateway predeterminado.

Nota: Las opciones de configuración y direccionamiento IPv6 son similares a IPv4.



Nota: La dirección del servidor DNS es la dirección IPv4 del servidor del sistema de nombres de dominio (DNS), que se utiliza para traducir direcciones IP a direcciones web, como www.cisco.com.

2.7.2

Configuración automática de direcciones IP para dispositivos finales

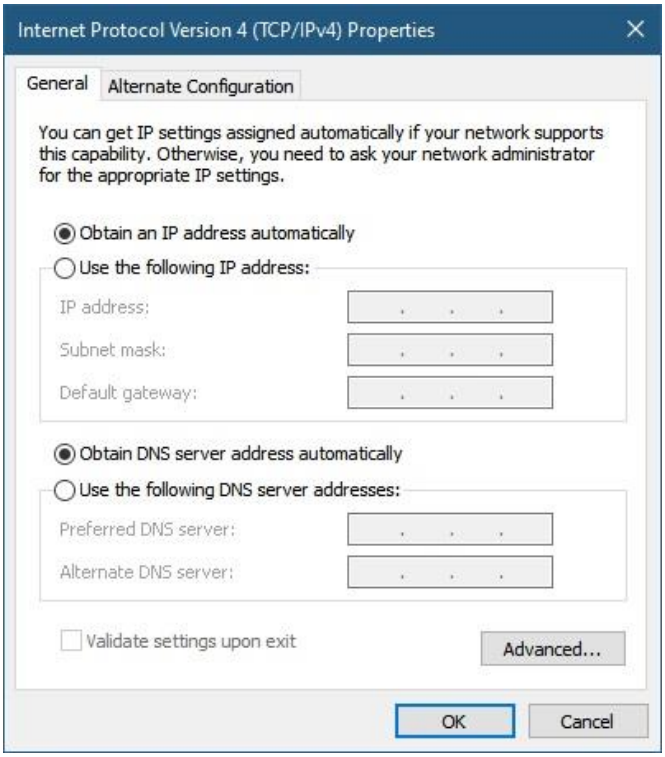
Los dispositivos finales suelen usar DHCP de manera predeterminada para la configuración automática de la dirección IPv4. DHCP es una tecnología que se utiliza en casi todas las redes. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo.

En una red, DHCP habilita la configuración automática de direcciones IPv4 para cada dispositivo final habilitado para DHCP. Imagine la cantidad de tiempo que le llevaría si cada vez que se conectara a la red tuviera que introducir manualmente la dirección IPv4, la máscara de subred, el gateway predeterminado y el servidor DNS. Multiplique eso por cada usuario y cada uno de los dispositivos en una organización y se dará cuenta del problema. La

configuración manual también aumenta las posibilidades de configuraciones incorrectas provocadas por la duplicación de la dirección IPv4 de otro dispositivo.

Como se muestra en la figura, para configurar DHCP en una PC con Windows, solo necesita seleccionar **Obtain an IP address automatically** y **Obtain DNS server address automatically**. Su PC buscará un servidor DHCP y se le asignarán los ajustes de dirección necesarios para comunicarse en la red.

Nota: IPv6 utiliza DHCPv6 y SLAAC (configuración automática de direcciones sin estado) para la asignación dinámica de direcciones.

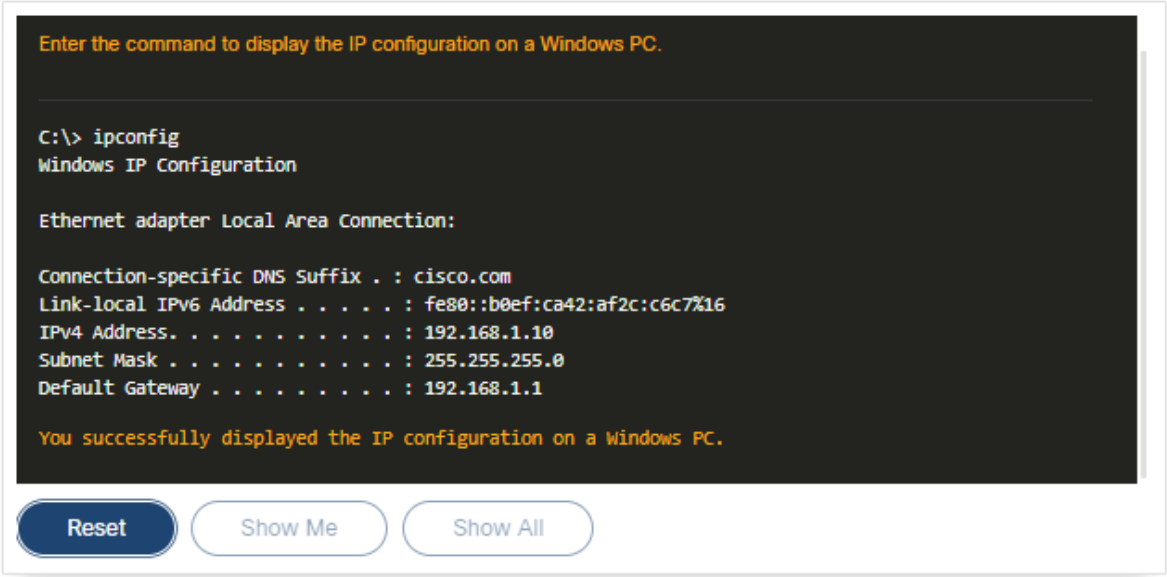


2.7.3

Comprobador de sintaxis - Verificar la configuración IP de Windows PC

Es posible mostrar los ajustes de configuración IP en una PC con Windows usando el comando **ipconfig,** cuando el sistema se lo solicite. El resultado muestra la información de dirección IPv4, máscara de subred y gateway que se recibió del servidor DHCP.

Introduzca el comando para que se muestre la configuración IP en un equipo Windows.



2.7.4

Configuración de interfaz virtual de switch

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI. Para configurar una SVI en un switch, utilice el comando de **interface vlan 1** configuración global. La Vlan 1 no es una interfaz física real, sino una virtual. A continuación, asigne una dirección IPv4 mediante el comando **ip address** *ip-address subnet-mask* de la configuración de interfaz. Finalmente, habilite la interfaz virtual utilizando el comando de configuración de la interfaz **no shutdown**.

Una vez que se configuran estos comandos, el switch tiene todos los elementos IPv4 listos para la comunicación a través de la red.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

2.7.5

Verificador de sintaxis: Configuración de una interfaz virtual de switch

Enter interface configuration mode for VLAN 1.

```
Switch(config)#interface vlan 1
```

Configure the IPv4 address as 192.168.1.20 and the subnet mask as 255.255.255.0.

```
Switch(config-if)#ip address 192.168.1.20 255.255.255.0
```

Enable the interface.

```
Switch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
You have successfully configured the switch virtual interface for VLAN 1.
```

2.7.6

Packet Tracer: Implementación de conectividad básica

En esta actividad, primero se efectuarán las configuraciones básicas del switch. A continuación, implementará conectividad básica mediante la configuración de la asignación de direcciones IP en switches y PCs. Cuando se complete la configuración de direccionamiento IP, usará varios comandos **show** para verificar las configuraciones, y usará el comando **ping** para verificar la conectividad básica entre dispositivos.

Implementación de conectividad básica

Implementación de conectividad básica

1. Basic Switch and End Device Configuration / Vericar Connectividad

Verificar la conectividad

2.8.1

Actividad de vídeo - Prueba la asignación de interfaz

En el tema anterior, implementó la conectividad básica configurando el direccionamiento IP en siwtches y PCs. Luego verificó sus configuraciones y conectividad, porque, ¿cuál es el punto de configurar un dispositivo si no verifica que la configuración está funcionando? Continuará este proceso en este tema. Mediante la CLI, verificará las interfaces y las direcciones de los switches y routers de su red.

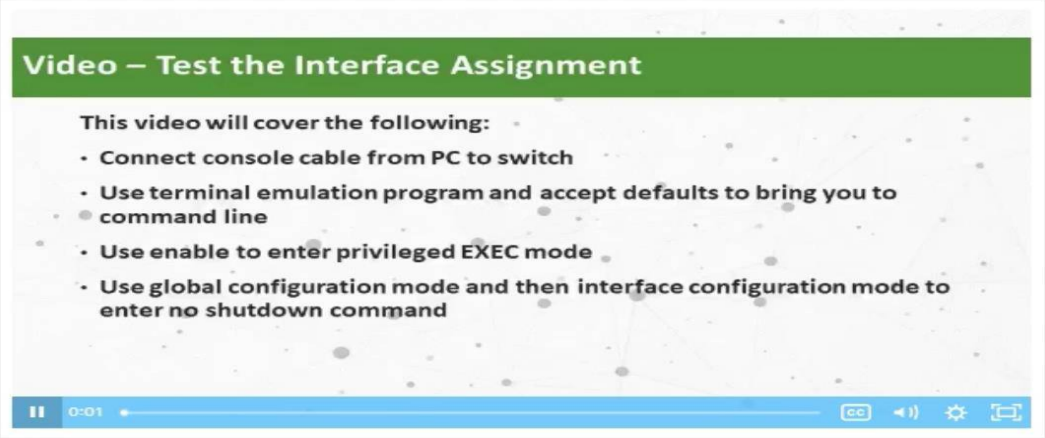
De la misma manera que usa comandos y utilidades como **ipconfig** para verificar la configuración de red de un host de PC, también usa comandos para verificar las interfaces y la configuración de direcciones de dispositivos intermediarios como switches y routers.

Haga clic en Reproducir en la figura para ver una demostración en video del comando. **show ip interface brief** Este comando es útil para verificar la condición de las interfaces de switch.

Seguir en Packet Tracer

Descargue el mismo archivo PKT que se usa en el video. Practique usando los comandos **ipconfig** y **show ip interface brief**, como se muestra en el video.

Test the Interface Assignment



2.8.2

Video - Prueba de conectividad de extremo a extremo

El comando **ping** se puede usar para probar la conectividad a otro dispositivo en la red o un sitio web en Internet.

Haga clic en Reproducir en la figura para ver una demostración en video usando el comando **ping** para probar la conectividad a un switch y a otra PC.

Follow Along in Packet Tracer

Descargue el mismo archivo PKT que se usa en el video. Practique usando el **ping** comando, como se muestra en el video.

Test End-to-End Connectivity

Basic Switch and End Device Configuration / Module Practice and Quiz

Module Practice and Quiz

2.9.1

Packet Tracer — Configuración básica del switch y del dispositivo final

Como técnico de LAN recientemente contratado, su administrador de red le ha pedido que demuestre su capacidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante Cisco IOS y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad completa. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

Configuración básica de switches y terminales

Configuración básica de switches y terminales

2.9.2

Lab - Configuración básica de switch y dispositivo final

En este laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Configurar la topología de red
- Parte 2: Configurar hosts en las PC
- Parte 3: Configurar y verificar los parámetros básicos del switch

Configuración básica de switches y terminales

2.9.3

¿Qué aprendió en este módulo?

Todos los dispositivos finales y dispositivos de red requieren un sistema operativo (OS). El usuario puede interactuar con el shell mediante una interfaz de línea de comandos (CLI) para utilizar un teclado para ejecutar programas de red basados en CLI, utilizar un teclado para introducir comandos basados en texto y texto y ver los resultados en un monitor.

Como función de seguridad, el software Cisco IOS separa el acceso de administración en los siguientes dos modos de comandos: modo EXEC del usuario y modo EXEC con privilegios.

Antes de acceder a otros modos de configuración específicos, se accede al modo de configuración global. Desde el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. Dos modos de subconfiguración comunes incluyen: Modo de configuración de línea y Modo de configuración de interfaz. Para entrar y salir del modo de configuración global, use el comando **configure terminal** del modo EXEC privilegiado. Para volver al modo EXEC privilegiado, ingrese el comando **exit,** del modo de configuración global.

Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando es el comando seguido de las palabras clave y los argumentos correspondientes. El IOS tiene dos formas de ayuda disponibles: la ayuda contextual y el verificador de sintaxis de comandos.

El primer comando de configuración en cualquier dispositivo debe ser darle un nombre de dispositivo único o nombre de host. Los dispositivos de red siempre deben tener contraseñas configuradas para limitar el acceso administrativo. Cisco IOS puede configurarse para utilizar contraseñas en modo jerárquico y permitir diferentes privilegios de acceso al dispositivo de red. Configure y encripte todas las contraseñas. Proporcione un método para declarar que solo el personal autorizado debe intentar acceder al dispositivo agregando un banner a la salida del dispositivo.

Hay dos archivos del sistema que almacenan la configuración del dispositivo: startup-config y running-config. Los archivos de configuración en ejecución se pueden modificar si no se han guardado. Los archivos de configuración pueden guardarse y archivarse en un documento de texto.

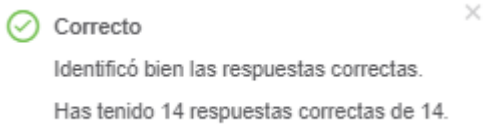
Las direcciones IP permiten a los dispositivos ubicarse entre sí y establecer una comunicación de extremo a extremo en Internet. Cada terminal en una red se debe configurar con direcciones IP. La estructura de una dirección IPv4 se denomina notación decimal punteada y se representa con cuatro números decimales entre 0 y 255.

La información de la dirección IPv4 se puede ingresar en los dispositivos finales de forma manual o automática mediante el Protocolo de configuración dinámica de host (DHCP). En una red, DHCP habilita la configuración automática de direcciones IPv4 para cada dispositivo final habilitado para DHCP. Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI. Para configurar una SVI en un switch, utilice el comando de configuración global **interface vlan 1.** La Vlan 1 no es una interfaz física real, sino una virtual.

De la misma manera que usa comandos y utilidades para verificar la configuración de red de un host de PC, también usa comandos para verificar las interfaces y la configuración de direcciones de dispositivos intermediarios como switches y routers. **show ip interface brief**. Este comando es útil para verificar la condición de las interfaces de switch. El comando **ping** se puede usar para probar la conectividad a otro dispositivo en la red o un sitio web en Internet.

2.9.4

Prueba del módulo - Configuración básica del switch y el dispositivo final



1. ¿Qué declaración es verdadera sobre el archivo de configuración en ejecución en un dispositivo Cisco IOS?

Tema 2.5.0 - Tan pronto como se introducen los comandos de configuración en un router, modifican el dispositivo inmediatamente. Los archivos de configuración en ejecución no se pueden eliminar ni se guardan automáticamente.

- (•) Afecta el funcionamiento del dispositivo inmediatamente cuando se modifica.
- ( ) Se almacena en NVRAM.
- ( ) Se debe eliminar usando el **erase running-config** comando.
- ( ) Se guarda automáticamente cuando el router se reinicia.

2. ¿Cuáles son las dos afirmaciones verdaderas con respecto al modo EXEC del usuario? (Escoja dos.)

Tema 2.2.0 - El modo EXEC del usuario limita el acceso a algunos **show** y comandos. **debug** Es el primer nivel de interfaz de usuario que se encuentra en la configuración de un router y está diseñado para investigar ciertas funciones del dispositivo. La petición de entrada del modo EXEC del usuario se identifica con el símbolo ">".

- [ ] Todos los comandos del router están disponibles.
- [ ] Se puede acceder al modo de configuración global introduciendo el comando **enable**
- [x] La petición de entrada del dispositivo para este modo termina con el símbolo ">".
- [ ] Se pueden configurar interfaces y protocolos de routing.
- [x] Solo se pueden ver algunos aspectos de la configuración del router.

3. ¿Qué tipo de acceso está asegurado en un router o switch Cisco con el **enable secret** comando?

Tema 2.4.0 - El **enable secret** comando asegura el acceso al modo EXEC privilegiado de un router o switch Cisco.

- ( ) Terminales virtuales
- (•) EXEC con privilegios
- ( ) Puerto auxiliar
- ( ) Línea de consola

4. ¿Cuál es el SVI predeterminado en un switch Cisco?

Tema 2.6.0 - Los switches de capa 2 utilizan interfaces virtuales de switch (SVIs) para proporcionar un medio para el acceso remoto a través de IP. El SVI predeterminado en un switch Cisco es VLAN1.

- (•) VLAN1
- ( ) VLAN99
- ( ) VLAN100
- ( ) VLAN999

5. Cuando se configura un nombre de host a través de la CLI de Cisco, ¿cuáles son las tres convenciones de nomenclatura que forman parte de las pautas? (Elija tres.)

Tema 2.4.0 - Un nombre de host se puede configurar con mayúsculas o minúsculas y debe terminar con una letra o dígito, no con un carácter especial. El nombre de host debe empezar con una letra, y no se permite el uso de espacios para los nombres de host.

- [x] El nombre de host debe tener menos 64 caracteres.
- [ ] El nombre de host debe estar escrito completamente en letras minúsculas.
- [x] El nombre de host no deber tener espacios.
- [ ] El nombre de host debe terminar con un carácter especial.
- [x] El nombre de host debe comenzar con una letra.

6. ¿Cuál es la función del shell en un OS?

Tema 2.1.0 - La mayoría de los sistemas operativos tienen un shell y un kernel. El kernel interactúa con el hardware y las interfaces del shell entre el kernel y los usuarios.

- ( ) Interactúa con el hardware del dispositivo.
- (•) Comunica a los usuarios y el kernel.
- ( ) Proporciona servicios de firewall exclusivos.
- ( ) Proporciona los servicios de protección contra intrusiones para el dispositivo.

7. Un router con un sistema operativo válido tiene un archivo de configuración almacenado en la NVRAM. El archivo de configuración posee una contraseña secreta de enable, pero ninguna contraseña de consola. Cuando el router inicia, ¿qué modo se muestra?

Tema 2.2.0 - Si un dispositivo con Cisco IOS tiene una versión de IOS y un archivo de configuración válidos, arranca en el modo EXEC del usuario. Se requiere una contraseña para entrar al modo EXEC privilegiado.

- ( ) Modo de configuración global
- ( ) Modo de configuración
- ( ) Modo EXEC privilegiado
- (•) Modo EXEC del usuario

8. Un administrador acaba de cambiar la dirección IP de una interfaz en un dispositivo IOS. ¿Qué más se debe hacer para aplicar esos cambios al dispositivo?

Tema 2.5.0 - Los cambios en las configuraciones del router y del switch surten efecto tan pronto como se introduce el comando. Por esta razón, es muy importante que los cambios en los dispositivos de producción en vivo siempre se planifiquen cuidadosamente antes de ser implementados. Si se introducen comandos que hacen que el dispositivo sea inestable o inaccesible, es posible que deba volver a cargarlo, lo que provoca un tiempo de inactividad de la red.

- ○ Copie la configuración en ejecución en la configuración de inicio.
- ○ Copie la información en el archivo de configuración de inicio a la configuración en ejecución.
- ○ Vuelva a cargar el dispositivo y escriba **yes** cuando se le pida que guarde la configuración.
- ◉ No hay que hacer nada. Los cambios en la configuración de un dispositivo IOS surten efecto tan pronto como el comando se escribe correctamente y se presiona la tecla Intro.

9. ¿Qué ubicación de memoria en un router o switch Cisco perderá todo el contenido cuando se reinicie el dispositivo?

Tema 2.5.0 - La memoria RAM es una memoria volátil y perderá todo el contenido si se reinicia o se apaga el router o el switch.

- ○ ROM
- ○ Memoria flash
- ○ NVRAM
- ◉ RAM

10. ¿Por qué un técnico ingresaría el comando **copy startup-config running-config**?

Tema 2.5.0 - Por lo general, los cambios a una configuración en ejecución se realizan en la RAM y se copian en la NVRAM. Sin embargo, en este caso, el técnico desea copiar una configuración guardada anteriormente de la NVRAM a la RAM para realizarle cambios.

- ○ Para eliminar todas las configuraciones del switch.
- ○ Para guardar una configuración activa en la NVRAM.
- ◉ Para copiar una configuración existente en la RAM.
- ○ Para establecer una configuración modificada como la nueva configuración de inicio.

11. ¿Qué funcionalidad proporciona DHCP?

Tema 2.7.0 - DHCP proporciona una asignación dinámica y automática de direcciones IP a los hosts.

- (●) asignación automática de una dirección IP a cada host
- ( ) administración remota del switch
- ( ) Traducir nombres de dominios en direcciones IP
- ( ) prueba de conectividad de extremo a extremo

12. ¿Qué dos funciones se proporcionan a los usuarios mediante la función de ayuda sensible al contexto de la CLI de Cisco IOS?(Escoja dos.)

Tema 2.3.0 - La ayuda contextual proporciona al usuario una lista de comandos y los argumentos asociados con dichos comandos en el modo actual de un dispositivo de red. Un corrector de sintaxis proporciona comprobaciones de errores en los comandos enviados y la tecla TAB se puede utilizar para completar el comando si se introduce un comando parcial.

- [ ] proporcionar un mensaje de error cuando se envía un comando incorrecto
- [x] mostrar una lista de todos los comandos disponibles en el modo actual
- [ ] permitiendo al usuario completar el resto de un comando abreviado con la tecla TAB
- [x] determinar qué opción, palabra clave o argumento está disponible para el comando introducido
- [ ] seleccionar el mejor comando para realizar una tarea

13. ¿Qué ubicación de memoria en un router o switch de Cisco almacena el archivo de configuración de inicio?

Tema 2.5.0 - El archivo de configuración de inicio de un router o switch Cisco se almacena en NVRAM, que es memoria no volátil.

- ( ) RAM
- ( ) ROM
- (●) NVRAM
- ( ) Memoria flash

14. ¿A qué subred pertenece la dirección IP 10.1.100.50 si se utiliza una máscara de subred 255.255.0.0?

Tema 2.6.0 - El propósito de una máscara de subred es separar la parte de red de la dirección de la parte de host de la dirección IP. La parte de red de la dirección IP se identifica por todos los binarios 1s de la máscara de subred. El uso de una máscara de subred 255.255.0.0 identifica los dos primeros octetos de la dirección IP como parte de la red.

- (●) 10.1.0.0
- ( ) 10.0.0.0
- ( ) 10.1.100.32
- ( ) 10.1.100.0

Correct

You have successfully identified the correct answers.

You got 14 out of 14 questions correct.

1. Which statement is true about the running configuration file in a Cisco IOS device?

Topic 2.5.0 - As soon as configuration commands are entered into a router, they modify the device immediately. Running configuration files can not be deleted nor are they saved automatically.

- (●) It affects the operation of the device immediately when modified.
- ( ) It is stored in NVRAM.
- ( ) It should be deleted using the **erase running-config** command.
- ( ) It is automatically saved when the router reboots.

2. Which two statements are true regarding the user EXEC mode? (Choose two.)

Topic 2.2.0 - User EXEC mode limits access to some **show** and **debug** commands. It is the first level of user interface encountered when configuring a router and is intended for investigation of certain functions of the device. The User EXEC prompt is identified with the ">" symbol.

- [ ] All router commands are available.
- [ ] Global configuration mode can be accessed by entering the **enable** command.
- [x] The device prompt for this mode ends with the ">" symbol.
- [ ] Interfaces and routing protocols can be configured.
- [x] Only some aspects of the router configuration can be viewed.

3. Which type of access is secured on a Cisco router or switch with the **enable secret** command?

Topic 2.4.0 - The **enable secret** command secures access to the privileged EXEC mode of a Cisco router or switch.

- ( ) virtual terminal
- (●) privileged EXEC
- ( ) AUX port
- ( ) console line

4. What is the default SVI on a Cisco switch?

Topic 2.6.0 - Layer 2 switches use switch virtual interfaces (SVIs) to provide a means for remote access over IP. The default SVI on a Cisco switch is VLAN1.

- (●) VLAN1
- ( ) VLAN99
- ( ) VLAN100
- ( ) VLAN999

5. When a hostname is configured through the Cisco CLI, which three naming conventions are part of the guidelines? (Choose three.)

Topic 2.4.0 - A hostname can be configured with upper or lower case characters and should end with a letter or digit, not a special character. A hostname should start with a letter and no space is allowed for a hostname.

- [x] the hostname should be fewer than 64 characters in length
- [ ] the hostname should be written in all lower case characters
- [x] the hostname should contain no spaces
- [ ] the hostname should end with a special character
- [x] the hostname should begin with a letter

6. What is the function of the shell in an OS?

Topic 2.1.0 - Most operating systems contain a shell and a kernel. The kernel interacts with the hardware and the shell interfaces between the kernel and the users.

- ( ) It interacts with the device hardware.
- (•) It interfaces between the users and the kernel.
- ( ) It provides dedicated firewall services.
- ( ) It provides the intrusion protection services for the device.

7. A router with a valid operating system contains a configuration file stored in NVRAM. The configuration file has an enable secret password but no console password. When the router boots up, which mode will display?

Topic 2.2.0 - If a Cisco IOS device has a valid IOS and a valid configuration file, it will boot into user EXEC mode. A password will be required to enter privileged EXEC mode.

- ( ) global configuration mode
- ( ) setup mode
- ( ) privileged EXEC mode
- (•) user EXEC mode

8. An administrator has just changed the IP address of an interface on an IOS device. What else must be done in order to apply those changes to the device?

Topic 2.5.0 - Changes to router and switch configurations take effect as soon as the command is entered. For this reason, it is very important that changes to live production devices are always carefully planned before being implemented. If commands are entered that render the device unstable or inaccessible, the device may have to be reloaded, resulting in network downtime.

- ( ) Copy the running configuration to the startup configuration file.
- ( ) Copy the information in the startup configuration file to the running configuration.
- ( ) Reload the device and type **yes** when prompted to save the configuration.
- (•) Nothing must be done. Changes to the configuration on an IOS device take effect as soon as the command is typed correctly and the Enter key has been pressed.

9. Which memory location on a Cisco router or switch will lose all content when the device is restarted?

Topic 2.5.0 - RAM is volatile memory and will lose all contents if the router or switch is restarted or shutdown.

- ROM
- flash
- NVRAM
- RAM

10. Why would a technician enter the command **copy startup-config running-config**?

Topic 2.5.0 - Usually, changes are made to a running configuration in RAM and copied to NVRAM. However, in this case, the technician wants to copy a previously saved configuration from NVRAM into RAM in order to make changes to it.?

- to remove all configurations from the switch
- to save an active configuration to NVRAM
- to copy an existing configuration into RAM
- to make a changed configuration the new startup configuration

11. Which functionality is provided by DHCP?

Topic 2.7.0 - DHCP provides dynamic and automatic IP address assignment to hosts.

- automatic assignment of an IP address to each host
- remote switch management
- translation of IP addresses to domain names
- end-to-end connectivity test

12. Which two functions are provided to users by the context-sensitive help feature of the Cisco IOS CLI? (Choose two.)

Topic 2.3.0 - Context-sensitive help provides the user with a list of commands and the arguments associated with those commands within the current mode of a networking device.
A syntax checker provides error checks on submitted commands and the TAB key can be used for command completion if a partial command is entered.

- [ ] providing an error message when a wrong command is submitted
- [x] displaying a list of all available commands within the current mode
- [ ] allowing the user to complete the remainder of an abbreviated command with the TAB key
- [x] determining which option, keyword, or argument is available for the entered command
- [ ] selecting the best command to accomplish a task

13. Which memory location on a Cisco router or switch stores the startup configuration file?

Topic 2.5.0 - The startup configuration file of a Cisco router or switch is stored in NVRAM, which is nonvolatile memory.

- RAM
- ROM
- NVRAM
- flash

14. To what subnet does the IP address 10.1.100.50 belong if a subnet mask of 255.255.0.0 is used?

Topic 2.6.0 - The purpose of a subnet mask is to separate the network portion of the address from the host portion of the IP address. The network portion of the IP address is identified by all binary 1s in the subnet mask. Using a subnet mask of 255.255.0.0 identifies the first two octets of the IP address as the network portion.

- 10.1.0.0
- 10.0.0.0
- 10.1.100.32
- 10.1.100.0

Capítulo 3_Protocolos y modelos Introducción

3.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Protocolos y modelos!

Usted conoce los componentes básicos de una red simple, así como la configuración inicial. Pero después de haber configurado y conectado estos componentes, ¿cómo sabe que trabajarán juntos? ¡Protocolos! Los protocolos son conjuntos de reglas acordadas que han sido creadas por organizaciones de normalización. Pero, como no puedes tomar una regla y mirarla de cerca, ¿cómo entiendes realmente por qué hay tal regla y qué se supone que debe hacer? ¡Modelos! Los modelos le dan una forma de visualizar las reglas y su lugar en su red. Este módulo le ofrece una visión general de los protocolos y modelos de red. ¡Estás a punto de tener una comprensión mucho más profunda de cómo funcionan las redes en realidad!

3.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Protocolos y modelos

Objetivos del módulo: Explique cómo los protocolos de red permiten que los dispositivos tengan acceso a recursos de red local y remota.

Título del tema	Objetivo del tema
Las reglas	Describa los tipos de reglas que se necesitan para que comunicarse se realice correctamente.
Protocolos	Explique por qué los protocolos son necesarios en la comunicación de redes.
Suites de protocolos	Explique el propósito de adherirse a una suite de protocolos.
Organizaciones estándares	Explique la función de las organizaciones de estandarización en el establecimiento de protocolos para la Interoperabilidad de la red.
Modelos de referencia	Explique la forma en que se utilizan los modelos TCP/IP y OSI para facilitar la estandarización en el proceso de comunicación.
Encapsulamiento de datos	Explique la forma en que el encapsulamiento de datos permite que estos se transporten a través e inalámbrica.
Acceso a los datos	Explique la forma en que los hosts locales acceden a recursos locales en una red.

3.0.3

Actividad de clase: diseño de un sistema de comunicaciones

Acaba de adquirir un automóvil nuevo para uso personal. Después de conducir el automóvil durante alrededor de una semana, descubre que no funciona correctamente. Analiza el problema con varios de sus pares y decide llevarlo un taller de reparaciones de automóviles muy recomendado. Se trata del único taller de reparaciones que le queda cerca.

Cuando llega al taller de reparaciones, advierte que todos los mecánicos hablan otro idioma. Tiene dificultades para explicar los problemas de funcionamiento del automóvil, pero es realmente necesario realizar las reparaciones. No está seguro de poder conducirlo de regreso a su hogar para buscar otras opciones.

Debe encontrar una manera de trabajar con el taller para asegurarse de que el automóvil se repare correctamente.

¿Cómo se comunicará con los mecánicos de esa empresa? Diseñe un modelo de comunicaciones para asegurar que el vehículo se repare correctamente.

Diseño de un sistema de comunicaciones

Protocolos y modelos / Las reglas

Las reglas

3.1.1

Vídeo - Dispositivos en una burbuja

Haga clic en Reproducir en la figura para ver un vídeo que explica cómo funciona un dispositivo de red dentro de una red.

3.1.2

Fundamentos de la comunicación

Las redes pueden variar en lo que respecta al tamaño, la forma y la función. Una red puede ser tan compleja como los dispositivos conectados a través de Internet, o tan simple como dos PC conectadas directamente entre sí mediante un único cable, o puede tener cualquier grado de complejidad intermedia. Sin embargo, realizar simplemente la conexión física por cable o inalámbrica entre los terminales no es suficiente para habilitar la comunicación. Para que se produzca la comunicación, los dispositivos deben saber "cómo" comunicarse.

Las personas intercambian ideas mediante diversos métodos de comunicación. Sin embargo, todos los métodos de comunicación tienen tres elementos en común:

- **Los orígenes de los mensajes** - Los orígenes de los mensajes son las personas o los dispositivos electrónicos que deben enviar un mensaje a otras personas o dispositivos.
- **Destino del mensaje(recibidor)** - El destino recibe el mensaje y lo interpreta.
- **Canal** - está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.

3.1.3

Protocolos de comunicación

El envío de este mensaje, ya sea mediante comunicación cara a cara o a través de una red, está regido por reglas llamadas “protocolos”. Estos protocolos son específicos del tipo de método de comunicación en cuestión. En nuestra comunicación personal diaria, las reglas que utilizamos para comunicarnos por un medio, como una llamada telefónica, no son necesariamente las mismas que los protocolos para utilizar otro medio, como enviar una carta.

El proceso de enviar una carta es similar a la comunicación que ocurre en las redes informáticas.

Haga clic en cada botón para obtener una analogía y un ejemplo de red del proceso de comunicación.

Haga clic en Reproducir en la figura para ver una animación de dos personas que se comunican cara a cara.

3.1.4

Establecimiento de reglas

Antes de comunicarse entre sí, las personas deben utilizar reglas o acuerdos establecidos que rijan la conversación. Considere este mensaje, por ejemplo:

```
humanos comunicaciones las entre los gobiernan reglas. Es muydifícilcomprender mensajes que no están correctamente formateados y quenosiguen las reglas y los protocolos establecidos. La estructura de la gramática, el lenguaje, la puntuación y la oración hace que la configuración humana sea comprensible para muchos individuos diferentes.
```

Observe cómo es difícil leer el mensaje porque no está formateado correctamente. Debe escribirse usando reglas (es decir, protocolos) que son necesarias para una comunicación efectiva. El ejemplo muestra el mensaje que ahora está correctamente formateado para el lenguaje y la gramática.

```
Las reglas gobiernan las comunicaciones entre los humanos. Es muy difícil comprender mensajes que no están correctamente formateados y que no siguen las reglas y los protocolos establecidos. La estructura de la gramática, el idioma, la puntuación y la oración hacen que la configuración sea humanamente comprensible para muchos individuos diferentes.
```

Los protocolos deben tener en cuenta los siguientes requisitos para entregar correctamente un mensaje que sea comprendido por el receptor:

- Un emisor y un receptor identificados
- Idioma y gramática común
- Velocidad y momento de entrega
- Requisitos de confirmación o acuse de recibo

3.1.5

Requisitos de protocolo de red

Los protocolos utilizados en las comunicaciones de red comparten muchos de estos fundamentos. Además de identificar el origen y el destino, los protocolos informáticos y de

red definen los detalles sobre la forma en que los mensajes se transmiten a través de una red. Los protocolos informáticos comunes incluyen los siguientes requisitos:

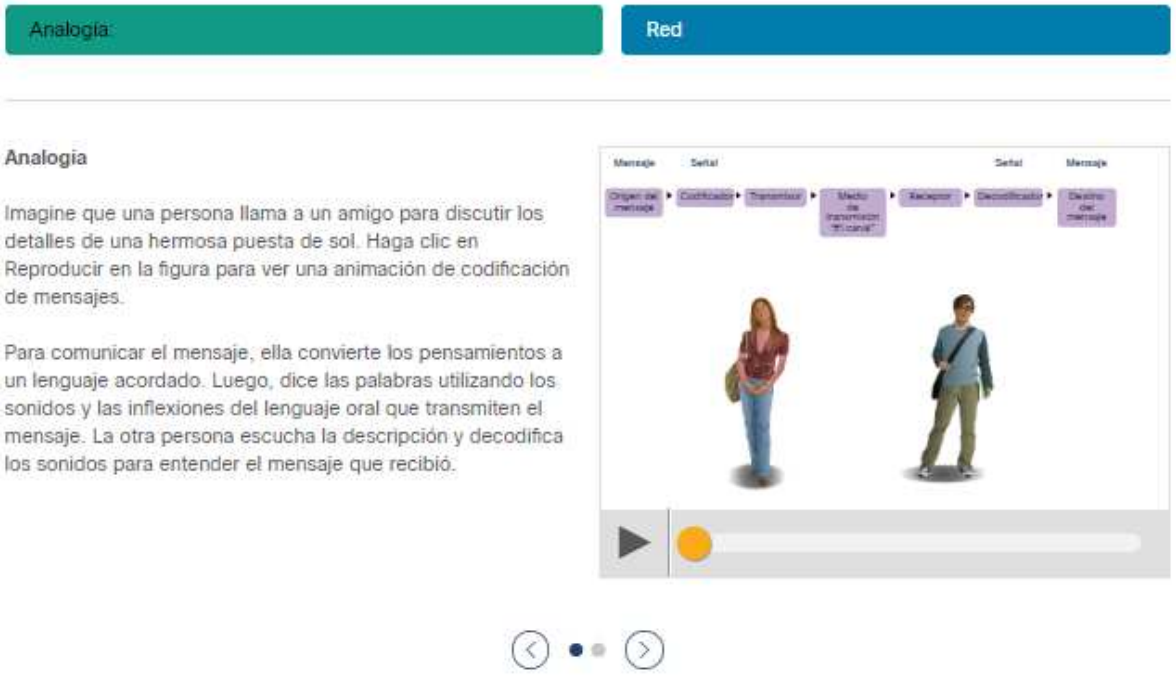
- Codificación de los mensajes
- Formato y encapsulamiento del mensaje
- Tamaño del mensaje
- Sincronización del mensaje
- Opciones de entrega del mensaje

3.1.6

Codificación de los mensajes

Uno de los primeros pasos para enviar un mensaje es codificarlo. La codificación es el proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación revierte este proceso para interpretar la idea.

Haga clic en cada botón para obtener una analogía y un ejemplo de red de codificación de mensajes.

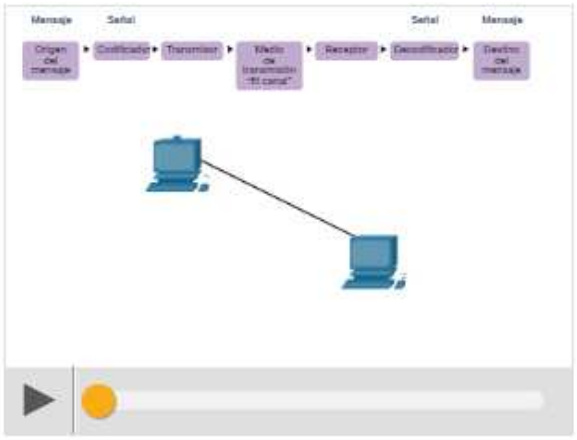


Analogía: | Red

Red

Haga clic en Reproducir en la figura para ver una animación de codificación de mensajes que también se produce en la comunicación del equipo.

La codificación entre hosts debe tener el formato adecuado para el medio. El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit está codificado en un patrón de voltajes en cables de cobre, luz infrarroja en fibras ópticas o microondas para sistemas inalámbricos. El host de destino recibe y decodifica las señales para interpretar el mensaje.



3.1.7

Formato y encapsulamiento del mensaje

Cuando se envía un mensaje desde el origen hacia el destino, se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje.

Haga clic en cada botón para obtener una analogía y un ejemplo de red de formato y encapsulación de mensajes.

Analogía: | Red

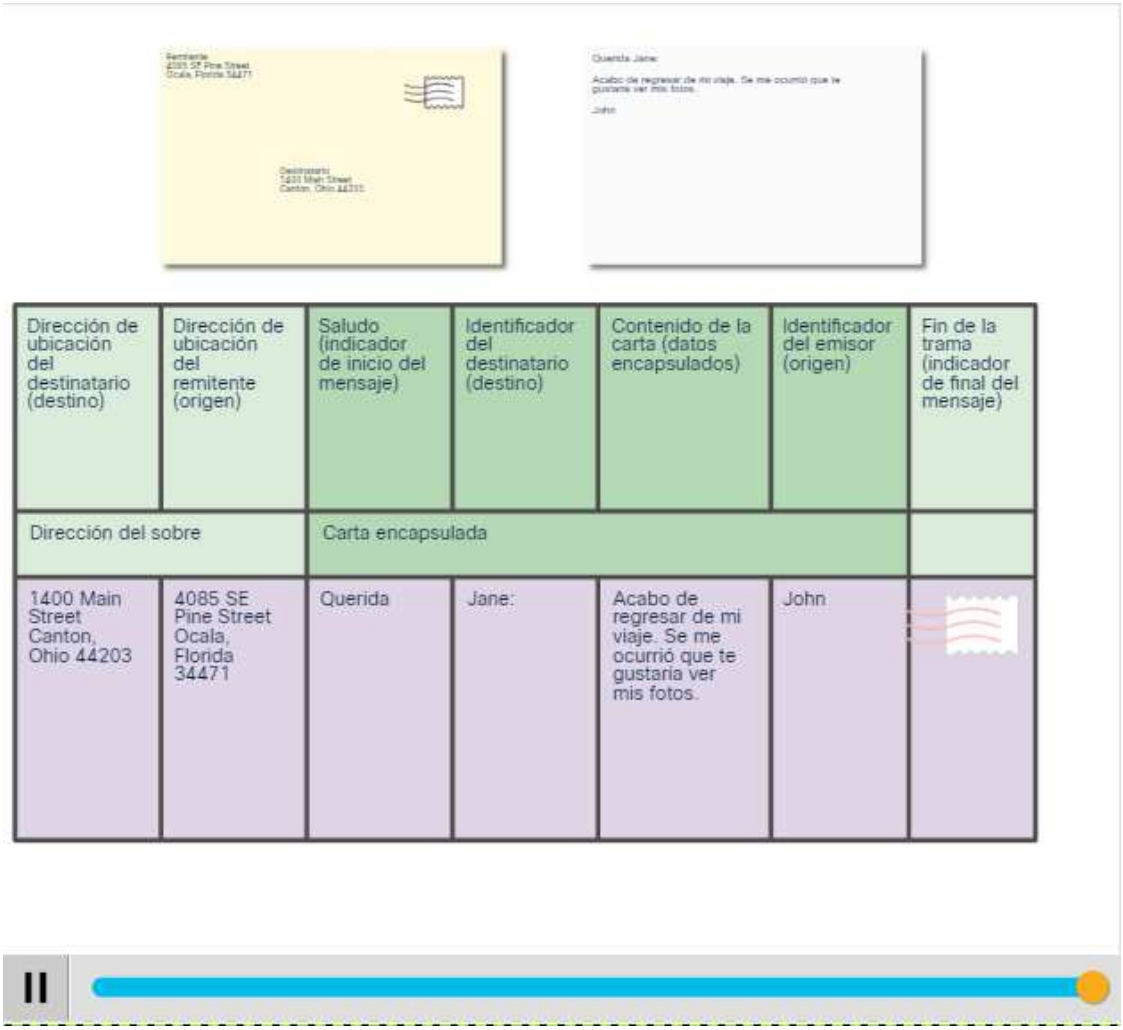
Analogía

Un ejemplo común de requerir el formato correcto en las comunicaciones humanas es cuando se envía una carta. Haga clic en Reproducir en la figura para ver una animación de formato y encapsulación de una letra.

El sobre tiene la dirección del emisor y la del receptor, cada una escrita en el lugar adecuado del sobre. Si la dirección de destino y el formato no son correctos, la carta no se entrega.

El proceso que consiste en colocar un formato de mensaje (la carta) dentro de otro formato de mensaje (el sobre) se denomina encapsulamiento. Cuando el destinatario revierte este proceso y quita la carta del sobre se produce el desencapsulamiento del mensaje.

Los campos de un paquete IPv6 incluyendo la dirección IP de origen y la dirección IP de destino.

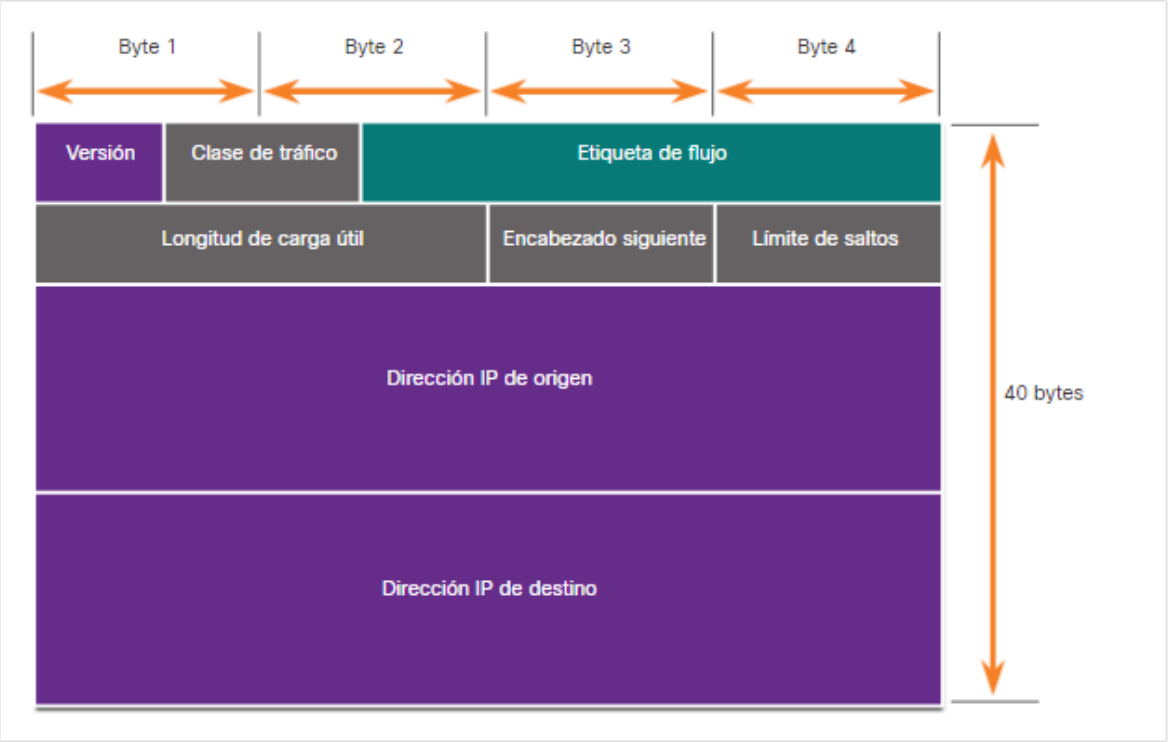


Red

Semejante a enviar una carta. Un mensaje que se envía a través de una red de computadoras sigue reglas de formato específicas para que pueda ser entregado y procesado.

Protocolo de Internet (IP) es un protocolo con una función similar a la del ejemplo sobre. En la figura, los campos del paquete de Protocolo de Internet versión 6 (IPv6) identifican el origen del paquete y su destino. IP es responsable de enviar un mensaje desde el origen del mensaje al destino a través de una o más redes.

Nota: Los campos del paquete IPv6 se analizan en detalle en otro módulo.



3.1.8

Tamaño del mensaje

Otra regla de comunicación es el tamaño del mensaje.

Haga clic en cada botón para ver una analogía y un ejemplo de red del tamaño del mensaje.

Analogía | Red

Analogía

Haga clic en Reproducir en la figura para ver una animación del tamaño del mensaje en las comunicaciones cara a cara.

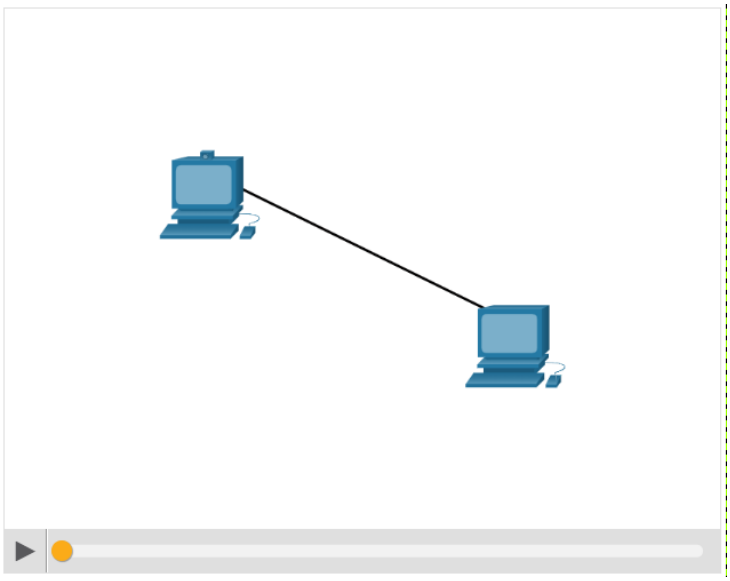
Cuando las personas se comunican, los mensajes que envían, normalmente, están divididos en fragmentos más pequeños u oraciones. El tamaño de estas oraciones se limita a lo que la persona que recibe el mensaje puede procesar por vez, como se muestra en la figura. También hace que sea más fácil para el receptor leer y comprender.

Analogía: Red

Red

La codificación también tiene lugar en la comunicación por computadora. Haga clic en Reproducir en la figura para ver una animación del tamaño del mensaje en redes informáticas.

La codificación entre hosts debe tener el formato adecuado para el medio. El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje.



3.1.9

Sincronización del mensaje

El tiempo de los mensajes también es muy importante en las comunicaciones de red. El tiempo de los mensajes incluye lo siguiente:

Control de **flujo -** Este es el proceso de gestión de la velocidad de transmisión de datos. La sincronización también afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse. Por ejemplo, si una persona habla demasiado rápido, la otra persona tendrá dificultades para escuchar y comprender el mensaje. En la comunicación de red, existen protocolos de red utilizados por los dispositivos de origen y destino para negociar y administrar el flujo de información.

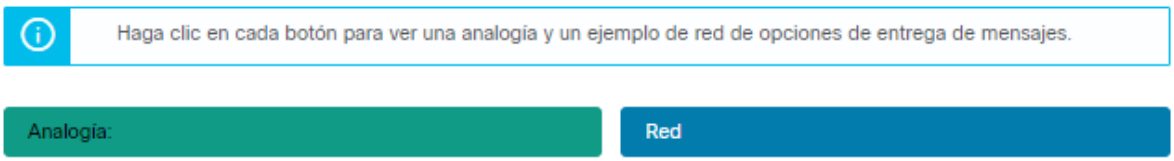
- **Tiempo de espera de respuesta (Response Timeout) -** Si una persona hace una pregunta y no escucha una respuesta antes de un tiempo aceptable, la persona supone que no habrá ninguna respuesta y reacciona en consecuencia. La persona puede repetir la pregunta o puede continuar la conversación. Los hosts de las redes tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta.
- **El método de acceso-** Determina en qué momento alguien puede enviar un mensaje. Haga clic en Reproducir en la figura para ver una animación de dos personas hablando al mismo tiempo, luego se produce una "colisión de información" y es necesario que las dos retrocedan y comiencen de nuevo. Del mismo modo, cuando un dispositivo desea transmitir en una LAN inalámbrica, es necesario que la tarjeta de interfaz de red (NIC) WLAN determine si el medio inalámbrico está disponible.

La animación muestra a una mujer y un hombre hablando al mismo tiempo. La mujer dice ¿A qué hora es la película? y el hombre dice ¿Cuándo nos reuniremos para cenar? Porque hablaron simultáneamente, ni entendieron al otro y ambos dicen «Lo siento»? No te entendí.

3.1.10

Opciones de entrega del mensaje

Un mensaje se puede entregar de diferentes maneras.



Unidifusión (Unicast)

Multidifusión (Multicast)

Transmisión/Difusión (Broadcast)

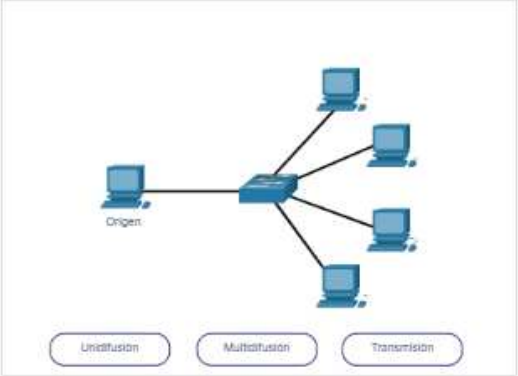
Analogía:	Red

Red

Las comunicaciones de red tienen opciones de entrega similares para comunicarse. Como se muestra en la figura, hay tres tipos de comunicaciones de datos:

- **Unicast** - La información se transmite a un único dispositivo final.
- **Multicast** - La información se transmite a uno o varios dispositivos finales.
- **Transmisión** - La información se transmite a todos los dispositivos finales.

Haga clic en los botones de unidifusión, multidifusión y difusión de la figura para ver un ejemplo de cada uno.

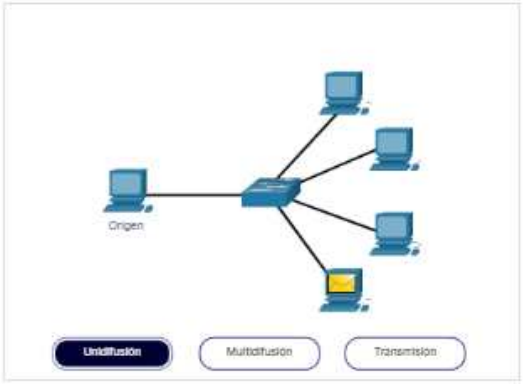


Red

Las comunicaciones de red tienen opciones de entrega similares para comunicarse. Como se muestra en la figura, hay tres tipos de comunicaciones de datos:

- **Unicast** - La información se transmite a un único dispositivo final.
- **Multicast** - La información se transmite a uno o varios dispositivos finales.
- **Transmisión** - La información se transmite a todos los dispositivos finales.

Haga clic en los botones de unidifusión, multidifusión y difusión de la figura para ver un ejemplo de cada uno.

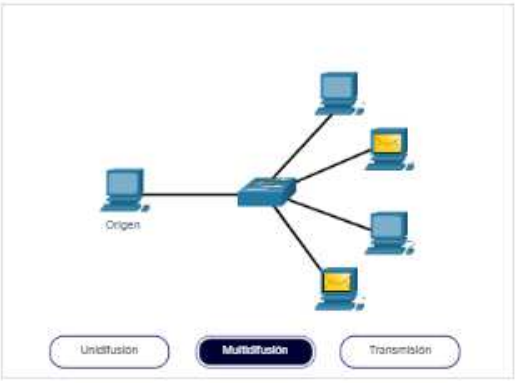


Red

Las comunicaciones de red tienen opciones de entrega similares para comunicarse. Como se muestra en la figura, hay tres tipos de comunicaciones de datos:

- **Unicast** - La información se transmite a un único dispositivo final.
- **Multicast** - La información se transmite a uno o varios dispositivos finales.
- **Transmisión** - La información se transmite a todos los dispositivos finales.

Haga clic en los botones de unidifusión, multidifusión y difusión de la figura para ver un ejemplo de cada uno.

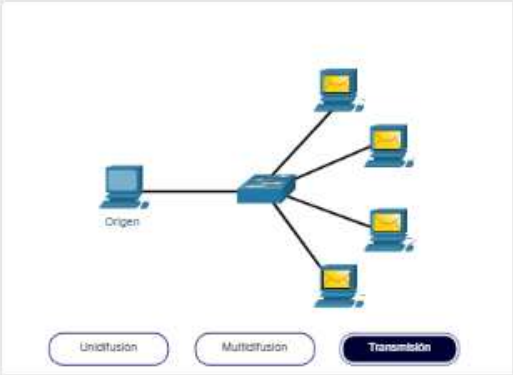


Red

Las comunicaciones de red tienen opciones de entrega similares para comunicarse. Como se muestra en la figura, hay tres tipos de comunicaciones de datos:

- **Unicast** - La información se transmite a un único dispositivo final.
- **Multicast** - La información se transmite a uno o varios dispositivos finales.
- **Transmisión** - La información se transmite a todos los dispositivos finales.

Haga clic en los botones de unidifusión, multidifusión y difusión de la figura para ver un ejemplo de cada uno.

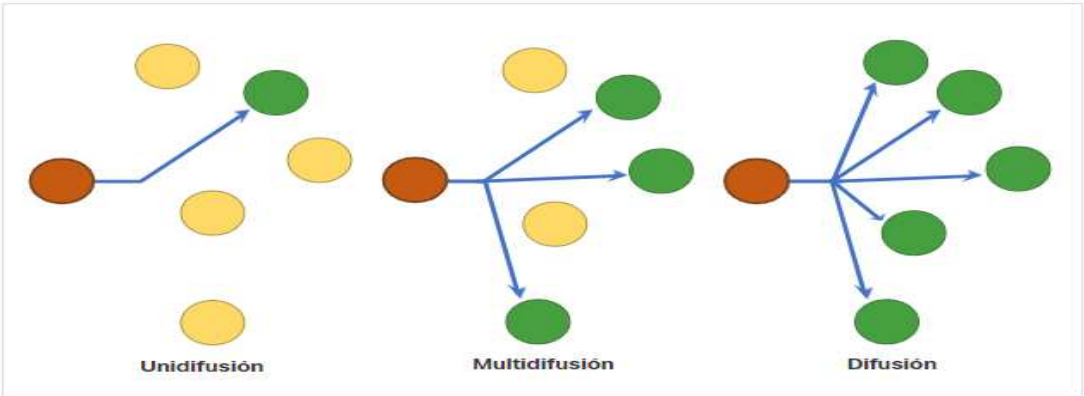


3.1.11

Una nota sobre el icono de nodo

Los documentos y topologías de red suelen representar dispositivos de red y finales mediante un icono de nodo. Los nodos se suelen representar como un círculo. La figura muestra una comparación de las tres opciones de entrega diferentes utilizando iconos de nodo en lugar de iconos de ordenador.

La figura utiliza círculos que representan nodos de red para ilustrar las tres opciones de entrega de mensajes diferentes. Hay tres topologías mostradas de izquierda a derecha. La topología de la izquierda representa un mensaje de unidifusión y consta de un nodo rojo, un nodo verde y cuatro nodos amarillos. Tiene una flecha desde el nodo rojo que conduce al nodo verde. La topología central representa un mensaje de multidifusión y consta de un nodo rojo, tres nodos verdes y dos nodos amarillos. Tiene una flecha desde el nodo rojo que conduce a cada uno de los nodos verdes. La topología de la derecha representa una difusión. Tiene un nodo rojo y cinco nodos verdes. Tiene una flecha desde el nodo rojo que conduce a cada uno de los nodos verdes.



3.1.12

Verifique su comprensión- Las reglas

Verifique su comprensión de las reglas de comunicación exitosa eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. One of the first steps to sending a message is encoding. During the encoding process, information is converted from its original form into an acceptable form for transmission.
2. Messages sent over a computer network must be in the correct format for them to be delivered and processed. Part of the formatting process is properly identifying the source of the message and its destination.
3. Flow control is the managing of the rate of transmission. Response timeout is how long to wait for responses. Access methods determine when someone can send a message. These are the three components of message timing.
4. Multicast messages are addressed for transmission to one or more end devices on a network. Broadcast messages are addressed for transmission to all devices on the network. Unicast messages are addressed for transmission to one device on the network.

You got 4 out of 4 questions correct.

1. What is the process of converting information into the proper form for transmission?

You got it!

- ○ Formatting
- ◉ Encoding
- ○ Encapsulation

2. Which step of the communication process is concerned with properly identifying the address of the sender and receiver?

You got it!

- ◉ Formatting
- ○ Encoding
- ○ Encapsulation

3. Which three are components of message timing? (Choose three.)

You got it!

- [x] Flow control
- [ ] Sequence numbers
- [x] Access method
- [ ] Retransmit time
- [x] Response timeout

4. Which delivery method is used to transmit information to one or more end devices, but not all devices on the network?

You got it!

- ( ) Unicast
- (•) Multicast
- ( ) Broadcast

Correcto

Identificó bien las respuestas correctas.

1. Uno de los primeros pasos para enviar un mensaje es codificarlo. Durante el proceso de codificación, la información se convierte de su forma original a una forma aceptable para su transmisión.
2. Los mensajes enviados a través de una red informática deben estar en el formato correcto para que se entreguen y procesen. Parte del proceso de formateo es identificar correctamente el origen del mensaje y su destino.
3. El control de flujo es la gestión de la velocidad de transmisión. El tiempo de espera de respuesta es el tiempo que se espera a las respuestas. El método de acceso-determina en qué momento alguien puede enviar un mensaje. Estos son los tres componentes de la sincronización de mensajes.
4. Los mensajes de multidifusión se dirigen para su transmisión a uno o varios dispositivos finales de una red. Los mensajes de difusión se dirigen para su transmisión a todos los dispositivos de la red. Los mensajes de unidifusión se dirigen para su transmisión a un dispositivo de la red.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuál es el proceso de convertir la información en la forma adecuada para la transmisión?

¡Lo tienes!

- ○ Formateo
- ◉ Codificación
- ○ Encapsulamiento

2. ¿Qué paso del proceso de comunicación se ocupa de identificar correctamente la dirección del remitente y del destinatario?

¡Lo tienes!

- ◉ Formateo
- ○ Codificación
- ○ Encapsulamiento

3. ¿Cuáles son los tres componentes de la sincronización de mensajes? (Escoja tres opciones).

¡Lo tienes!

- ☑ Control de flujo
- ☐ Números de secuencia
- ☑ Método de acceso
- ☐ Tiempo de retransmisión
- ☑ Tiempo de espera de respuesta

4. ¿Qué método de entrega se utiliza para transmitir información a uno o más dispositivos finales, pero no a todos los dispositivos de la red?

¡Lo tienes!

- ○ Unidifusión
- ◉ Multidifusión
- ○ Difusión

Protocolos y modelos / Protocolos

Protocolos

3.2.1

Descripción general del protocolo de red

Usted sabe que para que los dispositivos finales puedan comunicarse a través de una red, cada dispositivo debe cumplir el mismo conjunto de reglas. Estas reglas se denominan protocolos y tienen muchas funciones en una red. En este tema se ofrece una descripción general de los protocolos de red.

Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Los protocolos son implementados por dispositivos finales y dispositivos intermediarios en software, hardware o ambos. Cada protocolo de red tiene su propia función, formato y reglas para las comunicaciones.

En la tabla se enumeran los distintos tipos de protocolos que se necesitan para habilitar las comunicaciones en una o más redes.

Tipo de protocolo	Descripción
Protocolos de comunicaciones de red	Los protocolos permiten que dos o más dispositivos se comuniquen a través de uno o más compatibles. La familia de tecnologías Ethernet implica una variedad de protocolos como IP, Protocolo de control de transmisión (TCP), HyperText Protocolo de transferencia (HTTP) y muchos más.
Protocolos de seguridad de red	Los protocolos protegen los datos para proporcionar autenticación, integridad de los datos y Cifrado de datos Ejemplos de protocolos seguros incluyen Secure Shell (SSH), Secure Sockets Layer (SSL) y Capa de transporte Security (TLS).
Protocolos de routing	Los protocolos permiten a los routeres intercambiar información de ruta, comparar ruta y, a continuación, seleccionar la mejor ruta al destino e inalámbrica. Ejemplos de protocolos de enrutamiento incluyen Abrir ruta más corta primero OSPF y Protocolo de puerta de enlace de borde (BGP).
Protocolos de Detección de servicios	Los protocolos se utilizan para la detección automática de dispositivos o servicios. Entre los ejemplos de protocolos de

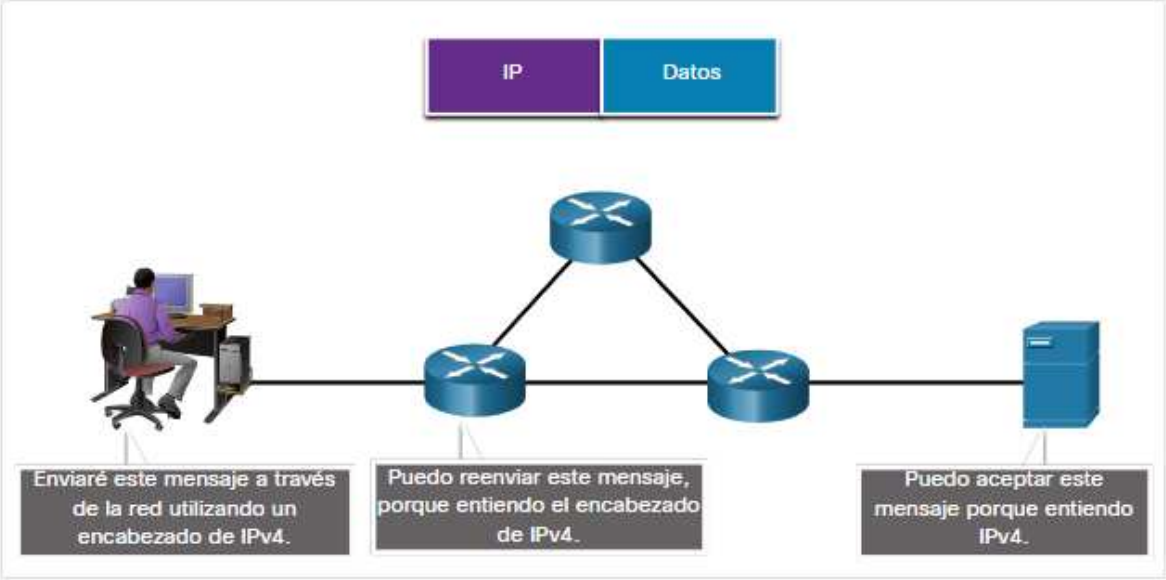
Tipo de protocolo	Descripción
	descubrimiento de servicios se incluyen Dynamic Host Protocolo de configuración (DHCP) que descubre servicios para la dirección IP y Sistema de nombres de dominio (DNS) que se utiliza para realizar traducción de nombre a dirección IP.

3.2.2

Funciones de protocolo de red

Los protocolos de comunicación de red son responsables de una variedad de funciones necesarias para las comunicaciones de red entre dispositivos finales. Por ejemplo, en la figura, ¿cómo envía el equipo un mensaje, a través de varios dispositivos de red, al servidor?

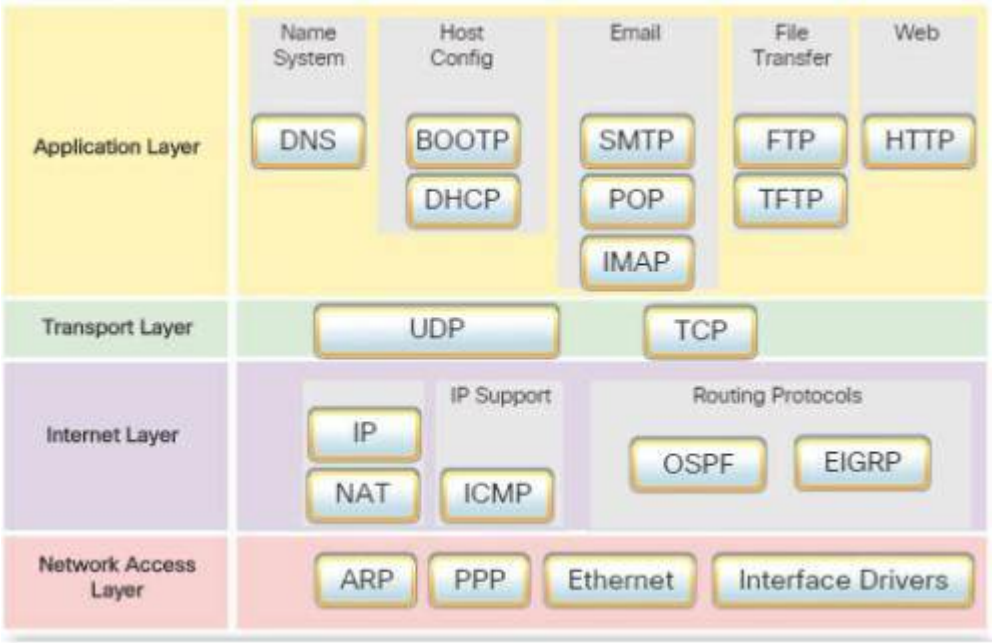
La figura muestra cómo se puede utilizar el protocolo IPv4 para enviar un mensaje desde un equipo a través de una red a un servidor. En el centro de la figura hay tres routeres conectados entre sí en un triángulo. El router de la izquierda está conectado a una computadora. El Router a la derecha está conectado a un servidor. Un mensaje abajo de la computadora dice: Enviaré este mensaje a través de la red utilizando un encabezado de IPv4. Se lee un mensaje debajo del router adjunto: puedo reenviar este mensaje porque entiendo el encabezado IPv4. Un mensaje debajo del servidor dice: Puedo aceptar este mensaje porque entiendo IPv4.



Enviaré este mensaje a través de la red utilizando un encabezado de IPv4.Puedo reenviar este mensaje, porque entiendo el encabezado de IPv4.Puedo aceptar este mensaje porque entiendo IPv4.

Los equipos y dispositivos de red utilizan protocolos acordados para comunicarse. La tabla enumera las funciones de estos protocolos.

Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet PPP Frame Relay ATM WLAN			

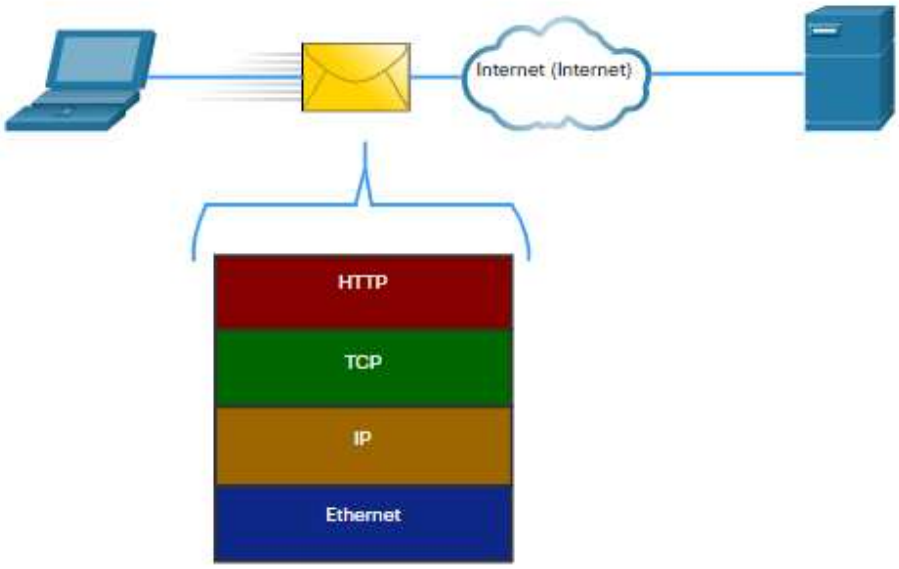


3.2.3

Interacción de protocolos

Un mensaje enviado a través de una red informática normalmente requiere el uso de varios protocolos, cada uno con sus propias funciones y formato. La figura muestra algunos

protocolos de red comunes que se utilizan cuando un dispositivo envía una solicitud a un servidor web para su página web.



Un pequeño diagrama de red muestra, de izquierda a derecha, un portátil conectado a la nube de Internet que está conectado a un servidor. Un sobre está cruzando la conexión entre el portátil y la nube. Debajo del sobre hay una lista de protocolos utilizados cuando un dispositivo envía una solicitud a un servidor web para una página web. El texto en la parte inferior de la figura describe estos protocolos y dice: Protocolo de transferencia de hipertexto (HTTP) - Este protocolo gobierna la forma en que interactúan un servidor web y un cliente web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor. Protocolo de control de transmisión (TCP) - Este protocolo administra las conversaciones individuales. TCP se encarga de garantizar la entrega fiable de la información y de gestionar el control de flujo entre los dispositivos finales. Protocolo de Internet (IP) - Este protocolo es responsable de entregar los mensajes del remitente al receptor. IP es utilizado por los routeres para reenviar los mensajes a través de varias redes. Ethernet: este protocolo es responsable de la entrega de mensajes de una NIC a otra NIC en la misma red de área local (LAN) Ethernet.

Los protocolos de la figura se describen de la siguiente manera:

- **Protocolo de Transferencia de Hipertexto (HTTP)** - este protocolo de aplicación rige la manera en que interactúan un servidor web y un cliente web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el

software del servidor web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor.

- **Protocolo de control de transmisión (TCP)** - Este protocolo administra las conversaciones individuales. TCP se encarga de garantizar la entrega fiable de la información y de gestionar el control de flujo entre los dispositivos finales.
- **Protocolo de Internet (IP) -** Este protocolo es responsable de entregar los mensajes del remitente al receptor. IP es utilizado por los enrutadores para reenviar los mensajes a través de varias redes.
- **Ethernet** \ - Este protocolo es responsable de la entrega de mensajes de una NIC a otra NIC en la misma red de área local (LAN) Ethernet.

3.2.4

Verifique su compresión: Protocolos

Compruebe su comprensión de los protocolos utilizados en la comunicación de red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. BGP y OSPF son protocolos de enrutamiento. Permiten a los routeres intercambiar información de ruta para llegar a redes remotas.
2. Los protocolos de detección de servicios, como DNS y DHCP, permiten la detección automática del servicio. DHCP se utiliza para detectar servicios para la asignación automática de direcciones IP y DNS para los servicios de resolución de nombres a direcciones IP.
3. La secuenciación identifica o etiqueta de forma exclusiva cada segmento transmitido con un número de secuencia utilizado por el receptor para volver a ensamblar los segmentos en el orden adecuado.
4. Transmission Control Protocol (TCP) gestiona la conversación entre los dispositivos finales y garantiza la entrega fiable de la información.

Has tenido 4 respuestas correctas de 4.

1. BGP and OSPF are examples of which type of protocol?

You got it!

- ○ network communication
- ○ network security
- ◉ routing
- ○ service discovery

2. Which two protocols are service discovery protocols? (Choose two.)

You got it!

- ☑ DNS
- ☐ TCP
- ☐ SSH
- ☑ DHCP

3. What is the purpose of the sequencing function in network communication?

You got it!

- ◉ to uniquely label transmitted segments of data for proper reassembly by the receiver
- ○ to determine if data is corrupted during transmission
- ○ to ensure data flows at an efficient rate between sender and receiver
- ○ to guarantee delivery of data

4. This protocol is responsible for guaranteeing the reliable delivery of information.

You got it!

- ◉ TCP
- ○ IP
- ○ HTTP
- ○ Ethernet

1. BGP y OSPF son ejemplos de qué tipo de protocolo?

¡Lo tienes!

- ○ Comunicaciones de red
- ○ Seguridad de la red
- ◉ enrutamiento
- ○ Detección de servicios

2. ¿Cuáles dos protocolos son protocolos de descubrimiento de servicios? (Elija dos opciones).

¡Lo tienes!

- ☑ DNS
- ☐ TCP
- ☐ SSH
- ☑ DHCP

3. ¿Cuál es el propósito de la función de secuenciación en la comunicación de red?

¡Lo tienes!

- ◉ para etiquetar de forma exclusiva los segmentos de datos transmitidos para que el receptor lo vuelva a montar correctamente.
- ○ para determinar si los datos están dañados durante la transmisión
- ○ para garantizar flujos de datos a una velocidad eficiente entre el remitente y el receptor
- ○ para garantizar la entrega de los datos

4. ¿Cuál protocolo es responsable de garantizar la entrega fiable de la información?

¡Lo tienes!

- ◉ TCP
- ○ IP
- ○ HTTP
- ○ Ethernet

Protocolos y modelos / Suites de protocolos

Suites de protocolos

3.3.1

Conjuntos de protocolos de red

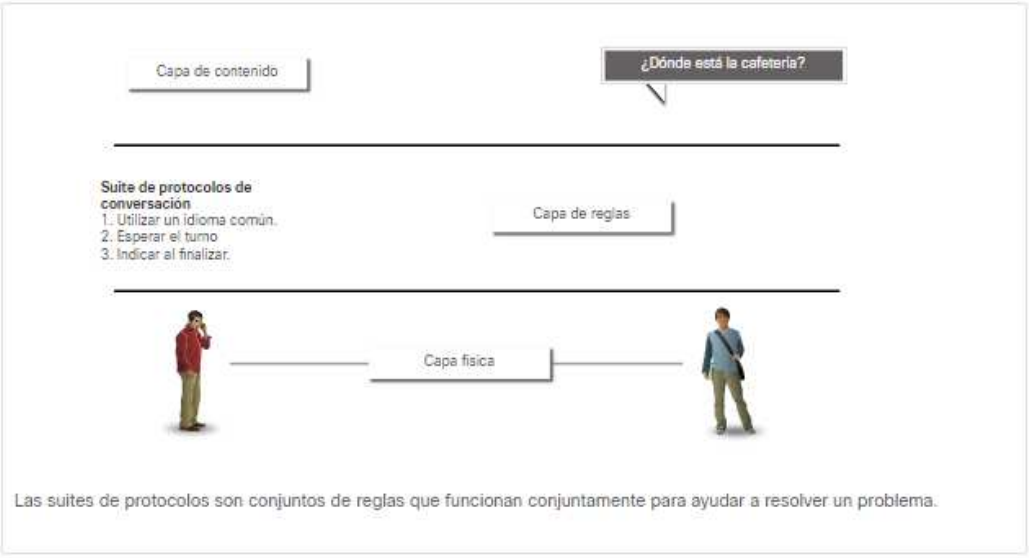
En muchos casos, los protocolos deben poder trabajar con otros protocolos para que su experiencia en línea le proporcione todo lo que necesita para las comunicaciones de red. Los conjuntos de protocolos están diseñados para funcionar entre sí sin problemas.

Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos.

Una de las mejores formas para visualizar el modo en que los protocolos interactúan dentro de una suite es ver la interacción como una pila. Una pila de protocolos muestra la forma en que los protocolos individuales se implementan dentro de una suite. Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores de la pila se encargan del movimiento de datos por la red y proporcionan servicios a las capas superiores, las cuales se enfocan en el contenido del mensaje que se va a enviar.

Como se muestra en la figura, podemos utilizar capas para describir la actividad que tiene lugar en el ejemplo de comunicación cara a cara. En la capa inferior, la capa física, hay dos personas, cada una con una voz que puede pronunciar palabras en voz alta. En el medio está la capa de reglas que estipula los requisitos de comunicación incluyendo que se debe elegir un lenguaje común. En la parte superior está la capa de contenido y aquí es donde se habla realmente el contenido de la comunicación.

La figura muestra tres capas diferentes utilizadas para describir lo que ocurre durante las comunicaciones cara a cara. La capa inferior, etiquetada como capa física, muestra a dos personas intercambiando un mensaje. La capa intermedia, etiquetada capa de reglas, enumera el conjunto de protocolos de conversación que se va a utilizar, incluyendo: utilizar un lenguaje común; esperar su turno; y la señal cuando termine. La capa superior está etiquetada capa de contenido e incluye el mensaje: ¿Dónde está el café? Las suites de protocolos son conjuntos de reglas que funcionan conjuntamente para ayudar a resolver un problema.



3.3.2

Evolución de los conjuntos de protocolos

Una suite de protocolos es un grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red. Desde la década de 1970 ha habido varios conjuntos de protocolos diferentes, algunos desarrollados por una organización de estándares y otros desarrollados por varios proveedores.

Durante la evolución de las comunicaciones de red e Internet hubo varios conjuntos de protocolos competidores, como se muestra en la figura.

Nombre de capa TCP / IP	TCP/IP	ISO	AppleTalk	Novell Netware
Aplicación	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transporte	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acceso a la red	Ethernet ARP WLAN			

La figura es una tabla. La tabla consta de cuatro filas y cinco columnas. El primer encabezado de columna es el nombre de capa TCP/IP y lee de arriba a abajo: Aplicación, Transporte, Internet y Acceso a la red. El segundo encabezado de columna es TCP/IP. Los protocolos de aplicación son HTTP, DNS, DHCP y FTP. Los protocolos de la capa de transporte son TCP y UDP. Los protocolos de Internet son IPv4, IPv6, ICMPv4 e ICMPv6. Los protocolos de acceso a la red son Ethernet, ARP y WLAN. El encabezado de la tercera columna es ISO. Los protocolos de aplicación son ACSE, ROSE, TRSE y SESE. Los protocolos de transporte son TP0, TP1, TP2, TP3 y TP4. Los protocolos de Internet son CONP/CMNS y CLNP/CLNS. Los protocolos de acceso a la red son Ethernet, ARP y WLAN. El encabezado de la cuarta columna es AppleTalk. El Protocolo de aplicación es AFP. Los protocolos de transporte son ATP, AEP, NBP y RTMP. Los Protocolos de Internet son AARP Los protocolos de acceso a la red son Ethernet, ARP y WLAN. El encabezado de la quinta columna es Novell Netware. El Protocolo de aplicación es NDS. Protocolo de transporte es SPX. Protocolo de Internet es IPX. Los protocolos de acceso a la red son Etherent, ARP y WLAN. El texto debajo de la tabla dice: Internet Protocol Suite o TCP/IP - Este es el conjunto de protocolos más común y relevante utilizado hoy en día. El conjunto de protocolos TCP/IP es un conjunto de protocolos estándar abierto mantenido por Internet Engineering Task Force (IETF). Protocolos de interconexión de sistemas abiertos (OSI) - Esta es una familia de protocolos desarrollados conjuntamente en 1977 por la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT). El protocolo OSI también incluía un modelo de siete capas llamado modelo de referencia OSI. El modelo de referencia OSI categoriza las funciones de sus protocolos. Hoy OSI es conocido principalmente por su modelo en capas. Los protocolos OSI han sido reemplazados en gran medida por TCP/IP. AppleTalk - Un paquete de protocolos propietario de corta duración lanzado por Apple Inc. en 1985 para dispositivos Apple. En 1995, Apple adoptó TCP/IP para reemplazar AppleTalk. Novell NetWare - Un conjunto de protocolos propietarios de corta duración y sistema operativo de red desarrollado por Novell Inc. en 1983 utilizando el protocolo de red IPX. En 1995, Novell adoptó TCP/IP para reemplazar a IPX.

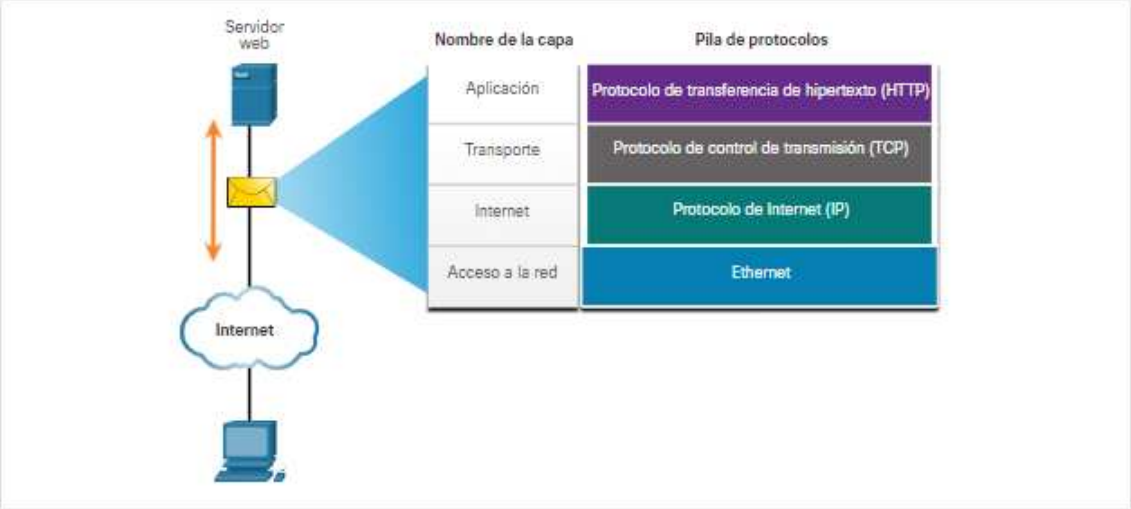
- **Internet Protocol Suite o TCP/IP** - Este es el conjunto de protocolos más común y relevante que se utiliza hoy en día. El conjunto de protocolos TCP/IP es un conjunto de protocolos estándar abierto mantenido por Internet Engineering Task Force (IETF). Protocolos de interconexión de sistemas* **abiertos (OSI)** - Esta es una familia de protocolos desarrollados conjuntamente en 1977 por la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT). El protocolo OSI también incluía un modelo de siete capas llamado modelo de referencia OSI. El modelo de referencia OSI categoriza las funciones de sus protocolos. Hoy OSI es conocido principalmente por su modelo en capas. Los protocolos OSI han sido reemplazados en gran medida por TCP/IP.
- **AppleTalk** - Un paquete de protocolos propietario de corta duración lanzado por Apple Inc. en 1985 para dispositivos Apple. En 1995, Apple adoptó TCP/IP para reemplazar AppleTalk.
- **Novell NetWare** - Un conjunto de protocolos propietarios de corta duración y sistema operativo de red desarrollado por Novell Inc. en 1983 utilizando el protocolo de red IPX. En 1995, Novell adoptó TCP/IP para reemplazar a IPX.

3.3.3

Ejemplo de protocolo TCP/IP

Los protocolos TCP/IP son específicos de las capas Aplicación, Transporte e Internet. No hay protocolos TCP/IP en la capa de acceso a la red. Los protocolos LAN de capa de acceso a la red más comunes son los protocolos Ethernet y WLAN (LAN inalámbrica). Los protocolos de la capa de acceso a la red son responsables de la entrega de los paquetes IP en los medios físicos.

La figura muestra un ejemplo de los tres protocolos TCP/IP utilizados para enviar paquetes entre el navegador web de un host y el servidor web. HTTP, TCP e IP son los protocolos TCP/IP utilizados. En la capa de acceso a la red, Ethernet se utiliza en el ejemplo. Sin embargo, esto también podría ser un estándar inalámbrico como WLAN o servicio celular.

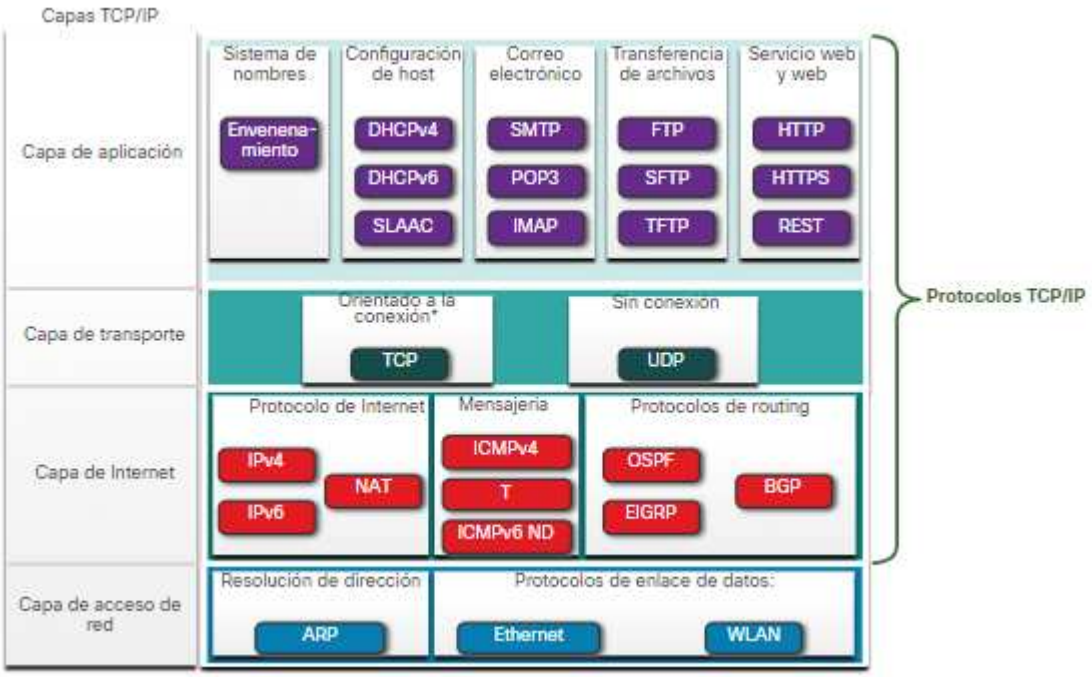


La figura muestra los protocolos TCP/IP utilizados para enviar paquetes entre el navegador web de un host y un servidor web. Una topología de red muestra un host conectado a la nube de Internet con una conexión a un servidor Web. Se muestra un sobre que representa un paquete que fluye entre Internet y el servidor. Irradiando desde el paquete es información sobre los protocolos utilizados en cada capa. De arriba a abajo: capa de aplicación y protocolo de transferencia de hipertexto (HTTP); capa de transporte y protocolo de control de transmisión (TCP); capa de Internet y protocolo de Internet (IP); y capa de acceso a la red y Ethernet.

3.3.4

Conjunto de TCP/IP

Hoy en día, el conjunto de protocolos TCP/IP incluye muchos protocolos y continúa evolucionando para admitir nuevos servicios. Algunos de los más populares se muestran en la figura.

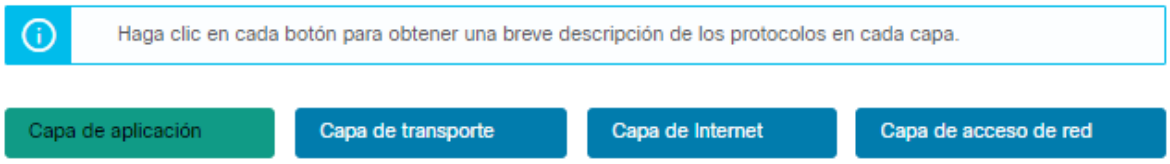


La figura muestra las capas TCP/IP y los protocolos asociados. En la capa de aplicación: DNS es un protocolo de sistema de nombres; DHCPv4, DHCPv6 y SLAAC son protocolos de configuración de host; SMTP, POP3 e IMAP son protocolos de correo electrónico; FTP, SFTP y TFTP son protocolos de transferencia de archivos; y HTTP, HTTPS y REST son protocolos de servicio web y web. En la capa de transporte: TCP es un protocolo orientado a la conexión y UDP es un protocolo sin conexión. En la capa de Internet: IPv4, IPv6 y NAT son protocolos de Internet; ICMPv4, ICMPv6 e ICMPv6 ND son protocolos de mensajería; y OSPF, EIGRP y BGP son protocolos de enrutamiento. En la capa de acceso a la red: ARP es un protocolo de resolución de direcciones; y Ethernet y WLAN son protocolos de enlace de datos. El texto en la parte inferior dice: TCP/IP es el conjunto de protocolos utilizado por Internet y las redes de hoy. TCP/IP tiene dos aspectos importantes para los proveedores y fabricantes: conjunto de protocolos estándar abierto - Esto significa que está disponible gratuitamente para el público y puede ser utilizado por cualquier proveedor en su hardware o en su software. Un protocolo basado en estándares es un proceso que recibió el aval del sector de redes y fue aprobado por una organización de estandarización. Esto asegura que productos de distintos fabricantes puedan interoperar correctamente.

TCP/IP es el conjunto de protocolos utilizado por Internet y las redes de hoy. TCP/IP tiene dos aspectos importantes para proveedores y fabricantes:

- **Suite de protocolo estándar abierto** - Esto significa que está disponible gratuitamente para el público y puede ser utilizado por cualquier proveedor en su hardware o en su software.

- **Suite de protocolo basado en estándares** -Esto significa que ha sido respaldado por la industria de redes y aprobado por una organización de estándares. Esto asegura que productos de distintos fabricantes puedan interoperar correctamente.



Capa de aplicación

Sistema de nombres

- **DNS** - Sistema de nombres de dominio. Traduce los nombres de dominio tales como cisco.com a direcciones IP

Configuración de host

- **DHCPv4** - Protocolo de configuración dinámica de host para IPv4. Un servidor DHCPv4 asigna dinámicamente información de direccionamiento IPv4 a clientes DHCPv4 al inicio y permite que las direcciones se reutilicen cuando ya no sean necesarias.
- **DHCPv6** - Protocolo de configuración dinámica de host para IPv6. DHCPv6 es similar a DHCPv4. Un servidor DHCPv6 asigna dinámicamente información de direccionamiento IPv6 a clientes DHCPv6 al inicio.
- **SLAAC** - Configuración automática de dirección sin estado. Método que permite a un dispositivo obtener su información de direccionamiento IPv6 sin utilizar un servidor DHCPv6.

Correo electrónico

- **SMTP** - Protocolo simple de transferencia de correo. Les permite a los clientes enviar correo electrónico a un servidor de correo y les permite a los servidores enviar correo electrónico a otros servidores.
- **POP3** -Protocolo de oficina de correos, versión 3. Permite a los clientes recuperar el correo electrónico de un servidor de correo y descargarlo en la aplicación de correo local del cliente.
- **IMAP** - Protocolo de acceso a mensajes de Internet. Permite que los clientes accedan a correos electrónicos almacenados en un servidor de correo.

Transferencia de archivos

- **FTP** - Protocolo de transferencia de archivos Establece las reglas que permiten a un usuario en un host acceder y transferir archivos hacia y desde otro host a través de una red. FTP Es un protocolo confiable de entrega de archivos, orientado a la conexión y con acuse de recibo.
- **SFTP** - SSH Protocolo de transferencia de archivos Como una extensión al protocolo Shell seguro (SSH), el SFTP se puede utilizar para establecer una sesión segura de transferencia de archivos, en el que el archivo transferido está cifrado. SSH es un método para el inicio de sesión remoto seguro que se utiliza normalmente para acceder a la línea de comandos de un dispositivo.

- **TFTP** - Protocolo trivial de transferencia de archivos. Un protocolo de transferencia de archivos simple y sin conexión con la entrega de archivos sin reconocimiento y el mejor esfuerzo posible. Utiliza menos sobrecarga que FTP.

Servicio web y web

- **HTTP** - Protocolo de transferencia de hipertexto Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.
- **HTTPS** - HTTP seguro. Una forma segura de HTTP que cifra los datos que se intercambian a través de la World Wide Web.
- **REST** - transferencia de estado representacional Servicio web que utiliza interfaces de programación de aplicaciones (API) y solicitudes HTTP para crear aplicaciones web.

Capa de transporte

Orientado a la conexión*

- **TCP** - Protocolo de control de transmisión. Permite la comunicación confiable entre procesos que se ejecutan en hosts independientes y tiene transmisiones fiables y con acuse de recibo que confirman la entrega exitosa.

Sin conexión

- **UDP** - Protocolo de datagrama de usuario. Habilita un proceso que se ejecuta en un host para enviar paquetes a un proceso que se ejecuta en otro host. Sin embargo, UDP No confirma la transmisión correcta de datagramas.

Capa de internet

Protocolo de Internet

- **IPv4** - Protocolo de Internet versión 4 Recibe segmentos de mensajes de la capa de transporte, empaqueta mensajes en paquetes y dirige paquetes para entrega end-to-end a través de una red. IPv4 utiliza una dirección de 32 bits.
- **IPv6** - IP version 6. Similar a IPv4, pero usa una dirección de 128 bits.
- **NAT** Traducción de direcciones de redes. Traduce las direcciones IPv4 de una red privada en direcciones IPv4 públicas globalmente únicas.

Mensajería

- **ICMPv4:** Internet Control Message Protocol (Protocolo de mensajes de control de Internet) Proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes
- **ICMPv6** - ICMP para IPv6. Funcionalidad similar a ICMPv4, pero se utiliza para paquetes IPv6.
- **ICMPv6 ND** - Detección de vecinos IPv6. Incluye cuatro mensajes de protocolo que se utilizan para la resolución de direcciones y la detección de direcciones duplicadas.

Protocolos de routing

- **OSPF** - brir la ruta más corta en primer lugar. Protocolo de enrutamiento de estado de vínculo que utiliza un diseño jerárquico basado en áreas. OSPFe s un protocolo de routing interior de estándar abierto.
- **EIGRP:** Enhanced Interior Gateway Routing Protocol (Protocolo de enrutamiento de gateway interior mejorado) Es un protocolo de routing exclusivo de Cisco, utiliza una métrica compuesta en función del ancho de banda, la demora, la carga y la confiabilidad.
- **BGP** - Protocolo de gateway fronterizo. Un protocolo de enrutamiento de puerta de enlace exterior estándar abierto utilizado entre los proveedores de servicios de Internet (ISP). BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de enrutamiento.

Capa de acceso de red

Resolución de dirección

- **ARP** - Protocolo de resolución de direcciones. Proporciona la asignación de direcciones dinámicas entre una dirección IP y una dirección de hardware.

Protocolos de enlace de datos:

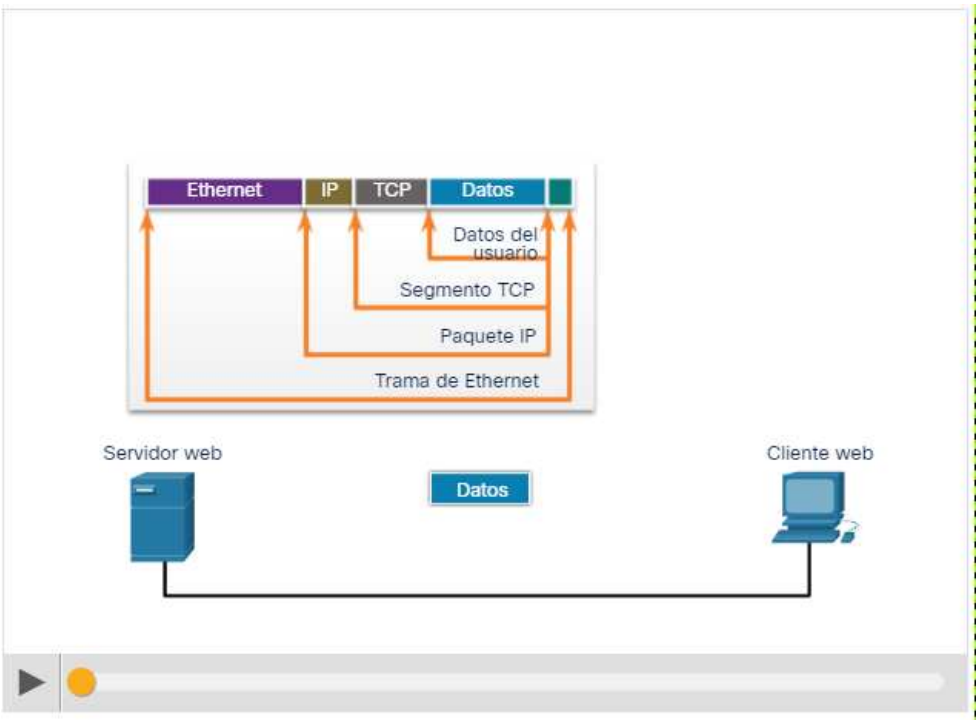
- **Ethernet** - define las reglas para conectar y señalizar estándares de la capa de acceso a la red.
- **WLAN** - red de área local inalámbrica, Define las reglas para la señalización inalámbrica a través de las frecuencias de radio de 2,4 GHz y 5 GHz.

3.3.5

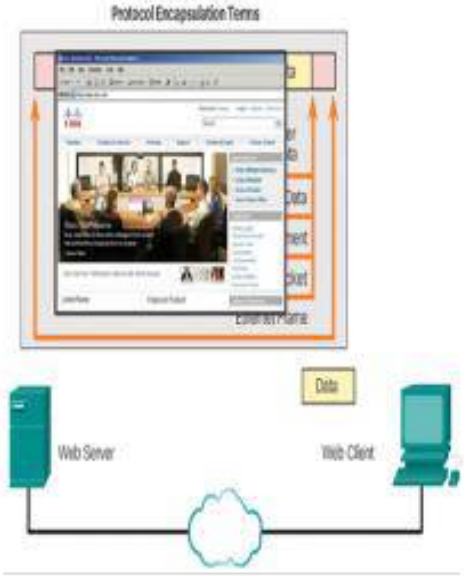
Proceso de comunicación TCP/IP

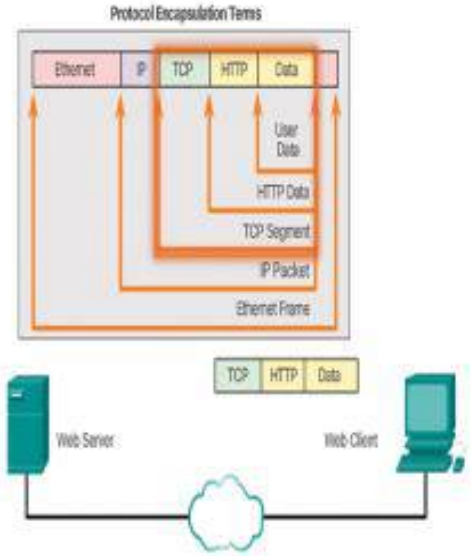
La animación en las figuras demuestra el proceso de comunicación completo mediante un ejemplo de servidor web que transmite datos a un cliente.

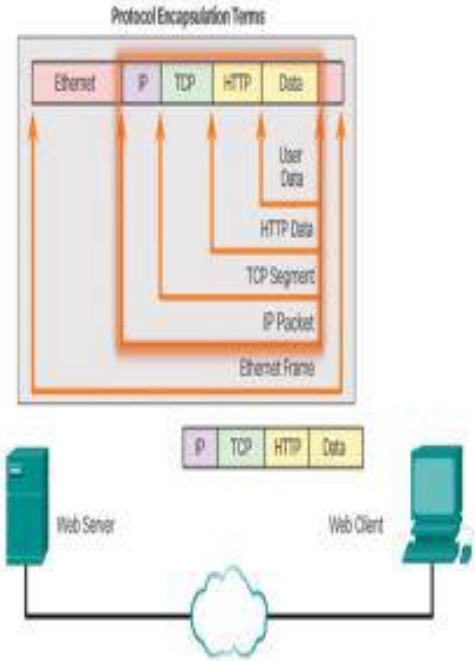
En la figura, haga clic en Reproducir para ver el proceso de encapsulamiento cuando un servidor web envía una página web a un cliente web.

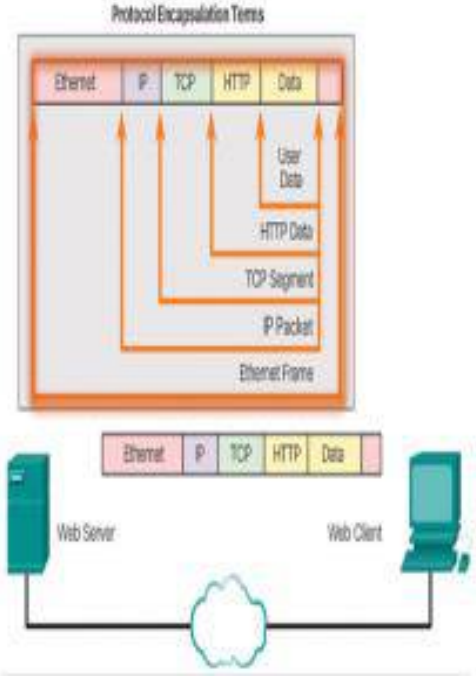


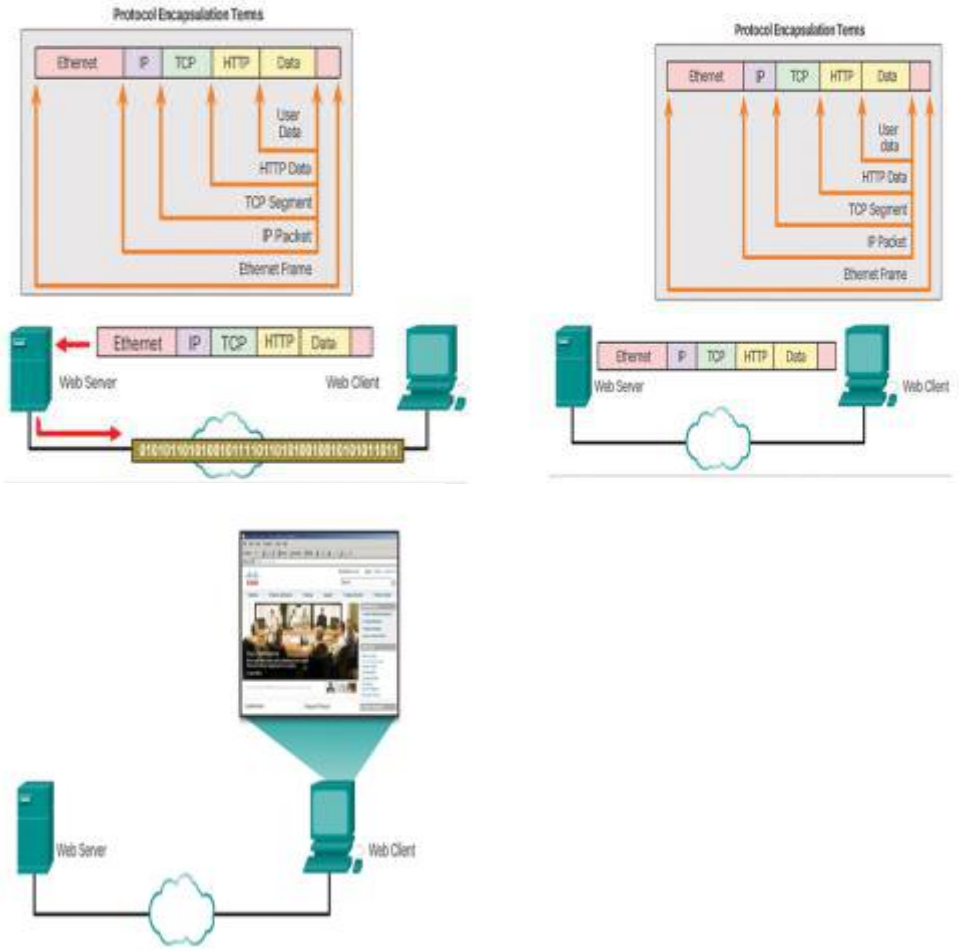
La animación muestra una pequeña red con un servidor web y un cliente web. Hay un gráfico que muestra los componentes que forman un mensaje. Una trama de Ethernet y un paquete de IP, un segmento TCP y los datos del usuario. La animación comienza con el servidor web que prepara la página del Lenguaje de marcado de hipertexto (HTML) como datos a enviar. El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente web. El protocolo de capa de aplicación HTTP entrega los datos de la página web con formato HTML a la capa de transporte. El protocolo de la capa de transporte antepone información adicional a los datos HTTP para gestionar el intercambio de información entre el servidor web y el cliente web. La información de IP se antepone a la información de TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP. El protocolo Ethernet antepone y agrega al final (agrega) información al paquete IP para crear una trama de enlace de datos. A continuación, el marco se convierte en una cadena de bits binarios que se envían a lo largo de la ruta de red al cliente web.


Protocol Encapsulation Terms
Data
Web Server
Web Client


Protocol Encapsulation Terms
Ethernet
IP
TCP
HTTP
Data
User Data
HTTP Data
TCP Segment
IP Packet
Ethernet Frame
TCP
HTTP
Data
Web Server
Web Client

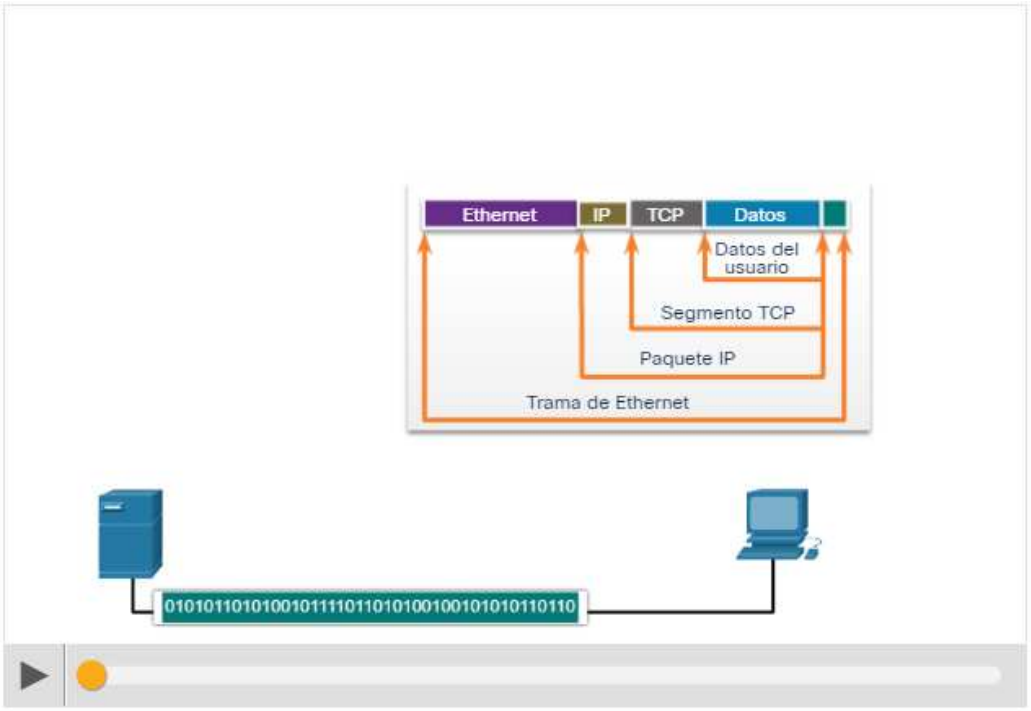

Protocol Encapsulation Terms
Ethernet
IP
TCP
HTTP
Data
User Data
HTTP Data
TCP Segment
IP Packet
Ethernet Frame
IP
TCP
HTTP
Data
Web Server
Web Client


Protocol Encapsulation Terms
Ethernet
IP
TCP
HTTP
Data
User Data
HTTP Data
TCP Segment
IP Packet
Ethernet Frame
Ethernet
IP
TCP
HTTP
Data
Web Server
Web Client



Haga clic en Reproducir en la siguiente figura para ver una animación del cliente que recibe y desencapsular la página Web para mostrarla en el explorador Web.

La animación muestra una pequeña red con un servidor y un cliente. El cliente recibe una cadena de bits binarios del servidor. El cliente toma la cadena binaria de bits y la convierte en una trama Ethernet. El marco contiene el encabezado Ethernet, el paquete IP, el segmento TCP y los datos. Cada encabezado de protocolo se procesa y luego se elimina en el orden inverso al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP. La información de la página web HTML se pasa al software del navegador web del cliente.



3.3.6

Verifique su compresión: - Protocolos

Verifique su comprensión de los conjuntos de protocolos eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. TCP y UDP son protocolos de la capa de transporte.
2. DHCP y DNS son protocolos de capa de aplicación.
3. Ethernet es un protocolo de capa de acceso a la red.
4. ICMPv4 e ICMPv6 proporcionan comentarios cuando se producen errores.
5. Los datos se desencapsulan por lo que la siguiente capa para recibir los datos sería la capa de Internet.
6. IP (Protocolo de Internet), ICMP (Mensajería) y Protocolos de enrutamiento son servicios proporcionados en la Capa de Internet.

Has tenido 6 respuestas correctas de 6.

1. UDP y TCP pertenecen a qué capa del protocolo TCP/IP?

¡Lo tienes!

- ○ Aplicación
- ◉ Transporte
- ○ Internet
- ○ Acceso a la red

2. ¿Cuáles dos protocolos pertenecen a la capa de aplicación del modelo TCP/IP?

¡Lo tienes!

- ☐ EIGRP
- ☑ Envenenamiento
- ☐ Funciones
- ☐ ICMP
- ☑ DHCP

3. ¿Cuál protocolo opera en la capa de acceso del modelo TCP/IP?

¡Lo tienes!

- ○ HTTP
- ○ IP
- ○ DNS
- ◉ Ethernet

4. ¿Cuáles de los siguientes son protocolos que proporcionan comentarios desde el host de destino al host de origen en relación con errores en la entrega de paquetes? (Escoja dos opciones).

¡Lo tienes!

- ☐ IPv4
- ☐ TCP
- ☑ ICMPv4
- ☐ IPv6
- ☐ UDP
- ☑ T

5. Un dispositivo recibe un marco de enlace de datos con datos y procesos y elimina la información de Ethernet. ¿Qué información sería la siguiente en ser procesada por el dispositivo receptor?

¡Lo tienes!

- ○ HTTP funciona en la capa de aplicación.
- ○ HTML en la capa de aplicación
- ◉ IP funciona en la capa de Internet.
- ○ UDP funciona en la capa de Internet.
- ○ TCP funciona en la capa de transporte.

6. ¿Qué servicios proporciona la capa de Internet del conjunto de protocolos TCP/IP? (Escoja tres opciones).

¡Lo tienes!

- [ ] Transferencia de archivos
- [ ] Resolución de dirección
- [x] Protocolos de routing
- [x] Mensajería
- [ ] Ethernet
- [x] Protocolo de Internet

Correct

You have successfully identified the correct answers.

1. TCP and UDP are both transport layer protocols.
2. DHCP and DNS are both application layer protocols.
3. Ethernet is a network access layer protocol.
4. ICMPv4 and ICMPv6 provide feedback when errors occur.
5. Data is de-encapsulated so the next layer to receive the data would be the internet layer.
6. IP (Internet Protocol), ICMP (Messaging), and Routing Protocols are services provided at the Internet Layer.

You got 6 out of 6 questions correct.

1. UDP and TCP belong to which layer of the TCP/IP protocol?

You got it!

- ( ) application
- (•) transport
- ( ) internet
- ( ) network access

2. Which two protocols belong in the TCP/IP model application layer?

You got it!

- [ ] EIGRP
- [x] DNS
- [ ] OSPF
- [ ] ICMP
- [x] DHCP

3. Which protocol operates at the network access layer of the TCP/IP model?

You got it!

- ○ HTTP
- ○ IP
- ○ DNS
- ◉ Ethernet

4. Which of the following are protocols that provide feedback from the destination host to the source host regarding errors in packet delivery? (Choose two.)

You got it!

- ☐ IPv4
- ☐ TCP
- ☑ ICMPv4
- ☐ IPv6
- ☐ UDP
- ☑ ICMPv6

5. A device receives a data link frame with data and processes and removes the Ethernet information. What information would be the next to be processed by the receiving device?

You got it!

- ○ HTTP at the application layer
- ○ HTML at the application layer
- ◉ IP at the internet layer
- ○ UDP at the internet layer
- ○ TCP at the transport layer

6. Which services are provided by the internet layer of the TCP/IP protocol suite? (Choose three.)

You got it!

- ☐ File Transfer
- ☐ Address Resolution
- ☑ Routing Protocols
- ☑ Messaging
- ☐ Ethernet
- ☑ Internet Protocol

1. Protocolos y modelos / Organizaciones estándares

Organizaciones estándares

3.4.1

Estándares abiertos

Al comprar neumáticos nuevos para un automóvil, hay muchos fabricantes que puede elegir. Cada uno de ellos tendrá al menos un tipo de neumático que se adapte a su coche. Esto se debe a que la industria automotriz utiliza estándares cuando se producen automóviles. Es lo mismo con los protocolos. Debido a que hay muchos fabricantes diferentes de componentes de red, todos deben usar los mismos estándares. En el establecimiento de redes, las normas son elaboradas por organizaciones internacionales de normalización.

Los estándares abiertos fomentan la interoperabilidad, la competencia y la innovación. También garantizan que ningún producto de una sola empresa pueda monopolizar el mercado o tener una ventaja desleal sobre la competencia.

La compra de un router inalámbrico para el hogar constituye un buen ejemplo de esto. Existen muchas opciones distintas disponibles de diversos proveedores, y todas ellas incorporan protocolos estándares, como IPv4, DHCP, 802.3 (Ethernet) y 802.11 (LAN inalámbrica). Estos estándares abiertos también permiten que un cliente con el sistema operativo OS X de Apple descargue una página web de un servidor web con el sistema operativo Linux. Esto se debe a que ambos sistemas operativos implementan los protocolos de estándar abierto, como los de la suite TCP/IP.

Las organizaciones de estandarización generalmente son organizaciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos. Las organizaciones de estandarización son importantes para mantener una Internet abierta con especificaciones y protocolos de libre acceso que pueda implementar cualquier proveedor.

Las organizaciones de estandarización pueden elaborar un conjunto de reglas en forma totalmente independiente o, en otros casos, pueden seleccionar un protocolo exclusivo como base para el estándar. Si se utiliza un protocolo exclusivo, suele participar el proveedor que creó el protocolo.

La figura muestra el logotipo de cada organización de normas.

Logotipos para organizaciones de estándares como IEEE, IETF, IANA, ICANN, ITU y TIA.

3.4.2

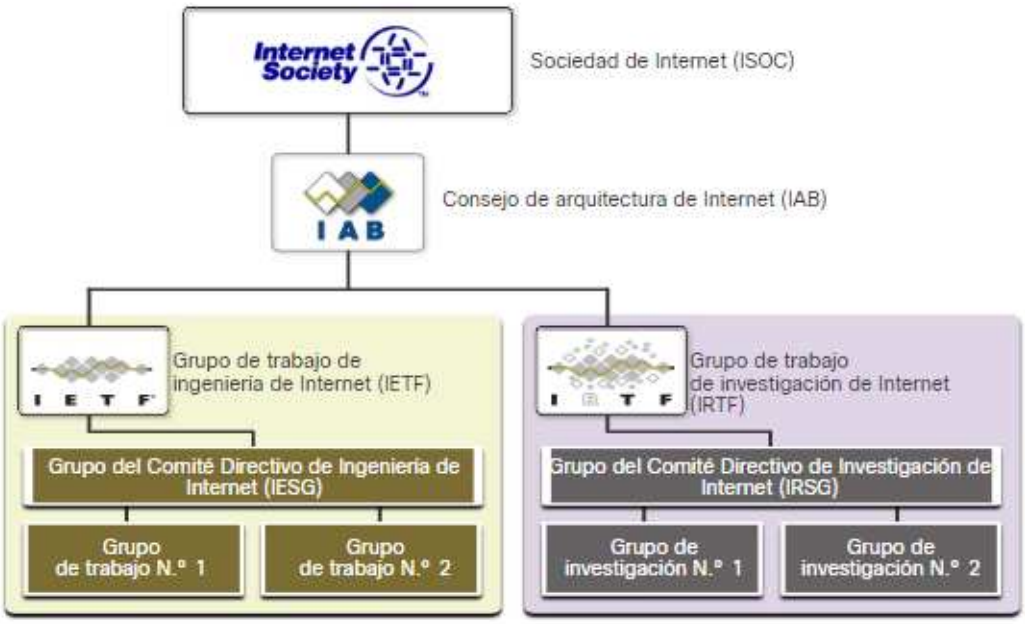
Estándares de Internet

Distintas organizaciones tienen diferentes responsabilidades para promover y elaborar estándares para el protocolo TCP/IP.

La figura muestra las organizaciones de estándares involucradas con el desarrollo y soporte de Internet.

La figura muestra las organizaciones de estándares que participan en el desarrollo y el apoyo de Internet. En la parte superior de la figura está el logotipo de Internet Society (ISOC). Una línea debajo se conecta al logotipo de Internet Architecture Board (IAB). Debajo y a la

izquierda está el Internet Engineering Task Force (IETF) y a la derecha está el Internet Research Task Force (IRTF). Debajo del IETF se encuentra el Grupo de Dirección de Ingeniería de Internet (IESG) y debajo del Grupo de Trabajo #1 y el Grupo de Trabajo #2. Debajo del IRTF se encuentra el Grupo Directivo de Investigación en Internet (IRSG) y debajo del Grupo de Investigación #1 y el Grupo de Investigación #2. El texto en la parte inferior dice: Internet Society (ISOC): responsable de promover el desarrollo abierto y la evolución del uso de Internet en todo el mundo. Consejo de Arquitectura de Internet (IAB): es responsable de la administración y el desarrollo general de los estándares de Internet. Grupo de trabajo de ingeniería de Internet (IEFT): desarrolla, actualiza y mantiene las tecnologías de Internet y de TCP/IP. Esto incluye el proceso y documentación para el desarrollo de nuevos protocolos y la actualización de los protocolos existentes, conocidos como documentos de petición de comentarios (RFC). Grupo de trabajo de investigación de Internet (IRTF): está enfocado en la investigación a largo plazo en relación con los protocolos de Internet y TCO/IP, como los grupos Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) y Peer-to-Peer Research Group (P2PRG).

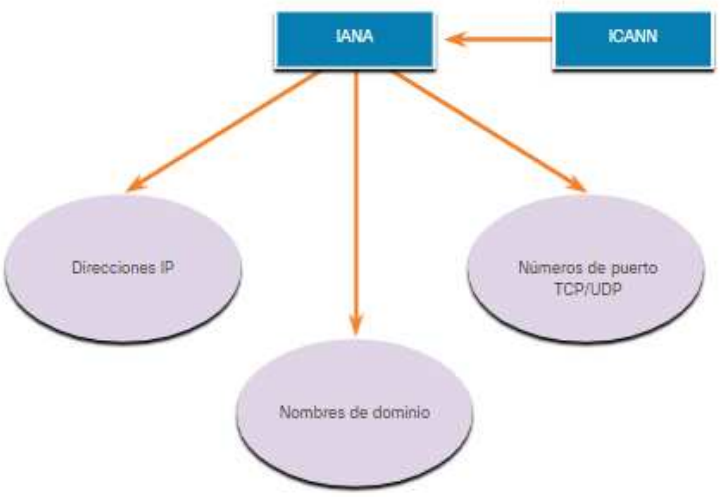


- **Sociedad de Internet (ISOC):** es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo.
- **Consejo de Arquitectura de Internet (IAB):** es responsable de la administración y el desarrollo general de los estándares de Internet.
- **Grupo de trabajo de ingeniería de Internet (IEFT):** desarrolla, actualiza y mantiene las tecnologías de Internet y de TCP/IP. Esto incluye el proceso y documentación para el desarrollo de nuevos protocolos y la actualización de los protocolos existentes, conocidos como documentos de petición de comentarios (RFC).

- **Grupo de trabajo de investigación de Internet (IRTF):** está enfocado en la investigación a largo plazo en relación con los protocolos de Internet y TCO/IP, como los grupos Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) y Peer-to-Peer Research Group (P2PRG).

La siguiente figura muestra las organizaciones de estándares involucradas en el desarrollo y soporte de TCP/IP e incluyen IANA e ICANN.

La figura muestra las organizaciones de estándares involucradas en el desarrollo y soporte de TCP/IP. La imagen muestra ICANN a la derecha con una flecha apuntando a IANA. Debajo de IANA hay tres flechas que conducen a direcciones IP, nombres de dominio y números de puerto TCP/UDP. Corporación de Internet para la Asignación de Nombres y Números (ICANN): con base en los Estados Unidos, coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información utilizada por los protocolos TCP/IP. Autoridad de Números Asignados de Internet (IANA): responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.



- **Corporación de Internet para la Asignación de Nombres y Números (ICANN)**: con base en los Estados Unidos, coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información utilizada por los protocolos TCP/IP.
- **Autoridad de Números Asignados de Internet (IANA)**: responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

3.4.3

Organizaciones de estándares para comunicaciones y electrónica

Otras organizaciones de estandarización tienen responsabilidades de promoción y creación de estándares de comunicación y electrónica que se utilizan en la entrega de paquetes IP como señales electrónicas en medios inalámbricos o por cable.

Estas organizaciones estándar incluyen las siguientes:

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced "I-triple-E"): organización de electrónica e ingeniería eléctrica dedicada a avanzar en innovación tecnológica y a elaborar estándares en una amplia gama de sectores, que incluyen energía, servicios de salud, telecomunicaciones y redes. Los estándares importantes de red IEEE incluyen 802.3 Ethernet y 802.11 WLAN. Busque en Internet otros estándares de red IEEE.
- **Asociación de Industrias Electrónicas (EIA)**: es conocida principalmente por sus estándares relacionados con el cableado eléctrico, los conectores y los racks de 19 in que se utilizan para montar equipos de red.
- **Asociación de las Industrias de las Telecomunicaciones (TIA)**: es responsable de desarrollar estándares de comunicación en diversas áreas, entre las que se incluyen equipos de radio, torres de telefonía móvil, dispositivos de voz sobre IP (VoIP), comunicaciones satelitales y más. La figura muestra un ejemplo de un cable Ethernet certificado que fue desarrollado cooperativamente por la TIA y la EIA.
- **Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T)**: es uno de los organismos de estandarización de comunicación más grandes y más antiguos. El UIT-T define estándares para la compresión de vídeos, televisión de protocolo de Internet (IPTV) y comunicaciones de banda ancha, como la línea de suscriptor digital (DSL).

3.4.4

Laboratorio: Investigación de estándares de redes

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Investigación de las organizaciones de estandarización de redes
- Parte 2: Reflexión sobre las experiencias de Internet y redes informáticas

Investigación de estándares de redes

3.4.5

Compruebe su comprensión - Organizaciones de Estándares

Verifique su comprensión de las organizaciones de estándares eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es verdadero. Las organizaciones de estandarización generalmente son organizaciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos.
2. El IETF desarrolla y mantiene las especificaciones para nuevos protocolos y actualizaciones de protocolos existentes a través de documentos publicados llamados Request for Comments (RFC).
3. Autoridad de Números Asignados de Internet (IANA): responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.
4. Asociación de Industrias Electrónicas (EIA): es conocida principalmente por sus estándares relacionados con el cableado eléctrico, los conectores y los racks que se utilizan para montar equipos de red.

Has tenido 4 respuestas correctas de 4.

1. Verdadero o falso Las organizaciones de normas suelen ser neutrales con el proveedor.

¡Lo tienes!

- (•) Verdadero
- ( ) Falso

2. Esta organización de normas se ocupa de los documentos de solicitud de comentarios (RFC) que especifican nuevos protocolos y actualizan los existentes.

¡Lo tienes!

- ( ) Sociedad de Internet (ISOC)
- (•) Grupo de trabajo de ingeniería de Internet (IETF)
- ( ) Consejo de Arquitectura de Internet (IAB)
- ( ) Grupo de trabajode investigación de Internet (IRTF)

3. Esta organización es responsable de controlar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo.

¡Lo tienes!

- ( ) Sociedad de Internet (ISOC)
- ( ) Grupo de trabajo de ingeniería de Internet (IETF)
- ( ) Consejo de Arquitectura de Internet (IAB)
- (•) Autoridad de números asignados de Internet (IANA)

4. ¿Qué tipos de estándares están desarrollados por Electronics Industries Alliance (EIA)?

¡Lo tienes!

- (•) cableado eléctrico y conectores
- ( ) equipos de radio y torres de telefonía celular
- ( ) compresión de vídeo y comunicaciones de banda ancha
- ( ) Voz sobre IP (VoIP) y comunicaciones por satélite

Correct

You have successfully identified the correct answers.

1. The correct answer is True. Most standards organizations are vendor-neutral, non-profit organizations that develop and promote open standards.
2. The IETF develops and maintains the specifications for new protocols and updates to existing protocols through published documents called Request for Comments (RFCs).
3. IANA is responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.
4. The Electronics Industries Alliance (EIA) develops standards related to electrical wiring, connectors, and network equipment racks.

You got 4 out of 4 questions correct.

1. True or false. Standards organizations are usually vendor-neutral.

You got it!

- (•) True
- ( ) False

2. This standards organization is concerned with the Request for Comments (RFC) documents that specify new protocols and update existing ones.

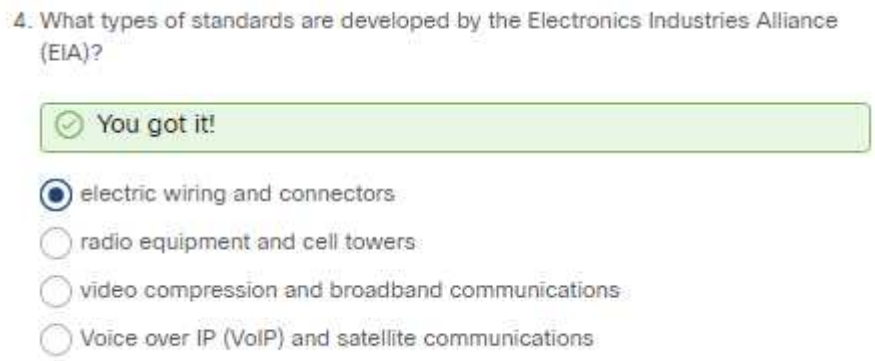
You got it!

- ( ) Internet Society (ISOC)
- (•) Internet Engineering Task Force (IETF)
- ( ) Internet Architecture Board (IAB)
- ( ) Internet Research Task Force (IRTF)

3. This standards organization is responsible for IP address allocation and domain name management.

You got it!

- ( ) Internet Society (ISOC)
- ( ) Internet Engineering Task Force (IETF)
- ( ) Internet Architecture Board (IAB)
- (•) Internet Assigned Numbers Authority (IANA)



Protocolos y modelos / Modelos de referencia

Modelos de referencia

3.5.1

Beneficios del uso de un modelo en capas

En realidad, no se puede ver que los paquetes reales viajan a través de una red real, la forma en que se pueden ver los componentes de un coche que se ensamblan en una línea de ensamble. Por lo tanto, ayuda tener una forma de pensar acerca de una red para que usted pueda imaginar lo que está sucediendo. Un modelo es útil en estas situaciones.

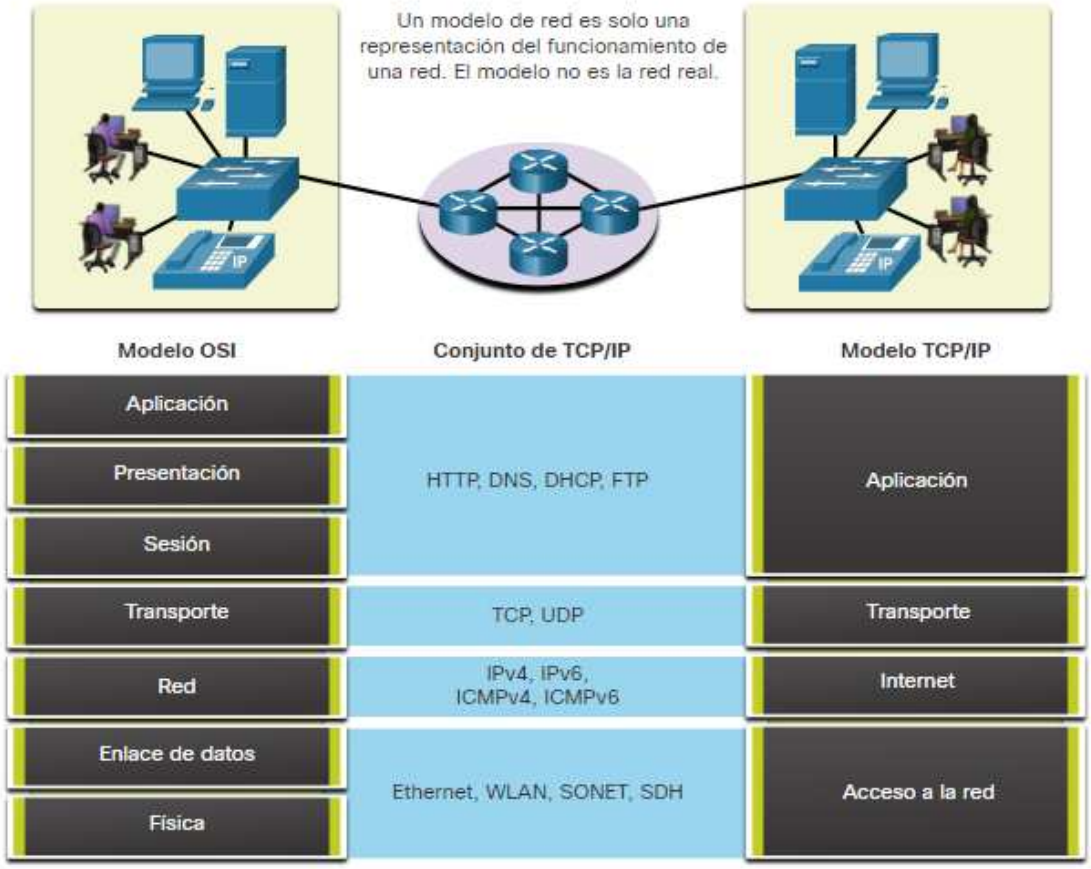
Conceptos complejos, como el funcionamiento de una red, pueden ser difíciles de explicar y comprender. Por esta razón, un modelo en capas se utiliza para modularizar las operaciones de una red en capas manejables.

Los beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones incluyen lo siguiente:

Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores. Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto. Evita que los cambios en la tecnología o en las funcionalidades de una capa afecten otras capas superiores e inferiores. Proporciona un lenguaje común para describir las funciones y capacidades de red.

Como se muestra en la figura, hay dos modelos en capas que se utilizan para describir las operaciones de red:

Modelo de referencia de interconexión de sistemas abiertos.
Modelo de referencia TCP/IP



En la parte superior de la imagen hay dos LAN conectadas a través de una WAN con el texto: Un modelo de red es solo una representación de una operación de red. El modelo no es la red real. Debajo están las capas y protocolos de modelo OSI y TCP/IP. Las siete capas del modelo OSI de arriba a abajo y sus protocolos asociados son: aplicación, presentación, sesión (los protocolos en las tres capas superiores son HTTP, DNS, DHCP y FTP), transporte (TCP y UDP), red (IPv4, IPv6, ICMPv4 e ICMPv6), enlace de datos y físico (protocolos en las dos inferiores). son Ethernet, WLAN, SONET y SDH). Las cuatro capas del modelo TCP/IP de arriba a abajo y sus protocolos asociados son: aplicación (HTTP, DNS, DHCP y FTP), transporte (TCP y UDP), Internet (IPv4, IPv6, ICMPv4 e ICMPv6) y acceso a la red (Ethernet, WLAN, SONET y SDH).

3.5.2

El modelo de referencia OSI

El modelo de referencia OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. este tipo de modelo es coherente con todos los tipos de servicios y protocolos de red al describir qué es lo que se debe hacer en una capa determinada, pero sin regir la forma en que se debe lograr.

También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Los protocolos TCP/IP que se analizan en este curso se estructuran en torno a los modelos OSI y TCP/IP. La tabla muestra detalles sobre cada capa del modelo OSI. La funcionalidad de cada capa y la relación entre ellas será más evidente a medida que avance en el curso y que se brinden más detalles acerca de los protocolos.

OSI Model Layer	Description
7 - Application	The application layer contains protocols used for process-to-process communications.
6 - Presentation	The presentation layer provides for common representation of the data transferred between application layer services.
5 - Session	The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.
4 - Transport	The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
3 - Network	The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
2 - Data Link	The data link layer protocols describe methods for exchanging data frames between devices over a common media
1 - Physical	The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device.

Capa del modelo OSI	**Descripción**
7 - Aplicación	La capa de aplicación contiene protocolos utilizados para comunicaciones proceso a proceso. de comunicaciones.
6 - Presentación	la capa de presentación proporciona una representación común de los datos transferido entre los servicios de capa de aplicación.
5 - Sesión	La capa de sesión proporciona servicios a la capa de presentación para Organiza el diálogo y administra el intercambio de datos

Capa del modelo OSI	Descripción
4-Transporte	La capa de transporte define servicios para segmentar, transferir y volver a montar los datos para las comunicaciones individuales entre el final.
3 - Red	La capa de red proporciona servicios para intercambiar las piezas individuales de a través de la red entre los dispositivos finales identificados.
2 - Enlacede datos	Los protocolos de la capa de enlace de datos describen métodos para intercambiar datos. tramas entre dispositivos a través de un medio común
1-Física	Los protocolos de capa física describen los componentes mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para una transmisión de bits hacia y desde una red dispositivo.

Nota: mientras las capas del modelo TCP/IP se mencionan solo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre. Por ejemplo, la capa física se conoce como Capa 1 del modelo OSI, la capa de enlace de datos es Layer2, y así sucesivamente.

3.5.3

Modelo de protocolo TCP/IP

El modelo de protocolo TCP/IP para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Este tipo de modelo coincide con precisión con la estructura de una suite de protocolos determinada. El modelo TCP/IP es un protocolo modelo porque describe las funciones que ocurren en cada capa de protocolos dentro de una suite de TCP/IP. TCP/IP también es un ejemplo de un modelo de referencia. La tabla muestra detalles sobre cada capa del modelo OSI.

TCP/IP Model Layer	Description
4 – Application	Represents data to the user, plus encoding and dialog control.
3 – Transport	Supports communication between various devices across diverse networks.
2 – Internet	Determines the best path through the network.
1 – Network Access	Controls the hardware devices and media that make up the network.

Capa del modelo TCP/IP	Descripción
4 - Aplicación	Representa datos para el usuario más el control de codificación y de diálogo.
3-Transporte	Admite la comunicación entre distintos dispositivos a través de diversas redes.
2 - Internet	Determina el mejor camino a través de una red.
1 - Acceso a la red	Controla los dispositivos del hardware y los medios que forman la red.

Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos de petición de comentarios (RFC) disponibles al público. Un RFC es creado por ingenieros de redes y enviado a otros miembros de IETF para comentarios.

3.5.4

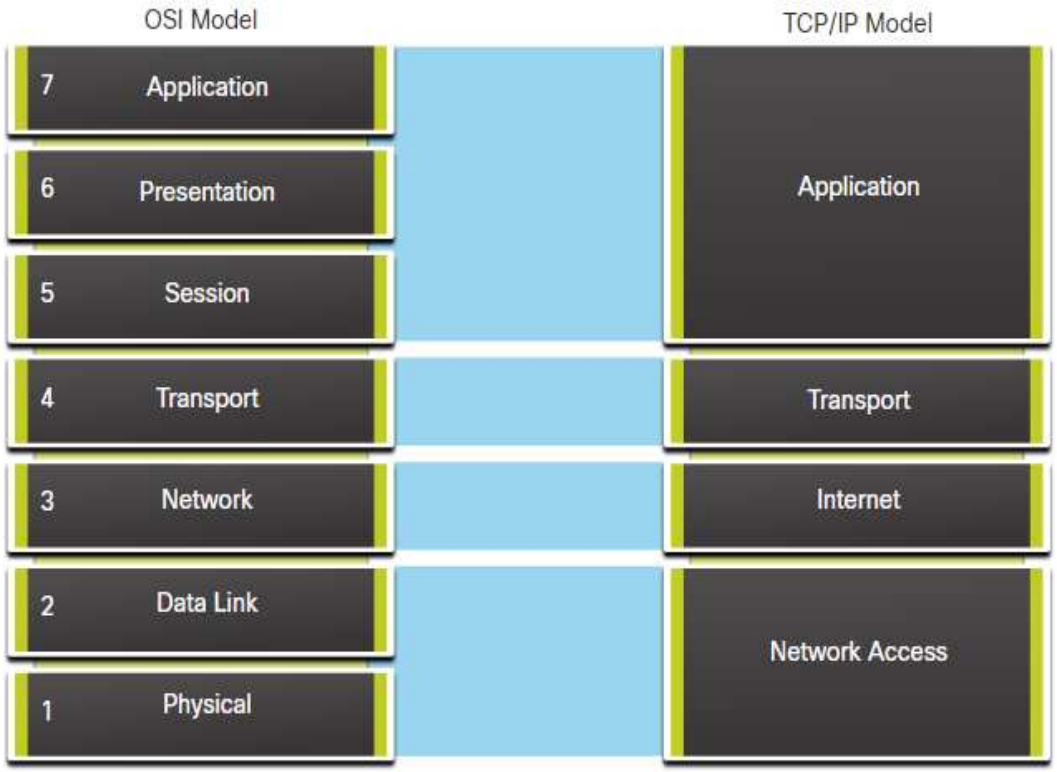
Comparación del modelo OSI y el modelo TCP/IP

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI. En el modelo OSI, la capa de acceso a la red y la capa de aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.

En la capa de acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; solo describe la transferencia desde la capa

de Internet a los protocolos de red física. Las capas OSI 1 y 2 tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos por la red.

La figura es una comparación de las capas de modelo OSI y TCP/IP. El modelo OSI se muestra a la izquierda. De arriba a abajo se encuentran los siguientes números de capa y nombres: 7) Aplicación, 6) Presentación, 5) Sesión, 4) Transporte, 3) Red, 2) Enlace de datos y 1) Física. El modelo TCP/IP se muestra a la derecha. De arriba a abajo, los nombres de capa y los números de capa del modelo OSI asociados son: Aplicación (Capas OSI 7, 6 y 5), Transporte (Capa OSI 4), Internet (Capa OSI 3) y Acceso de red (Capas OSI 2 y 1). El texto al pie de la figura dice que Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en el que se relacionan con las capas que están por encima y por debajo de cada capa. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork. La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes. Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores.



Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en que se relacionan con las capas que están por encima y por debajo de cada capa.

- La capa OSI 3, la capa de red, asigna directamente a la capa de Internet TCP/IP. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork.
- La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino.
- La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes.
- Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores.

3.5.5

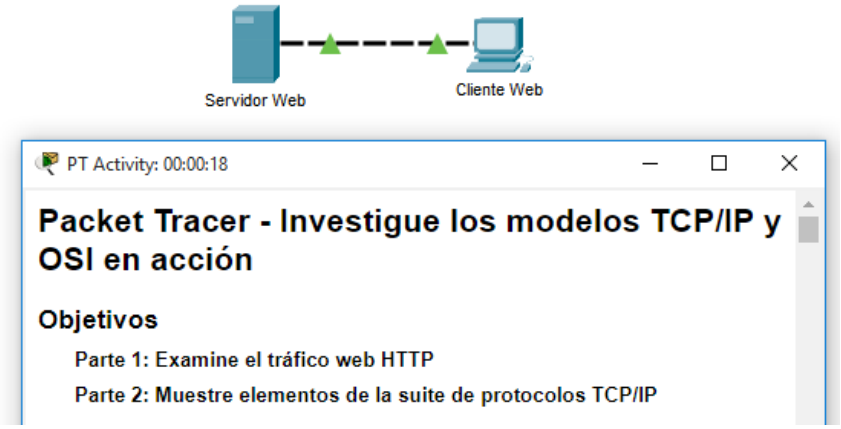
Packet Tracer: Investigación de los modelos TCP/IP y OSI en acción

Esta actividad de simulación tiene como objetivo proporcionar una base para comprender la suite de protocolos TCP/IP y la relación con el modelo OSI. El modo de simulación le permite ver el contenido de los datos que se envían a través de la red en cada capa.

A medida que los datos se desplazan por la red, se dividen en partes más pequeñas y se identifican de modo que las piezas se puedan volver a unir cuando lleguen al destino. A cada pieza se le asigna un nombre específico (unidad de datos del protocolo [PDU]) y se la asocia a una capa específica de los modelos TCP/IP y OSI. El nombre asignado se denomina unidad de datos de protocolo (PDU). El modo de simulación de Packet Tracer le permite ver cada una de las capas y la PDU asociada. Los siguientes pasos guían al usuario a través del proceso de solicitud de una página web desde un servidor web mediante la aplicación de navegador web disponible en una PC cliente.

Aunque gran parte de la información mostrada se analizará en mayor detalle más adelante, esta es una oportunidad de explorar la funcionalidad de Packet Tracer y de ver el proceso de encapsulamiento.

Investigación de los modelos TCP/IP y OSI en acción



Investigación de los modelos TCP/IP y OSI en acción

Protocolos y modelos / Encapsulamiento de datos

Encapsulamiento de datos

3.6.1

Segmentación del mensaje

Conocer el modelo de referencia OSI y el modelo de protocolo TCP/IP será útil cuando aprenda acerca de cómo se encapsulan los datos a medida que se mueven a través de una red. No es tan simple como una carta física que se envía a través del sistema de correo.

En teoría, una comunicación simple, como un vídeo musical o un correo electrónico puede enviarse a través de la red desde un origen hacia un destino como una transmisión de bits masiva y continua. Sin embargo, esto crearía problemas para otros dispositivos que necesitan utilizar los mismos canales de comunicación o enlaces. Estas grandes transmisiones de datos originarán retrasos importantes. Además, si falla un enlace en la infraestructura de la red interconectada durante la transmisión, el mensaje completo se perdería y tendría que retransmitirse completamente.

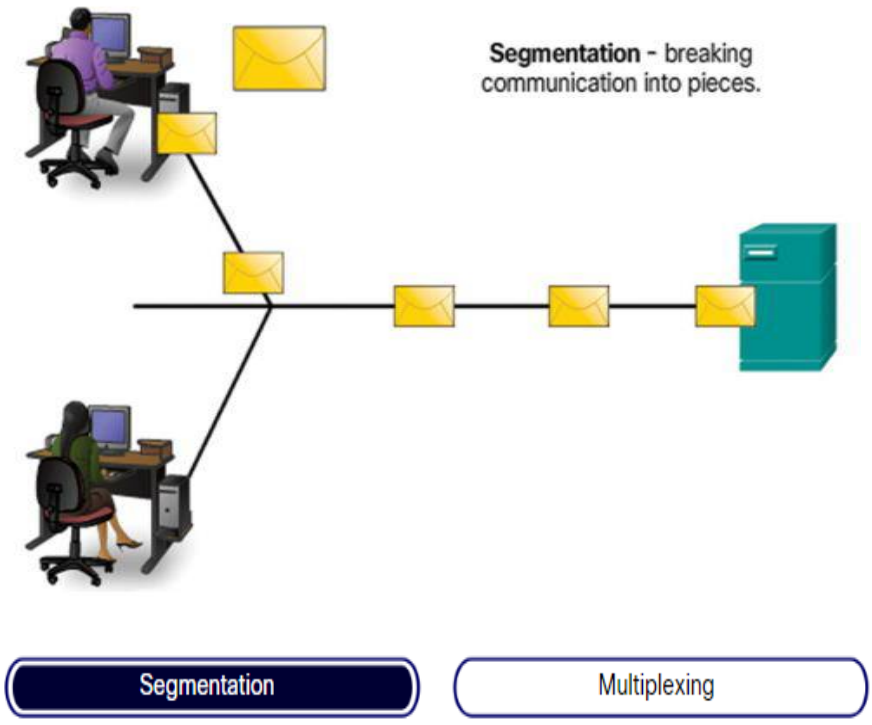
Un método mejor es dividir los datos en partes más pequeñas y manejables para enviarlas por la red. La segmentación es el proceso de dividir un flujo de datos en unidades más pequeñas para transmisiones a través de la red. La segmentación es necesaria porque las redes de datos utilizan el conjunto de protocolos TCP/IP para enviar datos en paquetes IP individuales. Cada paquete se envía por separado, similar al envío de una carta larga como

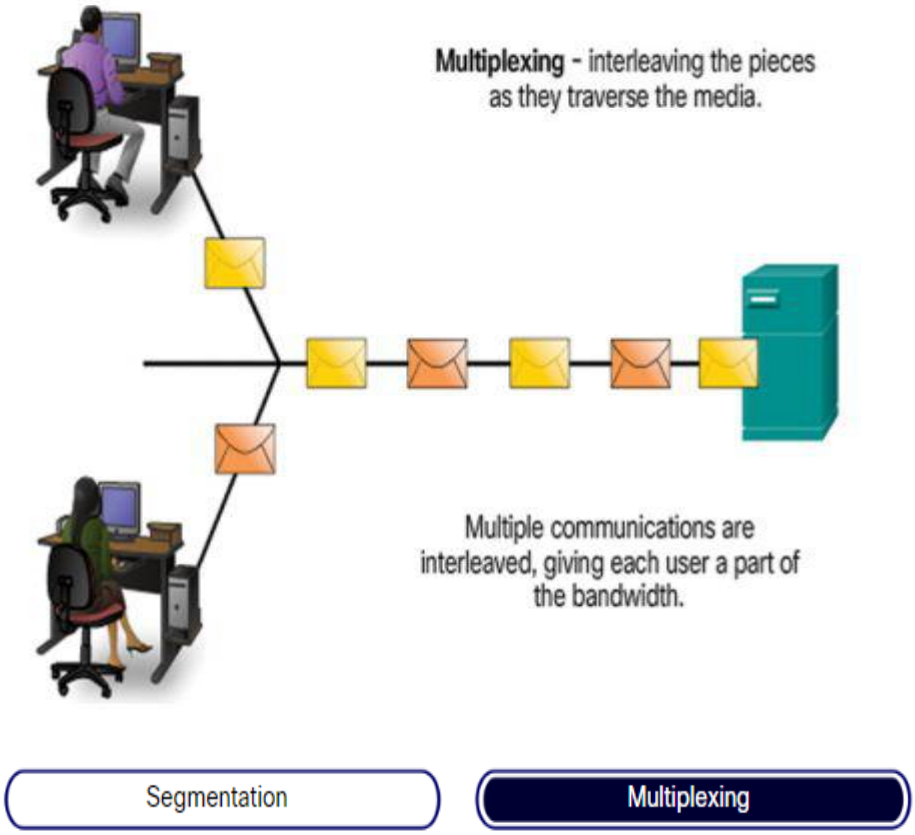
una serie de postales individuales. Los paquetes que contienen segmentos para el mismo destino se pueden enviar a través de diferentes rutas.

La segmentación de mensajes tiene dos beneficios principales.

- **Aumenta la velocidad** - Debido a que un flujo de datos grande se segmenta en paquetes, se pueden enviar grandes cantidades de datos a través de la red sin atar un enlace de comunicaciones. Esto permite que muchas conversaciones diferentes se intercalen en la red llamada multiplexación.
- **Aumenta la eficiencia:** si un solo segmento no llega a su destino debido a una falla en la red o congestión de la red, solo ese segmento necesita ser retransmitido en lugar de volver a enviar toda la secuencia de datos.

Haga clic en cada botón de la figura 1 y, a continuación, haga clic en el botón Reproducir para ver las animaciones de segmentación y de multiplexión.





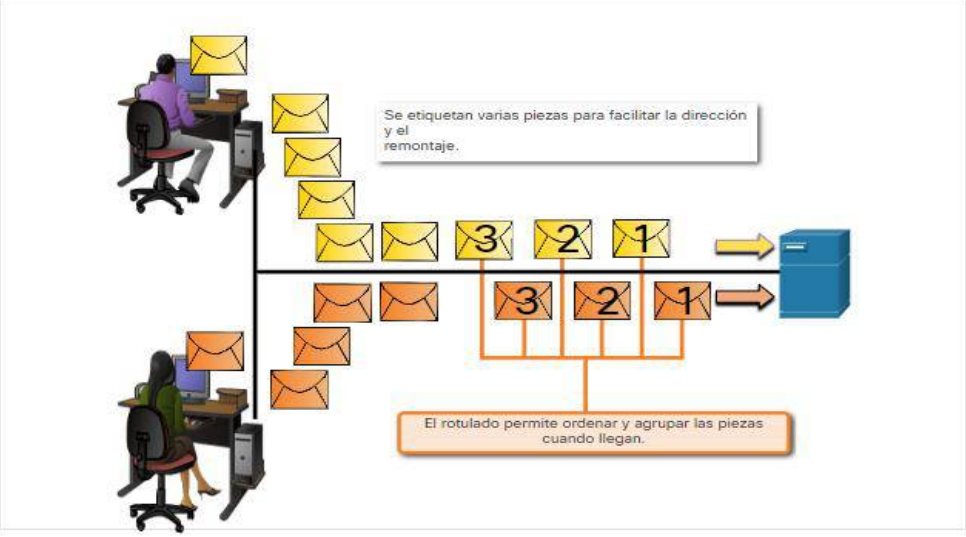
La animación muestra una pequeña LAN con dos hosts y un servidor. Cuando se presiona el botón Segmentación, un mensaje grande del primer host se divide en mensajes más pequeños que se envían por la red al servidor. A continuación, se presiona el botón Multiplexación los mensajes de ambos hosts se envían a la red uno tras otro al servidor.

3.6.2

Secuenciación

La desventaja de utilizar segmentación y multiplexación para transmitir mensajes a través de la red es el nivel de complejidad que se agrega al proceso. Supongamos que tuviera que enviar una carta de 100 páginas, pero en cada sobre solo cabe una. Por lo tanto, se necesitarían 100 sobres y cada sobre tendría que dirigirse individualmente. Es posible que la carta de 100 páginas en 100 sobres diferentes llegue fuera de pedido. En consecuencia, la información contenida en el sobre tendría que incluir un número de secuencia para garantizar que el receptor pudiera volver a ensamblar las páginas en el orden adecuado.

En las comunicaciones de red, cada segmento del mensaje debe seguir un proceso similar para asegurar que llegue al destino correcto y que puede volverse a ensamblar en el contenido del mensaje original, como se muestra en la figura 2. TCP es responsable de secuenciar los segmentos individuales.



La figura muestra dos equipos que envían mensajes en una red a un servidor. Cada mensaje se ha dividido en varias piezas que se muestran como sobres amarillos y naranjas, algunos están entrelazados y numerados. Lecturas de texto: se etiquetan varias piezas para facilitar la dirección y el reensamblaje. El rotulado permite ordenar y agrupar las piezas cuando llegan.

3.6.3

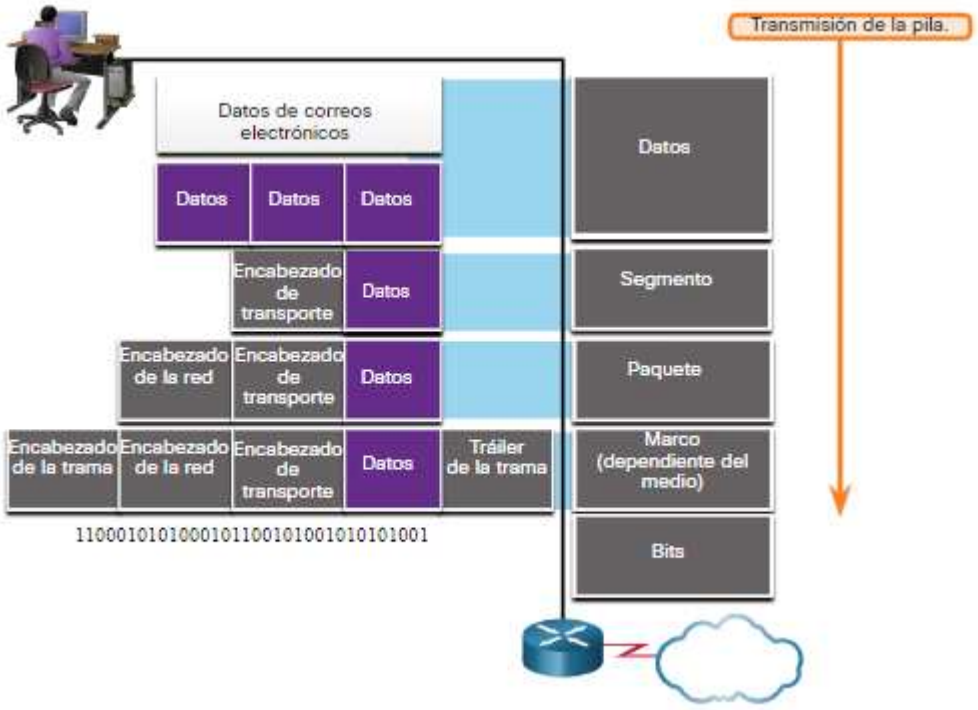
Unidades de datos de protocolo

Mientras los datos de la aplicación bajan a la pila del protocolo y se transmiten por los medios de la red, se agrega diversa información de protocolos en cada nivel. Esto comúnmente se conoce como proceso de encapsulamiento.

Nota: Aunque la PDU UDP se denomina datagrama, los paquetes IP a veces también se conocen como datagramas IP.

La manera que adopta una porción de datos en cualquier capa se denomina unidad de datos del protocolo (PDU). Durante el encapsulamiento, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus funciones nuevas. Aunque no existe una convención universal de nombres para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite TCP/IP. Las PDU de cada tipo de datos se muestran en la figura.

La figura muestra las unidades de datos de protocolo (PDU) en varias capas del modelo OSI. En la parte superior de la imagen hay una persona sentada en una estación de trabajo de computadora enviando datos de correo electrónico. Estos datos se pasan por la pila y se encapsulan en una nueva PDU en cada capa. En la parte superior, los datos de correo electrónico se dividen en trozos más pequeños de datos. Debajo de eso, se agrega un encabezado de transporte delante del fragmento de datos y se convierte en un segmento. Debajo de eso, se agrega un encabezado de red delante del encabezado de transporte y se convierte en un paquete. Debajo de eso, se agrega un encabezado de trama delante del encabezado de red y se agrega un tráiler de trama detrás de los datos y se convierte en un fotograma (dependiente del medio). La trama se muestra como una secuencia de bits antes de ser recibida por un router que está conectado a la nube. El texto en la parte inferior dice: Datos - El término general para la PDU utilizada en la capa de aplicación; Segmento - PDU de capa de transporte; Packet - PDU de capa de red; Frame - PDU de capa de enlace de datos; Bits - PDU de capa física utilizada al transmitir datos físicamente a través del medio. Nota: Si el encabezado Transporte es TCP, entonces es un segmento. Si el encabezado Transporte es UDP, entonces es un datagrama.



- Datos: término general que se utiliza en la capa de aplicación para la PDU
- Segmento: PDU de la capa de transporte
- Paquete: PDU de la capa de red
- Trama: PDU de la capa de enlace de datos
- Bits: PDU de capa física que se utiliza cuando se transmiten datos físicamente por el medio

Nota: Si el encabezado Transporte es TCP, entonces es un segmento. Si el encabezado de transporte es UDP, entonces es un datagrama.

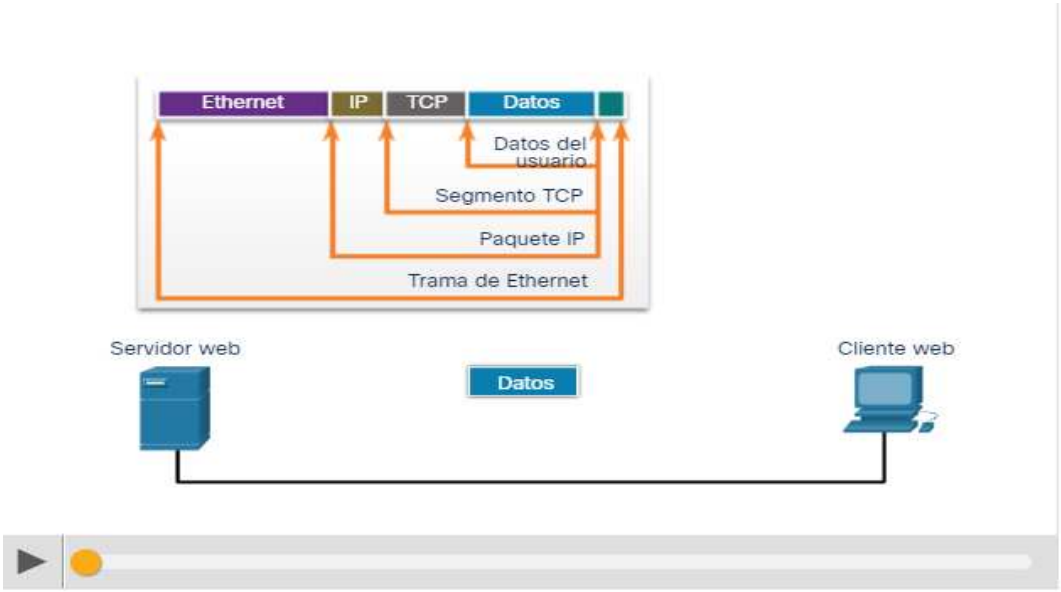
3.6.4

Ejemplo de encapsulamiento

Cuando se envían mensajes en una red, el proceso de encapsulamiento opera desde las capas superiores hacia las capas inferiores. En cada capa, la información de la capa superior se considera como datos en el protocolo encapsulado. Por ejemplo, el segmento TCP se considera como datos en el paquete IP.

Usted vio esta animación anteriormente en este módulo. Esta vez, haga clic en Reproducir y concéntrese en el proceso de encapsulación ya que un servidor web envía una página web a un cliente web.

La animación muestra una pequeña red con un servidor web y un cliente web. Hay un gráfico que muestra los componentes que forman un mensaje. Una trama de Ethernet y un paquete de IP, un segmento TCP y los datos del usuario. La animación comienza con el servidor web que prepara la página del Lenguaje de marcado de hipertexto (HTML) como datos a enviar. El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente web. El protocolo de capa de aplicación HTTP entrega los datos de la página web con formato HTML a la capa de transporte. El protocolo de la capa de transporte antepone información adicional a los datos HTTP para gestionar el intercambio de información entre el servidor web y el cliente web. La información de IP se antepone a la información de TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP. El protocolo Ethernet antepone y agrega al final (agrega) información al paquete IP para crear una trama de enlace de datos. A continuación, el marco se convierte en una cadena de bits binarios que se envían a lo largo de la ruta de red al cliente web.



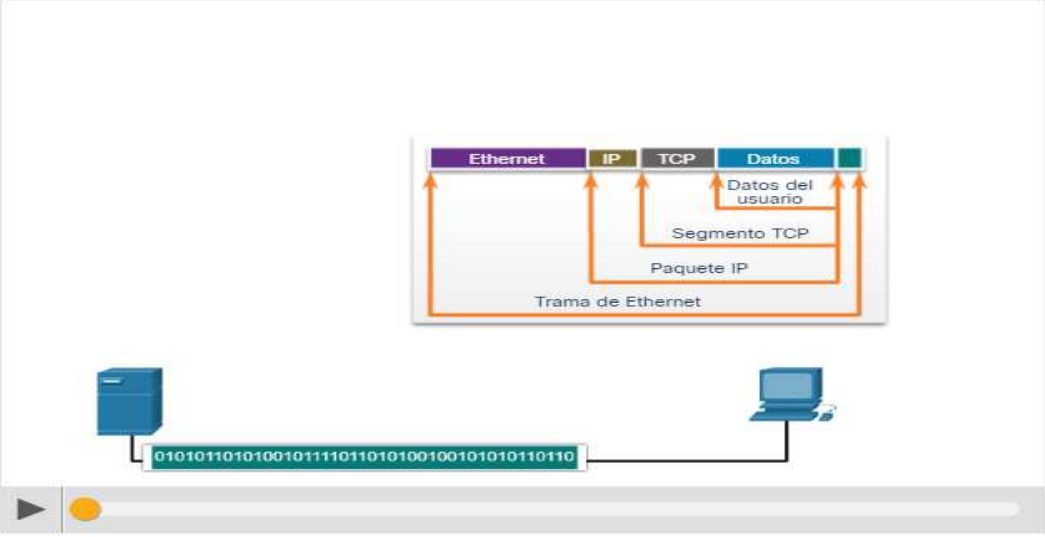
3.6.5

Ejemplo de desencapsulamiento

Este proceso se invierte en el host receptor, y se conoce como desencapsulamiento. El desencapsulamiento es el proceso que utilizan los dispositivos receptores para eliminar uno o más de los encabezados de protocolo. Los datos se desencapsulan mientras suben por la pila hacia la aplicación del usuario final.

Usted vio esta animación anteriormente en este módulo. Esta vez, haga clic en Reproducir y concéntrese en el proceso de desencapsulación.

La animación muestra una pequeña red con un servidor y un cliente. El cliente recibe una cadena de bits binarios del servidor. El cliente toma la cadena binaria de bits y la convierte en una trama Ethernet. El marco contiene el encabezado Ethernet, el paquete IP, el segmento TCP y los datos. Cada encabezado de protocolo se procesa y luego se elimina en el orden inverso al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP. La información de la página web HTML se pasa al software del navegador web del cliente.



3.6.6

Verifique su comprensión: protección de datos

Verifique su comprensión de la encapsulación de datos eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. Segmentation is the process of dividing a large data stream into smaller pieces which are then transmitted to the receiver.
2. The transport layer PDU is known as a segment.
3. The data link layer encapsulates data into a frame.
4. As data moves down the protocol stack, protocol data is added to the original data. This process is known as encapsulation.

You got 4 out of 4 questions correct.

1. What is the process of dividing a large data stream into smaller pieces prior to transmission?

You got it!

- ○ sequencing
- ○ duplexing
- ○ multiplexing
- ◉ segmentation

2. What is the PDU associated with the transport layer?

You got it!

- ◉ segment
- ○ packet
- ○ bits
- ○ frame

3. Which protocol stack layer encapsulates data into frames?

You got it!

- ◉ data link
- ○ transport
- ○ network
- ○ application

4. What is the name of the process of adding protocol information to data as it moves down the protocol stack?

You got it!

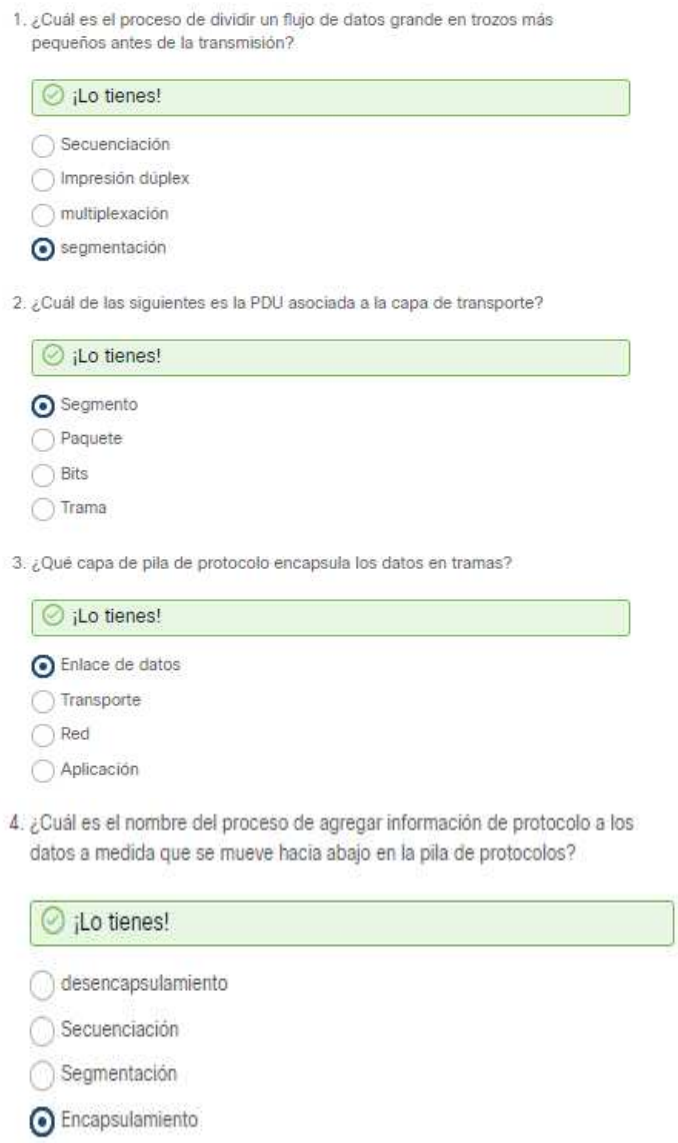
- ○ de-encapsulation
- ○ sequencing
- ○ segmentation
- ◉ encapsulation

Correcto

Identificó bien las respuestas correctas.

1. La segmentación es el proceso de dividir un flujo de datos grande en trozos más pequeños que luego se transmiten al receptor.
2. La PDU de la capa de transporte se conoce como segmento.
3. La capa de vínculo de datos encapsula los datos en un marco.
4. A medida que los datos se mueven hacia abajo en la pila de protocolos, los datos de protocolo se agregan a los datos originales. Esto comúnmente se conoce como proceso de encapsulamiento.

Has tenido 4 respuestas correctas de 4.



Protocolos y modelos / Acceso a los datos

Acceso a los datos

3.7.1

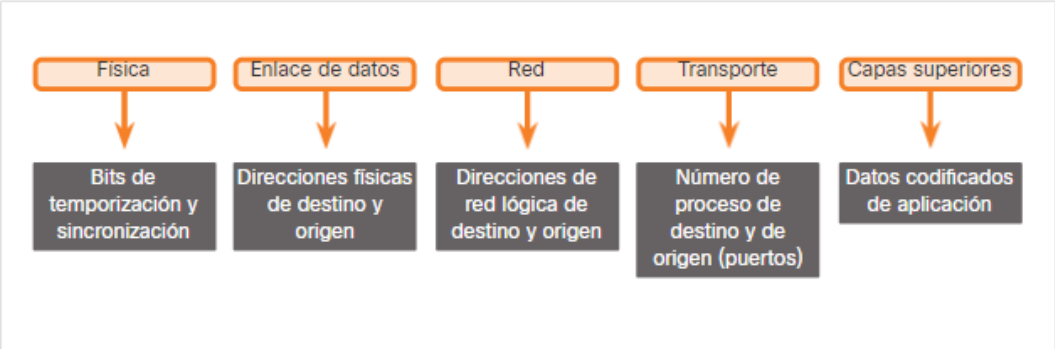
Direcciones

Como acaba de aprender, es necesario segmentar los mensajes en una red. Pero esos mensajes segmentados no irán a ninguna parte si no se abordan correctamente. En este tema se ofrece una descripción general de las direcciones de red. También tendrá la oportunidad de usar la herramienta Wireshark, que le ayudará a 'ver' el tráfico de la red.

La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor. Como se muestra en la figura 1, los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

- **Direcciones de origen y de destino de la capa de red**: son responsables de enviar el paquete IP desde el dispositivo de origen hasta el dispositivo final, ya sea en la misma red o a una red remota.
- **Direcciones de origen y de destino de la capa de enlace de datos**: son responsables de enviar la trama de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra en la misma red.

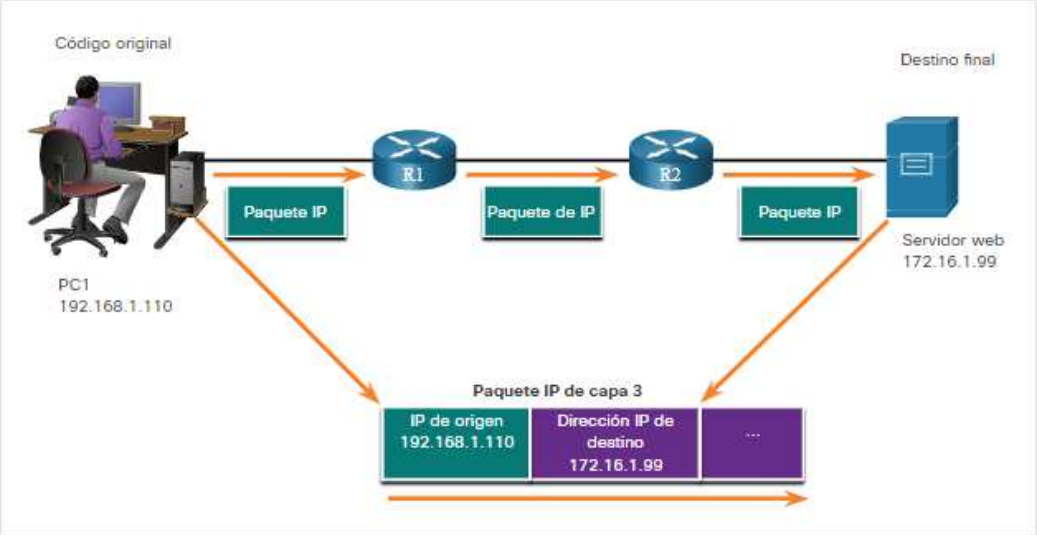
La figura muestra el direccionamiento y el etiquetado utilizados en varias capas del modelo OSI para la entrega de datos. Comenzando de izquierda a derecha, muestra: la capa física proporciona bits de sincronización y sincronización; la capa de enlace de datos proporciona direcciones físicas de destino y origen; la capa de red proporciona direcciones de red lógicas de destino y origen; la capa de transporte proporciona destino y proceso de origen número (puertos); y las capas superiores proporcionan datos codificados de la aplicación.



3.7.2

Dirección lógica de capa 3

Una dirección lógica de la capa de red, o capa 3, se utiliza para enviar el paquete IP desde el dispositivo de origen hasta el dispositivo de destino, como se muestra en la figura.



La figura muestra un paquete IP de capa 3 que se mueve desde el origen original hasta el destino final. La fuente original es PC1, que se muestra a la izquierda, con dirección IP 192.168.1.110. El destino final es un servidor web, que se muestra en el extremo derecho, con dirección IP 172.16.1.99. Se muestra un paquete IP dejando PC1 dirigiéndose al router R1. A continuación, se muestra el paquete IP dejando el router R1 y dirigiéndose al router R2. A continuación, se muestra el paquete IP dejando R2 y dirigiéndose hacia el servidor web. Debajo de la topología de red hay un diagrama de un encabezado de paquete IP de capa 3 que muestra 192.168.1.110 como origen y 172.16.1.99 como destino.

Los paquetes IP contienen dos direcciones IP:

- **Dirección IP de origen**: la dirección IP del dispositivo emisor, la fuente de origen del paquete.
- **Dirección IP de destino**: la dirección IP del dispositivo receptor, es decir, el destino final del paquete.

Las direcciones de la capa de red, o direcciones IP, indican el origen y el destino final. Esto es cierto si el origen y el destino están en la misma red IP o redes IP diferentes.

Un paquete IP contiene dos partes:

- **Porción de red (IPv4) o Prefijo (IPv6)**: la sección más a la izquierda de la dirección que indica la red de la que es miembro la dirección IP. Todos los dispositivos de la misma red tienen la misma porción de red de la dirección.
- **Porción de host (IPv4) o ID de interfaz (IPv6)**: la parte restante de la dirección que identifica un dispositivo específico de la red. La sección de host es única para cada dispositivo o interfaz en la red.

Nota: La máscara de subred (IPv4) o la longitud del prefijo (IPv6) se utiliza para identifica la porción de red de una dirección IP de la porción del host.

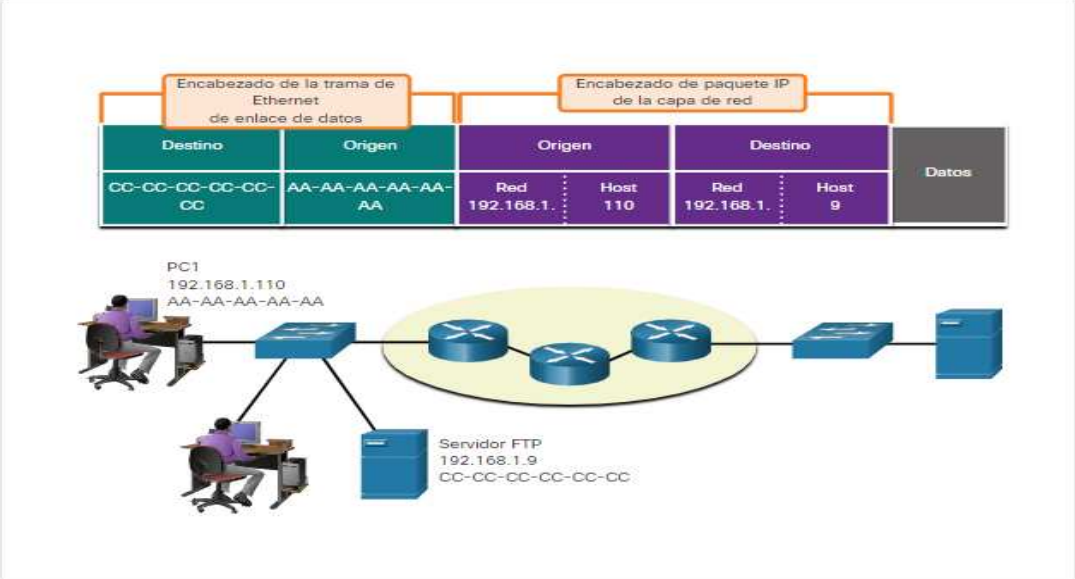
3.7.3

Dispositivos en la misma red

En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor FTP, en la misma red IP.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
- **Destination IPv4 address** - The IPv4 address of the receiving device, FTP server: 192.168.1.9.

En la figura, observe que la porción de red de las direcciones IP de origen y de destino se encuentran en la misma red. Observe en la figura que la parte de red de la dirección IPv4 de origen y la parte de red de la dirección IPv4 de destino son iguales y, por tanto, el origen y el destino están en la misma red.



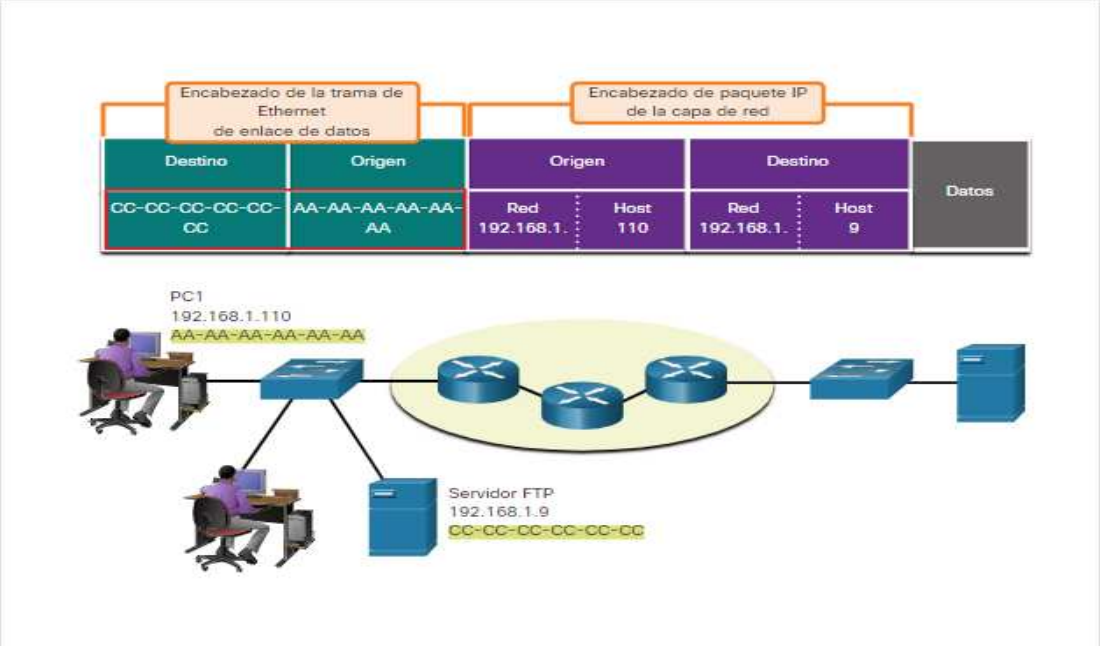
La figura muestra el encabezado de trama Ethernet de enlace de datos y el encabezado de paquete IP de capa de red para la información que fluye desde un origen a un destino en la misma red. En la parte inferior hay una topología de red. Comenzando por la izquierda, consta de PC1 con dirección IP 192.168.1.110 y dirección MAC AA-AA-AA-AA-AA, un servidor FTP con dirección IP 192.168.1.9 y dirección MAC CC-CC-CC-CC-CC-CC, y otro PC, todos conectados al mismo conmutador. En el medio de la topología hay una cadena de tres routeres a los que está conectado el conmutador. A la derecha hay otro conmutador conectado a un servidor. Por encima de la topología está el mensaje dividido en sus diversos componentes. Comienza a la izquierda con el encabezado de trama Ethernet de enlace de datos que muestra un destino de CC-CC-CC-CC-CC-CC y una fuente de AA-AA-AA-AA.

A continuación, se muestra el encabezado de paquete IP de capa de red que muestra un origen de 192.168.1 (red) 110 (host) y un destino de 192.168.1 (red) 9 (host). Por último, los datos.

3.7.4

Función de las direcciones de la capa de enlace de datos: la misma red IP

Cuando el emisor y el receptor del paquete IP están en la misma red, la trama de enlace de datos se envía directamente al dispositivo receptor. En una red Ethernet, las direcciones de enlace de datos se conocen como direcciones de Control de acceso a medios de Ethernet (MAC), como se resalta en la figura.



La figura muestra el encabezado de trama Ethernet de enlace de datos y el encabezado de paquete IP de capa de red para la información que fluye desde un origen a un destino en la misma red, resaltando el rol de la dirección MAC. En la parte inferior hay una topología de red. Comenzando por la izquierda, consta de PC1 con dirección IP 192.168.1.110 y dirección MAC AA-AA-AA-AA-AA (se muestra resaltado), un servidor FTP con dirección IP 192.168.1.9 y dirección MAC CC-CC-CC-CC-CC-CC (se muestra resaltado), y otro PC, todos conectados al mismo conmutador. En el medio de la topología hay una cadena de tres enrutadores a los que está conectado el conmutador. A la derecha hay otro conmutador conectado a un servidor. Por encima de la topología está el mensaje dividido en sus diversos

componentes. Comienza a la izquierda con el encabezado de trama Ethernet de enlace de datos que muestra un destino de CC-CC-CC-CC-CC-CC y una fuente de AA-AA-AA-AA. A continuación, se muestra el encabezado de paquete IP de capa de red que muestra un origen de 192.168.1 (red) 110 (host) y un destino de 192.168.1 (red) 9 (host). Por último, los datos.

Las direcciones MAC están integradas físicamente a la NIC Ethernet.

- **Dirección MAC de origen**: la dirección de enlace de datos, o la dirección MAC de Ethernet, del dispositivo que envía la trama de enlace de datos con el paquete IP encapsulado. La dirección MAC de la NIC Ethernet de PC1 es AA-AA-AA-AA-AA-AA, redactada en notación hexadecimal.
- **Destination MAC address**: When the receiving device is on the same network as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server: CC-CC-CC-CC-CC-CC, escrito en notación hexadecimal.

La trama con el paquete IP encapsulado ahora se puede transmitir desde PC1 directamente hasta el servidor FTP.

3.7.5

Dispositivos en una red remota

Sin embargo, ¿cuáles son las funciones de la dirección de la capa de red y de la dirección de la capa de enlace de datos cuando un dispositivo se comunica con un otro en una red remota? En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor, en este caso un servidor web, en una red IP diferente.

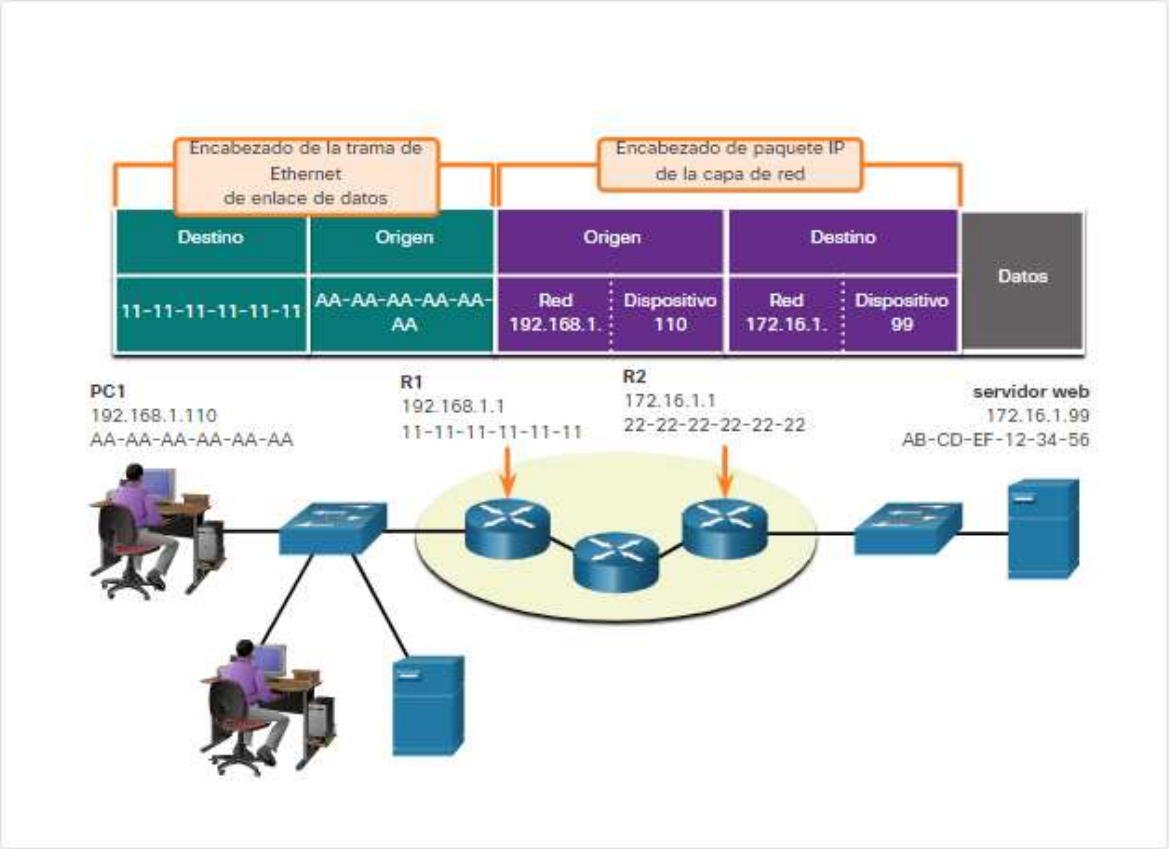
3.7.6

Función de las direcciones de la capa de red

Cuando el emisor del paquete se encuentra en una red distinta de la del receptor, las direcciones IP de origen y de destino representan los hosts en redes diferentes. Esto lo indica la porción de red de la dirección IP del host de destino.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
- **Destination IPv4 address** - The IPv4 address of the receiving device, the server, Web Server: 172.16.1.99.

En la figura, observe que la porción de red de las direcciones IP de origen y de destino se encuentran en redes diferentes.



La figura muestra el encabezado de trama Ethernet de enlace de datos y el encabezado de paquete IP de capa de red para la información que fluye desde un origen en una red a un destino en una red diferente. En la parte inferior hay una topología de red. Comenzando por la izquierda, consta de PC1 con IP 192.168.1.110 y MAC AA-AA-AA-AA, un servidor y otro PC, todos conectados al mismo conmutador. En el medio de la topología hay una cadena de tres routers a los que está conectado el switch. El router de la izquierda está etiquetado R1 con IP 192.168.1.1 y MAC 11-11-11-11-11-11. El router medio no está etiquetado. El router de la derecha está etiquetado R2 con IP 172.16.1.1 y MAC 22-22-22-22-22-22-22-22. A la derecha hay otro conmutador conectado a un servidor Web con IP 172.16.1.99 y MAC AB-CD-EF-12-34-56. Por encima de la topología está el mensaje dividido en sus diversos componentes. Comienza a la izquierda con el encabezado de trama Ethernet de enlace de datos que muestra un destino de 11-11-11-11-11-11-11-11 y una fuente de AA-AA-AA-AA. A continuación, se muestra el encabezado de paquete IP de capa de red que muestra un origen de 192.168.1 (red) 110 (dispositivo) y un destino de 172.16.1 (red) 99 (dispositivo). Por último, los datos.

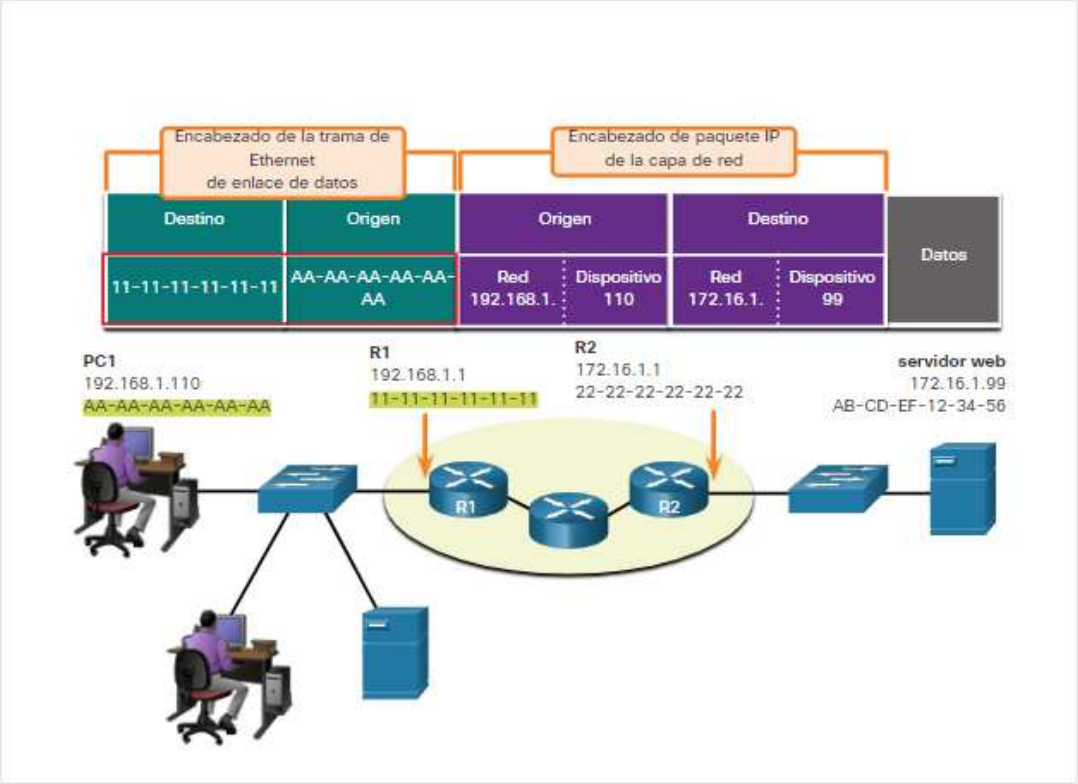
3.7.7

Rol de acceso a datos de las direcciones de capa de vínculo de datos: diferentes redes IP

Cuando el emisor y el receptor del paquete IP se encuentran en redes diferentes, la trama de enlace de datos de Ethernet no se puede enviar directamente al host de destino, debido a que en la red del emisor no se puede tener acceso directamente al host. La trama de Ethernet se debe enviar a otro dispositivo conocido como router o gateway predeterminado. En nuestro ejemplo, el gateway predeterminado es R1. R1 tiene una dirección de enlace de datos de Ethernet que se encuentra en la misma red que PC1. Esto permite que PC1 alcance el router directamente.

- **Dirección MAC de origen**: la dirección MAC de Ethernet del dispositivo emisor, PC1. La dirección MAC de la interfaz Ethernet de PC1 es AA-AA-AA-AA-AA-AA.
- **Dirección MAC de destino**: cuando el dispositivo receptor, la dirección IP de destino, está en una red distinta de la del dispositivo emisor, este utiliza la dirección MAC de Ethernet del gateway predeterminado o el router. En este ejemplo, la dirección MAC de destino es la dirección MAC de la interfaz Ethernet de R1, 11-11-11-11-11-11. Esta es la interfaz que está conectada a la misma red que PC1, como se muestra en la figura.

La figura muestra el encabezado de trama Ethernet de enlace de datos y el encabezado de paquete IP de capa de red para la información que fluye desde un origen en una red a un destino en una red diferente, resaltando el rol de la dirección MAC. En la parte inferior hay una topología de red. Comenzando por la izquierda, consta de PC1 con IP 192.168.1.110 y MAC AA-AA-AA-AA-AA (se muestra resaltado), un servidor y otro PC, todos conectados al mismo conmutador. En el medio de la topología hay una cadena de tres routers a los que está conectado el switch. El router de la izquierda está etiquetado R1 con IP 192.168.1.1 y MAC 11-11-11-11-11-11-11 (se muestra resaltado). El router medio no está etiquetado. El enrutador de la derecha está etiquetado R2 con IP 172.16.1.1 y MAC 22-22-22-22-22-22-22. A la derecha hay otro conmutador conectado a un servidor Web con IP 172.16.1.99 y MAC AB-CD-EF-12-34-56. Por encima de la topología está el mensaje dividido en sus diversos componentes. Comienza a la izquierda con el encabezado de trama Ethernet de enlace de datos que muestra un destino de 11-11-11-11-11-11-11-11 y una fuente de AA-AA-AA-AA. A continuación, se muestra el encabezado de paquete IP de capa de red que muestra un origen de 192.168.1 (red) 110 (dispositivo) y un destino de 172.16.1 (red) 99 (dispositivo). Por último, los datos.



La trama de Ethernet con el paquete IP encapsulado ahora se puede transmitir a R1. R1 reenvía el paquete al destino, el servidor web. Esto puede significar que R1 reenvía el paquete a otro router o directamente al servidor web si el destino se encuentra en una red conectada a R1.

Es importante que en la dirección IP del gateway predeterminado esté configurada en cada host de la red local. Todos los paquetes que tienen como destino redes remotas se envían al gateway predeterminado. Las direcciones MAC de Ethernet y el gateway predeterminado se analizan en capítulos más adelante.

3.7.8

Direcciones de enlace de datos

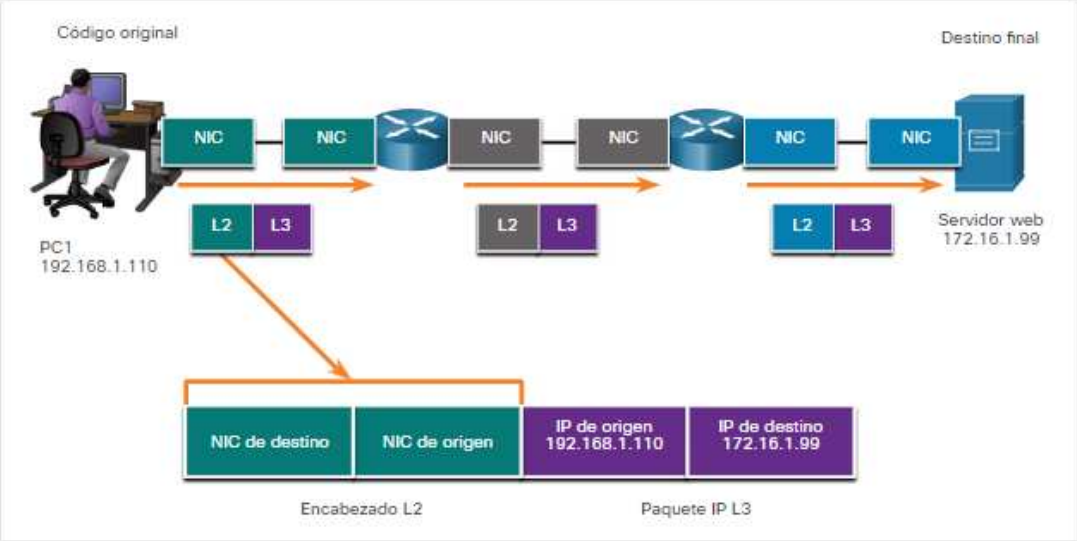
La dirección física de la capa de enlace de datos, o capa 2, tiene una función distinta. Su propósito es enviar la trama de enlace de datos desde una interfaz de red hasta otra interfaz de red en la misma red.

Antes de que un paquete IP pueda enviarse a través de una red conectada por cable o inalámbrica, se debe encapsular en una trama de enlace de datos de modo que pueda transmitirse a través del medio físico.

Haga clic en cada botón para ver una ilustración de cómo cambian las direcciones de la capa de vínculos de datos en cada salto de origen a destino

Host a router | Router a router | Router a Servidor

Host a enrutador



La figura muestra el encabezado L2 en el primer salto a medida que la información fluye desde un host en una red a un servidor en otra red. Una topología de red muestra el PC1 de origen original en 192.168.1.10 conectado a un router, conectado a otro router, conectado al servidor Web de destino final en 172.16.1.99. Debajo de la topología hay un paquete IP L3 con IP de origen 192.168.1.110 y IP de destino 172.16.1.99. Delante del paquete está el encabezado L2 con NIC de destino y NIC de origen. Estas direcciones de encabezado L2 coinciden con la NIC del origen original (PC1) y la interfaz del router de salto siguiente.

A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido. Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

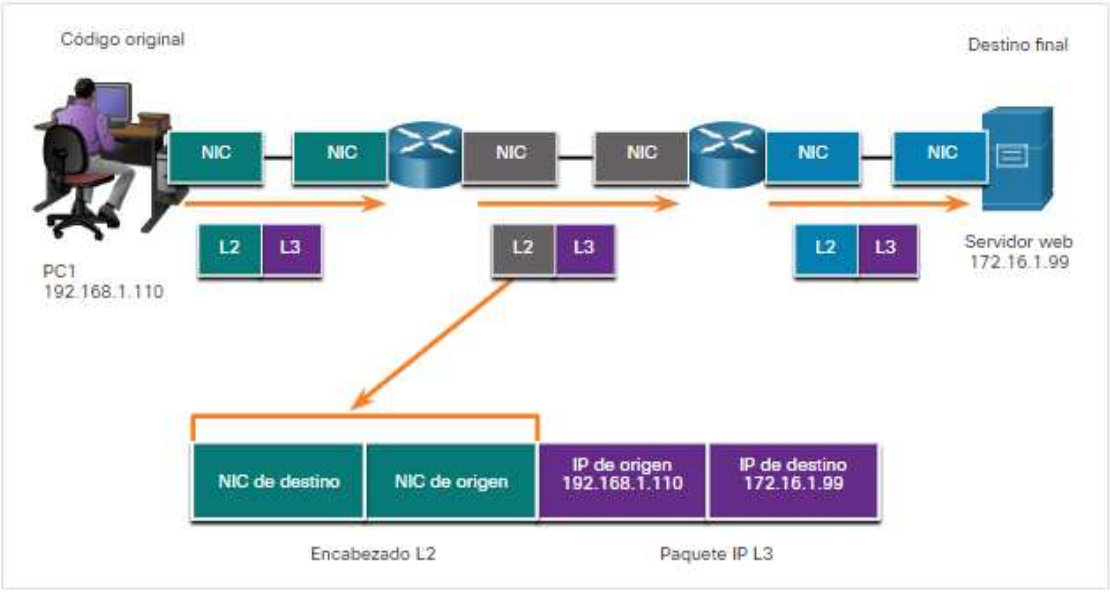
El protocolo de enlace de datos de capa 2 solo se utiliza para enviar el paquete de NIC a NIC en la misma red. El router elimina la información de la capa 2 a medida que una NIC la recibe

y agrega nueva información de enlace de datos antes de reenviarla a la NIC de salida en su recorrido hacia el dispositivo de destino final.

El paquete IP se encapsula en una trama de enlace de datos que contiene información de enlace de datos, como la siguiente:

- **Dirección de enlace de datos de origen**: la dirección física de la NIC del dispositivo que envía la trama de enlace de datos.
- **Dirección de enlace de datos de destino**: la dirección física de la NIC que recibe la trama de enlace de datos. Esta dirección es el router del salto siguiente o el dispositivo de destino final.

Enrutador a enrutador



La figura muestra el encabezado L2 a medida que la información fluye entre los routeres en su camino desde el PC de origen original hasta el servidor de destino final. Una topología de red muestra el PC1 de origen original en 192.168.1.10 conectado a un router, conectado a otro router, conectado al servidor Web de destino final en 172.16.1.99. Debajo de la topología hay un paquete IP L3 y un encabezado L2 que representan el direccionamiento a medida que los datos se mueven entre los dos routeres. El paquete IP L3 tiene una IP de origen 192.168.1.110 y una IP de destino 172.16.1.99. Delante del paquete está el encabezado L2 con NIC de destino y NIC de origen. Las direcciones de encabezado L2 coinciden con las NIC de las interfaces que conectan los dos routeres.

A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido.

Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

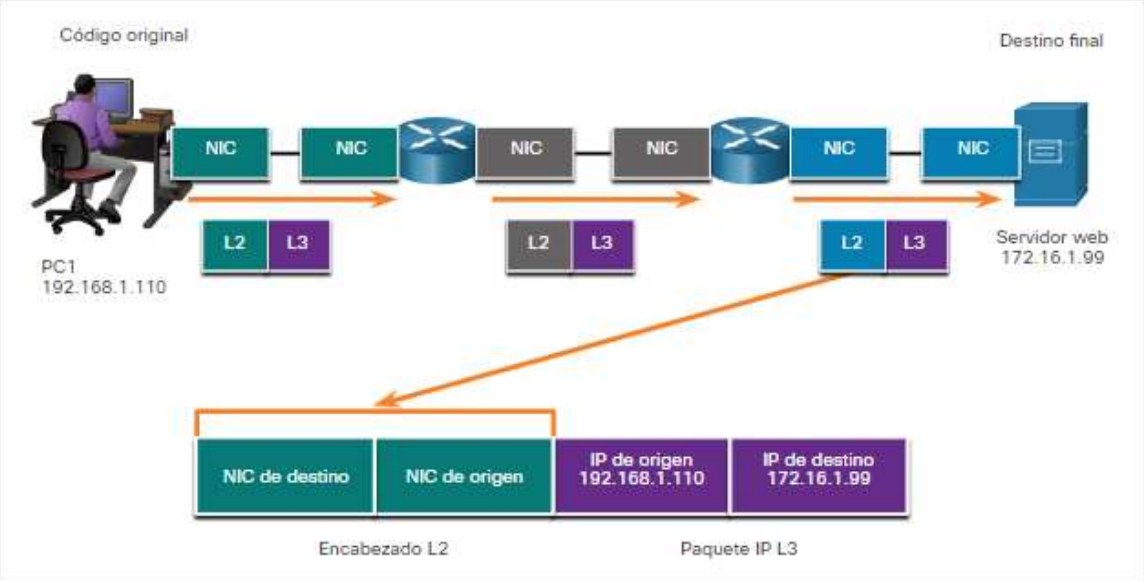
El protocolo de enlace de datos de capa 2 solo se utiliza para enviar el paquete de NIC a NIC en la misma red. El router elimina la información de la capa 2 a medida que una NIC la recibe y agrega nueva información de enlace de datos antes de reenviarla a la NIC de salida en su recorrido hacia el dispositivo de destino final.

El paquete IP se encapsula en una trama de enlace de datos que contiene información de enlace de datos, como la siguiente:

- **Dirección de enlace de datos de origen**: la dirección física de la NIC del dispositivo que envía la trama de enlace de datos.
- **Dirección de enlace de datos de destino**: la dirección física de la NIC que recibe la trama de enlace de datos. Esta dirección es el router del salto siguiente o el dispositivo de destino final.

Host a router | Router a router | Router a Servidor

Enrutador a servidor



La figura muestra el encabezado L2 a medida que la información fluye desde un router a un servidor de destino final. Una topología de red muestra el PC1 de origen original en 192.168.1.10 conectado a un router, conectado a otro router, conectado al servidor Web de destino final en 172.16.1.99. Debajo de la topología hay un paquete IP L3 y un encabezado L2 que representan el direccionamiento a medida que los datos se mueven desde el último router hasta el destino final. El paquete IP L3 tiene una IP de origen 192.168.1.110 y una IP de destino 172.16.1.99. Delante del paquete está el encabezado L2 con NIC de destino y NIC de origen. Las direcciones

de encabezado L2 coinciden con las NIC de la interfaz de routeres en la red de destino y el servidor web de destino final.

A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido. Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

El protocolo de enlace de datos de capa 2 solo se utiliza para enviar el paquete de NIC a NIC en la misma red. El router elimina la información de la capa 2 a medida que una NIC la recibe y agrega nueva información de enlace de datos antes de reenviarla a la NIC de salida en su recorrido hacia el dispositivo de destino final.

El paquete IP se encapsula en una trama de enlace de datos que contiene información de enlace de datos, como la siguiente:

- **Dirección de enlace de datos de origen**: la dirección física de la NIC del dispositivo que envía la trama de enlace de datos.
- **Dirección de enlace de datos de destino**: la dirección física de la NIC que recibe la trama de enlace de datos. Esta dirección es el router del salto siguiente o el dispositivo de destino final.

3.7.9

Práctica de laboratorio: Instalación de Wireshark

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolo y software y educación. Wireshark se utiliza en todo el curso para demostrar conceptos de red. En esta práctica de laboratorio, descargará e instalará Wireshark.

Instalación de Wireshark

3.7.10

Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red

En esta práctica de laboratorio se utilizará Wireshark para capturar y analizar el tráfico.

Uso de Wireshark para ver el tráfico de la red

3.7.11

Ponga a prueba su conocimiento: Acceso de datos

Verifique su comprensión de la encapsulación de datos eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es verdadero. Cuando dos dispositivos están en redes IP diferentes, las tramas no se pueden enviar directamente al receptor ya que se encuentra en una red lógica diferente. Las tramas primero deben reenviarse a una puerta de enlace predeterminada (router).
2. La respuesta correcta es falso. Es la parte situada más a la izquierda de una dirección IP que identifica la red. La parte situada más a la derecha se utiliza para identificar el dispositivo o interfaz específico.
3. La máscara de subred se utiliza para determinar la porción de red de una dirección IPv4.
4. Las direcciones MAC son direcciones físicas y 48 bits o 12 dígitos hexadecimales de longitud. Las direcciones IPv4 y las direcciones IPv6 son lógicas. Las direcciones IPv4 son de 32 bits y las direcciones IPv6 son de 128 bits.
5. El direccionamiento del marco de enlace de datos consiste en una dirección MAC de destino y origen en ese orden.
6. La respuesta correcta es falso. Las direcciones de enlace de datos cambian dentro del marco de enlace de datos cuando el dispositivo receptor no está en la misma red.

Has tenido 6 respuestas correctas de 6.

1. ¿Verdadero o falso? Las tramas intercambiadas entre dispositivos de diferentes redes IP deben reenviarse a una puerta de enlace predeterminada.

¡Lo tienes!

- (•) Verdadero
- ( ) Falso

2. ¿Verdadero o falso? La parte más derecha de una dirección IP se utiliza para identificar la red a la que pertenece un dispositivo.

¡Lo tienes!

- ( ) Verdadero
- (•) Falso

3. ¿Qué se utiliza para determinar las porciones de red y host de una dirección IPv4?

¡Lo tienes!

- (•) Máscara de subred
- ( ) Dirección MAC
- ( ) parte más derecha de la dirección IP
- ( ) parte más a la izquierda de la dirección MAC

4. ¿Cuáles de las siguientes instrucciones son verdaderas con respecto a las direcciones de capa de red y capa de enlace de datos? (Escoja tres opciones).

¡Lo tienes!

- [ ] Las direcciones de capa de vínculo de datos son lógicas y las direcciones de capa de red son físicas.
- [ ] Las direcciones de capa de red se expresan como 12 dígitos hexadecimales y las direcciones de capa de vínculo de datos son decimales.
- [x] Las direcciones de capa de red son lógicas y las direcciones de enlace de datos se expresan como 12 dígitos hexadecimales.
- [x] Las direcciones de capa de vínculo de datos son físicas y las direcciones de capa de red son lógicas.
- [x] Las direcciones de capa de red tienen 32 o 128 bits de longitud.
- [ ] Las direcciones de capa de enlace de datos tienen 32 bits de longitud.

5. ¿Cuál es el orden de las dos direcciones en el marco de enlace de datos?

¡Lo tienes!

- ○ MAC de origen a MAC de destino
- ○ MAC de destino, IP de origen
- ○ IP de destino, IP de origen
- ◉ MAC de destino a MAC de origen
- ○ IP de origen a IP de destino

6. ¿Verdadero o falso? Las direcciones de vínculo de datos son físicas, por lo que nunca cambian en el marco de vínculo de datos de origen a destino.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

Correct

You have successfully identified the correct answers.

1. The correct answer is True. When two devices are on different IP networks, frames cannot be sent directly to the receiver since it is on a different logical network. The frames must first be forwarded to a default gateway (router).
2. The correct answer is False. It is the left-most portion of an IP address that identifies the network. The right-most portion is used to identify the specific device or interface.
3. It is the subnet mask used in IPv4 that is used to determine the network portion of an IPv4 address.
4. MAC addresses are physical addresses and 48 bits or 12 hex digits in length. IPv4 addresses and IPv6 addresses are logical. IPv4 addresses are 32 bits and IPv6 addresses are 128 bits.
5. The data link frame addressing consists of a destination and source MAC address in that order.
6. The correct answer is False. Data link addresses change within the data link frame when the receiving device is not on the same network.

You got 6 out of 6 questions correct.

1. True or false? Frames exchanged between devices in different IP networks must be forwarded to a default gateway.

You got it!

- (●) True
- ( ) False

2. True or false? The right-most part of an IP address is used to identify the network that a device belongs to.

You got it!

- ( ) True
- (●) False

3. What is used to determine the network portion of an IPv4 address?

You got it!

- (●) subnet mask
- ( ) MAC address
- ( ) right-most part of the IP address
- ( ) left-most part of the MAC address

4. Which of the following statements are true regarding network layer and data link layer addresses? (Choose three.)

You got it!

- [ ] Data link layer addresses are logical and network layer addresses are physical.
- [ ] Network layer addresses are expressed as 12 hexadecimal digits and data link layer addresses are decimal.
- [x] Network layer addresses are logical and data link addresses are expressed as 12 hexadecimal digits.
- [x] Data link layer addresses are physical and network layer addresses are logical.
- [x] Network layer addresses are either 32 or 128 bits in length.
- [ ] Data link layer addresses are 32 bits in length.

5. What is the order of the two addresses in the data link frame?

You got it!

- ( ) source MAC, destination MAC
- ( ) destination MAC, source IP
- ( ) destination IP, source IP
- (●) destination MAC, source MAC
- ( ) source IP, destination IP

6. True or False? Data Link addresses are physical so they never change in the data link frame from source to destination.

You got it!

- ( ) True
- (●) False

Protocolos y modelos / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

3.8.1

¿Qué aprenderé en este módulo?

Las reglas

Todos los métodos de comunicación tienen tres elementos en común: origen del mensaje (remitente), destino del mensaje (receptor) y canal. El envío de un mensaje se rige por reglas denominadas *protocols*. Los protocolos deben incluir: un remitente y receptor identificado, lenguaje y gramática comunes, velocidad y tiempo de entrega, y requisitos de confirmación o acuse de recibo. Los protocolos de red determinan la codificación, el formato, la encapsulación, el tamaño, la distribución y las opciones de entrega del mensaje. La codificación es el proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación revierte este proceso para interpretar la idea. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje. Sincronización: incluye el método de acceso, control del flujo y tiempo de espera de respuesta. Las opciones de entrega de mensajes incluyen unidifusión, multidifusión y difusión.

Protocolos

Los protocolos son implementados por dispositivos finales y dispositivos intermediarios en software, hardware o ambos. Un mensaje enviado a través de una red informática normalmente requiere el uso de varios protocolos, cada uno con sus propias funciones y formato. Cada protocolo de red tiene su propia función, formato y reglas para las comunicaciones. La familia de protocolos Ethernet incluye IP, TCP, HTTP y muchos más. Los protocolos protegen los datos para proporcionar autenticación, integridad de los datos y cifrado de datos: SSH, SSL y TLS. Los protocolos permiten a los routeres intercambiar información de ruta, comparar información de ruta y, a continuación, seleccionar la mejor ruta de acceso a la red de destino: OSPF y BGP. Los protocolos se utilizan para la detección automática de dispositivos o servicios: DHCP y DNS. Los equipos y dispositivos de red utilizan protocolos acordados que proporcionan las siguientes funciones: direccionamiento, confiabilidad, control de flujo, secuenciación, detección de errores e interfaz de aplicación.

Suite de Protocolos

Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Una pila de protocolos muestra la forma en que los protocolos individuales se implementan dentro de una suite. Desde la década de 1970

ha habido varios conjuntos de protocolos diferentes, algunos desarrollados por una organización de estándares y otros desarrollados por varios proveedores. Los protocolos TCP/IP son específicos de las capas Aplicación, Transporte e Internet. TCP/IP es el conjunto de protocolos utilizado por las redes e Internet actuales. TCP/IP ofrece dos aspectos importantes a proveedores y fabricantes: conjunto de protocolos estándar abierto y conjunto de protocolos basado en estándares. El proceso de comunicación del conjunto de protocolos TCP/IP permite procesos tales como un servidor web encapsular y enviar una página web a un cliente, así como el cliente desencapsular la página web para mostrarla en un explorador web.

Organizaciones de estandarización

Los estándares abiertos fomentan la interoperabilidad, la competencia y la innovación. Las organizaciones de estandarización generalmente son organizaciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos. Varias organizaciones tienen diferentes responsabilidades para promover y crear estándares para Internet, incluyendo: ISOC, IAB, IETF e IRTF. Las organizaciones de estándares que desarrollan y soportan TCP/IP incluyen: ICANN e IANA. Las organizaciones de estándares electrónicos y de comunicaciones incluyen: IEEE, EIA, TIA y ITU-T.

Modelos de referencia

Los dos modelos de referencia que se utilizan para describir las operaciones de red son OSI y TCP/IP. El modelo de referencia OSI tiene siete capas:

7 - Aplicación

6 - Presentación

5 - Sesión

4-Transporte

3 - Red

2 - Enlacede datos

1-Física

El modelo TCP/IP incluye cuatro capas.

4 - Aplicación

3-Transporte

2 - Internet

1 - Acceso a la red

Encapsulación de datos

La segmentación de mensajes tiene dos beneficios principales.

- Al enviar partes individuales más pequeñas del origen al destino, se pueden intercalar muchas conversaciones diferentes en la red. Este proceso se denomina multiplexación.
- La segmentación puede aumentar la eficiencia de las comunicaciones de red. Si parte del mensaje no logra llegar al destino, solo deben retransmitirse las partes faltantes.

TCP es responsable de secuenciar los segmentos individuales. La manera que adopta una porción de datos en cualquier capa se denomina unidad de datos del protocolo (PDU). Durante el encapsulamiento, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. Cuando se envían mensajes en una red, el proceso de encapsulamiento opera desde las capas superiores hacia las capas inferiores. Este proceso se invierte en el host receptor, y se conoce como desencapsulamiento. El desencapsulamiento es el proceso que utilizan los dispositivos receptores para eliminar uno o más de los encabezados de protocolo. Los datos se desencapsulan mientras suben por la pila hacia la aplicación del usuario final.

Acceso a los datos

La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor. Los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

- **Direcciones de origen y de destino de la capa de red**: son responsables de enviar el paquete IP desde el dispositivo de origen hasta el dispositivo final, ya sea en la misma red o a una red remota.
- **Direcciones de origen y de destino de la capa de enlace de datos**: son responsables de enviar la trama de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra en la misma red.

Las direcciones de la capa de red, o direcciones IP, indican el origen y el destino final. Una dirección IP contiene dos partes: la parte de red (IPv4) o Prefijo (IPv6) y la parte de host (IPv4) o el ID de interfaz (IPv6). Cuando el emisor y el receptor del paquete IP están en la misma red, la trama de enlace de datos se envía directamente al dispositivo receptor. En una red Ethernet, las direcciones de enlace de datos se conocen como direcciones MAC de Ethernet. Cuando el emisor del paquete se encuentra en una red distinta de la del receptor, las direcciones IP de origen y de destino representan los hosts en redes diferentes. La trama de Ethernet se debe enviar a otro dispositivo conocido como router o gateway predeterminado.

3.8.2

Módulo Quiz - Protocolos y Modelos

Correcto

Identificó bien las respuestas correctas.

Has tenido 15 respuestas correctas de 15.

1. ¿Cuáles son los tres acrónimos o siglas que representan organismos de estandarización? Elija tres opciones.

Tema 3.4.0 TCP/IP es una pila de protocolos que contiene muchos otros protocolos, como HTTP, FTP y DNS. Durante la comunicación en Internet, se requiere el uso de la pila de protocolos TCP/IP. Una dirección MAC es una dirección grabada en una tarjeta de red Ethernet.OSI es el modelo de siete capas que se usa para explicar la forma en que funcionan las redes.

- [x] IANA
- [ ] TCP/IP
- [x] IEEE
- [x] IETF
- [ ] OSI
- [ ] MAC

2. ¿En qué tipo de comunicación se envía un mensaje a todos los dispositivos de una red de área local?

Tema 3.1.0 Las comunicaciones de difusión son comunicaciones de uno a todos. Las comunicaciones de unidifusión son comunicaciones de uno a uno. Las comunicaciones de multidifusión son comunicaciones de uno a muchos en las que el mensaje se distribuye a grupos de hosts específicos. "Omnidifusión" no es un término estándar para describir la distribución de mensajes.

- (•) Difusión
- ( ) Multidifusión
- ( ) Unidifusión
- ( ) Omnidifusión

3. En la comunicación por computadora, ¿cuál es el propósito de la codificación de mensajes?

Tema 3.1.0 Para que un mensaje se pueda enviar por una red, en primer lugar, se lo debe codificar. La codificación es el proceso de convertir el mensaje de datos en otro formato adecuado para la transmisión por el medio físico. Cada bit del mensaje se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje.

- (●) Convertir la información a la forma adecuada para la transmisión.
- ( ) Interpretar la información.
- ( ) Dividir los mensajes largos en tramas más pequeñas.
- ( ) Negociar la temporización adecuada para que la comunicación sea correcta.

4. ¿Qué opción de entrega de mensajes se utiliza cuando todos los dispositivos necesitan recibir el mismo mensaje simultáneamente?

Tema 3.1.0 - Cuando todos los dispositivos necesitan recibir el mismo mensaje simultáneamente, el mensaje se entregaría como una transmisión. La entrega de unidifusión se produce cuando un host de origen envía un mensaje a un host de destino. El envío del mismo mensaje desde un host a un grupo de hosts de destino es la entrega de multidifusión. Las comunicaciones dúplex se refieren a la capacidad del medio para llevar mensajes en ambas direcciones.

- ( ) desajuste
- ( ) Unidifusión
- ( ) Multidifusión
- (●) Difusión

5. ¿Cuáles de los siguientes beneficios corresponden a un modelo de red en capas? Elija dos opciones.

Tema 3.5.0 Algunos proveedores desarrollan sus propios modelos y protocolos de referencia. Hoy en día, si un dispositivo debe comunicarse a través de Internet, debe utilizar el modelo TCP/IP. Los beneficios de utilizar un modelo en capas son los siguientes:
Asistir en el diseño de protocolos.
Fomenta la competencia entre proveedores.
Evita que una tecnología que funciona en una capa afecte a las demás.
Proporciona un lenguaje común para describir la funcionalidad de red.
Permite visualizar la interacción y los protocolos entre cada capa.

- [x] Asiste en el diseño de protocolos.
- [ ] Acelera la distribución de paquetes.
- [ ] Impide a los diseñadores crear su propio modelo.
- [x] Impide que la tecnología de una capa afecte las demás.
- [ ] Asegura que un dispositivo que funciona en una capa pueda funcionar en la capa superior siguiente.

6. ¿Cuál es el propósito de los protocolos en las comunicaciones de datos?

Tema 3.1.0 Los protocolos proporcionan las reglas que definen cómo se transmite un mensaje a través de una red. Los requisitos de implementación, como los detalles electrónicos y de ancho de banda para la comunicación de datos, se especifican en estándares. Los sistemas operativos no están especificados por protocolos, pero implementan protocolos. Los protocolos determinan cómo y cuándo se envía un mensaje, pero no controlan su contenido.

- ○ Especificar el ancho de banda del canal o el medio para cada tipo de comunicación.
- ○ Especificar los sistemas operativos de los dispositivos que permiten la comunicación.
- ◉ Proporcionar las reglas requeridas para que se produzca un tipo específico de comunicación.
- ○ Definir el contenido del mensaje que se envía durante la comunicación.

7. ¿Qué dirección lógica se utiliza para la entrega de datos a una red remota?

Tema 3.7.0 - La dirección IP de destino se utiliza para la entrega de datos de extremo a extremo a una red remota. La dirección MAC de destino se utiliza para la entrega local de tramas de Ethernet. El número de puerto de destino identifica la aplicación que debe procesar los datos en el destino. Las direcciones de origen identifican al remitente de los datos.

- ○ Dirección MAC de destino
- ◉ Dirección IP de destino
- ○ Número de puerto de destino
- ○ Dirección MAC de origen
- ○ Dirección IP de origen

8. ¿Cuál es el término general que se utiliza para describir una pieza de datos en cualquier capa de un modelo de red?

Tema 3.6.0 - El término unidad de datos de protocolo (PDU) se utiliza para describir una pieza de datos en cualquier capa de un modelo de red. En la capa de red, la PDU se llama "paquete". Trama: PDU de la capa de enlace de datos El segmento es la PDU de la capa de transporte.

- ○ marco
- ○ paquete
- ◉ unidad de datos del protocolo
- ○ Segmento

9. ¿Cuáles son los dos protocolos que funcionan en la capa de Internet? Elija dos opciones.

Tema 3.3.0 - Tanto ICMP como IP funcionan en la capa de Internet, mientras que PPP es un protocolo de la capa de acceso a la red, y POP y BOOTP son protocolos de la capa de aplicación.

- ☐ POP
- ☐ BOOTP
- ☑ ICMP
- ☑ IP
- ☐ PPP

10. ¿Qué capa del modelo OSI define los servicios para segmentar y rearmar los datos de comunicaciones individuales entre terminales?

Tema 3.5.0: el modelo OSI consta de siete capas: aplicación, presentación, sesión, transporte, red, enlace de datos y físico. La capa de transporte define los servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales entre terminales.

- ○ Aplicación
- ○ Presentación
- ○ Sesión
- ◉ Transporte
- ○ Red

11. ¿Qué tipo de comunicación enviará un mensaje a un grupo de destinos anfitriones simultáneamente?

Tema 3.1.0: la multidifusión es una comunicación de uno a muchos en la que el mensaje se entrega a un grupo específico de hosts. Las comunicaciones de difusión son comunicaciones de uno a todos. Las comunicaciones de unidifusión son comunicaciones de uno a uno. Anycast es un término IPv6 y es el envío de datos en una comunicación uno a más cercana.

- ○ Difusión
- ◉ Multidifusión
- ○ Unidifusión
- ○ Difusión por proximidad

12. ¿Qué proceso se utiliza para recibir datos transmitidos y convertirlos en un mensaje legible?

Tema 3.1.0 – La decodificación es el proceso de recepción de datos transmitidos e inversión del proceso de codificación para interpretar la información. Un ejemplo es una persona que escucha un correo de voz y decodifica los sonidos para entender el mensaje recibido.

- ○ Control de acceso
- ◉ Decodificación
- ○ Encapsulamiento
- ○ Control del flujo

13. ¿Qué le sucede a un paquete IP antes de que se transmita por el medio físico?

Tema 3.6.0 – Cuando se envían mensajes en una red, el proceso de encapsulamiento se realiza de arriba abajo en los modelos OSI o TCP/IP. En cada capa del modelo, la información de la capa superior se encapsula en el campo de datos del siguiente protocolo. Por ejemplo, para que se pueda enviar un paquete IP por el medio físico, en primer lugar, se lo encapsula en una trama de enlace de datos en la capa 2.

- ○ Se lo etiqueta con información que garantiza la distribución confiable.
- ○ Se lo segmenta en porciones individuales más pequeñas.
- ○ Se lo encapsula en un segmento TCP.
- ◉ Se lo encapsula en una trama de capa 2.

14. ¿Cuál es el proceso que se utiliza para colocar un mensaje dentro de otro para transferirlo del origen al destino?

Tema 3.1.0 - El encapsulamiento es el proceso en el que se coloca un formato de mensaje dentro de otro. Un ejemplo de esto es la manera en la que un paquete se coloca entero en el campo de datos a medida que se encapsula en una trama.

- ○ Control de acceso
- ○ Decodificación
- ◉ Encapsulamiento
- ○ Control del flujo

15. Un cliente web está enviando una solicitud de una página web a un servidor web. Desde la perspectiva del cliente, ¿cuál es el orden correcto de la pila de protocolos que se usa para preparar la solicitud de transmisión?

Tema 3.3.0 - 1. HTTP Rige la manera en que interactúan un servidor web y un cliente. 2. Administra las conversaciones individuales entre servidores y clientes web. 3. IP es responsable de la entrega a través de la mejor ruta al destino. 4. Ethernet toma el paquete de IP y lo formatea para su transmisión.

- ○ HTTP, IP, TCP, Ethernet
- ◉ HTTP, TCP, IP, Ethernet
- ○ Ethernet, TCP, IP, HTTP
- ○ Ethernet, IP, TCP, HTTP

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. Which three acronyms/initialisms represent standards organizations? (Choose three.)

Topic 3.4.0 - TCP/IP is a protocol stack that contains a lot of other protocols such as HTTP, FTP, and DNS. The TCP/IP protocol stack is required to be used when communicating on the Internet. A MAC address is an address that is burned into an Ethernet network card. OSI is the 7 layer model that is used to explain how networking works.

- ☑ IANA
- ☐ TCP/IP
- ☑ IEEE
- ☑ IETF
- ☐ OSI
- ☐ MAC

2. What type of communication will send a message to all devices on a local area network?

Topic 3.1.0 – Broadcast communication is a one-to-all communication. A unicast communication is a one-to-one communication. Multicast is a one-to-many communication where the message is delivered to a specific group of hosts. Allcast is not a standard term to describe message delivery.

- (●) broadcast
- ( ) multicast
- ( ) unicast
- ( ) allcast

3. In computer communication, what is the purpose of message encoding?

Topic 3.1.0 – Before a message is sent across a network it must first be encoded. Encoding is the process of converting the data message into another format suitable for transmission across the physical medium. Each bit of the message is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message.

- (●) to convert information to the appropriate form for transmission
- ( ) to interpret information
- ( ) to break large messages into smaller frames
- ( ) to negotiate correct timing for successful communication

4. Which message delivery option is used when all devices need to receive the same message simultaneously?

Topic 3.1.0 – When all devices need to receive the same message simultaneously, the message would be delivered as a broadcast. Unicast delivery occurs when one source host sends a message to one destination host. The sending of the same message from a host to a group of destination hosts is multicast delivery. Duplex communications refers to the ability of the medium to carry messages in both directions.

- ( ) duplex
- ( ) unicast
- ( ) multicast
- (●) broadcast

5. What are two benefits of using a layered network model? (Choose two.)

Topic 3.5.0 – Some vendors have developed their own reference models and protocols. Today, if a device is to communicate on the Internet, the device must use the TCP/IP model. The benefits of using a layered model are as follows:

- assists in protocol design
- fosters competition between vendors
- prevents a technology that functions at one layer from affecting any other layer
- provides a common language for describing network functionality
- helps in visualizing the interaction between each layer and protocols between each layer

- [x] It assists in protocol design.
- [ ] It speeds up packet delivery.
- [ ] It prevents designers from creating their own model.
- [x] It prevents technology in one layer from affecting other layers.
- [ ] It ensures a device at one layer can function at the next higher layer.

6. What is the purpose of protocols in data communications?

Topic 3.1.0 - Protocols provide rules that define how a message is transmitted across a network. Implementation requirements such as electronic and bandwidth details for data communication are specified by standards. Operating systems are not specified by protocols, but will implement protocols. Protocols determine how and when to send a message but they do not control the contents of a message.

- specifying the bandwidth of the channel or medium for each type of communication
- specifying the device operating systems that will support the communication
- (●) providing the rules required for a specific type of communication to occur
- dictating the content of the message sent during communication

7. Which logical address is used for delivery of data to a remote network?

Topic 3.7.0 - The destination IP address is used for end-to-end delivery of data to a remote network. The destination MAC address is used for delivery on a local network. The destination port number identifies the application that should process the data at the destination. Source addresses identify the sender of the data.

- destination MAC address
- (●) destination IP address
- destination port number
- source MAC address
- source IP address

8. What is the general term that is used to describe a piece of data at any layer of a networking model?

Topic 3.6.0 - The term protocol data unit (PDU) is used to describe a piece of data at any layer of a networking model. A packet is the PDU at the network layer. A frame is the data link layer PDU. A segment is the PDU at the transport layer.

- frame
- packet
- (●) protocol data unit
- segment

9. Which two protocols function at the internet layer? (Choose two.)

Topic 3.3.0 - ICMP and IP both function at the internet layer, whereas PPP is a network access layer protocol, and POP and BOOTP are application layer protocols.

- [ ] POP
- [ ] BOOTP
- [x] ICMP
- [x] IP
- [ ] PPP

10. Which layer of the OSI model defines services to segment and reassemble data for individual communications between end devices?

Topic 3.5.0 - The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

- ( ) application
- ( ) presentation
- ( ) session
- (•) transport
- ( ) network

11. Which type of communication will send a message to a group of host destinations simultaneously?

Topic 3.1.0 - Multicast is a one-to-many communication where the message is delivered to a specific group of hosts. Broadcast communication is a one-to-all communication. A unicast communication is a one-to-one communication. Anycast is an IPv6 term and is the sending of data in a one-to-nearest communication.

- ( ) broadcast
- (•) multicast
- ( ) unicast
- ( ) anycast

12. What process is used to receive transmitted data and convert it into a readable message?

Topic 3.1.0 - Decoding is the process of receiving transmitted data and reversing the encoding process to interpret the information. An example is a person that listens to a voicemail and decodes the sounds to understand the received message.

- ○ access control
- ◉ decoding
- ○ encapsulation
- ○ flow control

13. What is done to an IP packet before it is transmitted over the physical medium?

Topic 3.6.0 - When messages are sent on a network, the encapsulation process works from the top of the OSI or TCP/IP model to the bottom. At each layer of the model, the upper layer information is encapsulated into the data field of the next protocol. For example, before an IP packet can be sent, it is encapsulated in a data link frame at Layer 2 so that it can be sent over the physical medium.

- ○ It is tagged with information guaranteeing reliable delivery.
- ○ It is segmented into smaller individual pieces.
- ○ It is encapsulated into a TCP segment.
- ◉ It is encapsulated in a Layer 2 frame.

14. What process is used to place one message inside another message for transfer from the source to the destination?

Topic 3.1.0 - Encapsulation is the process of placing one message format into another message format. An example is how a packet is placed in its entirety into the data field as it is encapsulated into a frame.

- ○ access control
- ○ decoding
- ◉ encapsulation
- ○ flow control

15. A web client is sending a request for a webpage to a web server. From the perspective of the client, what is the correct order of the protocol stack that is used to prepare the request for transmission?

Topic 3.3.0 - 1. HTTP governs the way that a web server and client interact.
2. TCP manages individual conversations between web servers and clients.
3. IP is responsible for delivery across the best path to the destination.
4. Ethernet takes the packet from IP and formats it for transmission.

- HTTP, IP, TCP, Ethernet
- (•) HTTP, TCP, IP, Ethernet
- Ethernet, TCP, IP, HTTP
- Ethernet, IP, TCP, HTTP

Capítulo 4_Capa física

Introducción

4.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Capa física!

La capa física del modelo OSI se encuentra en la parte inferior de la pila. Forma parte de la capa Acceso a red del modelo TCP/IP. Sin la capa física, no tendría una red. Este módulo explica, en detalle, las tres formas de conectarse a la capa física. ¡Las actividades y laboratorios de Packet Tracer le darán la confianza que necesita para cablear su propia red! ¡Vamos a estar ocupados!

4.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Capa física

Objetivos del módulo: Explique la forma en que los protocolos, servicios y medios de red de capa física admiten comunicaciones a través de las redes de datos.

Título del tema	Objetivo del tema
Propósito de la capa física	Describa el propósito y las funciones de la capa física en la red.
Características de la capa física	Describa las características de la capa física.
Cableado de cobre	Identifique las características básicas del cableado de cobre.
Cableado UTP	Explique cómo se utiliza el cable UTP en las redes Ethernet.
Cableado de fibra óptica	Describir el cableado de fibra óptica y sus ventajas principales sobre otros medios.
Medios inalámbricos	Conecte dispositivos utilizando medios conectados por cable e inalámbricos.

Propósito de la capa física

4.1.1

La conexión física

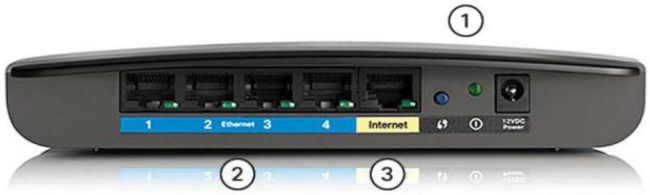
Ya sea una conexión a una impresora local en el hogar o a un sitio web en otro país, para que se pueda producir cualquier comunicación de red se debe establecer antes una conexión a una red local. Una conexión física puede ser una conexión por cable o una conexión inalámbrica mediante ondas de radio.

El tipo de conexión física utilizada depende de la configuración de la red. Por ejemplo, en muchas oficinas corporativas, los empleados tienen PC de escritorio o portátiles que se conectan físicamente, mediante cables, a un switch compartido. Este tipo de configuración se denomina red cableada. Los datos se transmiten a través de un cable físico.

Además de las conexiones por cable, muchas empresas también ofrecen conexiones inalámbricas para PC portátiles, tablets y smartphones. En el caso de los dispositivos

inalámbricos, los datos se transmiten mediante ondas de radio. La conectividad inalámbrica es común a medida que las personas y las empresas descubren sus ventajas. Los dispositivos en una red inalámbrica deben estar conectados a un punto de acceso inalámbrico (AP) o router inalámbrico como el que se muestra en la figura.

Router inalámbrico



Estos son los componentes de un punto de acceso:

1. Las antenas inalámbricas (Estas están integradas dentro de la versión del router que se muestra en la figura anterior).
2. Varios puertos de switch de Ethernet
3. Un puerto de internet

Al igual que una oficina corporativa, la mayoría de los hogares ofrecen conectividad cableada e inalámbrica a la red. Las cifras muestran un router doméstico y una computadora portátil que se conectan a la red de área local (LAN).

Conexión por cable al router inalámbrico

Tarjetas de interfaz de red

Las tarjetas de interfaz de red (NIC) conectan un dispositivo a la red. Las NIC de Ethernet se usan para una conexión por cable, como se muestra en la figura, mientras que las NIC de la red de área local inalámbrica (WLAN) se usan para la conexión inalámbrica. Los dispositivos para usuarios finales pueden incluir un tipo de NIC o ambos. Una impresora de red, por

ejemplo, puede contar solo con una NIC Ethernet y, por lo tanto, se debe conectar a la red mediante un cable Ethernet. Otros dispositivos, como las tabletas y los teléfonos inteligentes, pueden contener solo una NIC WLAN y deben utilizar una conexión inalámbrica.

Conexión por cable con una NIC Ethernet

En términos de rendimiento, no todas las conexiones físicas son iguales a la hora de conectarse a una red.

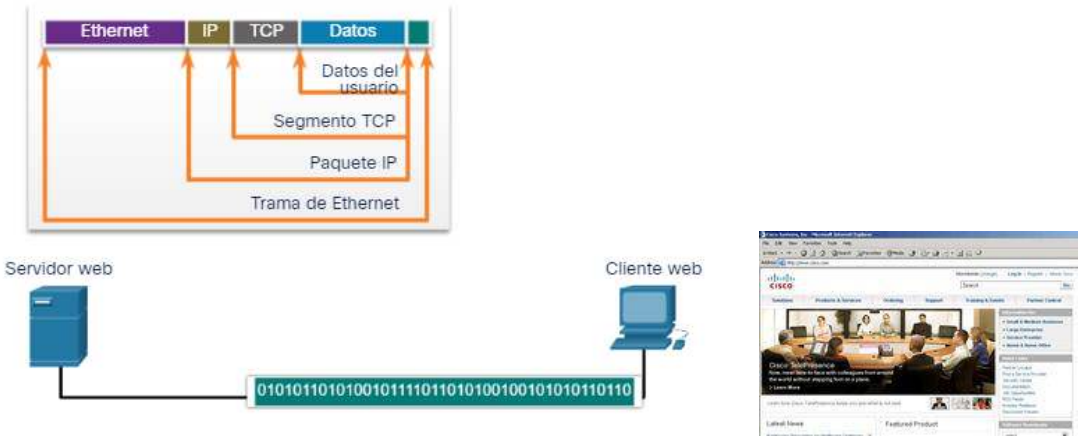
4.1.2

La capa física

La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de enlace de datos y la codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermediario recibe los bits codificados que componen una trama.

Haga clic en Reproducir en la figura para ver un ejemplo del proceso de encapsulación. La última parte de este proceso muestra los bits que se envían a través del medio físico. La capa física codifica las tramas y crea las señales eléctricas, ópticas o de ondas de radio que representan los bits en cada trama. Estas señales se envían por los medios, una a la vez.

La capa física del nodo de destino recupera estas señales individuales de los medios, las restaura a sus representaciones en bits y pasa los bits a la capa de enlace de datos en forma de trama completa.



La animación muestra una pequeña red con un servidor web y un cliente web. Hay un gráfico que muestra los componentes que forman un mensaje. Una trama de Ethernet y un paquete de IP, un segmento TCP y los datos del usuario. La animación comienza con el servidor web que prepara la página del Lenguaje de marcado de hipertexto (HTML) como datos a enviar. El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente web. El protocolo de capa de aplicación HTTP entrega los datos de la página web con formato HTML a la capa de transporte. El protocolo de la capa de transporte antepone información adicional a los datos HTTP para gestionar el intercambio de información entre el servidor web y el cliente web. La información de IP se antepone a la información de TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP. El protocolo Ethernet antepone y agrega al final (agrega) información al paquete IP para crear una trama de enlace de datos. A continuación, el marco se convierte en una cadena de bits binarios que se envían a lo largo de la ruta de red al cliente web.

4.1.3

Compruebe su comprensión - Propósito de la capa física

Verifique su comprensión de la capa física eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es falso. La capa física proporciona los medios para transportar bits a través de la red, ya sea que la red esté cableada o inalámbrica.
2. La respuesta correcta es falso. Cuando se codifican, los bits que componen una trama se transmiten a través del medio uno a la vez.
3. La capa física recibe fotogramas de la capa de enlace de datos y la convierte en bits para su transmisión. En el dispositivo de envío, la capa física pasa los bits transmitidos hasta la capa de enlace de datos como una trama completa.
4. La capa física recibe tramas de la capa de enlace de datos para su codificación y transmisión.

Has tenido 4 respuestas correctas de 4.

1. ¿Verdadero o falso? La capa física solo se refiere a las conexiones de red cableadas.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

2. ¿Verdadero o falso? Cuando una trama es codificada por la capa física, todos los bits se envían a través del medio al mismo tiempo.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

3. La capa física del dispositivo receptor pasa bits hasta qué capa de nivel superior?

¡Lo tienes!

- ○ Aplicación
- ○ Presentación
- ○ Red
- ◉ Enlace de datos

4. ¿Qué PDU recibe la capa física para la codificación y transmisión?

¡Lo tienes!

- ◉ trama
- ○ Segmento
- ○ Paquete

1. True or false? The physical layer is only concerned with wired network connections.

You got it!

- ○ true
- ◉ false

2. True or false? When a frame is encoded by the physical layer, all bits are sent over the media at the same time.

You got it!

- ○ true
- ◉ false

3. The physical layer of the receiving device passes bits up to which higher level layer?

You got it!

- ○ application
- ○ presentation
- ○ network
- ◉ data link

4. What PDU is received by the physical layer for encoding and transmission?

You got it!

- ◉ frame
- ○ segment
- ○ packet

Capa física / Características de la capa física

Características de la capa física

4.2.1

Estándares de la capa física

En el tema anterior, obtuvo una visión general de alto nivel de la capa física y su lugar en una red. Este tema profundiza un poco más en los detalles de la capa física. Esto incluye los componentes y los medios utilizados para construir una red, así como los estándares necesarios para que todo funcione en conjunto.

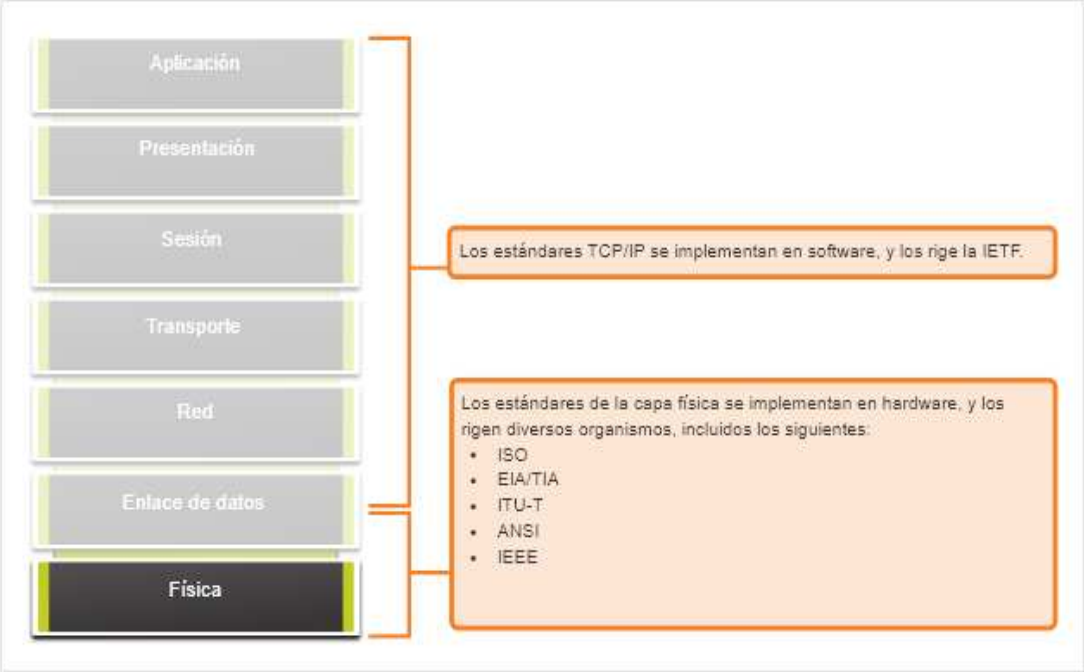
Los protocolos y las operaciones de las capas OSI superiores se llevan a cabo en software diseñado por ingenieros en software e informáticos. El grupo de trabajo de ingeniería de Internet (IETF) define los servicios y protocolos del conjunto TCP/IP.

La capa física consta de circuitos electrónicos, medios y conectores desarrollados por ingenieros. Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

Existen muchas organizaciones internacionales y nacionales, organizaciones de regulación gubernamentales y empresas privadas que intervienen en el establecimiento y el mantenimiento de los estándares de la capa física. Por ejemplo, los estándares de hardware, medios, codificación y señalización de la capa física están definidos y regidos por estas organizaciones de estándares:

- Organización Internacional para la Estandarización (ISO)
- Asociación de las Industrias de las Telecomunicaciones (TIA) y Asociación de Industrias Electrónicas (EIA)
- Unión Internacional de Telecomunicaciones (ITU)
- Instituto Nacional Estadounidense de Estándares (ANSI)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Autoridades nacionales reguladoras de las telecomunicaciones, incluida la Federal Communication Commission (FCC) de los Estados Unidos y el Instituto Europeo de Estándares de Telecomunicaciones (ETSI)

Además de estos, a menudo hay grupos de normas de cableado regionales como CSA (Asociación de Normas Canadienses), CENELEC (Comité Europeo de Normalización Electrotécnica) y JSA / JIS (Asociación de Normas Japonesas), que desarrollan especificaciones locales.



4.2.2

Componentes físicos

Los estándares de la capa física abarcan tres áreas funcionales:

- Componentes físicos
- Codificación
- Señalización

Componentes físicos

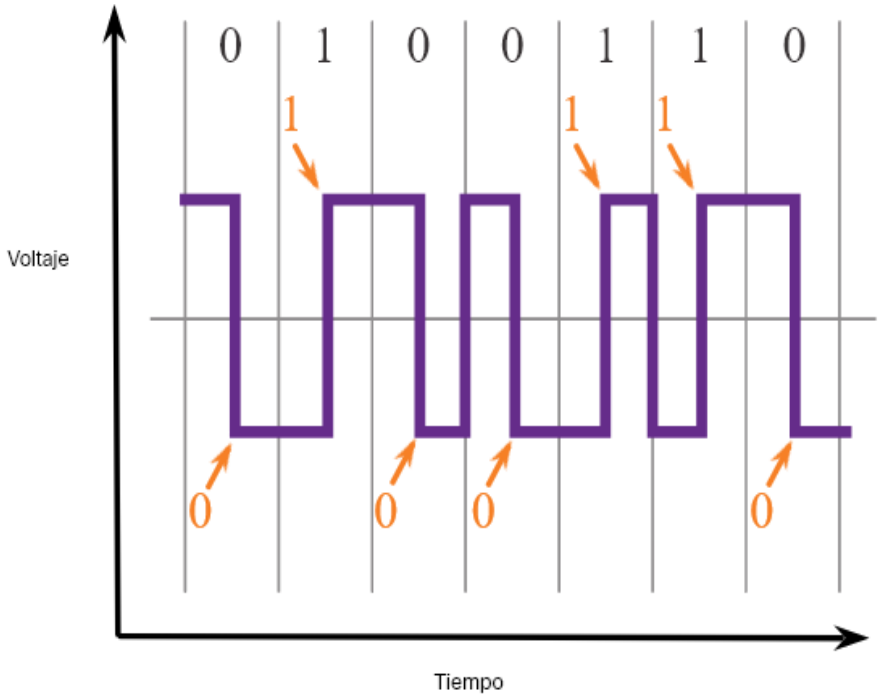
Los componentes físicos son los dispositivos de hardware electrónico, medios y otros conectores que transmiten las señales que representan los bits. Todos los componentes de hardware, como NIC, interfaces y conectores, materiales y diseño de los cables, se especifican en los estándares asociados con la capa física. Los diversos puertos e interfaces de un router Cisco 1941 también son ejemplos de componentes físicos con conectores y diagramas de pines específicos derivados de los estándares.

4.2.3

Codificación

La codificación, o codificación de línea, es un método que se utiliza para convertir una transmisión de bits de datos en un "código" predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. En otras palabras, la codificación es el método o patrón utilizado para representar la información digital. Similar a la forma en que el código Morse codifica un mensaje con una serie de puntos y guiones.

Por ejemplo, en la codificación Manchester los 0 se representan mediante una transición de voltaje de alto a bajo y los 1 se representan como una transición de voltaje de bajo a alto. Un ejemplo de codificación Manchester se ilustra en la figura. La transición se produce en el medio de cada período de bit. Este tipo de codificación se usa en Ethernet de 10 Mbps. Las velocidades de datos más rápidas requieren codificación más compleja. La codificación Manchester se utiliza en estándares Ethernet más antiguos, como 10BASE-T. Ethernet 100BASE-TX usa codificación 4B / 5B y 1000BASE-T usa codificación 8B / 10B.



La transición se produce en el medio de cada período de bit.

La imagen es un gráfico de línea de voltaje a lo largo del tiempo que representa la codificación Manchester de una corriente de siete bits. Hay líneas horizontales separadas

uniformemente que representan períodos de bits. También hay una línea vertical dibujada a mitad del eje y utilizada como punto de referencia. A medida que se envía el flujo de bits (señal), hay caídas y aumentos en los niveles de voltaje en el medio de cada período de bits. Si el bit es un cero binario, entonces el voltaje cae en el medio. Si el bit es binario, entonces el voltaje aumenta en el medio. Los bits transmitidos son 0100110.

4.2.4

Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan los "1" y los "0" en los medios. La forma en que se representan los bits se denomina método de señalización. Los estándares de la capa física deben definir qué tipo de señal representa un "1" y qué tipo de señal representa un "0". Esto puede ser tan simple como un cambio en el nivel de una señal eléctrica o de un pulso óptico. Por ejemplo, un pulso largo podría representar un 1 mientras que un pulso corto podría representar un 0.

Esto es similar al método de señalización que se utiliza en el código Morse, que puede utilizar una serie de tonos de encendido/apagado, luces o clics para enviar texto a través de cables telefónicos o entre barcos en el mar.

Las figuras muestran señalización

Haga clic en cada botón para ver ilustraciones de señalización para cable de cobre, cable de fibra óptica y medios inalámbricos.

Cable de cobre | Cable de fibra óptica | Medios inalámbricos

Señales eléctricas sobre cable

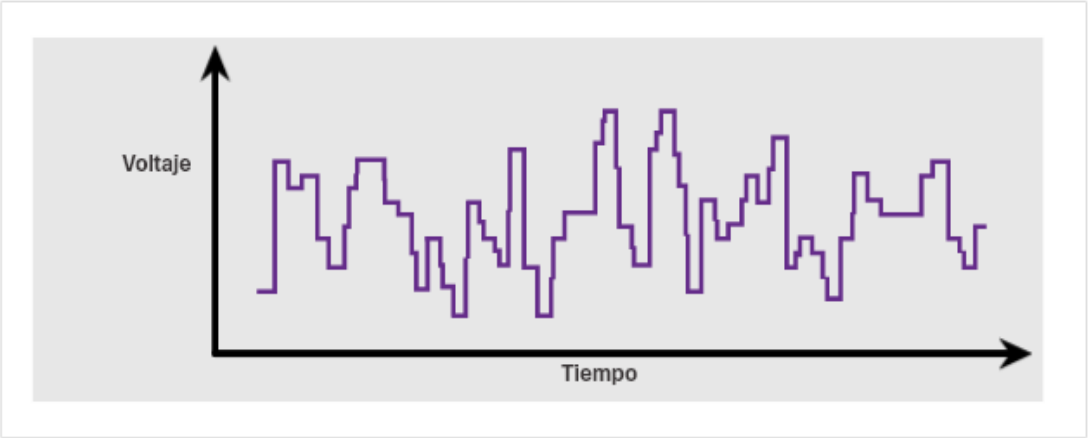
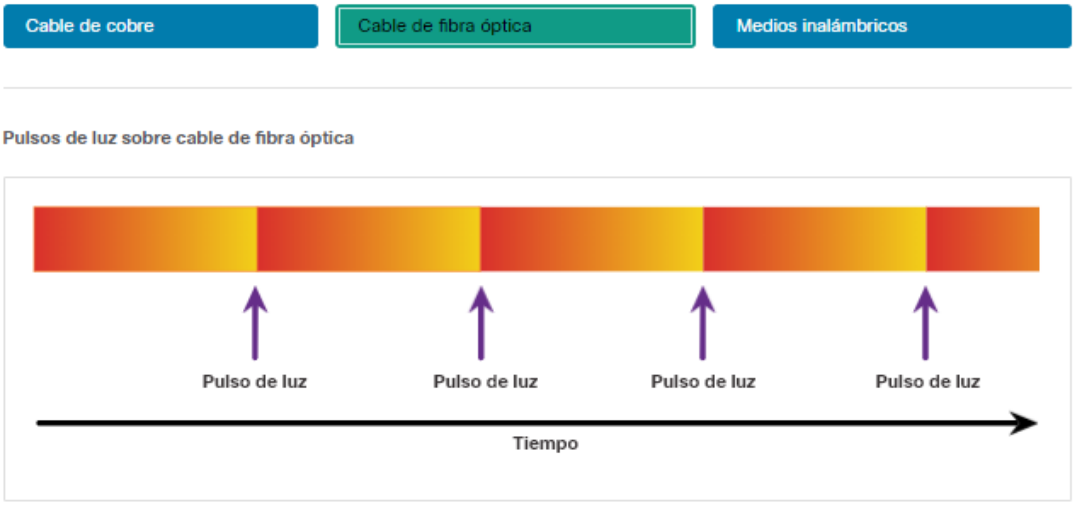
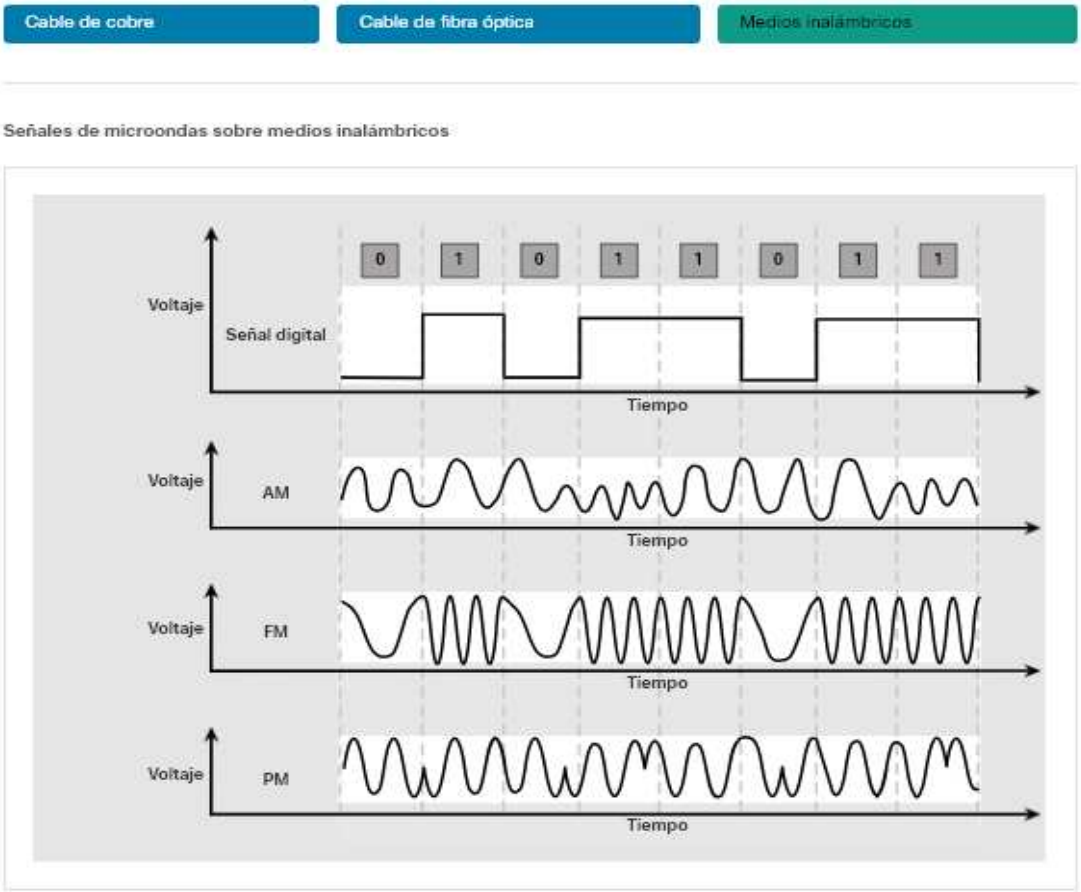


Gráfico de voltaje a lo largo del tiempo que muestra ondas cuadradas con diferentes niveles de picos y valles.





4.2.5

Ancho de banda

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. La transferencia de datos generalmente se discute en términos de ancho de banda. El ancho de banda es la capacidad a la que un medio puede transportar datos. El ancho de banda digital mide la cantidad de datos que pueden fluir desde un lugar hacia otro en un período de tiempo determinado. El ancho de banda generalmente se mide en kilobits por segundo (kbps), megabits por segundo (Mbps) o gigabits por segundo (Gbps). En ocasiones, el ancho de banda se piensa como la velocidad a la que viajan los bits, sin embargo, esto no es adecuado. Por ejemplo, tanto en Ethernet a 10 Mbps como a 100 Mbps, los bits se envían a la velocidad de la electricidad. La diferencia es el número de bits que se transmiten por segundo.

Una combinación de factores determina el ancho de banda práctico de una red:

- Las propiedades de los medios físicos
- Las tecnologías seleccionadas para la señalización y la detección de señales de red

Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física desempeñan una función al momento de determinar el ancho de banda disponible.

En la tabla, se muestran las unidades de medida comúnmente utilizadas para el ancho de banda.

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

4.2.6

Terminología del ancho de banda

Los términos utilizados para medir la calidad del ancho de banda incluyen:

- Latencia

- Rendimiento
- Capacidad de transferencia útil

Latencia

El concepto de latencia se refiere a la cantidad de tiempo, incluidas las demoras, que les toma a los datos transferirse desde un punto determinado hasta otro.

En una internetwork o una red con múltiples segmentos, el rendimiento no puede ser más rápido que el enlace más lento de la ruta de origen a destino. Incluso si todos los segmentos o gran parte de ellos tienen un ancho de banda elevado, solo se necesita un segmento en la ruta con un rendimiento inferior para crear un cuello de botella en el rendimiento de toda la red.

Rendimiento

El rendimiento es la medida de transferencia de bits a través de los medios durante un período de tiempo determinado.

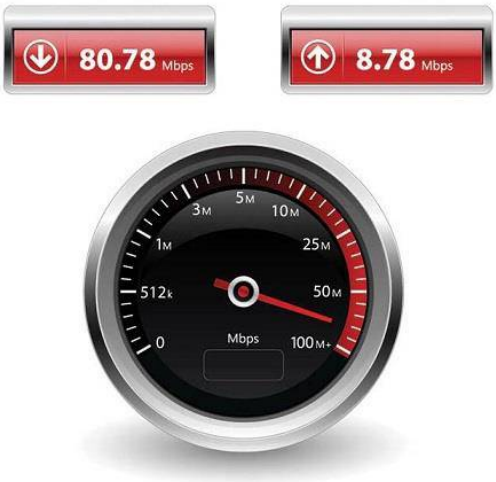
Debido a diferentes factores, el rendimiento generalmente no coincide con el ancho de banda especificado en las implementaciones de la capa física. El rendimiento suele ser menor que el ancho de banda. Hay muchos factores que influyen en el rendimiento:

- La cantidad de tráfico
- El tipo de tráfico
- La latencia creada por la cantidad de dispositivos de red encontrados entre origen y destino

Existen muchas pruebas de velocidad en línea que pueden revelar el rendimiento de una conexión a Internet. En la figura, se proporcionan resultados de ejemplo de una prueba de velocidad.

Capacidad de transferencia útil (Goodput)

Existe una tercera medición para evaluar la transferencia de datos utilizables, que se conoce como capacidad de transferencia útil. La capacidad de transferencia útil es la medida de datos utilizables transferidos durante un período determinado. La capacidad de transferencia útil es el rendimiento menos la sobrecarga de tráfico para establecer sesiones, acuses de recibo, encapsulación y bits retransmitidos. La capacidad de transferencia útil siempre es menor que el rendimiento, que generalmente es menor que el ancho de banda.



Velocidad de descarga / velocidad de carga

Un medidor que mide Mbps oscila entre 0 y 100 Mbps con una pantalla que muestra 80,78 Mbps para una velocidad de descarga y otra que muestra 8,78 Mbps para una velocidad de carga.

4.2.7

Verifique su comprensión - Características de la capa física

Verifique su comprensión de las características de la capa física eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. En las redes inalámbricas, los datos están representados por patrones de transmisiones de microondas.
2. Los cables de fibra óptica utilizan patrones de luz para representar bits.
3. Los pulsos eléctricos se utilizan para representar bits en redes utilizando medios de cable de cobre.
4. El ancho de banda es la capacidad de un medio para transportar datos.
5. La transferencia de bits a través de los medios de la red durante un período de tiempo se conoce como rendimiento.

Has tenido 5 respuestas correctas de 5.

1. ¿Qué medios utilizan patrones de microondas para representar bits?

¡Lo tienes!

- ○ Cobre
- ◉ Inalámbrica
- ○ Fibra óptica

2. ¿Qué medios utilizan patrones de luz para representar bits?

¡Lo tienes!

- ○ Cobre
- ○ Inalámbrica
- ◉ Fibra óptica

3. ¿Qué medios usan pulsos eléctricos para representar bits?

¡Lo tienes!

- ◉ Cobre
- ○ Inalámbrica
- ○ Fibra óptica

4. ¿Cuál de estos es el nombre de la capacidad de un medio para transportar datos?

¡Lo tienes!

- ◉ Ancho de banda
- ○ Rendimiento
- ○ Capacidad de transferencia útil

5. ¿Cuál de estos es una medida de la transferencia de bits a través de los medios?

¡Lo tienes!

- ○ Ancho de banda
- ◉ Rendimiento
- ○ Capacidad de transferencia útil

Correct

You have successfully identified the correct answers.

1. In wireless networks data is represented by patterns of microwave transmissions.
2. Fiber-optic cables use patterns of light to represent bits.
3. Electrical pulses are used to represent bits on networks using copper cable media.
4. Bandwidth is the capacity of a network medium to carry data.
5. The transfer of bits across the network media over a period of time is known as throughput.

You got 5 out of 5 questions correct.

1. Which media uses patterns of microwaves to represent bits?

You got it!

- ○ copper
- ◉ wireless
- ○ fiber-optic

2. Which media uses patterns of light to represent bits?

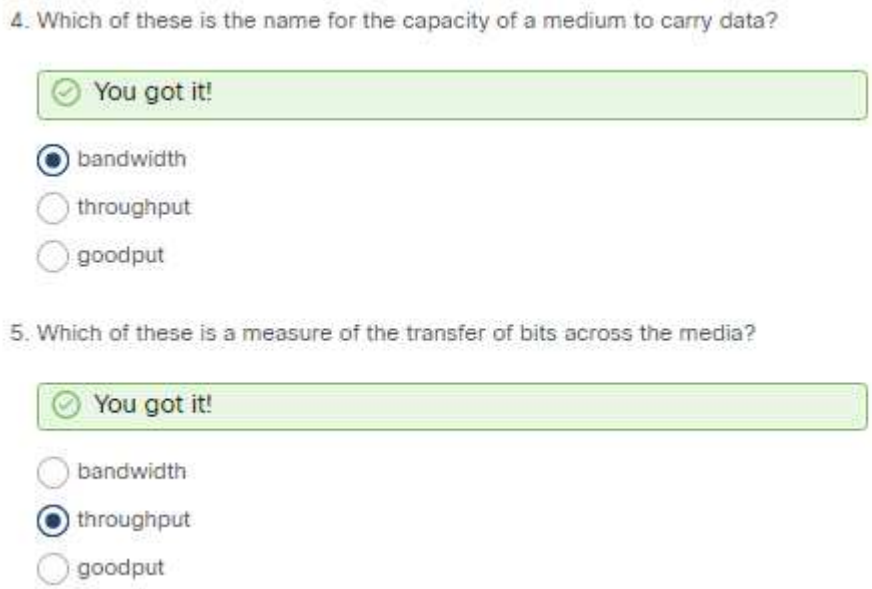
You got it!

- ○ copper
- ○ wireless
- ◉ fiber-optic

3. Which media uses electrical pulses to represent bits?

You got it!

- ◉ copper
- ○ wireless
- ○ fiber-optic



Capa física / Cableado de cobre

Cableado de cobre

4.3.1

Características del cableado de cobre

El cableado de cobre es el tipo más común de cableado utilizado en las redes hoy en día. De hecho, el cableado de cobre no es solo un tipo de cable. Hay tres tipos diferentes de cableado de cobre que se utilizan cada uno en situaciones específicas.

Las redes utilizan medios de cobre porque son económicos y fáciles de instalar, y tienen baja resistencia a la corriente eléctrica. Sin embargo, estos medios están limitados por la distancia y la interferencia de señal.

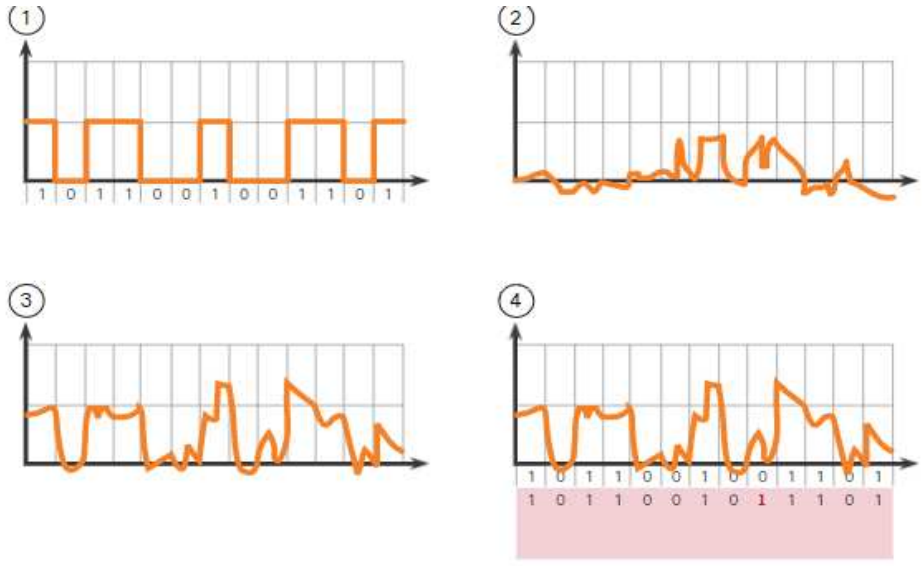
Los datos se transmiten en cables de cobre como impulsos eléctricos. Un detector en la interfaz de red de un dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la señal enviada. No obstante, cuanto más lejos viaja una señal, más se deteriora. Esto se denomina atenuación de señal. Por este motivo, todos los medios de cobre deben seguir limitaciones de distancia estrictas según lo especifican los estándares que los rigen.

Los valores de temporización y voltaje de los pulsos eléctricos también son vulnerables a las interferencias de dos fuentes:

- **Interferencia electromagnética (EMI) o interferencia de radiofrecuencia (RFI)**: las señales de EMI y RFI pueden distorsionar y dañar las señales de datos que transportan los medios de cobre. Las posibles fuentes de EMI y RFI incluyen las ondas de radio y dispositivos electromagnéticos, como las luces fluorescentes o los motores eléctricos.
- **Crosstalk** - Crosstalk se trata de una perturbación causada por los campos eléctricos o magnéticos de una señal de un hilo a la señal de un hilo adyacente. En los circuitos telefónicos, el crosstalk puede provocar que se escuche parte de otra conversación de voz de un circuito adyacente. En especial, cuando una corriente eléctrica fluye por un hilo, crea un pequeño campo magnético circular alrededor de dicho hilo, que puede captar un hilo adyacente.

En la figura, se muestra la forma en que la interferencia puede afectar la transmisión de datos.

El diagrama es de cuatro gráficos, cada uno con voltaje a lo largo del tiempo. El primer gráfico muestra ondas cuadradas de una señal digital pura y su equivalente binario, 1011001001101. El segundo gráfico es de una señal de interferencia con diversos grados de voltaje. El tercer gráfico muestra la señal digital con la interferencia. El cuarto gráfico muestra cómo el ordenador lee la señal cambiada como el equivalente binario de 1011001011101.



1. Se transmite una señal digital pura
2. En el medio, hay una señal de interferencia
3. La señal digital está dañada por la señal de interferencia.
4. El equipo receptor lee una señal cambiada. Observe que un bit 0 ahora se interpreta como un bit 1.

Para contrarrestar los efectos negativos de la EMI y la RFI, algunos tipos de cables de cobre se empaquetan con un blindaje metálico y requieren una conexión a tierra adecuada.

Para contrarrestar los efectos negativos del crosstalk, algunos tipos de cables de cobre tienen pares de hilos de circuitos opuestos trenzados que cancelan dicho tipo de interferencia en forma eficaz.

La susceptibilidad de los cables de cobre al ruido electrónico también se puede limitar utilizando estas recomendaciones:

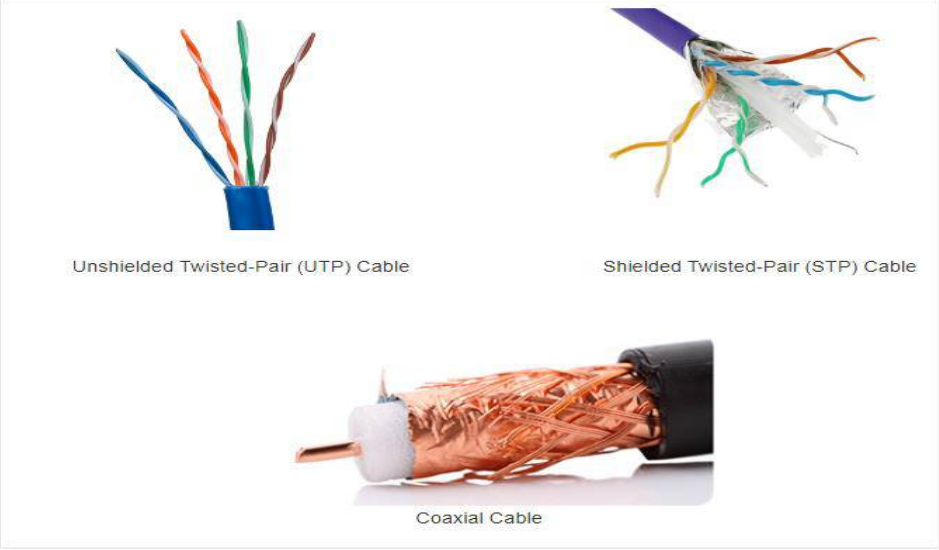
- La elección del tipo o la categoría de cable más adecuados a un entorno de red determinado.
- El diseño de una infraestructura de cables para evitar las fuentes de interferencia posibles y conocidas en la estructura del edificio.
- El uso de técnicas de cableado que incluyen el manejo y la terminación apropiados de los cables.

4.3.2

Tipos de cableado de cobre

Existen tres tipos principales de medios de cobre que se utilizan en las redes.

La figura se compone de imágenes que muestran los tres tipos de cableado de cobre, cada uno con una parte de la cubierta del cable exterior despojada para exponer la construcción del cable. La primera imagen muestra un cable de par trenzado sin blindaje (UTP) con cuatro pares de colores de cables trenzados: azul, naranja, verde y marrón. La segunda imagen es un cable de par trenzado blindado (STP) que muestra cuatro pares de cables trenzados - azul, verde, marrón y naranja - con un escudo de aluminio que rodea a los cuatro pares. La última imagen muestra un conductor de cobre central rodeado de aislamiento plástico rodeado por un escudo trenzado.



Cable de par trenzado no blindado (UTP) / Cable de par trenzado blindado (STP) / Cable coaxial

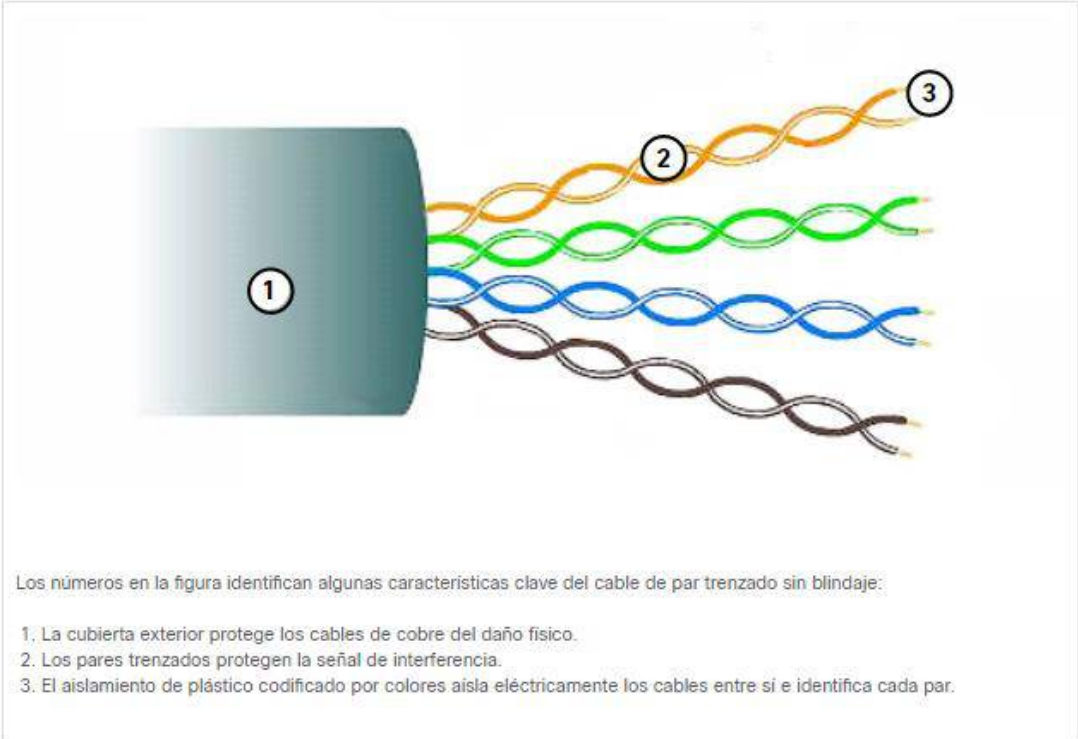
4.3.3

Par trenzado no blindado (UTP)

El cableado de par trenzado no blindado (UTP) es el medio de red más común. El cableado UTP, que se termina con conectores RJ-45, se utiliza para interconectar hosts de red con dispositivos intermediarios de red, como switches y routers.

En las redes LAN, el cable UTP consta de cuatro pares de hilos codificados por colores que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible que los protege contra daños físicos menores. El trenzado de los hilos ayuda a proteger contra las interferencias de señales de otros hilos.

Como se muestra en la figura, los códigos por colores identifican los pares individuales con sus alambres y sirven de ayuda para la terminación de cables.



Los números en la figura identifican algunas características clave del cable de par trenzado sin blindaje:

1. La cubierta exterior protege los cables de cobre del daño físico.
2. Los pares trenzados protegen la señal de interferencia.
3. El aislamiento de plástico codificado por colores aisla eléctricamente los cables entre sí e identifica cada par.

Cable UTP que muestra la cubierta del cable exterior (etiquetado 1), los pares de cables trenzados (etiquetado 2) y el aislamiento naranja, verde, azul y marrón (etiquetado 3).

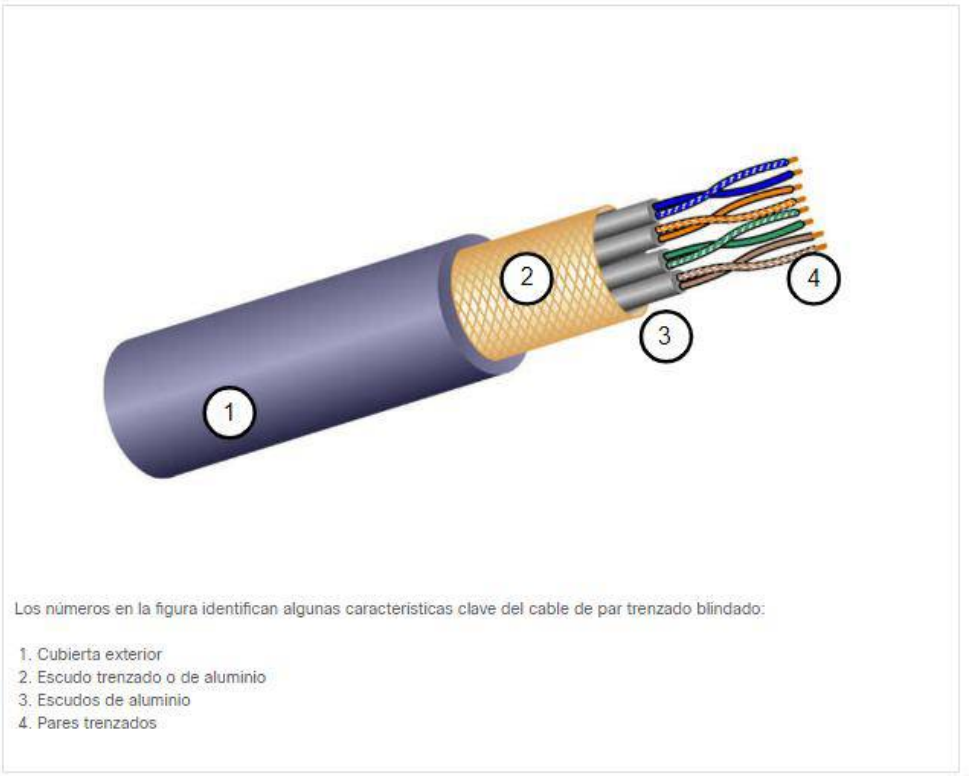
4.3.4

Par trenzado blindado (STP)

El par trenzado blindado (STP) proporciona una mejor protección contra ruido que el cableado UTP. Sin embargo, en comparación con el cable UTP, el cable STP es mucho más costoso y difícil de instalar. Al igual que el cable UTP, el STP utiliza un conector RJ-45.

El cable STP combina las técnicas de blindaje para contrarrestar la EMI y la RFI, y el trenzado de hilos para contrarrestar el crosstalk. Para obtener los máximos beneficios del blindaje, los cables STP se terminan con conectores de datos STP blindados especiales. Si el cable no se conecta a tierra correctamente, el blindaje puede actuar como antena y captar señales no deseadas.

El cable STP que se muestra utiliza cuatro pares de hilos. Cada uno de estos pares está empaquetado primero con un blindaje de hoja metálica y, luego, el conjunto se empaqueta con una malla tejida o una hoja metálica.



Los números en la figura identifican algunas características clave del cable de par trenzado blindado:

1. Cubierta exterior
2. Escudo trenzado o de aluminio
3. Escudos de aluminio
4. Pares trenzados

Cable STP que muestra la cubierta del cable exterior (etiquetado 1), un blindaje trenzado alrededor de todos los pares de cables (etiquetado 2), escudos de lámina alrededor de los pares de cables individuales (etiquetado 3) y los pares de cables trenzados de colores (etiquetado 4).

4.3.5

Cable coaxial

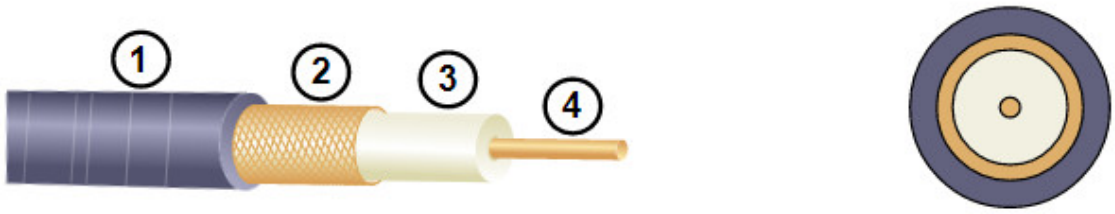
El cable coaxial obtiene su nombre del hecho de que hay dos conductores que comparten el mismo eje. Como se muestra en la figura, el cable coaxial consta de lo siguiente:

- Se utiliza un conductor de cobre para transmitir las señales electrónicas.
- Una capa de aislamiento plástico flexible que rodea al conductor de cobre.
- Sobre este material aislante, hay una malla de cobre tejida o una hoja metálica que actúa como segundo hilo en el circuito y como blindaje para el conductor interno. La segunda capa o blindaje reduce la cantidad de interferencia electromagnética externa.
- La totalidad del cable está cubierta por un revestimiento para evitar daños físicos menores.

Existen diferentes tipos de conectores con cable coaxial. Los conectores Bayoneta Neill—Concelman (BNC), tipo N y tipo F se muestran en la figura.

Aunque el cable UTP ha reemplazado esencialmente el cable coaxial en las instalaciones de Ethernet modernas, el diseño del cable coaxial se usa en las siguientes situaciones:

- **Instalaciones inalámbricas** - Los cables coaxiales conectan antenas a los dispositivos inalámbricos. También transportan energía de radiofrecuencia (RF) entre las antenas y el equipo de radio.
- **Instalaciones de Internet por cable** - Los proveedores de servicios de cable proporcionan conectividad a Internet a sus clientes mediante el reemplazo de porciones del cable coaxial y la admisión de elementos de amplificación con cables de fibra óptica. Sin embargo, el cableado en las instalaciones del cliente sigue siendo cable coaxial.



Tres figuras que muestran la construcción de un cable coaxial, una sección transversal de un cable coaxial y tres tipos de conectores de cable coaxial

Conectores coaxiales Tipo F / Tipo N / BNC

Los números en la figura identifican algunas características clave del cable coaxial:

1. Cubierta exterior
2. Blindaje de cobre trenzado
3. Aislamiento plástico
4. Conductor de cobre

4.3.6

Compruebe su comprensión - Cableado de cobre

Verifique su comprensión del cableado de cobre eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El cable coaxial, que se usa para la televisión por cable y el servicio de Internet, también se usa para conectar antenas a dispositivos inalámbricos.
2. El cable de par trenzado blindado (STP) incorpora blindaje y conectores especiales para evitar interferencias de señal de otros cables, EMI y RFI.
3. El cable de par trenzado sin blindaje (UTP) es el tipo más común de medios de red cableados.
4. El cable coaxial, que se utiliza para TV por cable y servicio de Internet y para conectar antenas a dispositivos inalámbricos, utiliza varios tipos de conectores para incluir conectores BNC, tipo N y tipo F.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuál de las siguientes antenas conecta a dispositivos inalámbricos? También se puede incluir con cableado de fibra óptica para la transmisión de datos bidireccional.

¡Lo tienes!

- ○ UTP
- ○ STP
- ◉ Coaxial

2. ¿Cuál de los siguientes contrarresta EMI y RFI utilizando técnicas de blindaje y conectores especiales?

¡Lo tienes!

- ○ UTP
- ◉ STP
- ○ Coaxial

3. ¿Cuál de los siguientes es el medio de red más común?

¡Lo tienes!

- ◉ UTP
- ○ STP
- ○ Coaxial

4. ¿Cuál de los siguientes termina con conectores BNC, tipo N y tipo F?

¡Lo tienes!

- ○ UTP
- ○ STP
- ◉ Coaxial

Correct

You have successfully identified the correct answers.

1. Coaxial cable, which is used for cable TV and internet service, is also used to attach antennas to wireless devices.
2. Shielded twisted pair cable (STP) incorporates shielding and special connectors to prevent signal interference from other wires, EMI, and RFI.
3. Unshielded twisted pair cable (UTP) is the most common type of wired network media.
4. Coaxial cable, which is used for cable TV and internet service and to attach antennas to wireless devices, uses several types of connectors to include BNC, N type, and F type connectors.

You got 4 out of 4 questions correct.

1. Which of the following attaches antennas to wireless devices? It can also be bundled with fiber-optic cabling for two-way data transmission.

You got it!

- ○ UTP
- ○ STP
- ◉ coaxial

2. Which of the following counters EMI and RFI by using shielding techniques and special connectors?

You got it!

- ○ UTP
- ◉ STP
- ○ coaxial

3. Which of the following is the most common network media?

You got it!

- ◉ UTP
- ○ STP
- ○ coaxial

4. Which of the following terminates with BNC, N type and F type connectors?

You got it!

- ○ UTP
- ○ STP
- ◉ coaxial

Capa física / Cableado UTP

Cableado UTP

4.4.1

Propiedades del cableado UTP

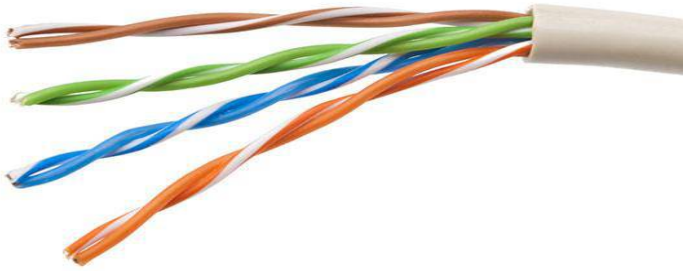
En el tema anterior, aprendió un poco sobre el cableado de cobre de par trenzado sin blindaje (UTP). Dado que el cableado UTP es el estándar para su uso en las LAN, en este tema se detallan sus ventajas y limitaciones, y qué se puede hacer para evitar problemas.

Cuando se utiliza como medio de red, el cableado (UTP) consta de cuatro pares de hilos codificados por colores que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible. Su tamaño pequeño puede ser una ventaja durante la instalación.

Los cables UTP no utilizan blindaje para contrarrestar los efectos de la EMI y la RFI. En cambio, los diseñadores de cable han descubierto otras formas de limitar el efecto negativo del crosstalk:

- **Anulación -** Los diseñadores ahora emparejan los hilos en un circuito. Cuando dos hilos en un circuito eléctrico están cerca, los campos magnéticos son exactamente opuestos entre sí. Por lo tanto, los dos campos magnéticos se anulan y también anulan cualquier señal de EMI y RFI externa.
- **Variando el número de vueltas por par de hilos -** Para mejorar aún más el efecto de anulación de los pares de hilos del circuito, los diseñadores cambian el número de vueltas de cada par de hilos en un cable. Los cables UTP deben seguir especificaciones precisas que rigen cuántas vueltas o trenzas se permiten por metro (3,28 ft) de cable. Observe en la figura que el par naranja y naranja/blanco está menos trenzado que el par azul y azul/blanco. Cada par coloreado se trenza una cantidad de veces distinta.

Los cables UTP dependen exclusivamente del efecto de anulación producido por los pares de hilos trenzados para limitar la degradación de la señal y proporcionar un autoblindaje eficaz de los pares de hilos en los medios de red.



4.4.2

Conectores y estándares de cableado UTP

El cableado UTP cumple con los estándares establecidos en conjunto por la TIA/EIA. En particular, la TIA/EIA-568 estipula los estándares comerciales de cableado para las

instalaciones LAN y es el estándar de mayor uso en entornos de cableado LAN. Algunos de los elementos definidos son los siguientes:

Tipos de cables Longitudes del cable Conectores Terminación del cable Métodos para realizar pruebas de cable

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define las características eléctricas del cableado de cobre. IEEE califica el cableado UTP según su rendimiento. Los cables se dividen en categorías según su capacidad para transportar datos de ancho de banda a velocidades mayores. Por ejemplo, el cable de Categoría 5 se utiliza comúnmente en las instalaciones de FastEthernet 100BASE-TX. Otras categorías incluyen el cable de categoría 5 mejorada, la categoría 6 y la categoría 6a.

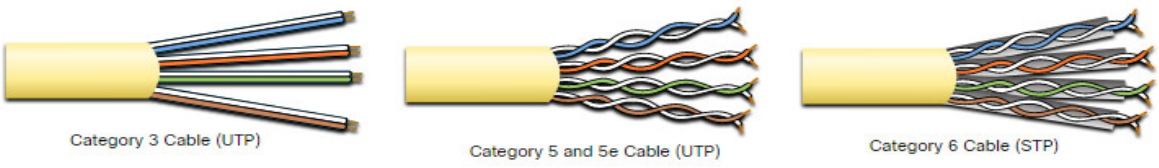
Los cables de categorías superiores se diseñan y fabrican para admitir velocidades superiores de transmisión de datos. A medida que se desarrollan y adoptan nuevas tecnologías Ethernet de velocidad gigabit, la categoría 5e es ahora el tipo de cable mínimamente aceptable, y la categoría 6 es el tipo recomendado para nuevas instalaciones de edificios.

La figura muestra tres categorías de cable UTP:

- La categoría 3 se utilizó originalmente para la comunicación de voz a través de líneas de voz, pero más tarde para la transmisión de datos.
- Las categorías 5 y 5e se utilizan para la transmisión de datos. La categoría 5 soporta 100Mbps y la categoría 5e soporta 1000 Mbps
- La categoría 6 tiene un separador añadido entre cada par de cables para soportar velocidades más altas. Categoría 6 soporta hasta 10 Gbps.
- Categoría 7 también soporta 10 Gbps.
- Categoría 8 soporta 40 Gbps.

Algunos fabricantes producen cables que exceden las especificaciones de la categoría 6a de la TIA/EIA y se refieren a estos como cables de Categoría 7.

La figura muestra la diferencia en la construcción entre las categorías de cable UTP. En la parte superior está la categoría 3 con cuatro cables. En el medio está la categoría 5 y 5e con cuatro pares de cables trenzados. En la parte inferior está la categoría 6 con cuatro pares de cables trenzados, cada uno con un separador de plástico.



Cable de Categoría 3 (UTP) / Cable de Categoría 5 o 5e (UTP) / Cable de Categoría 6 (UTP)

Los cables UTP generalmente se terminan con un conector RJ-45. El estándar TIA/EIA-568 describe las asignaciones de los códigos por colores de los hilos a la asignación de pines (diagrama de pines) de los cables Ethernet.

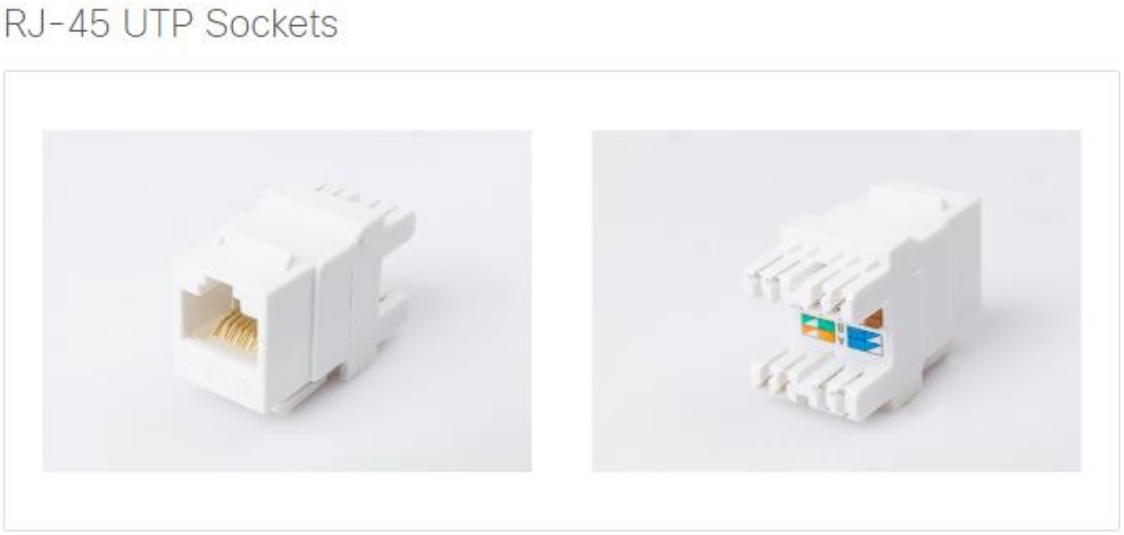
Como se muestra en la figura, el conector RJ-45 es el componente macho, engarzado al final del cable.

Conectores RJ-45 para UTP

Un conector RJ45 y un cable terminado con un conector RJ45.

El socket, que se muestra en la figura, es el componente hembra de un dispositivo de red, pared, salida de partición de cubículo o panel de conexiones. Cuando se realizan las terminaciones de manera incorrecta, cada cable representa una posible fuente de degradación del rendimiento de la capa física.

Vista frontal y lateral de un socket UTP RJ45, incluido el código de color para la terminación del cable.



Esta figura muestra un ejemplo de un cable UTP mal terminado. Este conector defectuoso tiene cables que están expuestos, sin torcer y no cubiertos completamente por la funda.

Cable UTP mal terminado

Cable UTP mal terminado que muestra cables sin torsión que se extienden fuera del conector RJ45.

La siguiente figura muestra un cable UTP correctamente terminado. En un buen conector, los hilos están sin trenzar solo en el trecho necesario para unir el conector.

Cable UTP correctamente terminado

Cable UTP de terminación correcta que muestra la cubierta del cable que se extiende al conector RJ45 lo suficiente como para engarzar de forma segura con los ocho cables que llegan al extremo del conector.

Nota: La terminación incorrecta de los cables puede afectar el rendimiento de la transmisión.

4.4.3

Cables UTP directos y cruzados

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los hilos individuales del cable deben conectarse en diferente orden para distintos grupos de pins en los conectores RJ-45.

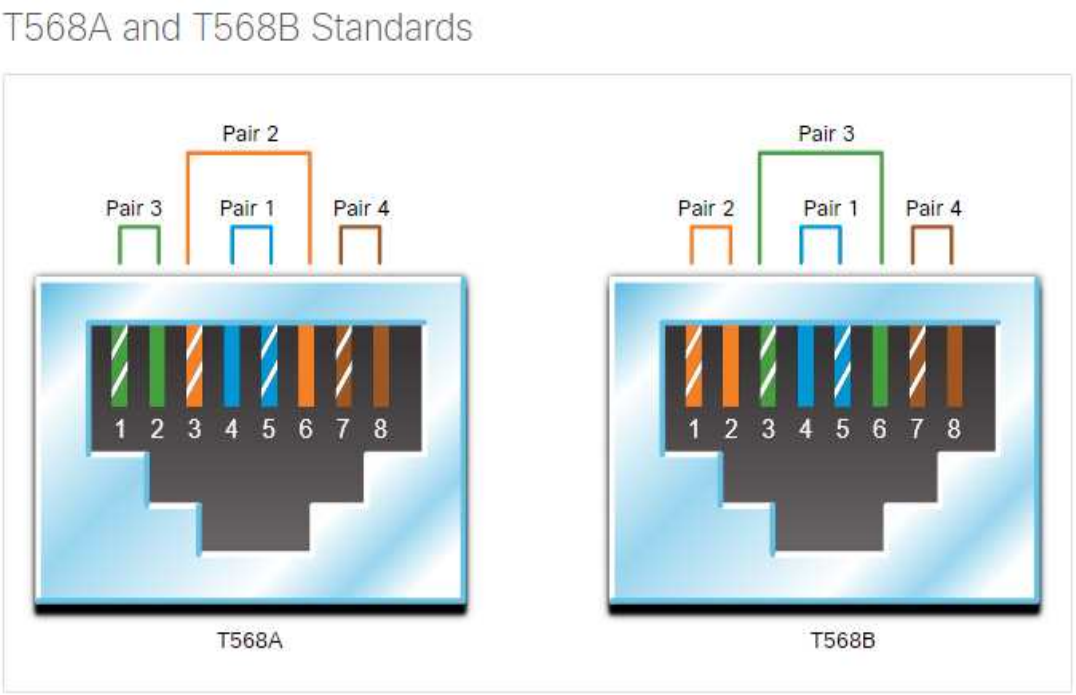
A continuación, se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

- **Cable directo de Ethernet -** El tipo más común de cable de red. Por lo general, se utiliza para interconectar un host con un switch y un switch con un router.
- **Cable cruzado Ethernet -** El cable utilizado para interconectar dispositivos similares. Por ejemplo, para conectar un switch a un switch, un host a un host o un router a un router. Sin embargo, los cables de cruce ahora se consideran heredados, ya que las NIC utilizan cruzado de interfaz dependiente medio (Auto-MDIX) para detectar automáticamente el tipo de cable y realizar la conexión interna.

Nota: Otro tipo de cable es un rollover, que es propiedad de Cisco. Se utiliza para conectar una estación de trabajo al puerto de consola de un router o de un switch.

Es posible que el uso de un cable de conexión cruzada o de conexión directa en forma incorrecta entre los dispositivos no dañe los dispositivos, pero tampoco se producirá la conectividad y la comunicación entre los dispositivos. Este es un error común de laboratorio. Si no se logra la conectividad, la primera medida para resolver este problema es verificar que las conexiones de los dispositivos sean correctas.

La figura identifica los pares de cables individuales para los estándares T568A y T568B.



La figura muestra diagramas de los estándares de cableado T568A y T568B. Cada uno muestra el pinout correcto para los pares de cables individuales. Cada par de cables de color está numerado y consta de un cable de color sólido y un cable rayado blanco. El par 1 es azul, el par 2 es naranja, el par 3 es verde y el par 4 es marrón. Cada estándar alterna entre cables blancos rayados y sólidos. Para el estándar T568A, el par azul se termina en los pines 4 y 5, el par naranja se termina en los pines 3 y 6, el par verde se termina en los pines 1 y 2, y el par marrón se termina en los pines 7 y 8. Para el estándar T568B, el par azul se termina en los pines 4 y 5, el par naranja se termina en los pines 1 y 2, el par verde es la terminación en los pines 3 y 6, y el par marrón se termina en los pines 7 y 8.

La tabla muestra el tipo de cable UTP, los estándares relacionados y la aplicación típica de estos cables.

Tipos de cables y estándares

Tipo de cable	Estándar	Aplicación
Cable directo de Ethernet	Ambos extremos son T568A o T568B.	Conecta un host de red a un dispositivo de red como un switch o concentrador.
Cruzado Ethernet	Un extremo T568A, otro extremo T568B.	Conecta dos hosts de red Conecta dos dispositivos intermediarios de red (switch a switch o router a router)
Rollover	Propietario de Cisco	Conecta el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador

4.4.4

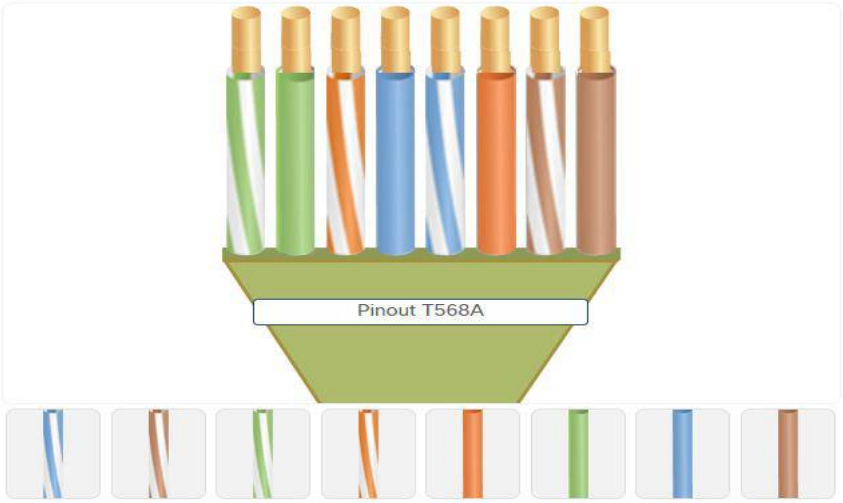
Actividad - Pinouts de cable

Para esta actividad, ordene correctamente los colores de los cables a un pinout de cable TIA/EIA. Seleccione un color de caja de cables haciendo clic en él. A continuación, haga clic en un cable para aplicarle esa carcasa.

Seleccione la caja del pin, luego el pin del cable para aplicar la carcasa.

Correcto

Ha elegido correctamente el pinout del cable T568A correcto.

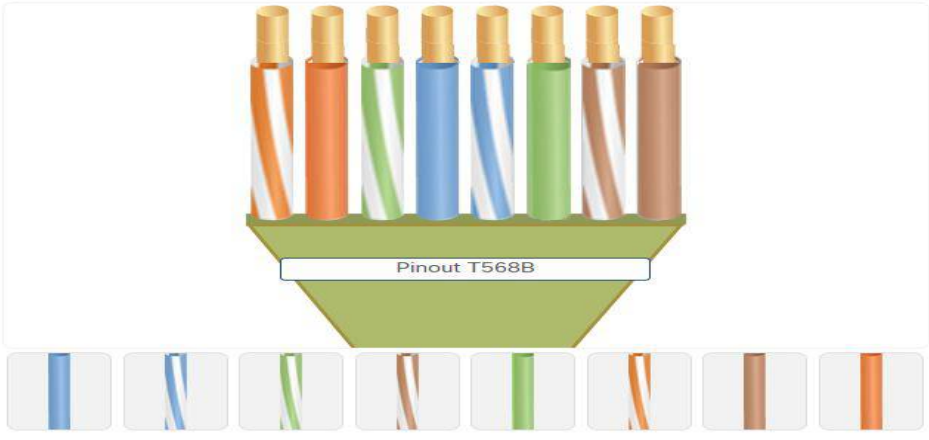


Verificar Mostrar Restablecer

Correcto

Ha elegido correctamente el pinout del cable T568B correcto.

Seleccione la caja del pin, luego el pin del cable para aplicar la carcasa.



Verificar Mostrar Restablecer

Capa física / Cableado de fibra óptica

Cableado de fibra óptica

4.5.1

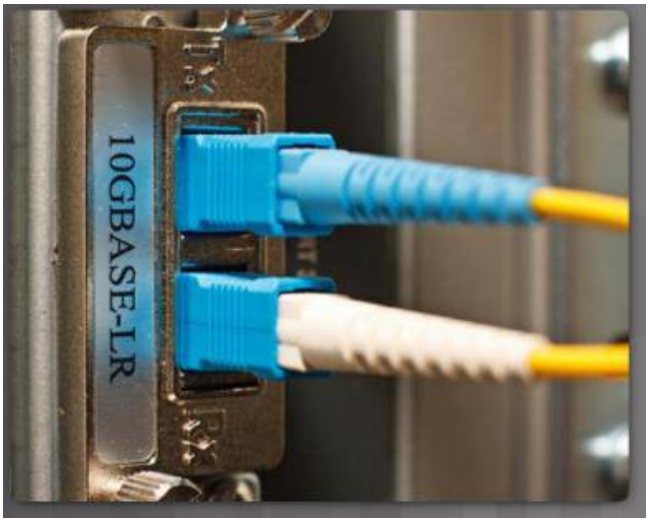
Propiedades del cableado de fibra óptica

Como ha aprendido, el cableado de fibra óptica es el otro tipo de cableado utilizado en las redes. Debido a que es caro, no es tan comúnmente utilizado en los diversos tipos de cableado de cobre. Pero el cableado de fibra óptica tiene ciertas propiedades que lo convierten en la mejor opción en ciertas situaciones, que descubrirá en este tema.

El cable de fibra óptica transmite datos a distancias más largas y con anchos de banda más altos que cualquier otro medio de red. A diferencia de los cables de cobre, el cable de fibra óptica puede transmitir señales con menos atenuación y es totalmente inmune a las EMI y RFI. El cable de fibra óptica se utiliza para interconectar dispositivos de red.

La fibra óptica es un hilo flexible, pero extremadamente delgado y transparente de vidrio muy puro, no mucho más grueso que un cabello humano. Los bits se codifican en la fibra como impulsos de luz. El cable de fibra óptica actúa como una guía de ondas, o una "tubería de luz", para transmitir la luz entre los dos extremos con una pérdida mínima de la señal.

A modo de analogía, imagine un rollo de toallas de papel vacío que tiene el interior recubierto con material reflectante. Este rollo mide mil metros de largo y tiene un pequeño puntero láser que se utiliza para enviar señales de Código Morse a la velocidad de la luz. Básicamente, así es cómo funciona un cable de fibra óptica, excepto que tiene un diámetro más pequeño y utiliza tecnologías de emisión y recepción de luz sofisticadas.



4.5.2

Tipos de medios de fibra

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos:

- Fibra óptica monomodo (SMF)
- Fibra multimodo (MMF)

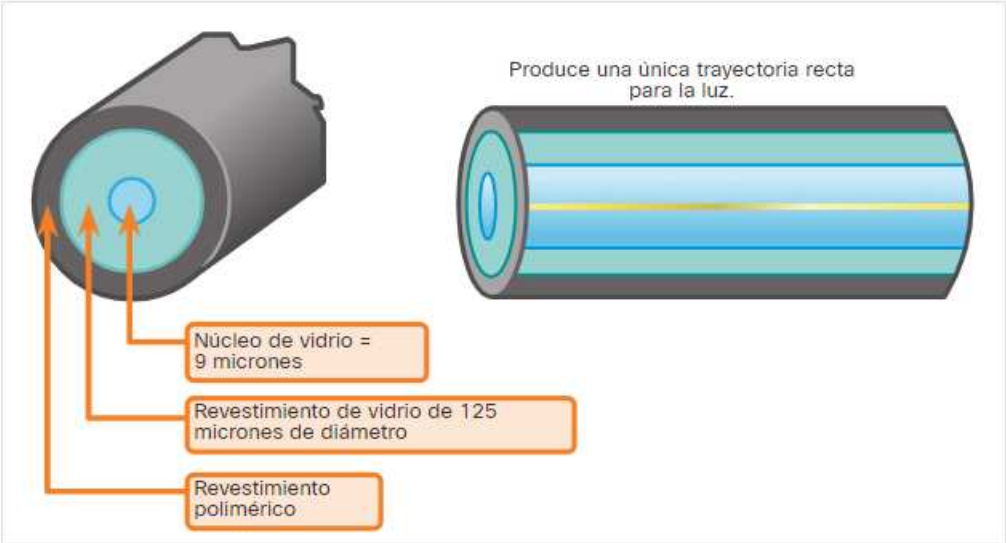
Haga clic en cada botón para ver una ilustración y una explicación de cada tipo.

Fibra monomodo | Fibra multimodo

Fibra monomodo (Single-Mode Fiber)

SMF consta de un núcleo muy pequeño y utiliza tecnología láser cara para enviar un solo rayo de luz, como se muestra en la figura. SMF es popular en situaciones de larga distancia que abarcan cientos de kilómetros, como las requeridas en aplicaciones de telefonía de larga distancia y televisión por cable.

Sección transversal de un cable de fibra óptica monomodo compuesto por un núcleo de vidrio central de 9 micras de diámetro, rodeado por un revestimiento de vidrio de 125 micras de diámetro, rodeado por un revestimiento polimérico. Una vista lateral de visión de rayos X muestra que este tipo de construcción de cable produce un único camino recto para la luz.

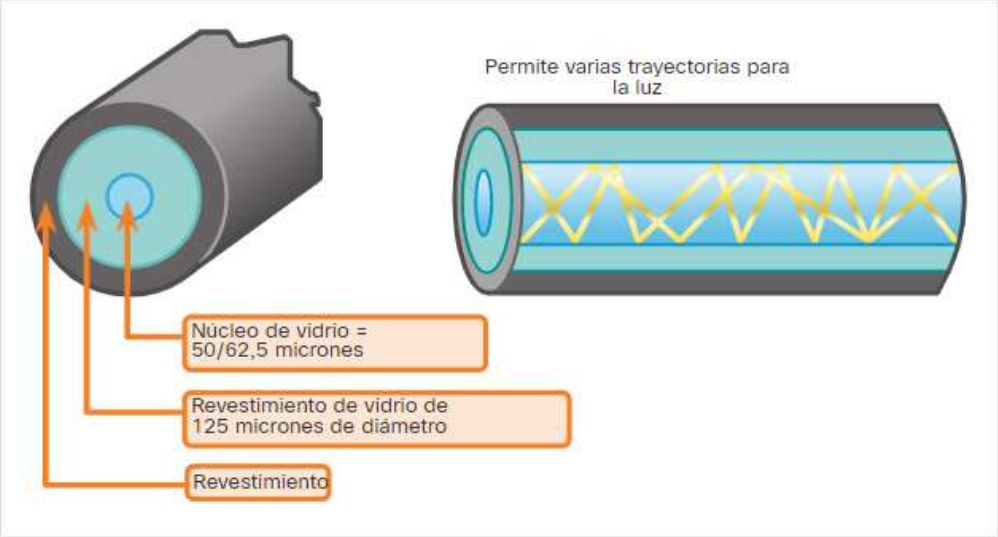


Fibra monomodo | Fibra multimodo

Fibra multimodo (Multimode Fiber)

MMF consta de un núcleo más grande y utiliza emisores LED para enviar pulsos de luz. Específicamente, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos, como se muestra en la figura. Se usa mucho en las redes LAN, debido a que pueden alimentarse mediante LED de bajo costo. Proporciona un ancho de banda de hasta 10 Gb/s a través de longitudes de enlace de hasta 550 metros.

Sección transversal de un cable de fibra óptica multimodo que consta de un núcleo central de vidrio de 50/62,5 micras de diámetro, rodeado por un revestimiento de vidrio de 125 micras de diámetro, rodeado por un revestimiento. Una vista lateral de visión de rayos X muestra que este tipo de construcción de cable permite múltiples trayectorias para la luz.



Una de las diferencias destacadas entre MMF y SMF es la cantidad de dispersión. La dispersión se refiere a la extensión de los pulsos de luz con el tiempo. El aumento de la dispersión significa una mayor pérdida de la intensidad de la señal. FMM tiene una mayor dispersión que SMF. Es por eso que MMF sólo puede viajar hasta 500 metros antes de la pérdida de señal.

4.5.3

Uso del cableado de fibra óptica

En la actualidad, el cableado de fibra óptica se utiliza en cuatro tipos de industrias:

- **Redes empresariales -** Se utilizan para aplicaciones de cableado backbone y dispositivos de infraestructura de interconexión

- **Fibra hasta el hogar (FTTH) -** se utiliza para proporcionar servicios de banda ancha siempre activos a hogares y pequeñas empresas
- **Redes de larga distancia -** Utilizadas por proveedores de servicios para conectar países y ciudades
- **Redes de cable submarino -** se utilizan para proporcionar soluciones confiables de alta velocidad y alta capacidad capaces de sobrevivir en entornos submarinos hostiles a distancias transoceánicas. Busque en Internet el "mapa de telegeografía de cables submarinos" para ver varios mapas en línea.

En este curso, nos centraremos en el uso de la fibra óptica en el nivel de empresa.

4.5.4

Conectores de fibra óptica

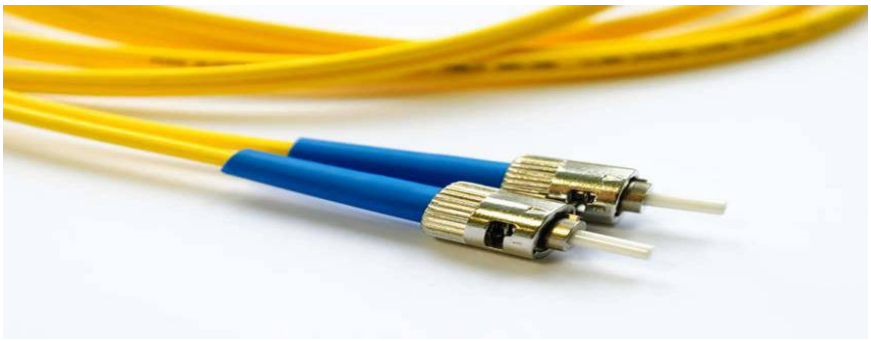
Un conector de fibra óptica termina el extremo de una fibra óptica. Hay una variedad de conectores de fibra óptica disponibles. Las diferencias principales entre los tipos de conectores son las dimensiones y los métodos de acoplamiento. Las empresas deciden qué tipos de conectores utilizarán en base a sus equipos.

Nota: Algunos switches y routers tienen puertos que admiten conectores de fibra óptica a través de un transceptor conectable de factor de forma pequeño (SFP). Busque en Internet varios tipos de SFP.

Haga clic en cada tipo de conector de fibra óptica para obtener una imagen y más información.

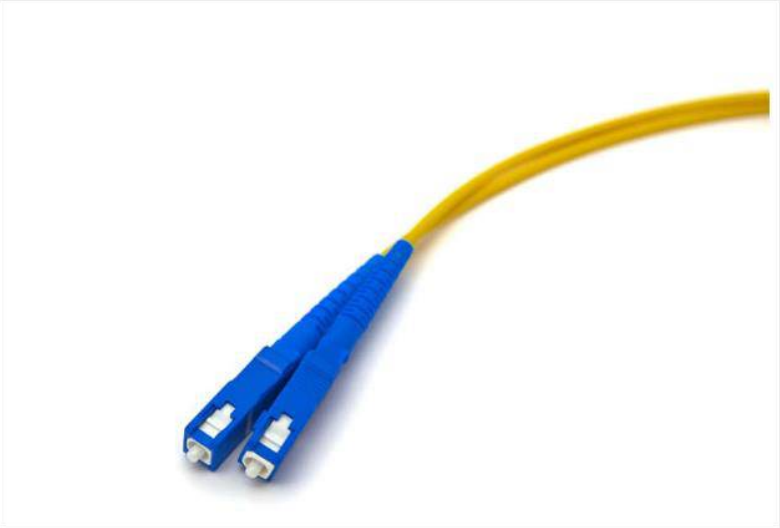
Conectores de punta directa (ST) | Conectores suscriptor (SC) | Conectores Lucent (LC) Conectores Simplex | Conectores LC multimodo dúplex

Los conectores ST fueron uno de los primeros tipos de conectores utilizados. El conector se bloquea de manera segura con un mecanismo tipo bayoneta "enroscable / desenroscable".



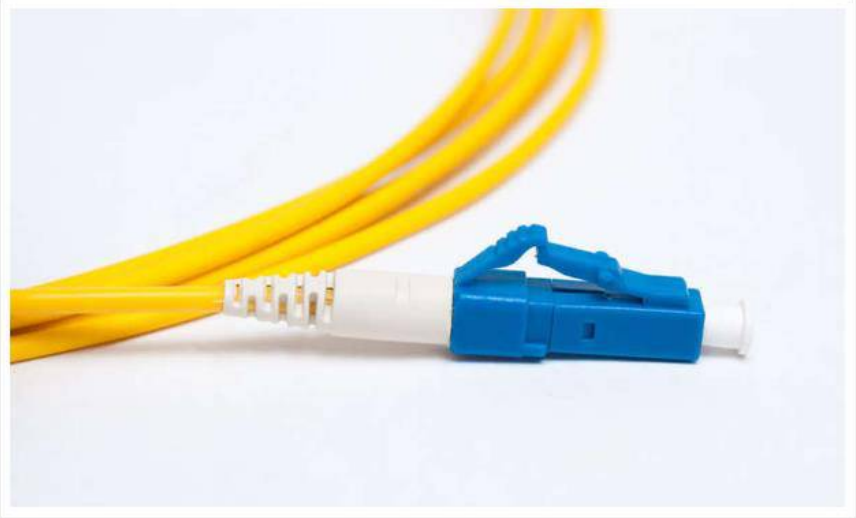
Conectores de punta directa (ST) | Conectores suscriptor (SC) | Conectores Lucent (LC) Conectores Simplex | Conectores LC multimodo dúplex

Los conectores SC a veces se denominan conector cuadrado o conector estándar. Es un conector LAN y WAN ampliamente adoptado que utiliza un mecanismo de inserción/extracción para asegurar la inserción correcta. Este tipo de conector se utiliza con la fibra óptica multimodo y monomodo.



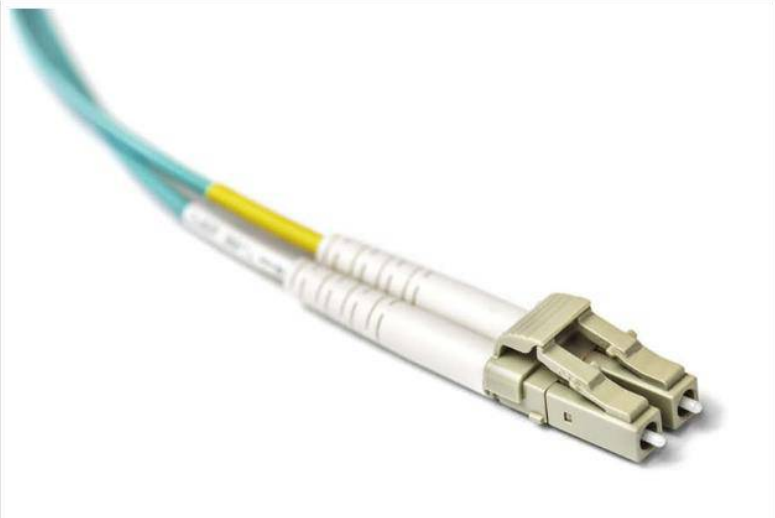
Conectores de punta directa (ST) | Conectores suscriptor (SC) | Conectores Lucent (LC) Conectores Simplex | Conectores LC multimodo dúplex

Los conectores LC simplex son una versión más pequeña del conector SC. A veces se denominan conectores pequeños o locales y están creciendo rápidamente en popularidad debido a su tamaño más pequeño.



Conectores de punta directa (ST) | Conectores suscriptor (SC) | Conectores Lucent (LC) Conectores Simplex | Conectores LC multimodo dúplex

Un conector LC multimodo dúplex es similar a un conector LC simplex, pero utiliza un conector dúplex.



Hasta hace poco, la luz solo podía viajar en una dirección sobre la fibra óptica. Se requirieron dos fibras para soportar la operación dúplex completa. En consecuencia, los cables de conexión de fibra óptica forman un haz de dos cables de fibra óptica, y su terminación incluye un par de conectores de fibra monomodo estándar. Algunos conectores de fibra aceptan tanto las fibras de transmisión como de recepción en un único conector, conocido como conector dúplex, como se muestra en el conector LC multimodo dúplex en la figura. Los estándares BX como 100BASE-BX utilizan diferentes longitudes de onda para enviar y recibir a través de una sola fibra.

4.5.5

Cables de conexión de fibra

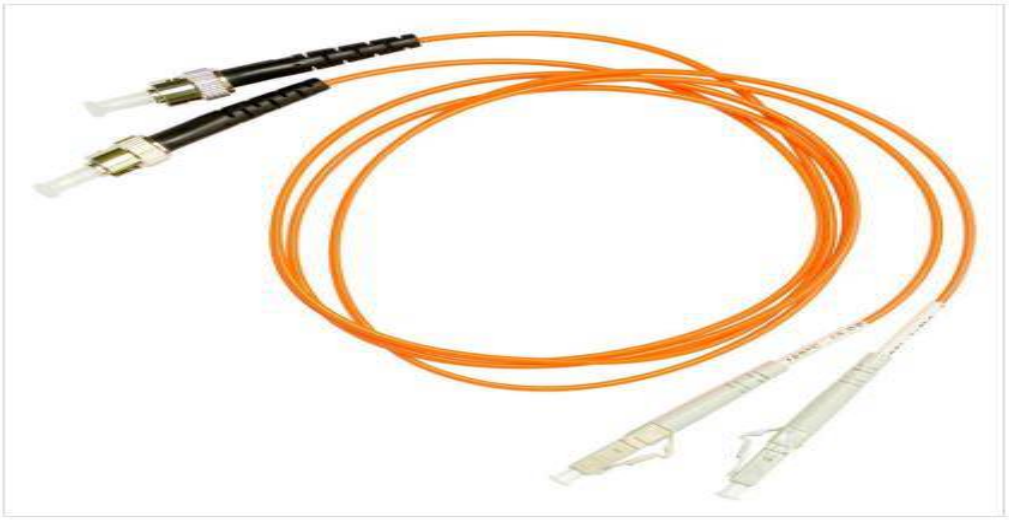
Los cables de conexión de fibra óptica son necesarios para interconectar dispositivos de infraestructura. El uso de colores distingue entre los cables de conexión monomodo y multimodo. El conector amarillo corresponde a los cables de fibra óptica monomodo y el naranja (o aqua) corresponde a los cables de fibra óptica multimodo.

Haga clic en cada cable de conexión de fibra para obtener una imagen.

Cable de conexión multimodo SC-SC | Cable de conexión monomodo LC-LC | Cable de conexión multimodo ST-LC | Cable de conexión monomodo SC-ST

Cable de conexión multimodo SC-SC | Cable de conexión monomodo LC-LC | Cable de conexión multimodo ST-LC | Cable de conexión monomodo SC-ST

Cable de conexión multimodo SC-SC | Cable de conexión monomodo LC-LC | Cable de conexión multimodo ST-LC | Cable de conexión monomodo SC-ST



Cable de conexión multimodo SC-SC | Cable de conexión monomodo LC-LC | Cable de conexión multimodo ST-LC | Cable de conexión monomodo SC-ST

Nota: Los cables de fibra óptica se deben proteger con un pequeño capuchón de plástico cuando no se utilizan.

4.5.6

Fibra versus cobre

La utilización de cables de fibra óptica ofrece muchas ventajas en comparación con los cables de cobre. La tabla destaca algunas de estas diferencias.

En la actualidad, en la mayoría de los entornos empresariales, la fibra óptica se utiliza principalmente como cableado troncal para conexiones punto a punto de alto tráfico entre instalaciones de distribución de datos. También se utiliza para la interconexión de edificios en campus de múltiples edificios. Debido a que los cables de fibra óptica no conducen electricidad y tienen una baja pérdida de señal, son adecuados para estos usos.

UTP and Fiber-Optic Cabling Comparison

Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Problemas de implementación	**Cableado UTP**	**Cableado de fibra óptica**
Ancho de banda soportado	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distancia	Relativamente corta (de 1 a 100 metros)	Relativamente largo (1 - 100,000 metros)
Inmunidad a EMI y RFI	Baja	Alta(Totalmente inmune)
Inmunidad a peligros eléctricos	Baja	Alta (Totalmente inmune)
Costos de medios y conectores	Más bajo	Más alto
Se necesitan habilidades de instalación	Más bajo	Más alto
Precauciones de seguridad	Más bajo	Más alto

4.5.7

Compruebe su comprensión - Cableado de fibra óptica

Verifique su comprensión del cableado de fibra óptica eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La fibra multimodo tiene una limitación de distancia más corta que la fibra monomodo. Comúnmente utilizado en LAN con una distancia de unos pocos cientos de metros, pero puede ser de hasta 2 km.
2. La fibra multimodo utiliza LED como fuente de luz.
3. La fibra monomodo utiliza tecnología láser como fuente de luz.
4. La fibra monomodo se usa comúnmente para aplicaciones de telefonía y televisión de largo alcance.
5. La fibra monomodo se utiliza para aplicaciones de larga distancia de hasta 100 km.
6. La fibra multimodo tiene una limitación de distancia más corta que la fibra monomodo. Comúnmente utilizado en LAN dentro de una red de campus.

Has tenido 6 respuestas correctas de 6.

1. ¿Cuál de los siguientes tipos de cables de fibra óptica puede ayudar a los datos a viajar aproximadamente 1,24 millas o 2 km/2000m?

¡Lo tienes!

- (•) multimodo
- ( ) monomodo

2. ¿Cuál de los siguientes tipos de cables de fibra óptica utiliza diodos emisores de luz (LED) como transmisor de fuente de luz de datos?

¡Lo tienes!

- (•) multimodo
- ( ) monomodo

3. ¿Cuál de los siguientes tipos de cable de fibra óptica utiliza láseres en una sola corriente como transmisor de fuente de luz de datos?

¡Lo tienes!

- ( ) multimodo
- (•) monomodo

4. ¿Cuál de los siguientes tipos de cable de fibra óptica se utiliza para conectar telefonía de larga distancia y aplicaciones de televisión por cable?

¡Lo tienes!

- ( ) multimodo
- (•) monomodo

5. ¿Cuál de los siguientes tipos de cables de fibra óptica puede recorrer aproximadamente 62,5 millas o 100 km/100000 m?

¡Lo tienes!

- multimodo
- monomodo

6. ¿Cuál de los siguientes tipos de cables de fibra óptica se utiliza dentro de una red de campus?

¡Lo tienes!

- multimodo
- monomodo

Correct

You have successfully identified the correct answers.

1. Multimode fiber has a shorter distance limitation than single-mode fiber. Commonly used on LANs with a distance of a few hundred meters but can be up to 2 km.
2. Multimode fiber used LEDs as the light source.
3. Single-mode fiber uses laser technology as the light source.
4. Single-mode fiber is commonly used for long haul TV and telephony applications.
5. Single-mode fiber is used for long haul applications up to 100 km.
6. Multimode fiber has a shorter distance limitation than single mode fiber. Commonly used on LANs within a campus network.

You got 6 out of 6 questions correct.

1. Which of the following fiber-optic cable types can help data travel approximately 500 meters?

You got it!

- multimode
- single-mode

2. Which of the following fiber-optic cable types use light emitting diodes (LEDs) as a data light source transmitter?

You got it!

- multimode
- single-mode

3. Which of the following fiber-optic cable types use lasers in a single stream as a data light source transmitter?

You got it!

- multimode
- (•) single-mode

4. Which of the following fiber-optic cable types is used to connect long-distance telephony and cable TV applications?

You got it!

- multimode
- (•) single-mode

5. Which of the following fiber-optic cable types can travel approximately 100 km?

You got it!

- multimode
- (•) single-mode

6. Which of the following fiber-optic cable types is used within a campus network?

You got it!

- (•) multimode
- single-mode

Capa física / Medios inalámbricos

Medios inalámbricos

4.6.1

Propiedades de los medios inalámbricos

Es posible que esté tomando este curso usando una tableta o un teléfono inteligente. Esto solo es posible debido a los medios inalámbricos, que es la tercera forma de conectarse a la capa física de una red.

Los medios inalámbricos transportan señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos mediante frecuencias de radio y de microondas.

Los medios inalámbricos proporcionan las mejores opciones de movilidad de todos los medios y la cantidad de dispositivos habilitados para tecnología inalámbrica sigue en aumento. La tecnología inalámbrica es ahora la principal forma en que los usuarios se conectan a las redes domésticas y empresariales.

Estas son algunas de las limitaciones de la tecnología inalámbrica:

- **Área de cobertura** - Las tecnologías inalámbricas de comunicación de datos funcionan bien en entornos abiertos. Sin embargo, existen determinados materiales de construcción utilizados en edificios y estructuras, además del terreno local, que limitan la cobertura efectiva.
- **Interferencia** - La tecnología inalámbrica también es vulnerable a la interferencia, y puede verse afectada por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.
- **Seguridad** - La cobertura de la comunicación inalámbrica no requiere acceso a un hilo físico de un medio. Por lo tanto, dispositivos y usuarios sin autorización para acceder a la red pueden obtener acceso a la transmisión. La seguridad de la red es un componente principal de la administración de redes inalámbricas.
- **Medio compartido** - WLAN opera en medio duplex, lo que significa que solo un dispositivo puede enviar o recibir a la vez. El medio inalámbrico se comparte entre todos los usuarios inalámbricos. Muchos usuarios que acceden a la WLAN simultáneamente resultan en un ancho de banda reducido para cada usuario.

Aunque la conectividad inalámbrica de escritorio está aumentando en popularidad, el cobre y la fibra son los medios de capa física más populares para la implementación de dispositivos de red intermedios, como routers y switches.

4.6.2

Tipos de medios inalámbricos

Los estándares de IEEE y del sector de las telecomunicaciones sobre las comunicaciones inalámbricas de datos abarcan la capa física y de enlace de datos. En cada uno de estos estándares, las especificaciones de la capa física se aplican a áreas que incluyen:

- Codificación de señales de datos a señales de radio
- Frecuencia e intensidad de la transmisión
- Requisitos de recepción y decodificación de señales
- Diseño y construcción de antenas

Estos son los estándares inalámbricos:

- **Wi-Fi (IEEE 802.11)** - Tecnología de red LAN inalámbrica (WLAN), comúnmente llamada Wi-Fi. WLAN utiliza un protocolo por contención conocido como acceso múltiple por detección de portadora con prevención de colisiones (CSMA/CA). La NIC inalámbrica primero debe escuchar antes de transmitir para determinar si el canal de radio está libre. Si otro dispositivo inalámbrico está transmitiendo, entonces la NIC deberá aguardar hasta que el canal esté libre. Wi-Fi es una marca comercial de Wi-Fi Alliance. Wi-Fi se utiliza con dispositivos WLAN certificados basados en los estándares IEEE 802.11.
- **Bluetooth (IEEE 802.15)** - Este es un estándar de red de área personal inalámbrica (WPAN), comúnmente conocido como «Bluetooth». Utiliza un proceso de emparejamiento de dispositivos para distancias de 1 a 100 metros.
- **WiMAX (IEEE 802:16)** - Comúnmente conocida como Interoperabilidad mundial para el acceso por microondas (WiMAX), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.
- **Zigbee (IEEE 802.15.4)** - Zigbee es una especificación utilizada para comunicaciones de baja velocidad de datos y baja potencia. Está diseñado para aplicaciones que requieren corto alcance, baja velocidad de datos y larga duración de la batería. Zigbee se utiliza normalmente para entornos industriales e Internet de las cosas (IoT), tales como interruptores de luz inalámbricos y recopilación de datos de dispositivos médicos.

Nota: Otras tecnologías inalámbricas como las comunicaciones celulares y satelitales también pueden proporcionar conectividad de red de datos. Sin embargo, estas tecnologías inalámbricas están fuera del alcance de este módulo.

4.6.3

LAN inalámbrica

Una implementación común de tecnología inalámbrica de datos permite a los dispositivos conectarse en forma inalámbrica a través de una LAN. En general, una WLAN requiere los siguientes dispositivos de red:

- **Punto de acceso inalámbrico (AP)** - Concentra las señales inalámbricas de los usuarios y se conecta a la infraestructura de red existente basada en cobre, como Ethernet. Los routers inalámbricos domésticos y de pequeñas empresas integran las funciones de un router, un switch y un punto de acceso en un solo dispositivo, como el que se ve en la figura.
- **Adaptadores NIC inalámbricos** - Brindan capacidad de comunicaciones inalámbricas a los hosts de red

A medida que la tecnología fue evolucionando, surgió una gran cantidad de estándares WLAN basados en Ethernet. Al comprar dispositivos inalámbricos, asegúrese de compatibilidad e interoperabilidad.

Los beneficios de las tecnologías inalámbricas de comunicación de datos son evidentes, especialmente en cuanto al ahorro en el cableado costoso de las instalaciones y en la

conveniencia de la movilidad del host. Los administradores de red deben desarrollar y aplicar políticas y procesos de seguridad estrictos para proteger las WLAN del acceso no autorizado y los daños.

Cisco Meraki MX64W

4.6.4

Compruebe su comprensión — Medios inalámbricos

Verifique su comprensión de los medios inalámbricos eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es falso. La tecnología inalámbrica proporciona la mayor movilidad de todos los medios y está ganando popularidad en las redes empresariales.
2. La respuesta correcta es falso. WLANs operan en medio duplex, lo que significa que solo un dispositivo puede enviar o recibir a la vez. Esto puede afectar el rendimiento de la red si hay muchos usuarios que acceden a la WLAN al mismo tiempo.
3. Zigbee está diseñado para aplicaciones que requieren corto alcance, bajas tasas de datos y larga duración de la batería, por lo que es ideal para aplicaciones industriales y IoT.
4. Este estándar inalámbrico se utiliza para redes de área personal (PAN) y permite que los dispositivos se comuniquen a distancias de 1 a 100 metros.

Has tenido 4 respuestas correctas de 4.

1. Verdadero o falso La tecnología inalámbrica no es adecuada para redes empresariales.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

2. Verdadero o falso Las LAN inalámbricas funcionan en dúplex completo, lo que permite que todos los dispositivos envíen o reciban datos al mismo tiempo para que el número de usuarios no afecte al rendimiento.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

3. ¿Cuál de los siguientes estándares inalámbricos es el más adecuado para entornos industriales e IoT?

¡Lo tienes!

- ◉ ZigBee
- ○ WiMAX
- ○ Wi-Fi
- ○ Bluetooth

4. ¿Cuál de los siguientes estándares inalámbricos se utiliza para redes de área personal (PAN) y permite que los dispositivos se comuniquen a distancias de 1 a 100 metros?

¡Lo tienes!

- ○ ZigBee
- ○ WiMAX
- ○ Wi-Fi
- ◉ Bluetooth

Correct

You have successfully identified the correct answers.

1. The correct answer is False. Wireless provides the greatest mobility of all media and is gaining popularity in enterprise networks.
2. The correct answer is False. WLANs operate in half-duplex, which means only one device can send or receive at a time. This can impact network performance if there are many users accessing the WLAN at the same time.
3. Zigbee is intended for applications that require short-range, low data-rates, and long battery life, making it well suited for industrial and IoT applications.
4. This wireless standard is used for Personal Area Networks (PANs) and allows devices to communicate over distances of 1 to 100 meters.

You got 4 out of 4 questions correct.

1. True or false. Wireless is not well suited for enterprise networks.

You got it!

- ○ true
- ◉ false

2. True or false. Wireless LANs operate in full-duplex allowing all devices to send or receive data at the same time so the number of users does not impact performance.

You got it!

- ○ true
- ◉ false

3. Which of the following wireless standards is best suited for industrial and IoT environments?

You got it!

- ◉ Zigbee
- ○ WiMAX
- ○ Wi-Fi
- ○ Bluetooth

4. Which of the following wireless standards is used for Personal Area Networks (PANs) and allows devices to communicate over distances of 1 to 100 meters?

You got it!

- ○ Zigbee
- ○ WiMAX
- ○ Wi-Fi
- ◉ Bluetooth

4.6.5

Packet Tracer - Conecte una LAN cableada e inalámbrica

Al trabajar en Packet Tracer, un entorno de laboratorio o un contexto empresarial, debe saber cómo seleccionar el cable adecuado y cómo conectar correctamente los dispositivos. En esta actividad se analizarán configuraciones de dispositivos en el Packet Tracer, se seleccionarán los cables adecuados según la configuración y se conectarán los dispositivos. Esta actividad también explorará la vista física de la red en el Packet Tracer.

conecte una LAN alámbrica e inalámbrica

conecte una LAN alámbrica e inalámbrica

4.6.6

Lab - Ver información de NIC cableada e inalámbrica

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Identificar y trabajar con NICs de PC
- Parte 2: Identificar y utilizar los íconos de red de la bandeja del sistema

Vea información de NIC alámbrica e inalámbrica

1. Capa física
2. Módulo de Práctica y Prueba

Módulo de Práctica y Prueba

4.7.1

Packet Tracer - Conectar la capa física

En esta actividad, explorará las diversas opciones disponibles en los dispositivos de interconexión de redes. También deberá determinar las opciones que proporcionan la conectividad necesaria cuando deba conectar varios dispositivos. Por último, agregará los módulos correctos y conectará los dispositivos.

Conectar la capa física

Conectar la capa física

4.7.2

¿Qué aprendió en este módulo?

Propósito de la capa física

Antes de que pueda ocurrir cualquier comunicación de red, se debe establecer una conexión física a una red local. Una conexión física puede ser una conexión por cable o una conexión inalámbrica mediante ondas de radio. Las tarjetas de interfaz de red (NIC) conectan un dispositivo a la red. Las NIC Ethernet se utilizan para una conexión por cable, mientras que las NIC WLAN (red de área local inalámbrica) se utilizan para la conexión inalámbrica. La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de enlace de datos y la codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermediario recibe los bits codificados que componen una trama.

Característica de la capa física

La capa física consta de circuitos electrónicos, medios y conectores desarrollados por ingenieros. Los estándares de la capa física abordan tres áreas funcionales: componentes físicos, codificación y señalización. El ancho de banda es la capacidad a la que un medio puede transportar datos. El ancho de banda digital mide la cantidad de datos que pueden fluir desde un lugar hacia otro en un período de tiempo determinado. El rendimiento es la medida de la transferencia de bits a través de los medios durante un período de tiempo determinado y generalmente es menor que el ancho de banda. El concepto de latencia se refiere a la cantidad de tiempo, incluidas las demoras, que les toma a los datos transferirse desde un punto determinado hasta otro. La capacidad de transferencia útil es la medida de datos utilizables transferidos durante un período determinado. La capa física produce la representación y las agrupaciones de bits para cada tipo de medio de la siguiente manera:

- **Cable de cobre** - Las señales son patrones de pulsos eléctricos.
- **Cable de fibra óptica** - Las señales son patrones de luz.
- **Conexión inalámbrica** - Las señales son patrones de transmisiones de microondas.

Cableado de cobre

Las redes utilizan medios de cobre porque son económicos y fáciles de instalar, y tienen baja resistencia a la corriente eléctrica. Sin embargo, estos medios están limitados por la distancia y la interferencia de señal. Los valores de tiempo y voltaje de los pulsos eléctricos también son susceptibles a la interferencia de dos fuentes: EMI y el crosstalk. Tres tipos de cableado de cobre son: UTP, STP y cable coaxial (coaxial). UTP tiene una cubierta exterior para proteger los cables de cobre de daños físicos, pares trenzados para proteger la señal de interferencias y aislamiento plástico codificado por colores que aísla eléctricamente los cables unos de otros e identifica cada par. El cable STP utiliza cuatro pares de cables, cada

uno envuelto en un blindaje de aluminio, que luego se envuelve en una trenza o lámina metálica general. El cable coaxial obtiene su nombre del hecho de que hay dos conductores que comparten el mismo eje. Coaxial se utiliza para conectar antenas a dispositivos inalámbricos. Los proveedores de Internet por cable utilizan coaxial dentro de las instalaciones de sus clientes.

UTP Cabling

Consta de cuatro pares de hilos codificados por colores que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible. Los cables UTP no utilizan blindaje para contrarrestar los efectos de la EMI y la RFI. En cambio, los diseñadores de cables han descubierto otras formas de limitar el efecto negativo del crosstalk: la cancelación y la variación del número de giros por par de cables. El cableado UTP cumple con los estándares establecidos en conjunto por la TIA/EIA. El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define las características eléctricas del cableado de cobre. Los cables UTP generalmente se terminan con un conector RJ-45. Los principales tipos de cables que se obtienen mediante el uso de convenciones de cableado específicas son Ethernet Directo y Ethernet Cruzado. Cisco tiene un cable UTP propietario llamado rollover que conecta una estación de trabajo a un puerto de consola del router.

Fiber-Optic Cabling

El cable de fibra óptica transmite datos a distancias más largas y con anchos de banda más altos que cualquier otro medio de red. El cable de fibra óptica puede transmitir señales con menos atenuación que el cable de cobre y es completamente inmune a EMI y RFI. La fibra óptica es un hilo flexible, pero extremadamente delgado y transparente de vidrio muy puro, no mucho más grueso que un cabello humano. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra óptica se está utilizando ahora en cuatro tipos de industria: redes empresariales, FTTH, redes de largo recorrido y redes de cable submarino. Hay cuatro tipos de conectores de fibra óptica: ST, SC, LC y LC multimodo dúplex. Los cables de conexión de fibra óptica incluyen SC-SC multimodo, LC-LC monomodo, ST-LC multimodo y SC-ST monomodo. En la mayoría de los entornos empresariales, la fibra óptica se utiliza principalmente como cableado de red troncal para conexiones punto a punto de alto tráfico entre instalaciones de distribución de datos y para la interconexión de edificios en campus de varios edificios.

Cableado Fibra óptica

Los medios inalámbricos transportan señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos mediante frecuencias de radio y de microondas. La tecnología inalámbrica tiene algunas limitaciones, entre ellas: área de cobertura, interferencia, seguridad y los problemas que se producen con cualquier medio compartido. Los estándares inalámbricos incluyen los siguientes: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16) y Zigbee (IEEE 802.15.4). LAN inalámbrica (WLAN) requiere un AP inalámbrico y adaptadores NIC inalámbricos.

4.7.3

Prueba del módulo: La Capa Física

Correcto

Identificó bien las respuestas correctas.

Has tenido 15 respuestas correctas de 15.

1. ¿Cuál es el objetivo de la capa física de OSI?

Tema 4.1.0 – La capa física es responsable de transmitir las señales reales a través de los medios físicos como bits. El intercambio de tramas, el control del acceso a los medios y la detección de errores son funciones de la capa de enlace de datos.

- Controlar el acceso a los medios
- Transmitir bits por los medios locales
- Realizar pruebas de detección de errores en las tramas recibidas
- Intercambiar tramas entre nodos por medios físicos de red

2. ¿Por qué se utilizan dos hilos de fibra para una sola conexión de fibra óptica?

Tema 4.5.0 – La luz solo puede viajar en una dirección por una sola hebra de fibra. Para permitir la comunicación dúplex completo, se deben conectar dos hilos de fibra entre cada dispositivo.

- Los dos hilos permiten que los datos viajen por distancias más largas sin degradarse.
- Evitan que la diafonía cause interferencias en la conexión.
- Aumentan la velocidad a la que los datos pueden viajar.
- Permiten conectividad dúplex completo.

3. ¿Cuál de las siguientes características describe el crosstalk?

Tema 4.4.0 – EMI y RFI pueden distorsionar las señales de red debido a la interferencia de luces fluorescentes o motores eléctricos. El resultado de la atenuación es el deterioro de la señal de red a medida que viaja por cableado de cobre. Los dispositivos inalámbricos pueden experimentar la pérdida de señal debido a la distancia excesiva del punto de acceso, pero esto no se trata de crosstalk. El crosstalk es la perturbación causada por los campos eléctricos o magnéticos de la señal que se transporta por un hilo adyacente dentro del mismo cable.

- La distorsión de la señal de la red por la iluminación fluorescente
- La distorsión de los mensajes transmitidos desde las señales que se transportan por hilos adyacentes
- El debilitamiento de la señal de la red debido a la longitud de los cables
- La pérdida de señal inalámbrica por la distancia excesiva del punto de acceso

4. ¿Qué procedimiento se utiliza para reducir el efecto de la diafonía en cables de cobre?

Tema 4.4.0 – En los cables de cobre, crosstalk es una perturbación causada por los campos eléctricos o magnéticos de una señal en un cable que interfiere con la señal en un cable adyacente. Trenzar los pares de cables opuestos del circuito juntos puede cancelar efectivamente el crosstalk. Las otras opciones son medidas eficaces para contrarrestar los efectos negativos de IME y RFI, pero no de crosstalk

- que requieren conexiones de puesta a tierra adecuadas
- trenzar pares de cables de circuito opuestos juntos
- envolviendo el paquete de cables con blindaje metálico
- diseñar una infraestructura de cable para evitar interferencias de crosstalk
- evitando curvas bruscas durante la instalación

5. ¿Qué tipo de cable UTP se utiliza para conectar una PC a un puerto de switch?

Tema 4.4.0 – Un cable rollover es un cable propiedad de Cisco que se utiliza para conectarse a un router o cambiar el puerto de consola. Por lo general, se utiliza un cable directo (también llamado "cable de conexión") para interconectar un host a un switch y un switch a un router. Un cable cruzado se utiliza para interconectar dispositivos similares, como dos switches, dos routers y dos hosts.

- ○ De consola
- ○ rollover
- ○ Cruzado
- ◉ Directo

6. ¿Cuál es la definición de ancho de banda?

Tema 4.2.0 – El ancho de banda es la medida de la capacidad de un medio de red para transportar datos. Es la cantidad de datos que pueden transmitirse entre dos puntos de la red durante un periodo específico, en general, un segundo.

- ○ La medida de transferencia de bits por los medios durante un período determinado
- ○ La velocidad en que los bits se transmiten por la red
- ◉ La cantidad de datos que pueden fluir desde un lugar hacia otro en un período determinado
- ○ La medida de datos utilizables transferidos durante un período determinado

7. ¿Cuál de estas afirmaciones describe correctamente la codificación de tramas?

Tema 4.2.0 – La codificación de tramas convierte una transmisión de bits de datos a un código predefinido que reconocen tanto el emisor como el receptor. Estos códigos se usan con diversos propósitos, como distinguir los bits de datos de los bits de control e identificar el comienzo y el final de una trama.

- ○ Usa la característica de una onda para modificar otra onda.
- ○ Transmite señales de datos junto con una señal de reloj que sucede en intervalos de igual duración.
- ○ Genera las señales eléctricas, ópticas o inalámbricas que representan los números binarios de la trama.
- ◉ Convierte los bits a un código predefinido para proporcionar un patrón predecible que ayude a distinguir los bits de datos de los bits de control.

8. ¿Cuál de las siguientes es una característica del cableado UTP?

Tema 4.4.0 – El revestimiento y la inmunidad a los peligros eléctricos son características del cableado de fibra óptica. La malla de cobre tejida o el papel metálico se utilizan como protección para el conductor interno de un cable coaxial. Una característica del cableado UTP es la anulación, en la que dos cables se ubican a la par, y cada campo magnético anula el campo magnético adyacente.

- ◉ Anulación
- ○ Revestimiento
- ○ Inmunidad a los peligros eléctricos
- ○ Malla de cobre tejida o papel metálico

9. Se está implementando una LAN inalámbrica dentro de la nueva oficina de una sala ocupada por el guardabosques. La oficina se encuentra en la parte más alta del parque nacional. Una vez finalizada la prueba de red, los técnicos informan que la señal de LAN inalámbrica se ve afectada ocasionalmente por algún tipo de interferencia. ¿Cuáles son dos posibles causas de la distorsión? (Escoja dos opciones).

Tema 4.6.0 - La conectividad LAN inalámbrica no se ve afectada por árboles ni por la elevación del equipo. Debido a que se trata de una oficina de una habitación en un área aislada, no habrá un gran número de dispositivos inalámbricos o fuente de interferencia operando en las inmediaciones, aparte de un teléfono celular o un horno de microondas.

- [x] el horno microondas
- [ ] el gran número de árboles que rodean la oficina
- [x] los teléfonos celulares utilizados por los empleados
- [ ] la ubicación elevada donde se instaló la LAN inalámbrica
- [ ] el número de dispositivos inalámbricos que se utilizan en la LAN inalámbrica

10. ¿Qué indica el término rendimiento?

Tema 4.2.0 - El rendimiento es la medida de transferencia de bits por los medios durante un período determinado. El rendimiento se ve afectado por varios factores, como la EMI y la latencia, por lo que no es común que coincida con el ancho de banda especificado para un medio de red. Las medidas de rendimiento incluyen los bits de datos de usuario y otros bits de datos, como la sobrecarga, el acuse de recibo y el encapsulamiento. La medida de los datos utilizables transferidos por los medios se llama "capacidad de transferencia útil".

- ( ) La velocidad de transferencia de datos garantizada por un ISP
- ( ) La capacidad de un medio en particular para transportar datos
- ( ) La medida de los datos utilizables transferidos por los medios
- (•) La medida de los bits transferidos por los medios durante un periodo determinado
- ( ) El tiempo que tarda un mensaje en viajar del emisor al receptor

11. ¿Cuál es una ventaja de usar cables de fibra óptica en lugar de cables de cobre?

Tema 4.5.0 - El cableado de cobre suele ser más barato y más fácil de instalar que el cableado de fibra óptica. Sin embargo, los cables de fibra generalmente tienen un rango de señalización mucho mayor que el cobre.

- ( ) Por lo general, es más barato que el cableado de cobre.
- ( ) Es capaz de instalarse alrededor de curvas afiladas.
- ( ) Es más fácil de terminar e instalar que el cableado de cobre.
- (•) Es capaz de transportar señales mucho más lejos que el cableado de cobre.

12. ¿Qué organización de estándares supervisa el desarrollo de estándares LAN inalámbrica?

Tema 4.2.0 - IANA supervisa la gestión de la asignación de direcciones IP y los nombres de dominio. ISO es el mayor desarrollador de estándares internacionales de red y es famoso por el modelo de interconexión de sistemas abiertos (OSI). TIA se centra en las normas de comunicación. Los estándares IEEE 802 son muchos, pero los que afectan a un profesional de red de nivel básico son Ethernet (802.3), LAN inalámbricas (802.11) y PAN inalámbricos (802.15).

- ( ) IANA
- (•) IEEE
- ( ) ISO
- ( ) TIA

13. Un administrador de red está diseñando una nueva infraestructura de red que incluye conectividad cableada e inalámbrica.¿En qué situación se recomienda una conexión inalámbrica?

Tema 4.6.0 - Cuando los dispositivos del usuario final necesitan movilidad para conectarse a la red, se recomienda la conexión inalámbrica. Si un dispositivo de usuario final sólo tiene una NIC Ethernet, el usuario sólo podrá utilizar el cableado Ethernet. Si RFI es un problema, no se recomienda la conexión inalámbrica. Un dispositivo de usuario final que requiera una conexión dedicada para el rendimiento funcionaría mejor con un cable Ethernet dedicado.

- ○ El dispositivo de usuario final sólo tiene una NIC Ethernet.
- ○ El dispositivo del usuario final requiere una conexión dedicada debido a los requisitos de rendimiento.
- ◉ El dispositivo del usuario final necesita movilidad al conectarse a la red.
- ○ El área del dispositivo del usuario final tiene una alta concentración de RFI.

14. Un administrador de red está solucionando problemas de conectividad en un servidor. Mediante un probador, el administrador observa que las señales generadas por la NIC del servidor están distorsionadas y no se pueden utilizar. ¿En qué capa del modelo OSI está categorizado el error?

Tema 4.2.0 - La NIC tiene responsabilidades tanto en la Capa 1 como en la Capa 2. La NIC codifica la trama como una serie de señales que se transmiten a los medios locales. Esta es la responsabilidad de la capa física del modelo OSI. La señal podría ser en forma de ondas eléctricas, ópticas o de radio.

- ○ Capa de presentación
- ○ Capa de red
- ◉ Capa física
- ○ Capa de enlace de datos

15. ¿Qué tipo de cable se usa para conectar un puerto serie de la estación de trabajo al puerto de consola de un router Cisco?

Tema 4.4.0 - Los pares de cables UTP pueden terminarse en diferentes configuraciones para su uso en diferentes aplicaciones. Para usar un cable UTP con el fin de acceder a un router Cisco mediante el puerto de consola desde un puerto serie de una PC, dicho cable debe tener una terminación de cable de consola.

- ○ Cruzado
- ◉ rollover
- ○ Directo
- ○ Coaxial

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. A network administrator is troubleshooting connectivity issues on a server. Using a tester, the administrator notices that the signals generated by the server NIC are distorted and not usable. In which layer of the OSI model is the error categorized?

Topic 4.2.0 - The NIC has responsibilities in both Layer 1 and Layer 2. The NIC encodes the frame as a series of signals that are transmitted onto the local media. This is the responsibility of the physical layer of the OSI model. The signal could be in the form of electrical, optical, or radio waves.

- ○ presentation layer
- ○ network layer
- ◉ physical layer
- ○ data link layer

2. What type of cable is used to connect a workstation serial port to a Cisco router console port?

Topic 4.4.0 - UTP cable wire pairs can be terminated in different configurations for use in different applications. To use a UTP cable for consoling into a Cisco router from a PC serial port, it must be terminated as a rollover or console cable.

- ○ crossover
- ◉ rollover
- ○ straight-through
- ○ coaxial

3. Why are two strands of fiber used for a single fiber optic connection?

Topic 4.5.0 - Light can only travel in one direction down a single strand of fiber. In order to allow for full-duplex communication two strands of fiber must be connected between each device.

- ○ The two strands allow the data to travel for longer distances without degrading.
- ○ They prevent crosstalk from causing interference on the connection.
- ○ They increase the speed at which the data can travel.
- ◉ They allow for full-duplex connectivity.

4. Which procedure is used to reduce the effect of crosstalk in copper cables?

Topic 4.4.0 - In copper cables, crosstalk is a disturbance caused by the electric or magnetic fields of a signal on one wire interfering with the signal in an adjacent wire. Twisting opposing circuit wire pairs together can effectively cancel the crosstalk. The other options are effective measures to counter the negative effects of EMI and RFI, but not crosstalk.

- ○ requiring proper grounding connections
- ◉ twisting opposing circuit wire pairs together
- ○ wrapping the bundle of wires with metallic shielding
- ○ designing a cable infrastructure to avoid crosstalk interference
- ○ avoiding sharp bends during installation

5. What is one advantage of using fiber optic cabling rather than copper cabling?

Topic 4.5.0 - Copper cabling is usually cheaper and easier to install than fiber optic cabling. However, fiber cables generally have a much greater signaling range than copper.

- ○ It is usually cheaper than copper cabling.
- ○ It is able to be installed around sharp bends.
- ○ It is easier to terminate and install than copper cabling.
- ◉ It is able to carry signals much farther than copper cabling.

6. A network administrator is designing a new network infrastructure that includes both wired and wireless connectivity. Under which situation would a wireless connection be recommended?

Topic 4.6.0 - When the end-user devices need mobility to connect to the network, wireless is recommended. If an end-user device only has an Ethernet NIC, the user will only be able to use Ethernet cabling. If RFI is an issue, wireless is not recommended. An end-user device that requires a dedicated connection for performance would perform better with a dedicated Ethernet cable.

- ○ The end-user device only has an Ethernet NIC.
- ○ The end-user device requires a dedicated connection because of performance requirements.
- ◉ The end-user device needs mobility when connecting to the network.
- ○ The end-user device area has a high concentration of RFI.

7. Which type of UTP cable is used to connect a PC to a switch port?

Topic 4.4.0 - A rollover cable is a Cisco proprietary cable used to connect to a router or switch console port. A straight-through (also called patch) cable is usually used to interconnect a host to a switch and a switch to a router. A crossover cable is used to interconnect similar devices together, for example, between two switches, two routers, and two hosts.

- ○ console
- ○ rollover
- ○ crossover
- ◉ straight-through

8. What is the definition of bandwidth?

Topic 4.2.0 - Bandwidth is the measure of the capacity of a network medium to carry data. It is the amount of data that can move between two points on the network over a specific period of time, typically one second.

- ○ the speed of bits across the media over a given period of time
- ○ the speed at which bits travel on the network
- ◉ the amount of data that can flow from one place to another in a given amount of time
- ○ the measure of usable data transferred over a given period of time

9. Which statement correctly describes frame encoding?

Topic 4.2.0 - Frame encoding converts a stream of data bits into a predefined code that is recognized by both the sender and receiver. These codes are used for a variety of purposes, such as distinguishing data bits from control bits, and identifying the beginning and end of a frame.

- ○ It uses the characteristic of one wave to modify another wave.
- ○ It transmits data signals along with a clock signal which occurs at evenly spaced time durations.
- ○ It generates the electrical, optical, or wireless signals that represent the binary numbers of the frame.
- ◉ It converts bits into a predefined code in order to provide a predictable pattern to help distinguish data bits from control bits.

10. What is a characteristic of UTP cabling?

Topic 4.4.0 - Cladding and immunization from electrical hazards are characteristics for fiber-optic cabling. A woven copper braid or metallic foil is used as a shield for the inner coaxial cable conductor. Cancellation is a property of UTP cabling where two wires are located adjacent to one another so each magnetic field cancels out the adjacent magnetic field.

- (●) cancellation
- ( ) cladding
- ( ) immunity to electrical hazards
- ( ) woven copper braid or metallic foil

11. A wireless LAN is being deployed inside the new one room office that is occupied by the park ranger. The office is located at the highest part of the national park. After network testing is complete, the technicians report that the wireless LAN signal is occasionally affected by some type of interference. What is a possible cause of the signal distortion?

Topic 4.6.0 - Wireless LAN connectivity is not affected by trees or the elevation of the equipment. Because this is a one room office in an isolated area, there will not be a large number of wireless devices or source of interference operating in the immediate vicinity. The use of a microwave oven could result in signal interference.

- (●) the microwave oven
- ( ) the large number of trees that surround the office
- ( ) the elevated location where the wireless LAN was installed
- ( ) the number of wireless devices that are used in the wireless LAN

12. What is the purpose of the OSI physical layer?

Topic 4.1.0 - The physical layer is responsible for transmitting the actual signals across the physical media as bits. Exchanging frames, controlling media access, and performing error detection are all functions of the data link layer.

- ( ) controlling access to media
- (●) transmitting bits across the local media
- ( ) performing error detection on received frames
- ( ) exchanging frames between nodes over physical network media

13. Which characteristic describes crosstalk?

Topic 4.4.0 - EMI and RFI can distort network signals because of interference from fluorescent lights or electric motors. Attenuation results in deterioration of the network signal as it travels along copper cabling. Wireless devices can experience loss of signals because of excessive distances from a access point, but this is not crosstalk. Crosstalk is the disturbance caused by the electric or magnetic fields of the signal carried on an adjacent wire within the same cable.

- ○ the distortion of the network signal from fluorescent lighting
- ◉ the distortion of the transmitted messages from signals carried in adjacent wires
- ○ the weakening of the network signal over long cable lengths
- ○ the loss of wireless signal over excessive distance from the access point

14. What is indicated by the term throughput?

Topic 4.2.0 - Throughput is the measure of the transfer of bits across the media over a given period of time. Throughput is affected by a number of factors such as, EMI and latency, so it rarely matches the specified bandwidth for a network medium. The throughput measurement includes user data bits and other data bits, such as overhead, acknowledging, and encapsulation. The measure of the usable data transferred across the media is called goodput.

- ○ the guaranteed data transfer rate offered by an ISP
- ○ the capacity of a particular medium to carry data
- ○ the measure of the usable data transferred across the media
- ◉ the measure of the bits transferred across the media over a given period of time
- ○ the time it takes for a message to get from sender to receiver

15. Which standards organization oversees development of wireless LAN standards?

Topic 4.2.0 - IANA oversees the management of IP address allocation and domain names. ISO is the largest developer of international networking standards and is famous for the Open Systems Interconnection (OSI) model. TIA focuses on communication standards. The IEEE 802 standards are many, but the ones that affect an entry-level network professional are Ethernet (802.3), wireless LANs (802.11), and wireless PANs (802.15).

- ○ IANA
- ◉ IEEE
- ○ ISO
- ○ TIA

Capítulo 5_ Sistemas numéricos

Introducción

5.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a sistemas de numeración!

¿Adivinen qué? Esta es una dirección IPv4 de 32 bits de un equipo en una red: 11000000.10101000.00001010.00001010. Se muestra en binario. Esta es la dirección IPv4 del mismo equipo en decimal punteado: 192.168.10.10. ¿Con cuál prefieres trabajar? Las direcciones IPv6 son 128 bits. Para que estas direcciones sean más manejables, IPv6 utiliza un sistema hexadecimal de 0-9 y las letras A-F.

Como administrador de red, debe saber cómo convertir direcciones binarias en decimales punteados y decimales punteados en binarias. También necesitará saber cómo convertir decimal punteado en hexadecimal y viceversa. (Sugerencia: Todavía necesita sus habilidades de conversión binaria para que esto funcione).

Sorprendentemente, no es tan difícil cuando aprendes algunos trucos. Este módulo contiene una actividad llamada el juego binario que realmente le ayudará a comenzar. Entonces, ¿por qué esperar?

5.0.2

¿Qué aprenderá en este módulo?

Título del módulo: Sistemas numéricos

Objetivos del módulo: Calcule los números entre los sistemas decimales, binarios y hexadecimales.

Título del tema	Objetivo del tema
Sistema de numeración binaria	Calcule los números entre los sistemas decimales y binarios.

Título del tema	Objetivo del tema
Sistema numérico hexadecimal	Calcule los números entre los sistemas decimales y hexadecimales.

Las redes en la actualidad / Sistema de numeración binaria

Sistema de numeración binaria

5.1.1

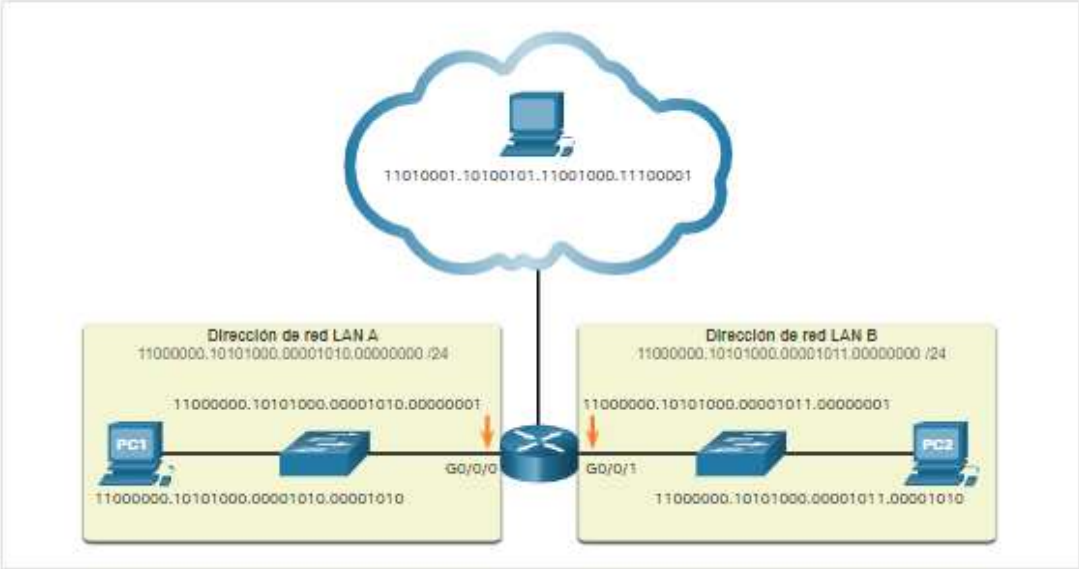
Direcciones binarias e IPv4

Las direcciones IPv4 comienzan como binarias, una serie de solo 1 y 0. Estos son difíciles de administrar, por lo que los administradores de red deben convertirlos a decimales. En este tema se muestran algunas formas de hacerlo.

Binario es un sistema de numeración que consta de los dígitos 0 y 1 llamados bits. En contraste, el sistema de numeración decimal consta de 10 dígitos que consisten en los dígitos desde el 0 al 9.

Es importante que comprendamos el sistema binario, ya que los hosts, los servidores y los dispositivos de red usan el direccionamiento binario. Específicamente, usan direcciones IPv4 binarias, como se muestra en la figura, para identificarse entre sí.

Hay un router central con dos LAN conectadas directamente y una WAN conectada a una nube. Cada LAN tiene un switch y una PC. La WAN tiene una PC. Cada dispositivo tiene una dirección IPv4 que está en notación binaria punteada en lugar de notación decimal punteada.

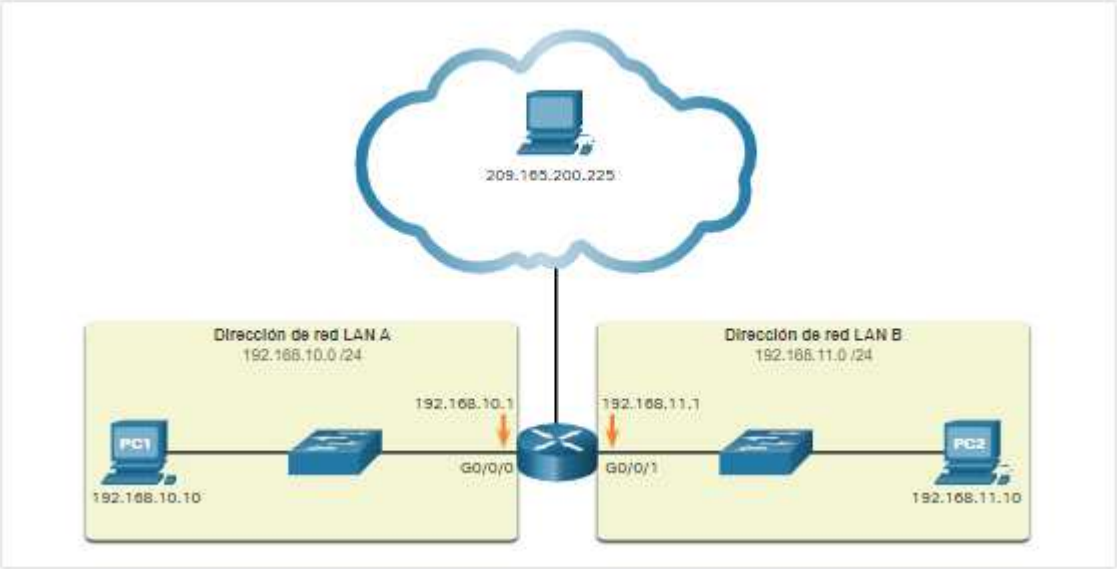


Cada dirección consta de una cadena de 32 bits, divididos en cuatro secciones denominadas octetos. Cada octeto contiene 8 bits (o 1 byte) separados por un punto. Por ejemplo, a la PC1 de la ilustración se le asignó la dirección IPv4 11000000.10101000.00001010.00001010. La dirección de gateway predeterminado sería la de la interfaz Gigabit Ethernet del R1, 11000000.10101000.00001010.00000001.

Binario funciona bien con hosts y dispositivos de red. Sin embargo, es muy difícil para los humanos trabajar con ellos.

Para facilitar el uso por parte de las personas, las direcciones IPv4 se expresan comúnmente en notación decimal con puntos. A la PC1 se le asigna la dirección IPv4 192.168.10.10, y su dirección de puerta de enlace predeterminada es 192.168.10.1, como se muestra en la figura.

Este diagrama es el mismo que el primero, un router central con dos LAN y una WAN conectada a una nube. Esto tiene los mismos dispositivos que el primer diagrama; sin embargo, en lugar de tener el direccionamiento IPv4 en binario, está en notación decimal con puntos.

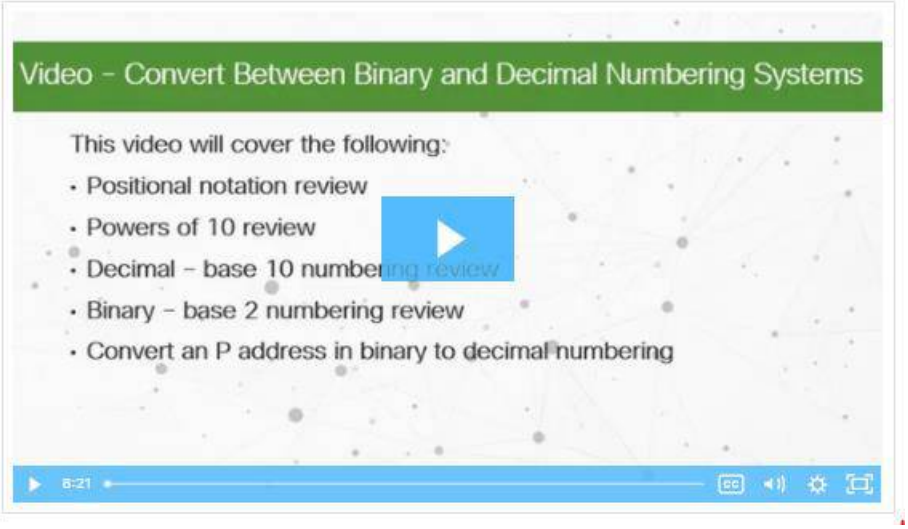


Para tener una buena comprensión del direccionamiento de red, es necesario comprender el direccionamiento binario y obtener habilidades prácticas en la conversión entre direcciones IPv4 binarias y decimales punteadas. Esta sección cubrirá cómo convertir entre sistemas de numeración de base dos (binario) y base 10 (decimal).

5.1.2

Video - Conversión entre sistemas de numeración binarios y decimales

Haga clic en reproducir en la figura para ver un video que muestra cómo convertir entre sistemas de numeración binarios y decimales.



5.1.3

Notación de posición binaria

Para aprender a convertir de sistema binario a decimal, es necesario entender la notación de posición. El término "notación de posición" significa que un dígito representa diferentes valores según la "posición" que el dígito ocupa en la secuencia de números. Ya conoce el sistema de numeración más común, el sistema de notación decimal (de base 10).

El sistema de notación posicional decimal funciona como se describe en la tabla.

Radix	**10**	**10**	**10**	**10**
Posición en número	3	2	1	0
Cálculo	(10^3)	(10^2)	(10^1)	(10^0)
Valor de la posición	1000	100	10	1

Las viñetas siguientes describen cada fila de la tabla.

- Fila 1, Radix es la base numérica. La notación decimal se basa en 10, por lo tanto, la raíz es 10.
- Fila 2, Posición en número considera la posición del número decimal que comienza con, de derecha a izquierda, 0 (1ª posición), 1 (2ª posición), 2 (3ª posición), 3 (4ª posición). Estos números también representan el valor exponencial utilizado para calcular el valor posicional en la cuarta fila.
- Fila 3 calcula el valor posicional tomando la raíz y elevándola por el valor exponencial de su posición en la fila 2.
  Nota: n^0 es = 1.
- El valor posicional de la fila 4 representa unidades de miles, cientos, decenas y unos.

Para usar el sistema de posición, una un número dado con su valor de posición. El ejemplo en la tabla ilustra cómo se usa la notación posicional con el número decimal 1234.

	Millares	**Centenas**	**Decenas**	**Unidades**
Valor de posición	1000	100	10	1
Número decimal (1234)	1	2	3	4
Cálculo	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up…	1000	+ 200	+ 30	+ 4

	Millares	Centenas	Decenas	Unidades
Resultado	**1,234**			

En contraste, la notación posicional binaria opera como se describe en la tabla.

Radix	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Posición en número	7	6	5	4	3	2	1	0
Cálculo	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Valor de la posición	128	64	32	16	8	4	2	1

Las viñetas siguientes describen cada fila de la tabla.

- Fila 1, Radix es la base numérica. La notación binaria se basa en 2, por lo tanto, el radix es 2.
- Fila 2, Posición en número considera la posición del número binario que comienza con, de derecha a izquierda, 0 (1ª posición), 1 (2ª posición), 2 (3ª posición), 3 (4ª posición). Estos números también representan el valor exponencial utilizado para calcular el valor posicional en la cuarta fila.
- Fila 3 calcula el valor posicional tomando la raíz y elevándola por el valor exponencial de su posición en la fila 2.
  Nota: n^0 es = 1.
- El valor posicional de la fila 4 representa unidades de uno, dos, cuatro, ocho, etc.

El ejemplo en la tabla ilustra cómo un número binario 11000000 corresponde al número 192. Si el número binario fuera 10101000, el número decimal correspondiente sería 168.

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario (11000000)	1	1	0	0	0	0	0	0
Cálculo	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Añádanlos.	128	+ 64	+0	+ 0	+ 0	+ 0	+ 0	+ 0
Resultado	**192**							

5.1.4

Verifique su comprensión - Sistema de números binarios

Compruebe su comprensión del sistema de números binarios eligiendo la mejor respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. 192.168.11.10 es equivalente a 11000000.10101000.00001011.00001010
2. 172.16.31.30 é equivalente a 10101100.00010000.00011111.000111110

Has tenido 2 respuestas correctas de 2.

1. ¿Cuál es el binario equivalente a la dirección IP 192.168.11.10?

¡Lo tienes!

- 11000000.11000000.00001011.00001010
- (•) 11000000.10101000.00001011.00001010
- 11000000.10101000.00001010.00001011
- 11000000.10101000.00001011.00010010

2. ¿Cuál de los siguientes es el binario equivalente a la dirección IP 172.16.31.30?

¡Lo tienes!

- 11000000.00010000.00011111.000111110
- 10101000.00010000.00011111.000111110
- 10101100.00010000.00011110.000111110
- (•) 10101100.00010000.00011111.000111110

Correct

You have successfully identified the correct answers.

1. 192.168.11.10 is equivalent to 11000000.10101000.00001011.00001010
2. 172.16.31.30 is equivalent to 10101100.00010000.00011111.000111110

You got 2 out of 2 questions correct.

1. Which is the binary equivalent to the 192.168.11.10 IP address?

You got it!

- 11000000.11000000.00001011.00001010
- 11000000.10101000.00001011.00001010
- 11000000.10101000.00001010.00001011
- 11000000.10101000.00001011.00010010

2. Which of the following is the binary equivalent to the 172.16.31.30 IP address?

You got it!

- 11000000.00010000.00011111.00011110
- 10101000.00010000.00011111.00011110
- 10101100.00010000.00011110.00011110
- 10101100.00010000.00011111.00011110

5.1.5

Convertir binario a decimal

Para convertir una dirección IPv4 binaria a su equivalente decimal punteada, divida la dirección IPv4 en cuatro octetos de 8 bits. A continuación, aplique el valor de posición binario al primer octeto del número binario y calcule según corresponda.

Por ejemplo, suponga que 11000000.10101000.00001011.00001010 es la dirección IPv4 binaria de un host. Para convertir la dirección binaria a decimal, comience con el primer octeto, como se muestra en la tabla. Introduzca el número binario de 8 bits en el valor de posición de la fila 1 y, después, calcule para producir el número decimal 192. Este número entra en el primer octeto de la notación decimal punteada.

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario (11000000)	1	1	0	0	0	0	0	0
Cálculo	128	64	32	16	8	4	2	1
Súmelos...	128	+64	+0	+0	+0	+0	+0	+0

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Resultado	**192**							

A continuación, convertir el segundo octeto de 10101000 como se muestra en la tabla. El valor decimal resultante es 168 y entra en el segundo octeto.

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario (10101000)	1	0	1	0	1	0	0	0
Cálculo	128	64	32	16	8	4	2	1
Súmelos...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
Resultado	**168**							

Convertir el tercer octeto de 00001011 como se muestra en la tabla.

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario (00001011)	0	0	0	0	1	0	1	1
Cálculo	128	64	32	16	8	4	2	1
Súmelos...	0	0	0	0	8	0	2	1
Resultado	**11**							

Convertir el cuarto octeto de 00001010 como se muestra en la tabla. Esto completa la dirección IP y produce **192.168.11.10**.

Valor de posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario (00001010)	0	0	0	0	1	0	1	0
Cálculo	128	64	32	16	8	4	2	1

Valor de posición	128	64	32	16	8	4	2	1
Súmelos...	0	0	0	0	8	0	2	0
Resultado	**10**							

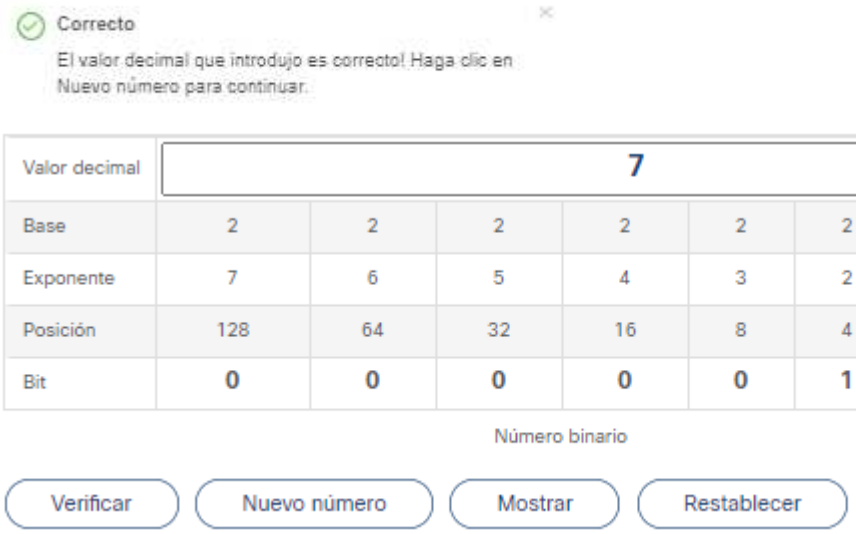
5.1.6

Actividad - Conversión de sistema binario a decimal

Instrucciones

Esta actividad le permite practicar la conversión de binario a decimal de 8 bits tanto como sea necesario. Le recomendamos que trabaje con esta herramienta hasta que pueda realizar la conversión sin errores. Convertir el número binario mostrado en el octeto a su valor decimal.

Introduzca la respuesta decimal a continuación.



5.1.7

Conversión de sistema decimal a binario

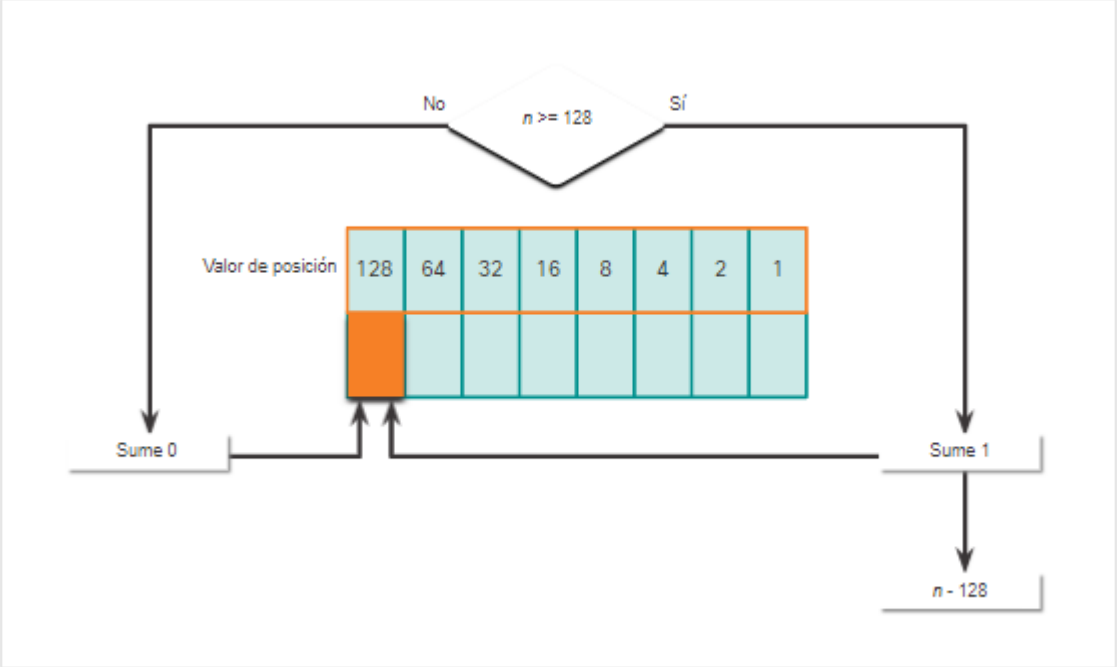
También es necesario comprender cómo convertir una dirección IPv4 decimal punteada a una binaria. La tabla de valores de posición binarios es una herramienta útil.

Haga clic en cada posición a partir de 128 y trabaje su camino de izquierda a derecha a la posición 1.

128	64	32	16	8	4	2	1

¿Es el número decimal del octeto (n) igual o mayor que el bit más significativo (**128**)?

- If no, then enter binary **0** in the **128 valor** posicional.
- If yes, then add a binary **1** in the **128** positional value and subtract **128** del número decimal.

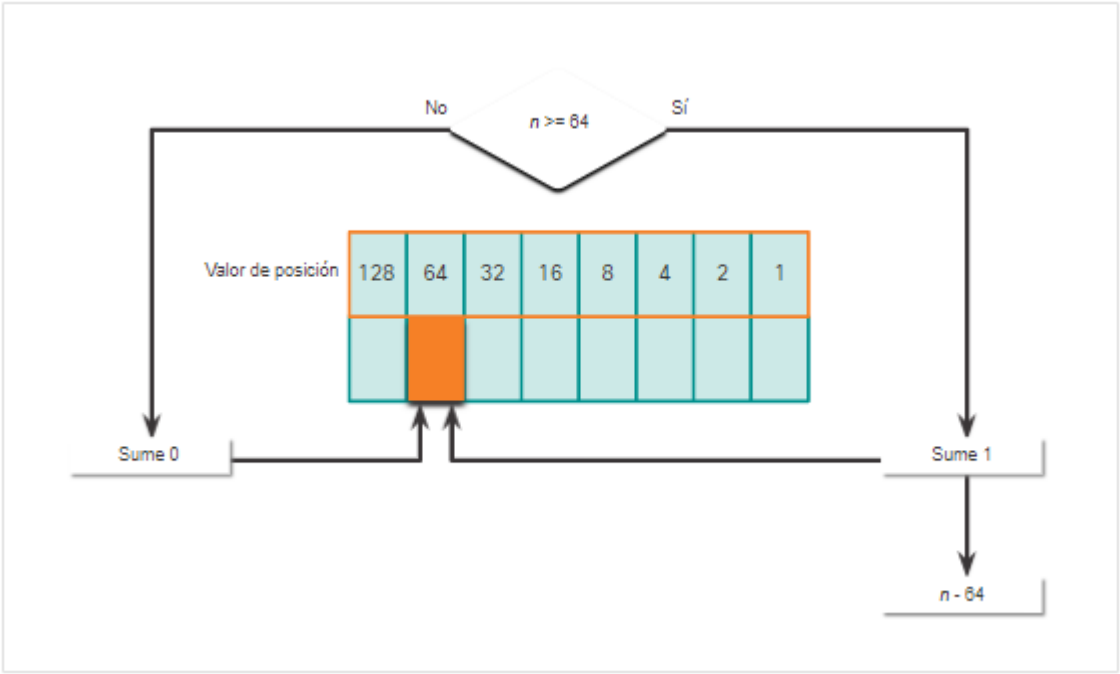


El gráfico muestra una tabla que tiene 8 columnas para un byte u 8 bits. La fila superior muestra los valores de izquierda a derecha; 128, 64, 32, 16, 8, 4, 2, 1. A la izquierda de esta línea superior están las palabras Valor Posicional. La fila inferior está en blanco, pero el campo debajo de 128 se resalta al seleccionar la pestaña 128. Encima de la tabla hay un diagrama de flujo que sólo tiene una propuesta n > o = 128. No está a la izquierda y Sí a la derecha. Hay una línea que va desde la proposición en el centro, una línea a la izquierda y una línea a la derecha. La línea se

mueve por la parte superior y, a continuación, una vez que borra el gráfico, la línea apunta hacia abajo. En el lado No o en la izquierda hay un cuadro con Agregar cero y una nueva línea apunta al campo resaltado. En el lado derecho o Sí, el cuadro tiene Agregar uno. A continuación, la línea continúa y apunta al campo resaltado bajo 128. Debajo del cuadro Agregar una es otra línea que apunta hacia abajo a otro cuadro que tiene n - 128. Donde el número original restará 128 de él y luego considerar la siguiente columna con 64.

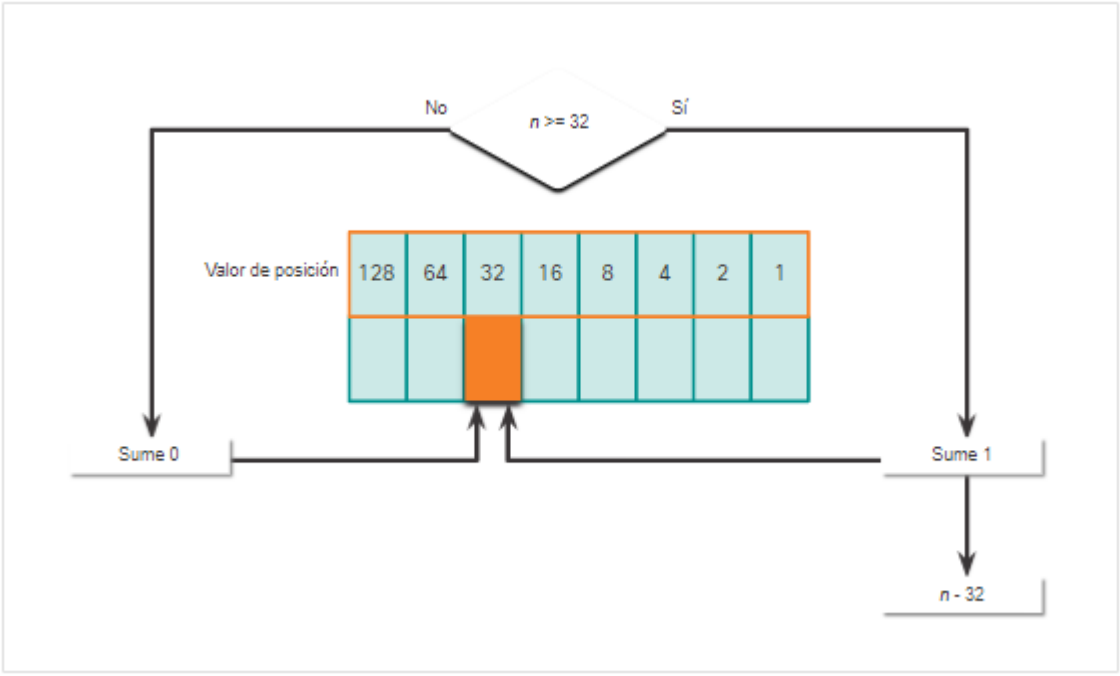
¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**64**)?

- If no, then enter binary **0** in the **64 valor** posicional.
- If yes, then add a binary **1** in the **64** positional value and subtract **64** desde el número decimal.



¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**32**)?

- If no, then enter binary **0** in the **32 valor** posicional.
- If yes, then add a binary **1** in the **32** positional value and subtract **32** del número decimal.

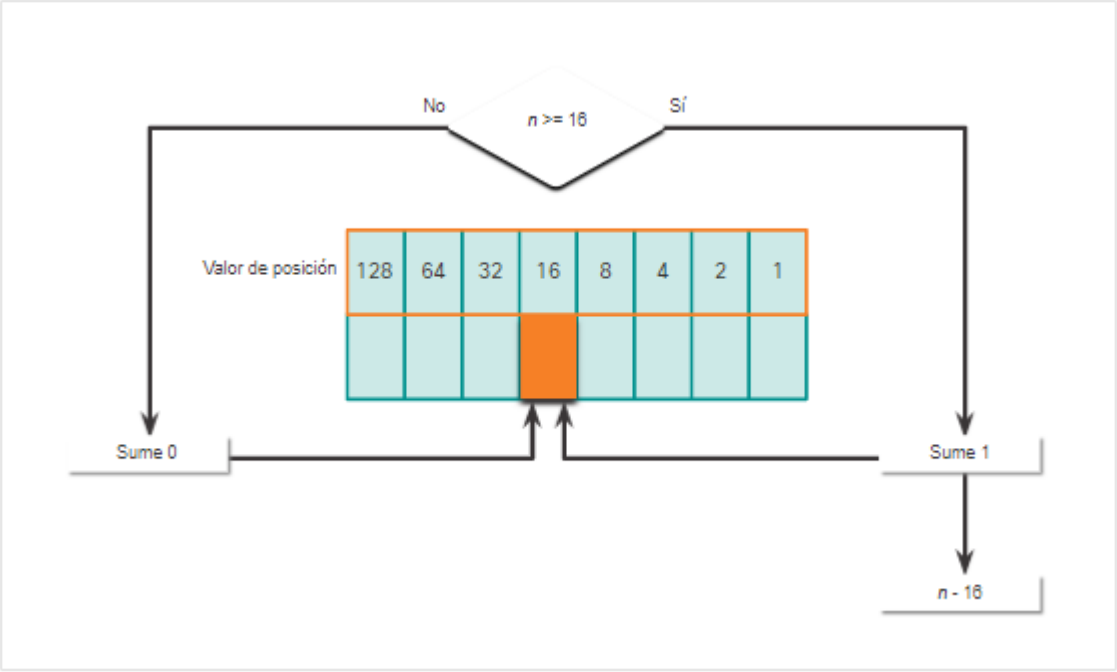


128	64	32	16	8	4	2	1

¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**16**)?

Valor* If no, then enter binary **posicional** in the **0** 16.

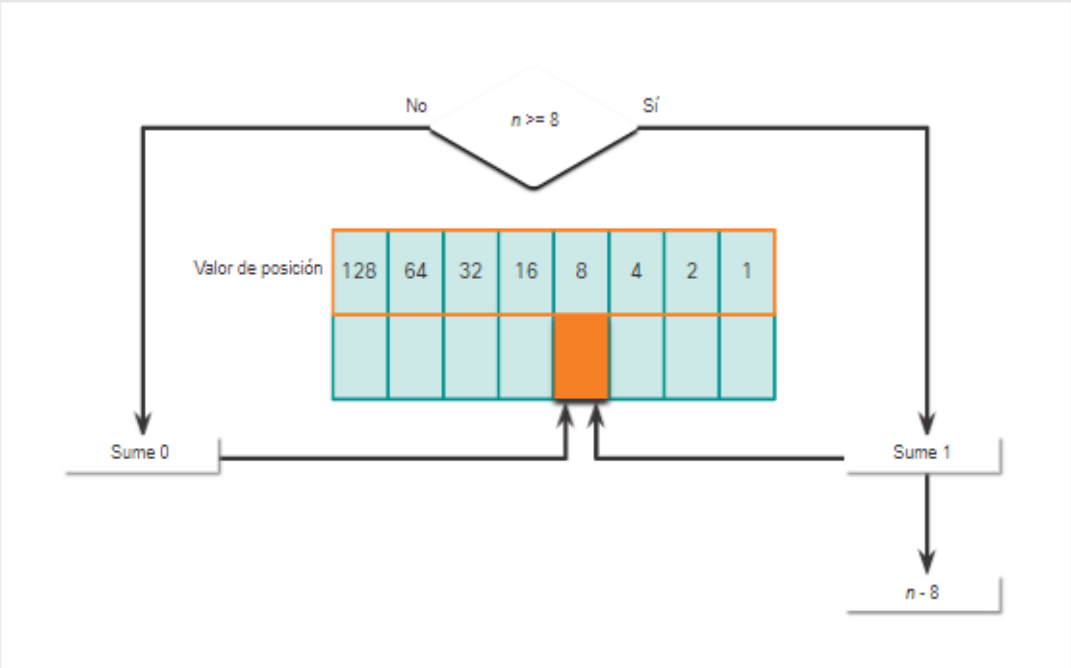
- If yes, then add a binary **1** in the **16** positional value and subtract **16** del número decimal.



128	64	32	16	8	4	2	1

¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**8**)?

- If no, then enter binary **0** in the **8 valor** posicional.
- If yes, then add a binary **1** in the **8** positional value and subtract **8** del número decimal.

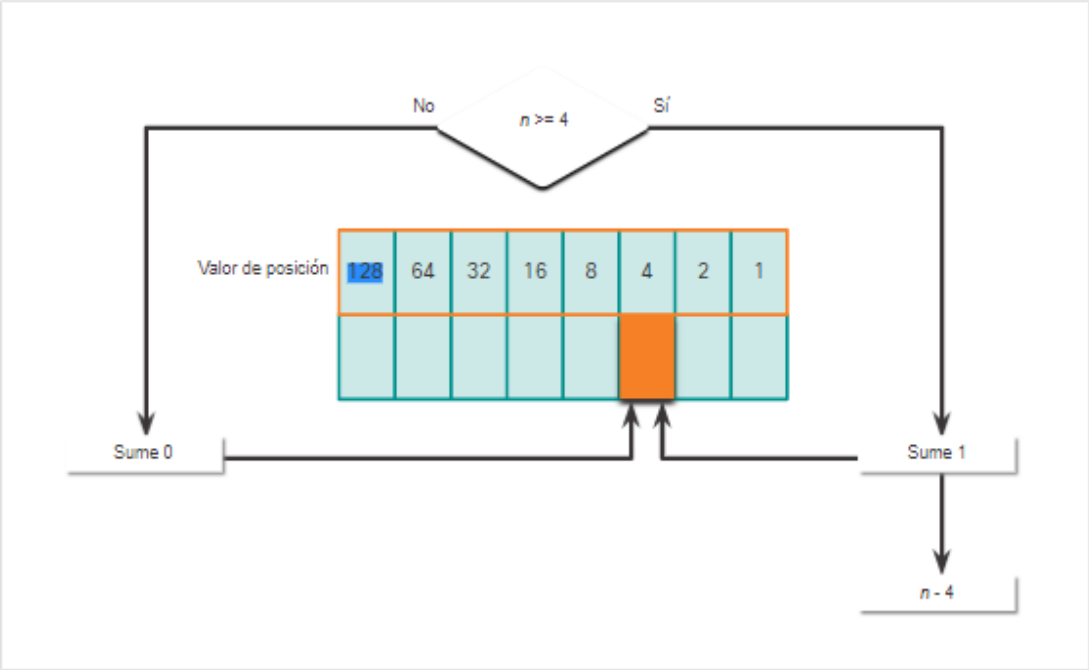


128	64	32	16	8	4	2	1

¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**4**)?

Valor* If no, then enter binary **posicional** in the **0** 4.

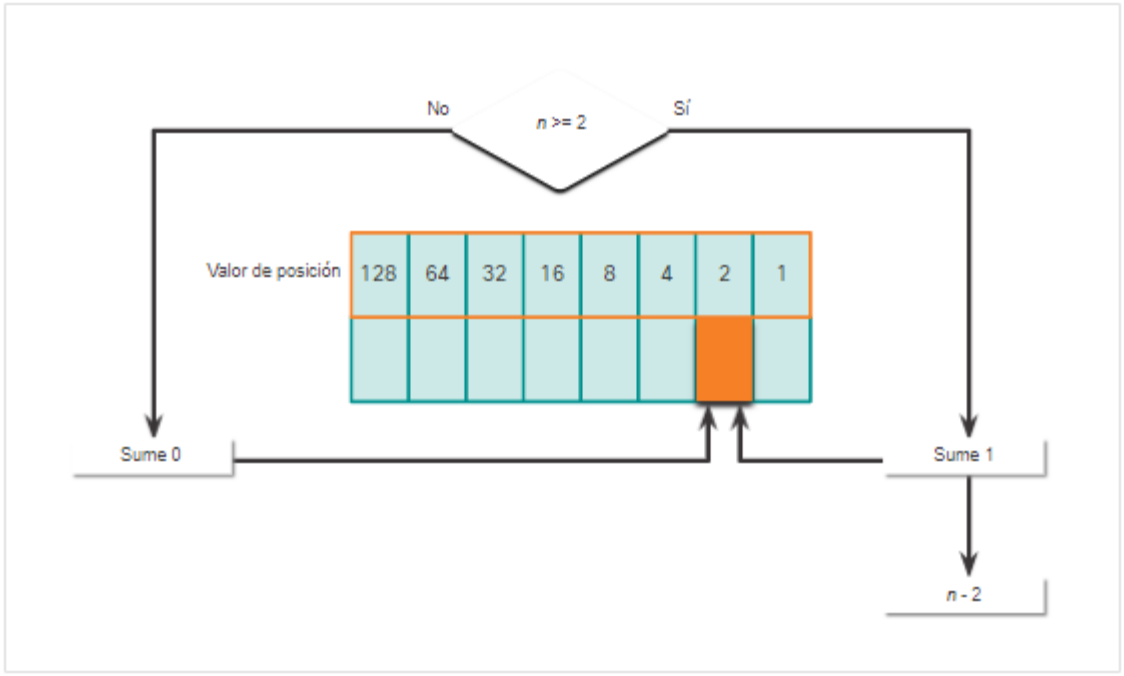
- If yes, then add a binary **1** in the **4** positional value and subtract **4** del número decimal.



¿Es el número decimal del octeto (n) igual o mayor que el siguiente bit más significativo (**2**)?

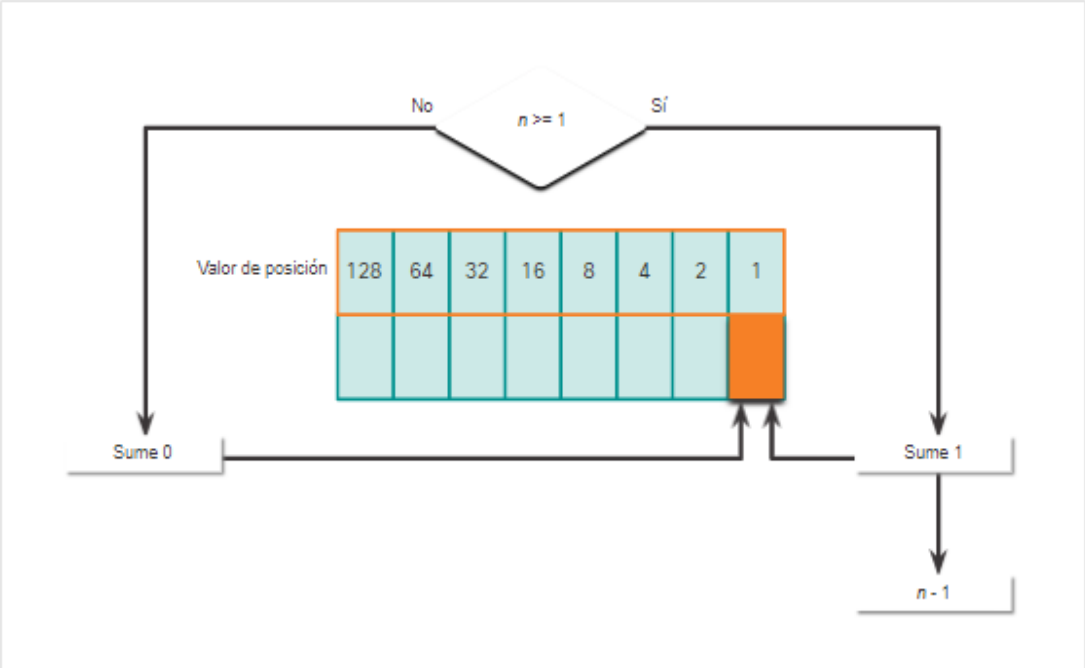
Valor* If no, then enter binary **posicional** in the **0** 2.

- If yes, then add a binary **1** in the **2** positional value and subtract **2** del número decimal.



¿Es el número decimal del octeto (n) igual o mayor que el último bit más significativo (**1**)?

- If no, then enter binary **0** in the **1 valor** posicional.
- If yes, then add a binary **1** in the **1** positional value and subtract **1** del último número decimal.



5.1.8

Ejemplo de conversión de sistema decimal a binario

Para poder comprender el proceso, considere la dirección IP 192.168.11.10.

El primer octeto número 192 se convierte a binario utilizando el proceso de notación posicional explicado anteriormente.

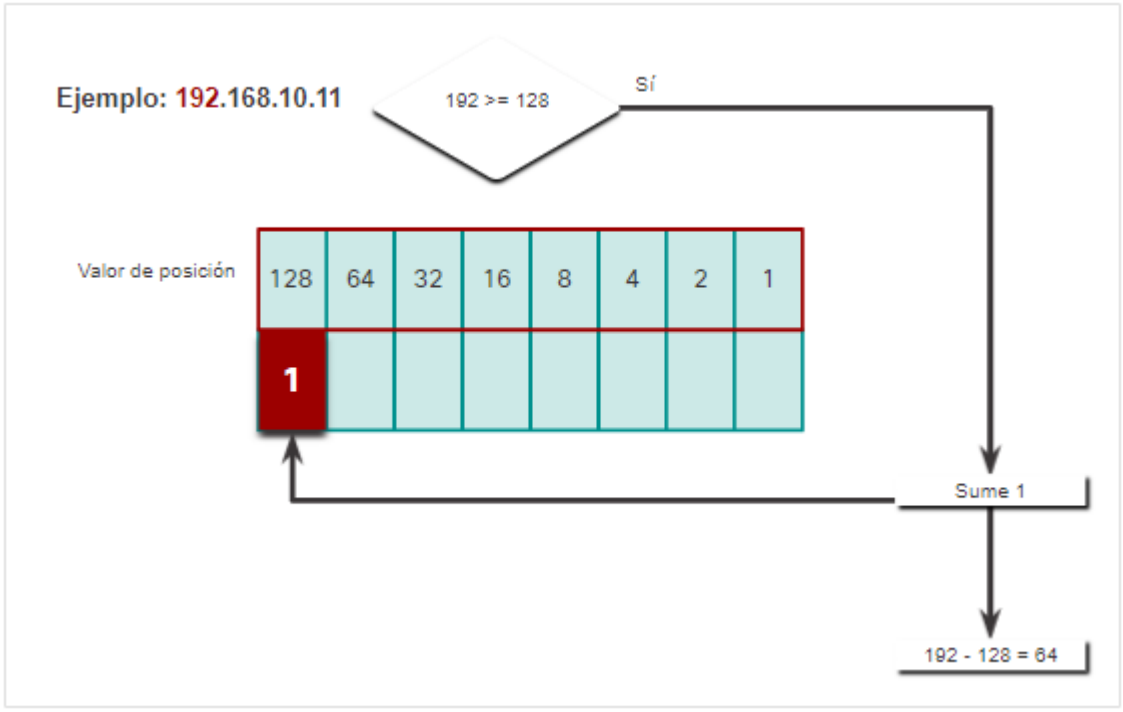
Es posible omitir el proceso de resta con números decimales menores o más pequeños. Por ejemplo, observe que es bastante fácil calcular el tercer octeto convertido a un número binario sin pasar realmente por el proceso de resta (8 + 2 = 10). El valor binario del tercer octeto es 00001010.

El cuarto octeto es 11 (8 + 2 + 1). El valor binario del cuarto octeto es 00001011.

La conversión de sistema binario a decimal puede parecer un desafío inicialmente, pero con la práctica resulta más fácil.

¿El primer octeto número 192 es igual o mayor que el bit de orden alto 128?

- Sí es, por lo tanto, añadir un 1 al valor posicional de orden alto a un representar 128.
- Resta 128 de 192 para producir un resto de 64.

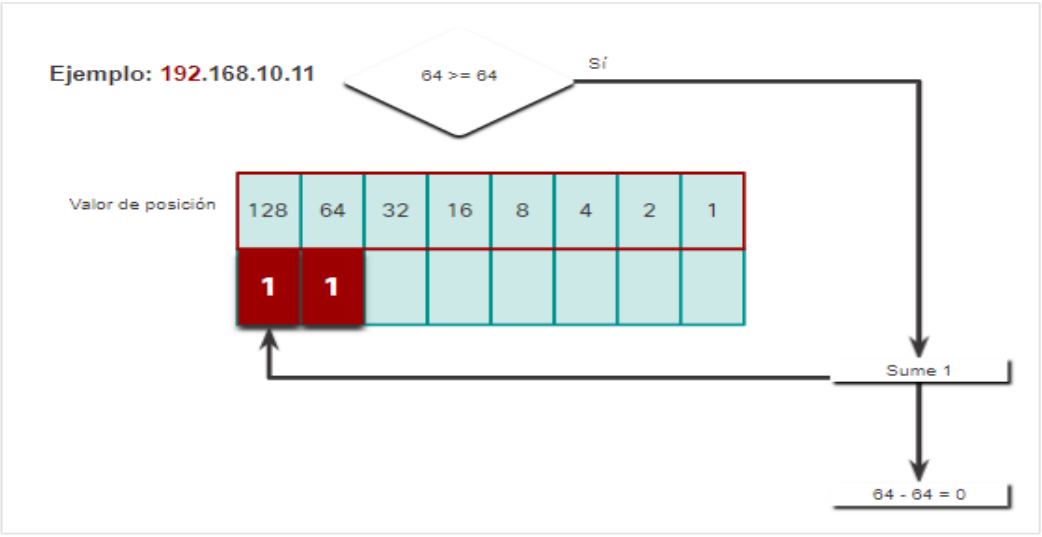


Al seleccionar el botón Paso 1, el gráfico indica Ejemplo: 192.168.10.11 con 192 en un color diferente. A la derecha de eso es un diamante que dice: 192 > o = 128. Hay un Sí en el lado derecho del diamante. A continuación, se muestra una tabla que contiene 8 columnas para un byte u 8 bits. La fila superior muestra los valores de izquierda a derecha: 128, 64, 32, 16, 8, 4, 2 y 1 con las palabras Valor posicional a la izquierda. Se resalta el campo de fila inferior bajo 128. Por encima de la tabla, desde el diamante del diagrama de flujo con Sí está a la derecha hay una línea que se mueve a través de la parte superior y luego una vez que borra el gráfico, la línea apunta directamente hacia abajo a un cuadro que tiene Agregar uno. A continuación, la línea continúa debajo del gráfico y apunta al campo resaltado bajo 128. Debajo del cuadro Agregar una hay otra línea que apunta hacia abajo a otro cuadro que tiene 192 - 128 = 64. También hay un 1 debajo del 128 en el campo resaltado; las otras columnas siguen en blanco en esta línea.

Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Pas 11

¿El resto 64 es igual o mayor que el siguiente bit de orden alto 64?

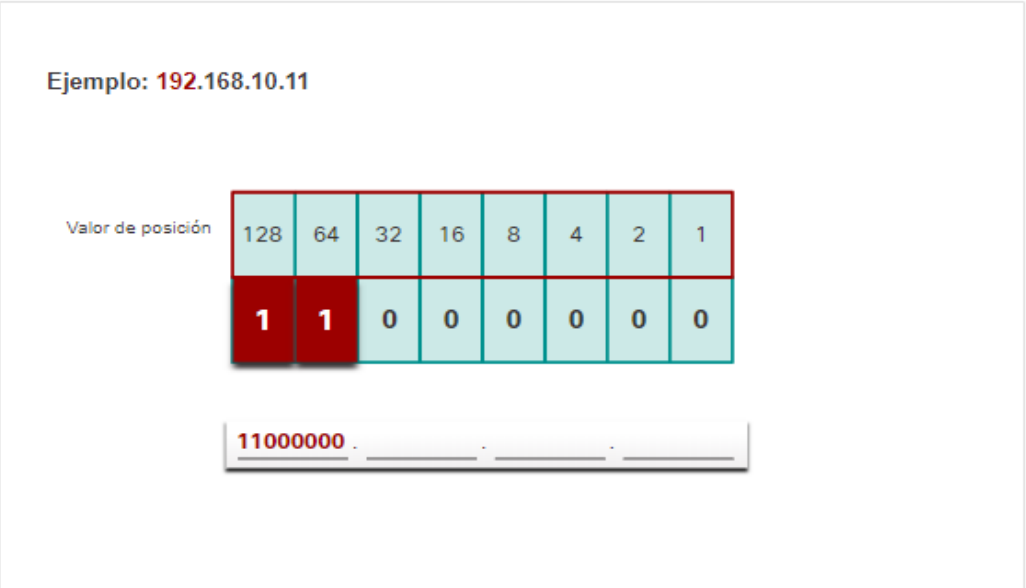
- Es igual, por lo tanto, agregue un 1 al siguiente valor posicional de alto orden.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Pas 11

Dado que no hay resto, introduzca binario **0** en los valores posicionales restantes.

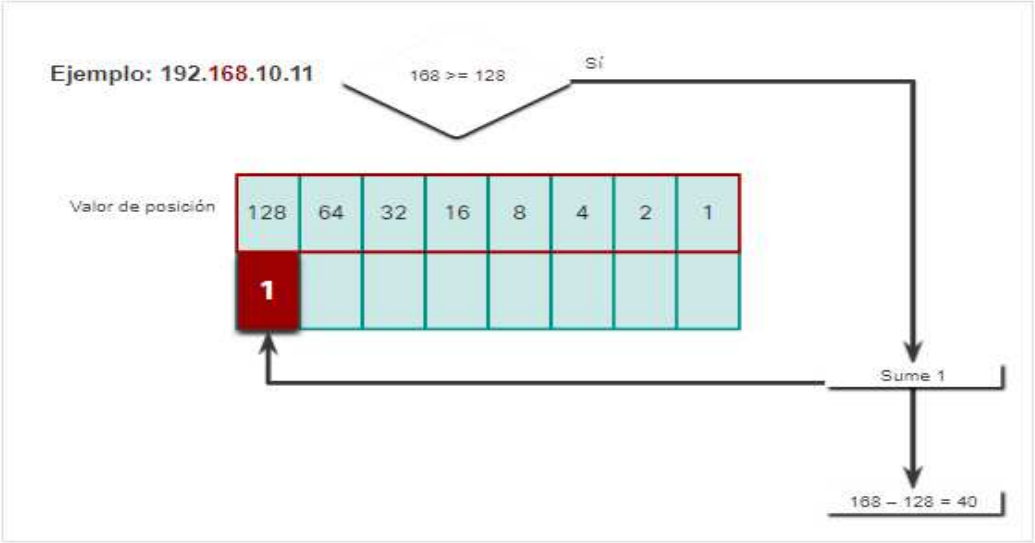
- El valor binario del primero octeto es **11000000**.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

¿El segundo número de octetos es **168** igual o mayor que el bit de orden alto **128**?

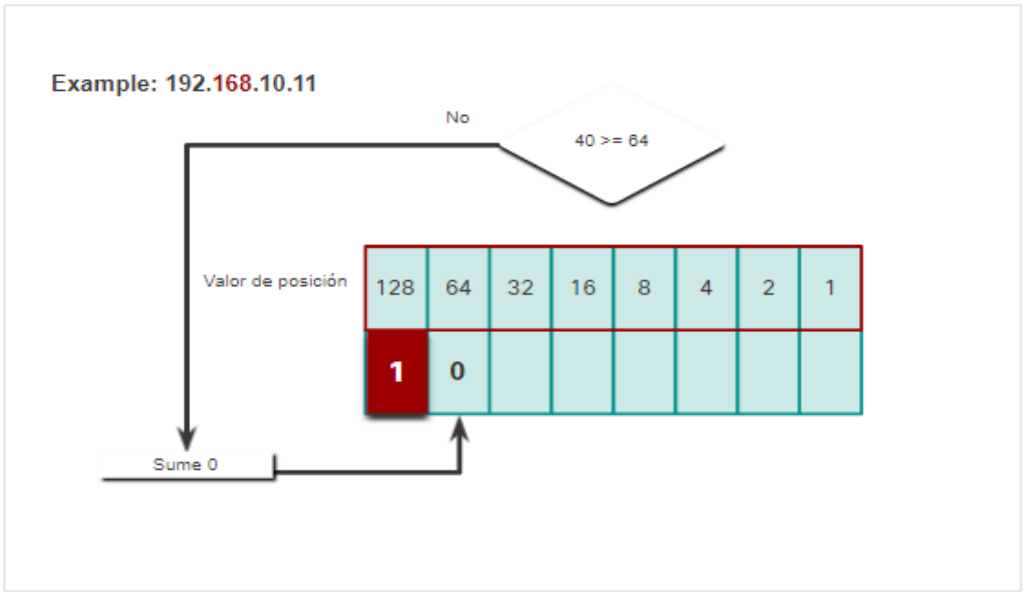
- Sí, esto es cierto, por lo tanto agregue un **1** al valor posicional de alto orden para representar **128**.
- Reste **128** de **168** para producir un resto de **40**.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

¿El resto es **40** igual o mayor que el siguiente bit de orden alto **64**?

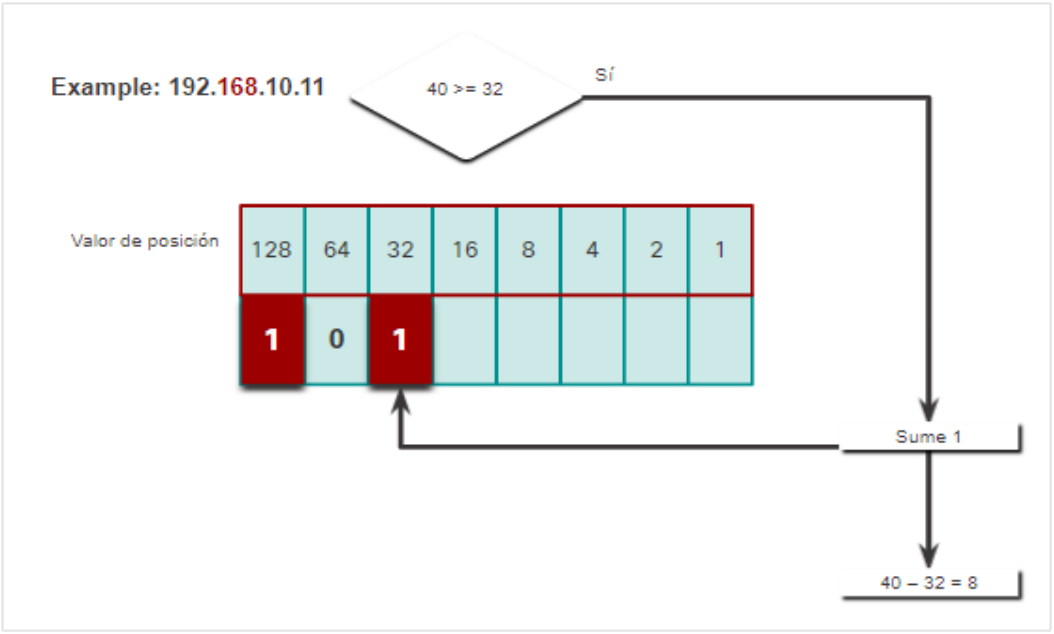
- No, no lo es, por lo tanto, ingrese un **0** binario en el valor posicional 64.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Pas 11

¿El resto es **40** igual o mayor que el siguiente bit de orden alto **32**?

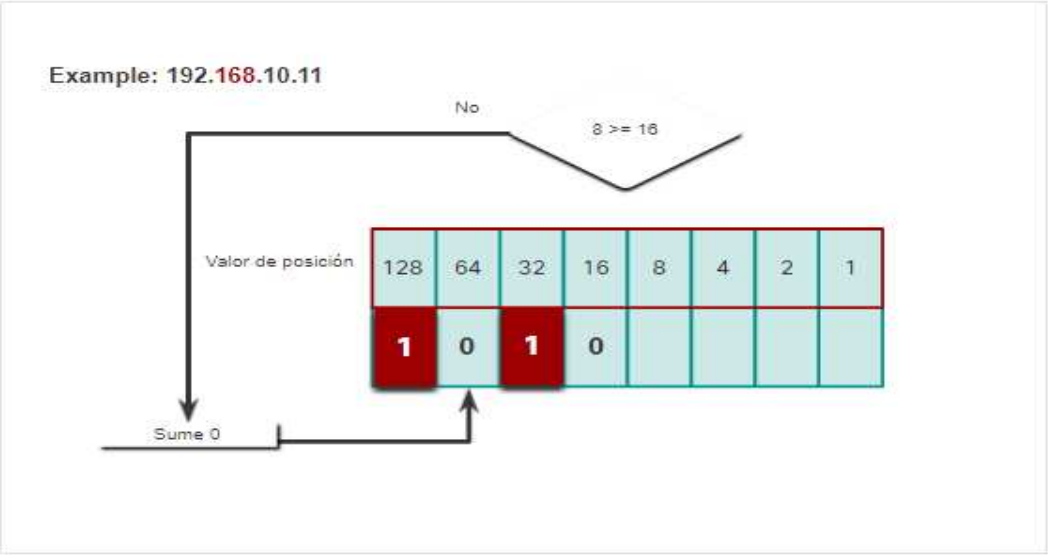
- Si, esto es cierto, por lo tanto agregue un **1** al valor posicional de alto orden para representar **32**.
- Reste **32** de 40 para producir un resto de **8**.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Pas 11

¿El resto es **8** igual o mayor que el siguiente bit de orden alto **16**?

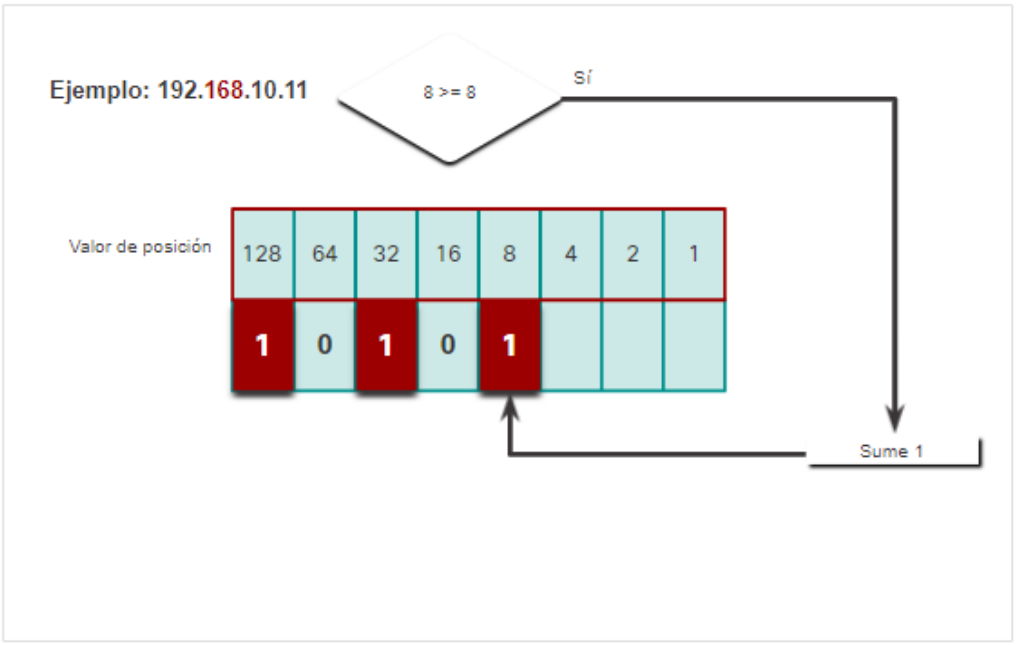
- No, no lo es, por lo tanto, introduzca un 0 binario en el valor posicional.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

¿El resto es **8** igual o mayor que el siguiente bit de orden alto **8**?

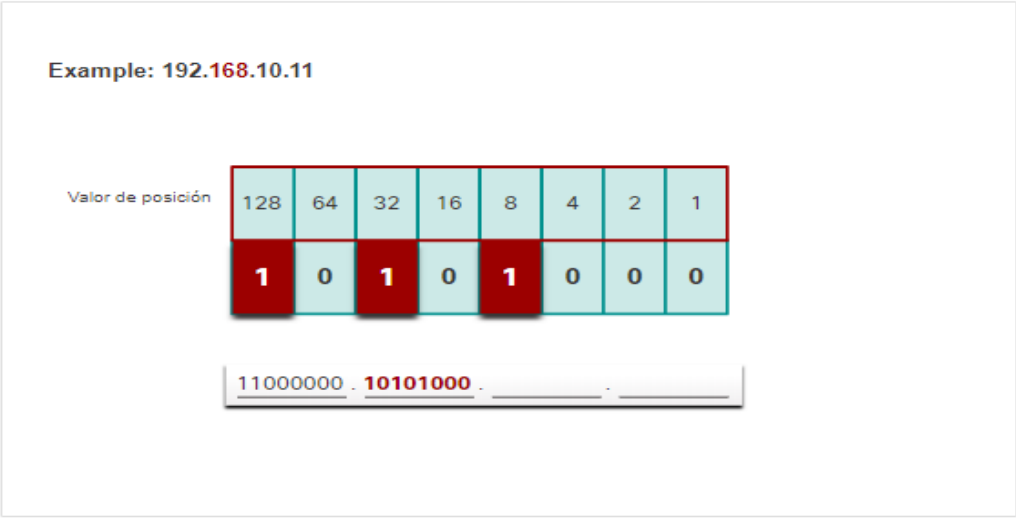
- Si, esto es cierto, por lo tanto agregue un **1**.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

Dado que no hay resto, introduzca binario **0** en los valores posicionales restantes.

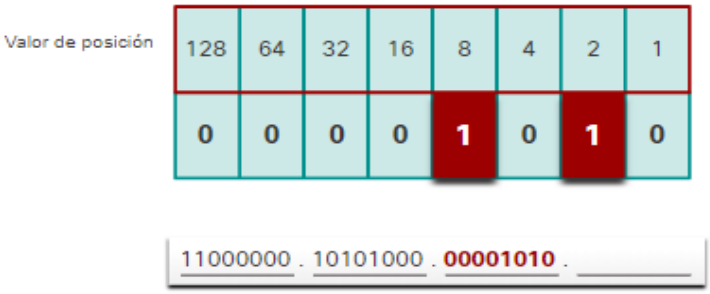
- El valor binario del segundo octeto es **10101000**.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

El valor binario del tercer octeto es.**00001010**

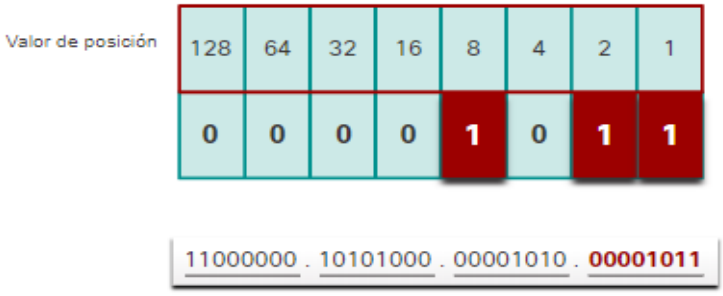
Ejemplo: 192.168.10.11



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 | Paso 7 | Paso 8 | Paso 9 | Paso 10 | Paso 11

El valor binario del cuarto octeto es. **00001011**

Ejemplo: 192.168.10.11

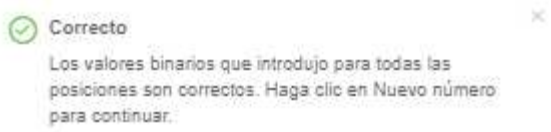


5.1.9

Actividad - Conversiones de decimal a binario

Instrucciones

Esta actividad le permite poner en práctica la conversión de valores decimales a valores binarios de 8 bits. Le recomendamos que trabaje con esta herramienta hasta que pueda realizar la conversión sin errores. Convierta el número decimal mostrado en la fila Valor decimal a sus bits binarios.



Valor decimal	106							
Base	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Posición	128	64	32	16	8	4	2	1
Bit	0	1	1	0	1	0	1	0

Verificar | Nuevo número | Mostrar | Restablecer

5.1.10

Actividad: Juego binario

Esta es una forma divertida de aprender números binarios para redes.

Game Link: https: //learningnetwork. cisco.com/docs/doc-1803

Deberá iniciar sesión en cisco.com para utilizar este enlace. Será necesario crear una cuenta si aún no tiene una.

Descarga móvil: https://learningnetwork.cisco.com/docs/DOC-11119

5.1.11

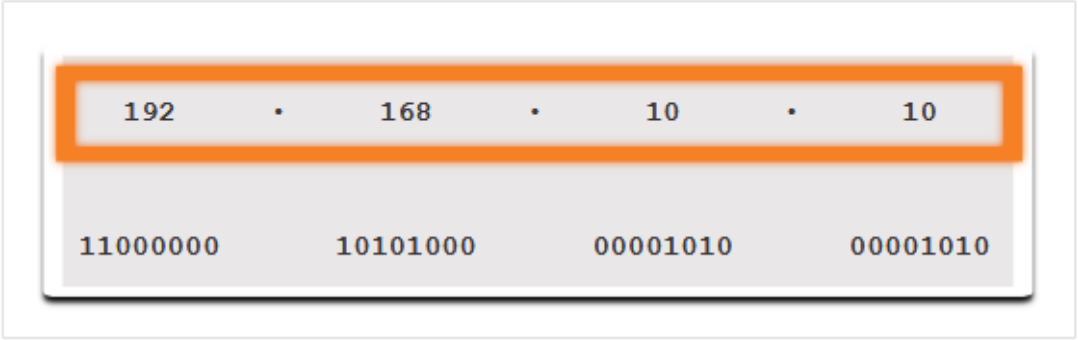
Direcciones IPv4

Como se mencionó al principio de este tema, los routers y las computadoras solo entienden binario, mientras que los humanos trabajan en decimal. Es importante que usted conozca a fondo estos dos sistemas de numeración y cómo se utilizan en redes.

Haga clic en cada botón para contrastar la dirección decimal con puntos y la dirección de 32 bits.

Dirección en formato decimal punteado | Octetos | Dirección de 32 bits

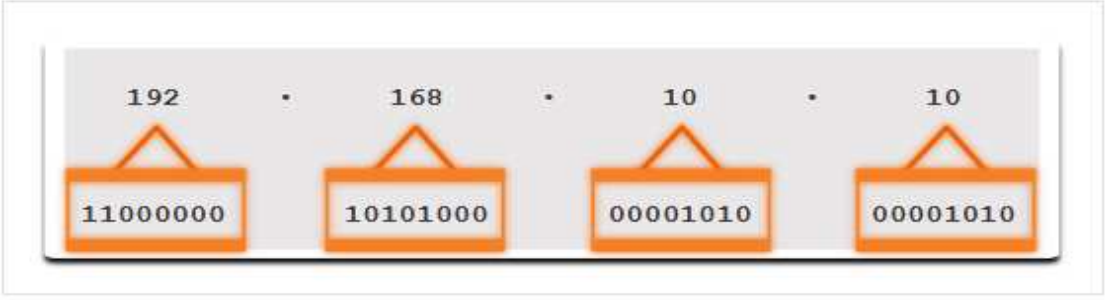
192.168.10.10 es una dirección IP asignada a una computadora.



El gráfico muestra los números 192.168.10.10 con el binario en un cuadro naranja alrededor de los números decimales punteados 192.168.10.10. 11000000 está bajo 192 en el primer octeto, 10101000 bajo 168 en el segundo octeto, 00001010 bajo 10 en el tercer octeto, y 00001010 bajo el último 10 en el cuarto octeto.

Dirección en formato decimal punteado | Octetos | Dirección de 32 bits

La dirección se compone de cuatro octetos diferentes.



Las redes en la actualidad / Sistema numérico hexadecimal

Sistema numérico hexadecimal

5.2.1

Direcciones hexadecimales e IPv6

Ahora sabes cómo convertir binario a decimal y decimal a binario. Necesita esa habilidad para comprender el direccionamiento IPv4 en su red. Pero es igual de probable que use direcciones IPv6 en su red. Para entender las direcciones IPv6, debe ser capaz de convertir hexadecimal a decimal y viceversa.

Así como el decimal es un sistema de base diez, el hexadecimal es un sistema de base dieciséis. El sistema base de dieciséis números usa los dígitos del 0 al 9 y las letras de la A a la F. La figura muestra los valores decimales y hexadecimales equivalentes para el binario 0000 a 1111.

Este gráfico tiene tres columnas. La primera columna tiene los números del 0 al 15 en decimal. La segunda columna tiene los números del 0 al 15 en binario. Todos los números en binario se expresan con 4 valores de posición. Por ejemplo 0 es 0000, 10 es 1010, 15 es 1111, etc. La tercera columna es paralela a las otras dos columnas. Esta columna tiene los números del 0 al 15 en hexadecimal. Estos se expresan con un valor. Por ejemplo 5 es 5, 10 es A, 11 es B, 12 es C, 13 es D, 14 es E y 15 es F. Cabe señalar que estos pueden expresarse con mayúsculas o minúsculas. En este diagrama son letras mayúsculas que representan los valores numéricos.

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Binario y hexadecimal funcionan bien juntos porque es más fácil expresar un valor como un solo dígito hexadecimal que como cuatro bits binarios.

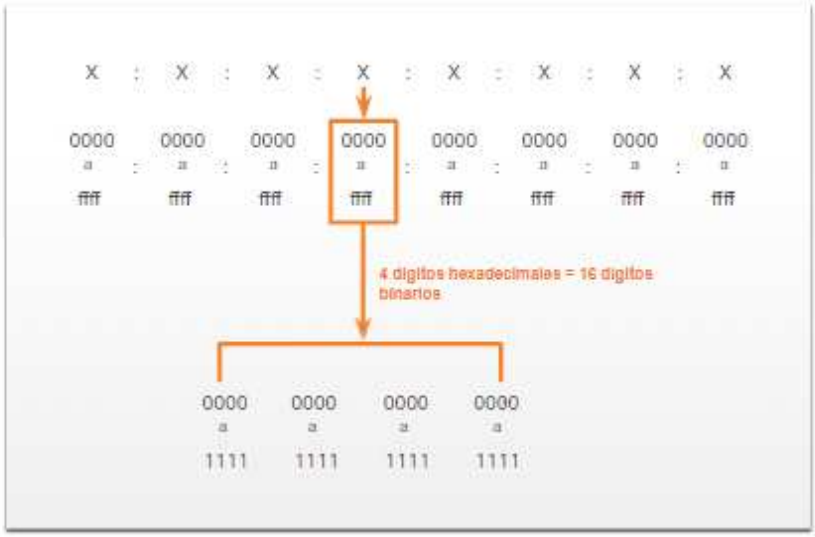
El sistema de numeración hexadecimal se usa en redes para representar direcciones IP Versión 6 y direcciones MAC Ethernet.

Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.

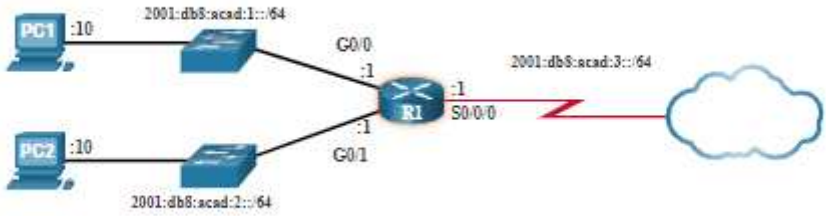
Como se muestra en la figura, el formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

Este gráfico tiene una línea superior con los 8 hexetos de la dirección IPv6 expresados como X:X:X:X:X:X:X:X:X:X. Debajo de cada X están los números 0000 que representan el primer número que puede estar en este campo debajo de cada 0 es el a y debajo que son los números en minúsculas ffff que representan el valor máximo que se puede hacer en un solo hexteto. Debajo de la X en el cuarto hexteto hay una flecha naranja que apunta a los números 0000 a ffff, que están en una caja. Debajo del cuadro hay otro punto de flecha hacia abajo hasta una sección de números. En el centro de la flecha está la instrucción 4 dígitos hexadecimales = 16 dígitos binarios. Debajo de la flecha hay una sección de números con cuatro partes. Cada una de las cuatro partes tiene 0000 bajo que la palabra a bajo que los números 1111. Esto es

para representar el binario de cada número hexadecimal, ya que cada número está hecho de 4 dígitos binarios y hay 4 dígitos hexadecimales en cada hexteto para un total de 16 bits.



La topología de ejemplo de la figura muestra direcciones hexadecimales IPv6.

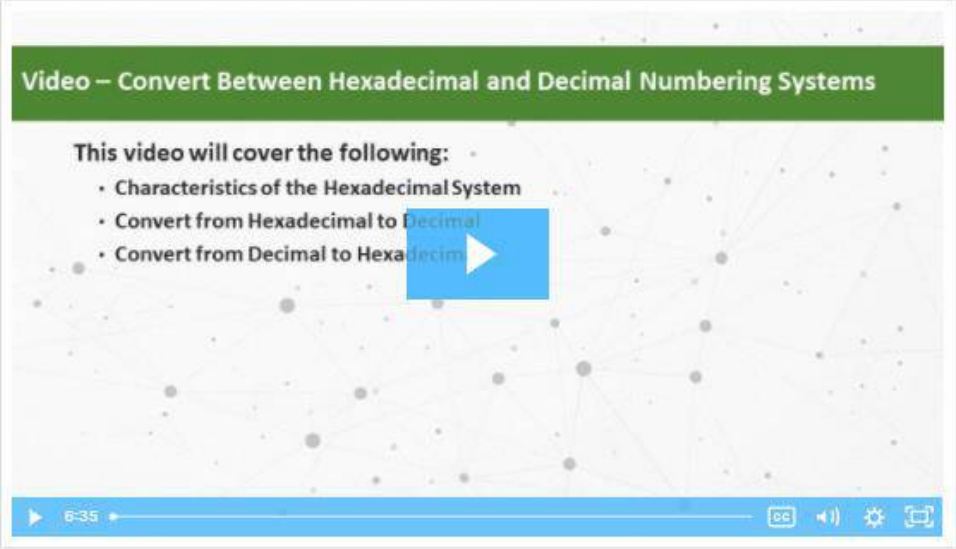


Este gráfico muestra un router central etiquetado R1. Fuera de la interfaz G0/0 es la primera LAN a la izquierda. Un switch está conectado directamente al router R1 y PC1 está conectado a la izquierda del switch. Por encima de esta LAN se encuentra la dirección del segmento de red IPv6 de 2001:db8:acad:1: :/64. En la interfaz G0/0 se asigna: 1 y:10 se asigna a PC1. Por debajo de G0/0 y también a la izquierda en R1 está la interfaz G0/1 para la segunda LAN. Un switch está conectado directamente a los routers G0/1 y PC2 está conectado a la izquierda de este switch. Por encima de esta LAN se encuentra la dirección del segmento de red IPv6 de 2001:db8:acad:2: :/64. En la interfaz G0/1 se asigna: 1 y:10 se asigna a PC2. En el lado derecho de R1 está la interfaz S0/0/0 y está conectada a una nube. Encima del cable serie rojo que está conectado a la nube está la dirección IPv6 2001:db8:acad:3: :/64. A la interfaz S0/0/0 se le ha asignado la dirección:1 IPv6.

5.2.2

Video - Conversión entre sistemas de numeración hexadecimales y decimales

Haga clic en Reproducir en el vídeo para ver cómo convertir entre sistemas de numeración hexadecimal y decimal.



5.2.3

Conversiones decimales a hexadecimales

La conversión de números decimales a valores hexadecimales es sencilla. Siga los pasos indicados:

1. Convertir el número decimal a cadenas binarias de 8 bits.
2. Divida las cadenas binarias en grupos de cuatro comenzando desde la posición más a la derecha.
3. Convierta cada cuatro números binarios en su dígito hexadecimal equivalente.

El ejemplo proporciona los pasos para convertir 168 a hexadecimal.

Por ejemplo, 168 convertido en hexadecimal usando el proceso de tres pasos.

1. 168 en binario es 10101000.
2. 10101000 en dos grupos de cuatro dígitos binarios es 1010 y 1000.

3. 1010 es hex A y 1000 es hex 8.

   Respuesta: 168 es A8 en hexadecimal.

5.2.4

Conversión hexadecimal a decimal

La conversión de números hexadecimales a valores decimales también es sencilla. Siga los pasos indicados:

1. Convertir el número hexadecimal en cadenas binarias de 4 bits.
2. Cree una agrupación binaria de 8 bits comenzando desde la posición más a la derecha.
3. Convierta cada agrupación binaria de 8 bits en su dígito decimal equivalente.

En este ejemplo se proporcionan los pasos para convertir D2 a decimal.

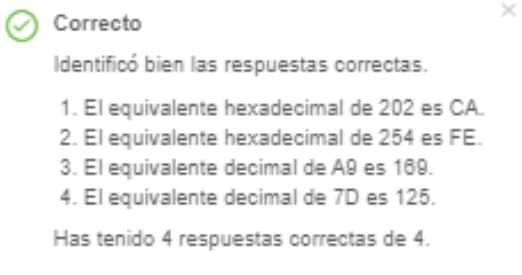
1. D2 en cadenas binarias de 4 bits es 1101 y 0010.
2. 1101 y 0010 es 11010010 en un grupo de 8 bits.
3. 11010010 en binario es equivalente a 210 en decimal.

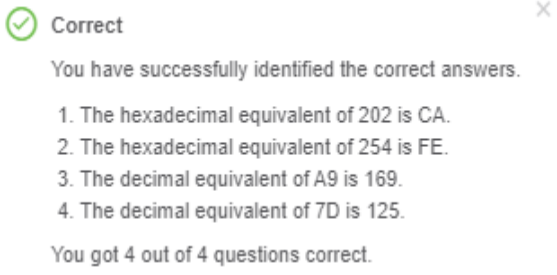
Respuesta: D2 en hexadecimal es 210 en decimal.

5.2.5

Compruebe su comprensión - Sistema de números hexadecimales

Compruebe su comprensión del sistema de números hexadecimales eligiendo la mejor respuesta a las siguientes preguntas.





1. ¿Cuál es el equivalente hexadecimal de 202?

¡Lo tienes!

- B10
- BA
- C10
- CA

2. ¿Cuál es el equivalente hexadecimal de 254?

¡Lo tienes!

- EA
- ED
- FA
- FE

3. ¿Cuál es el equivalente decimal de A9?

¡Lo tienes!

- 168
- 169
- 170
- 171

4. ¿Cuál de los siguientes es el equivalente decimal de 7D?

¡Lo tienes!

- 124
- 125
- 126
- 127

Módulo de Práctica y Prueba

5.3.1

¿Qué aprendió en este módulo?

Sistema númerico binario

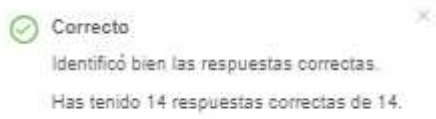
El sistema binario es un sistema numérico que consiste en los números 0 y 1, denominados bits. En comparación, el sistema numérico decimal consiste en 10 dígitos, que incluyen los números 0 a 9. Es importante que comprendamos el binario porque los hosts, servidores y dispositivos de red usan direccionamiento binario, específicamente, direcciones binarias IPv4, para identificarse entre sí. Debe conocer el direccionamiento binario y cómo convertir entre direcciones IPv4 decimales binarias y con puntos. En este tema se presentan algunas formas de convertir decimal a binario y binario a decimal.

Sistema numérico hexadecimal

Así como el decimal es un sistema de base diez, el hexadecimal es un sistema de base dieciséis. El sistema de numeración hexadecimal utiliza los números 0 a 9 y las letras A a F. El sistema de numeración hexadecimal se utiliza en redes para representar direcciones IPv6 y direcciones MAC Ethernet. Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Para convertir hexadecimal a decimal, primero debe convertir el hexadecimal a binario y, a continuación, convertir el binario a decimal. Para convertir decimal a hexadecimal, también debe convertir primero el decimal a binario.

5.3.2

Prueba de módulo - Sistemas numéricos



1. ¿Cuál es la representación binaria del número decimal 173?

Tema 5.1.0 - decimal 173 = 128 + 0 + 32 + 0 + 8 + 4 + 0 + 1

- ○ 10100111
- ○ 10100101
- ◉ 10101101
- ○ 10110101

2. Dada la dirección binaria de 11101100 00010001 00001100 00001010, ¿qué dirección representa esto en formato decimal de puntos?

Tema 5.1.0 - El número binario 11101100 00010001 00001100 00001010 se traduce en 236.17.12.10.

- ○ 234.17.10.9
- ○ 234.16.12.10
- ○ 236.17.12.6
- ◉ 236.17.12.10

3. ¿Cuántos bits binarios hay en una dirección IPv6?

Tema 5.2.0 - El espacio de direccionamiento IPv4 se agota por el rápido crecimiento de Internet y los dispositivos conectados a Internet. IPv6 extiende el espacio de asignación de direcciones IP porque aumenta la longitud de las direcciones de 32 a 128 bits.

- ○ 32
- ○ 48
- ○ 64
- ◉ 128
- ○ 256

4. ¿Cuál es el equivalente binario del número decimal 232?

El tema 5.1.0 - 232 en binario es 11101000. 128 + +64 + +32 + +8 = 232

- ◉ 11101000
- ○ 11000110
- ○ 10011000
- ○ 11110010

5. ¿Qué dos instrucciones son correctas acerca de las direcciones IPv4 e IPv6? (Escoja dos.)

Tema 5.2.0 - Las direcciones IPv4 se representan como números decimales punteados y tienen 32 bits de longitud. Las direcciones IPv6 están representadas por números hexadecimales y tienen 128 bits de longitud.

- ☑ Las direcciones IPv6 se representan con números hexadecimales.
- ☐ Las direcciones IPv4 están representadas por números hexadecimales.
- ☐ Las direcciones IPv6 tienen 32 bits de longitud.
- ☑ Las direcciones IPv4 tienen 32 bits de longitud.
- ☐ Las direcciones IPv4 tienen 128 bits de longitud.
- ☐ Las direcciones IPv6 tienen 64 bits de longitud.

6. ¿Qué formato de dirección IPv4 se creó para facilitar el uso de las personas y se expresa como 201.192.1.14?

Tema 5.1.0 - Para facilitar el uso por parte de las personas, los patrones binarios se representan como decimales punteados. Los sistemas informáticos fueron creados para entender el direccionamiento binario.

- ○ Binario
- ◉ Decimal punteada
- ○ Hexadecimal
- ○ ASCII

7. ¿Cuál de las siguientes es la representación decimal punteada de la dirección IPv4 11001011.00000000.01110001.11010011?

Tema 5.1.0: cada sección (octeto) contiene ocho dígitos binarios. Cada dígito representa un valor específico (128, 64, 32, 16, 8, 4, 2 y 1). Cada vez que aparece un 1, significa que el valor específico es relevante. Sume todos los valores relevantes de un octeto en particular para obtener el valor decimal. Por ejemplo, el número binario 11001011 equivale al número decimal 203.

- ○ 192.0.2.199
- ○ 198.51.100.201
- ◉ 203.0.113.211
- ○ 209.165.201.223

8. ¿Cuál es el equivalente decimal del número binario 10010101?

Tema 5.1.0 - El binario 10010101 se asigna a 149 en decimal. 128 + 16 + 4 + 1 = 149

- ◉ 149
- ○ 157
- ○ 168
- ○ 192

9. ¿Cuál es el equivalente decimal del número hexadecimal 0x3F?

Tema 5.2.0 - Hex 0x3F es 63 en decimal. (3*16)+(15*1) = 63

- (•) 63
- ( ) 77
- ( ) 87
- ( ) 93

10. ¿Cuál es la representación decimal punteada de la dirección IPv4 que se representa como la cadena binaria 00001010.01100100.00010101.00000001?

Tema 5.1.0 - Convertir la cadena binaria de 00001010.01100100.00010101.00000001 a decimal punteado da 10.100.21.1

- (•) 10.100.21.1
- ( ) 10.10.20.1
- ( ) 100.10.11.1
- ( ) 100.21.10.1

11. ¿Cuál es el equivalente decimal de 0xC9?

Tema 5.2.0 - 0x hace referencia al elemento como hexadecimal. Convierte cada carácter en su nibble correspondiente. A continuación, combine los nibbles juntos y calcule el equivalente decimal resultante. C tiene un valor de 12. 12 x 16 = 192. 192 + 9 = 201.

- ( ) 185
- ( ) 200
- (•) 201
- ( ) 199

12. ¿Cuál es un número hexadecimal válido?

Tema 5.2.0 - Los números hexadecimales son 0,1,2,3,4,5,6,7,8,9, a, b, c, d, e, f.. El número hexadecimal 0 representa 0 en decimal y se representa como 0000 en binario. El número hexadecimal f representa 15 en decimal.

- (•) f
- ( ) g
- ( ) h
- ( ) j

13. ¿Cuál es la representación de 0xCA en sistema binario?

Tema 5.2.0: Cuando se convierte, CA en hexadecimal es equivalente a 11011010 en binario. Una forma de realizar la conversión es de a un cuarteto por vez: C = 1100 y A = 1010. Al combinar ambos cuartetos, se obtiene 11001010.

- ( ) 10111010
- ( ) 11010101
- (•) 11001010
- ( ) 11011010

14. ¿Cuántos bits hay en una dirección IPv4?

Tema 5.1.0 - Una dirección IPv4 se compone de 4 octetos de dígitos binarios, cada uno con 8 bits, lo que resulta en una dirección de 32 bits.

- (•) 32
- ( ) 64
- ( ) 128
- ( ) 256

Correct

You have successfully identified the correct answers.

You got 14 out of 14 questions correct.

1. What is the binary representation for the decimal number 173?

Topic 5.1.0 - decimal 173 = 128 + 0 + 32 + 0 + 8 + 4 + 0 + 1

- 10100111
- 10100101
- (•) 10101101
- 10110101

2. Given the binary address of 11101100 00010001 00001100 00001010, which address does this represent in dotted decimal format?

Topic 5.1.0 - The binary number 11101100 00010001 00001100 00001010 translates to 236.17.12.10.

- 234.17.10.9
- 234.16.12.10
- 236.17.12.6
- (•) 236.17.12.10

3. How many binary bits exist within an IPv6 address?

Topic 5.2.0 - IPv4 addressing space is exhausted by the rapid growth of the Internet and the devices connected to the Internet. IPv6 expands the IP addressing space by increasing the address length from 32 bits to 128 bits.

- 32
- 48
- 64
- (•) 128
- 256

4. What is the binary equivalent of the decimal number 232?

Topic 5.1.0 - 232 in binary is 11101000. 128+64+32+8 = 232

- (•) 11101000
- 11000110
- 10011000
- 11110010

5. Which two statements are correct about IPv4 and IPv6 addresses? (Choose two.)

Topic 5.2.0 - IPv4 addresses are represented as dotted decimal numbers and are 32 bits in length. IPv6 addresses are represented by hexadecimal numbers and are 128 bits in length.

- [x] IPv6 addresses are represented by hexadecimal numbers.
- [ ] IPv4 addresses are represented by hexadecimal numbers.
- [ ] IPv6 addresses are 32 bits in length.
- [x] IPv4 addresses are 32 bits in length.
- [ ] IPv4 addresses are 128 bits in length.
- [ ] IPv6 addresses are 64 bits in length.

6. Which IPv4 address format was created for ease of use by people and is expressed as 201.192.1.14?

Topic 5.1.0 - For ease of use by people, binary patterns are represented as dotted decimal. Computer systems were created to understand binary addressing.

- ( ) binary
- (•) dotted decimal
- ( ) hexadecimal
- ( ) ASCII

7. What is the dotted decimal representation of the IPv4 address 11001011.00000000.01110001.11010011?

Topic 5.1.0 - Each section (octet) contains eight binary digits. Each digit represents a specific value (128, 64, 32, 16, 8, 4, 2, and 1). Everywhere there is a 1, the specific value is relevant. Add all relevant values in a particular octet to obtain the decimal value. For example binary 11001011 equals 203 in decimal.

- ( ) 192.0.2.199
- ( ) 198.51.100.201
- (•) 203.0.113.211
- ( ) 209.165.201.223

8. What is the decimal equivalent of the binary number 10010101?

Topic 5.1.0 - Binary 10010101 maps to 149 in decimal. 128+16+4+1 = 149

- (•) 149
- ( ) 157
- ( ) 168
- ( ) 192

9. What is the decimal equivalent of the hex number 0x3F?

Topic 5.2.0 - Hex 0x3F is 63 in decimal.
(3*16)+(15*1) = 63

- (•) 63
- ( ) 77
- ( ) 87
- ( ) 93

10. What is the dotted decimal representation of the IPv4 address which is represented as the binary string 00001010.01100100.00010101.00000001?

Topic 5.1.0 - Converting the binary string of 00001010.01100100.00010101.00000001 to dotted decimal gives 10.100.21.1

- (•) 10.100.21.1
- ( ) 10.10.20.1
- ( ) 100.10.11.1
- ( ) 100.21.10.1

11. What is the decimal equivalent of 0xC9?

Topic 5.2.0 - 0x refers to the item as hexadecimal. Convert each character into its corresponding nibble. Then combine the nibbles together and calculate the resulting decimal equivalent. C has a value of 12. 12 x 16 = 192. 192 + 9 = 201.

- ( ) 185
- ( ) 200
- (•) 201
- ( ) 199

12. Which is a valid hexadecimal number?

Topic 5.2.0 - The hexadecimal numbers are 0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f.. The hexadecimal number 0 represents 0 in decimal and is represented as 0000 in binary. The hexadecimal number f represents 15 in decimal .

- (•) f
- ( ) g
- ( ) h
- ( ) j

13. What is the binary representation of 0xCA?

Topic 5.2.0 - When converted, CA in hex is equivalent to 11011010 in binary. One way to do the conversion is one nibble at a time, C = 1100 and A = 1010. Combine the two nibbles gives 11001010.

- ○ 10111010
- ○ 11010101
- ◉ 11001010
- ○ 11011010

14. How many bits are in an IPv4 address?

Topic 5.1.0 - An IPv4 address is comprised of 4 octets of binary digits, each containing 8 bits, resulting in a 32-bit address.

- ◉ 32
- ○ 64
- ○ 128
- ○ 256

Capítulo 6_Capa de enlace de datos

Introducción

6.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a la capa de enlace de datos!

Cada red tiene componentes físicos y medios que conectan los componentes. Los diferentes tipos de medios necesitan información diferente sobre los datos para aceptarlos y moverlos a través de la red física. Piénsalo de esta manera: una pelota de golf bien golpeada se mueve por el aire rápido y lejos. También puede moverse a través del agua, pero no tan rápido o tan lejos a menos que sea ayudado por un golpe más contundente. Esto se debe a que la pelota de golf está viajando a través de un medio diferente; agua en lugar de aire.

Los datos deben tener ayuda para moverlos a través de diferentes medios. La capa de vínculo de datos proporciona esta ayuda. Como habrás adivinado, esta ayuda difiere en función de una serie de factores. Este módulo le ofrece una visión general de estos factores, cómo afectan a los datos y los protocolos diseñados para garantizar una entrega exitosa. Comencemos ya mismo.

6.0.2

¿Qué aprenderá en este módulo?

Título del módulo: Capa de enlace de datos

Objetivos del módulo: Explique cómo el control de acceso a medios en la capa de enlace de datos admite la comunicación entre redes.

Título del tema	Objetivo del tema
Propósito de la capa de enlace de datos	Describa el propósito y la función de la capa de enlace de datos al preparar comunicación para su transmisión en medios específicos.
Topologías	Compare las características de los métodos de control de acceso a medios en WAN y LAN. Topologías LAN
Trama de enlace de datos	Describa las características y las funciones de la trama de enlace de datos.

Capa de enlace de datos / Propósito de la capa de enlace de datos

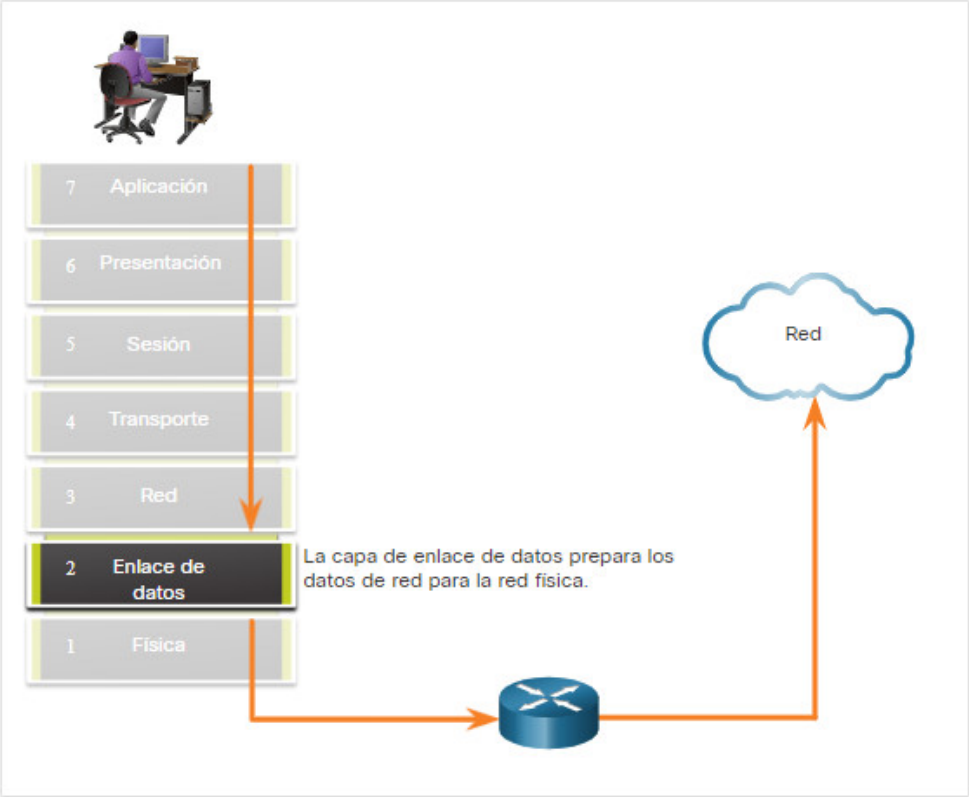
Propósito de la capa de enlace de datos

6.1.1

La capa de enlace de datos

La capa de enlace de datos del modelo OSI (Capa 2), como se muestra en la figura, prepara los datos de red para la red física. La capa de enlace de datos es responsable de las comunicaciones de tarjeta de interfaz de red (NIC) a tarjeta de interfaz de red. La capa de vínculo de datos realiza lo siguiente:

- Permite que las capas superiores accedan a los medios. El protocolo de capa superior no conoce completamente el tipo de medio que se utiliza para reenviar los datos.
- Acepta datos, generalmente paquetes de Capa 3 (es decir, IPv4 o IPv6) y los encapsula en tramas de Capa 2.
- Controla cómo los datos se colocan y reciben en los medios.
- Intercambia tramas entre puntos finales a través de los medios de red.
- Recibe datos encapsulados, generalmente paquetes de Capa 3, y los dirige al protocolo de capa superior adecuado.
- Realiza la detección de errores y rechaza cualquier trama dañada.

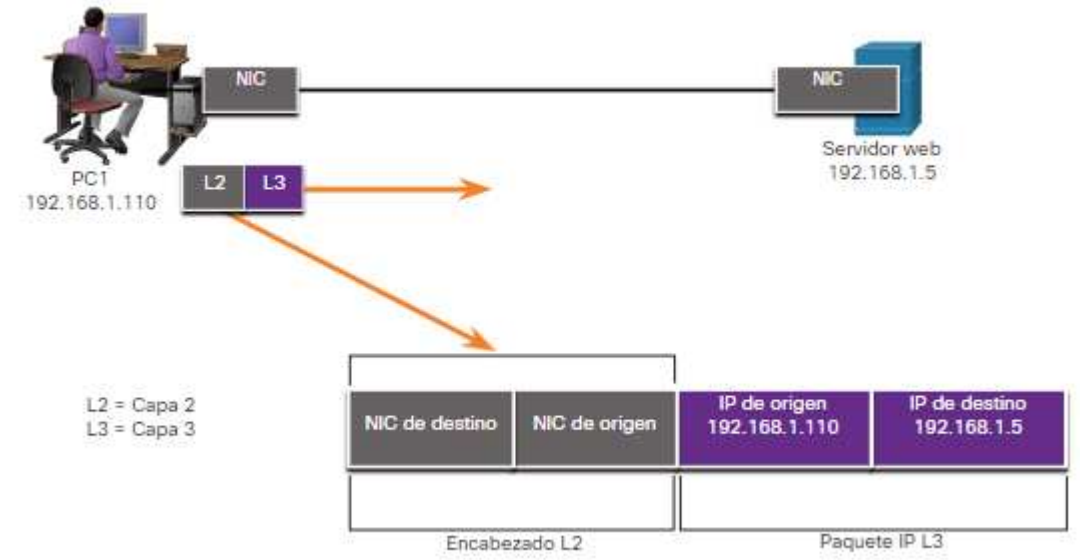


La imagen muestra las siete capas del modelo OSI en orden de arriba hacia abajo, Capa 7 Aplicación, Capa 6 Presentación, Capa 5 Sesión, Capa 4 Transporte, Capa 3 Red, Capa 2 Enlace de Datos, Capa 1 Física. La capa de vínculo de datos se resalta y junto a la capa de vínculo de datos aparece el texto que indica La capa de vínculo de datos prepara los datos de red para la red física. Una flecha que representa el flujo de tráfico de un usuario sentado encima de la capa de aplicación se dibuja sobre el modelo OSI hasta un router y termina en una nube de red.

En redes de equipos, un nodo es un dispositivo que puede recibir, crear, almacenar o reenviar datos a lo largo de una ruta de comunicaciones. Un nodo puede ser un dispositivo final como un portátil o un teléfono móvil, o un dispositivo intermediario como un Ethernet switch.

Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Además, cada vez que se desarrolla una nueva tecnología de red o medio IP, tendría que adaptarse.

La figura muestra un ejemplo de cómo la capa de enlace de datos agrega información de destino Ethernet de Capa 2 y NIC de origen a un paquete de Capa 3. A continuación, convertiría esta información a un formato compatible con la capa física (es decir, Capa 1).



La imagen muestra a un usuario en un equipo de escritorio con una dirección IP 192.168.1.110 que envía tráfico desde su NIC a la NIC de un servidor Web con la dirección IP 192.168.1.5. El usuario muestra un cuadro con la etiqueta L2, que representa el encabezado de la capa 2 y un cuadro con la etiqueta L3 que representa el encabezado de la capa 3. Una flecha del cuadro L2 apunta a un cuadro rectangular más grande con la NIC de destino de texto y la NIC de origen para representar la dirección de Capa 2 de destino y la dirección de Capa 3 de destino. A la derecha del encabezado L2 hay un cuadro rectangular llamado L3 IP Packet que tiene texto que indica la dirección IP de origen 192.168.1.110 y la dirección IP de destino 192.168.1.5.

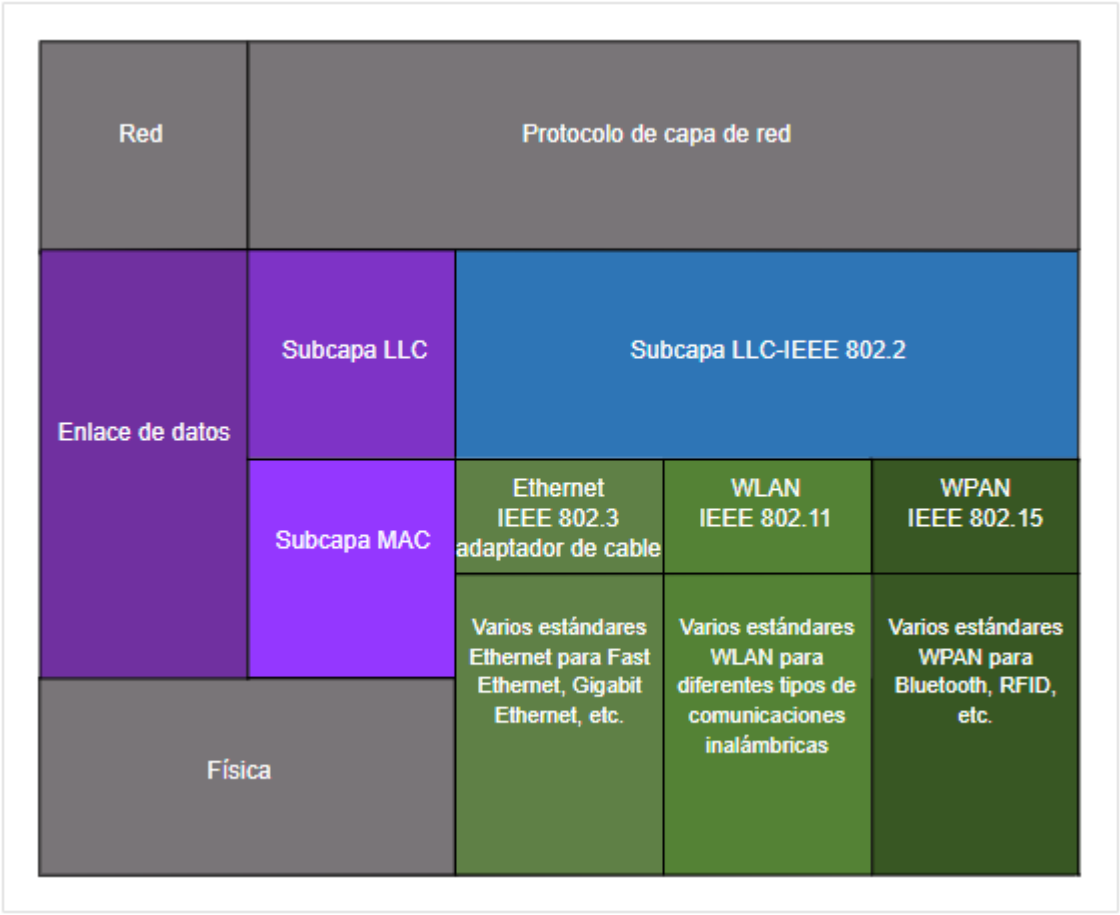
6.1.2

Subcapas de enlace de datos IEEE 802 LAN/MAN

Los estándares IEEE 802 LAN/MAN son específicos para LAN Ethernet, LAN inalámbricas (WLAN), redes de área personal inalámbrica (WPAN) y otros tipos de redes locales y metropolitanas. La capa de enlace de datos IEEE 802 LAN/MAN consta de las dos subcapas siguientes:

- **Control de enlace lógico (LLC):** Esta subcapa IEEE 802.2 se comunica entre el software de red en las capas superiores y el hardware del dispositivo en las capas inferiores. Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que múltiples protocolos de Capa 3, como IPv4 e IPv6, utilicen la misma interfaz de red y medios.
- **Control de acceso a medios (MAC)**: Implementa esta subcapa (IEEE 802.3, 802.11 o 802.15) en hardware. Es responsable de la encapsulación de datos y el control de acceso a los medios. Proporciona direccionamiento de capa de enlace de datos y está integrado con varias tecnologías de capa física.

La figura muestra las dos subcapas (LLC y MAC) de la capa de enlace de datos.



La imagen es de una tabla con tres filas para la red, el enlace de datos y la capa física. La fila superior de la tabla tiene red y Protocolo de capa de red. La segunda fila tiene enlace de datos y se divide furthur en dos filas, una para LLC Sublayer y otra para MAC Sublayer. La

subcapa LLC tiene una columna que indica LLC Sublayer - IEEE 802.2.La subcapa MAC tiene tres columnas que indican Ethernet IEEE 802.3, WLAN 802.11 y WPAN IEEE 802.15. Bajo la columna Ethernet 802.3, entre la subcapa MAC y la capa física indica varios estándares Ethernet para Fast Ethernet, Gigabit Ethernet, etc. Bajo la columna WLAN IEEE 802.11, entre la subcapa MAC y la capa física establece varios estándares WLAN para diferentes tipos de redes inalámbricas comunicaciones. Debajo de la columna WPAN entre la subcapa MAC y la capa física, indica varios estándares WPAN para Bluetooth, RFID, etc.

La subcapa LLC toma los datos del protocolo de red, que generalmente es un paquete IPv4 o IPv6, y agrega información de control de Capa 2 para ayudar a entregar el paquete al nodo de destino.

La subcapa MAC controla la NIC y otro hardware que es responsable de enviar y recibir datos en el medio LAN/MAN con cable o inalámbrico.

La subcapa MAC proporciona encapsulación de datos:

- **Delimitación de tramas:** El proceso de entramado proporciona delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Estos bits delimitadores proporcionan sincronización entre los nodos de transmisión y de recepción.
- **Direccionamiento**: proporciona direccionamiento de origen y destino para transportar la trama de capa 2 entre dispositivos en el mismo medio compartido.
- **Detección de errores** - Cada trama contiene un tráiler utilizado para detectar errores de transmisión.

La subcapa MAC también proporciona control de acceso a medios, lo que permite que varios dispositivos se comuniquen a través de un medio compartido (semidúplex). Las comunicaciones dúplex completo no requieren control de acceso.

6.1.3

Provisión de acceso a los medios

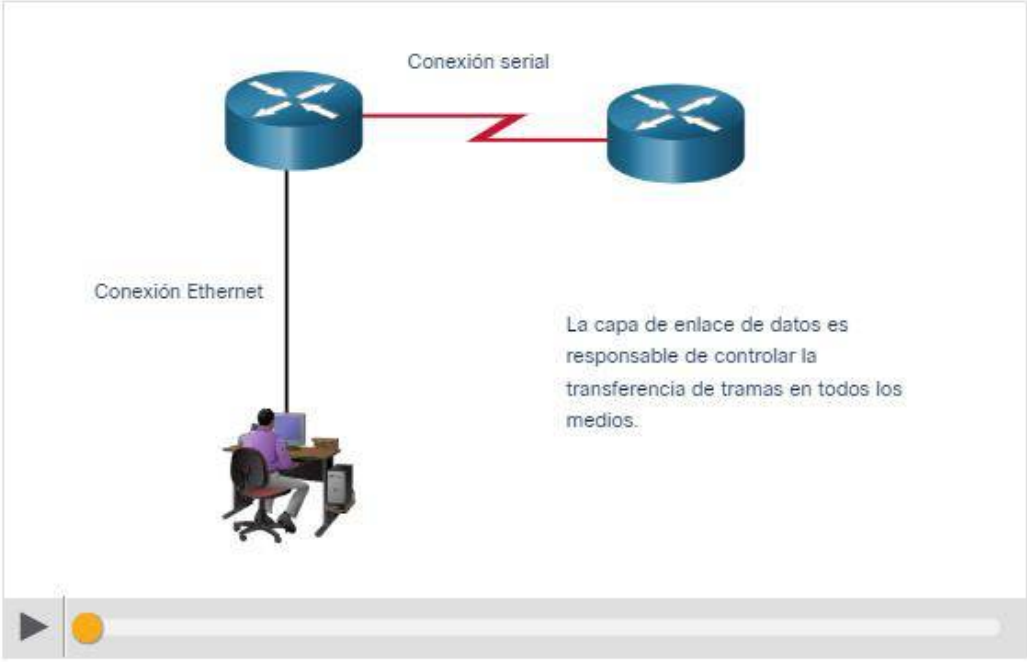
Cada entorno de red que los paquetes encuentran cuando viajan desde un host local hasta un host remoto puede tener características diferentes. Por ejemplo, una LAN Ethernet generalmente consta de muchos hosts que compiten por el acceso en el medio de red. La subcapa MAC resuelve esto. Con los enlaces serie, el método de acceso sólo puede consistir en una conexión directa entre solo dos dispositivos, generalmente dos routers. Por lo tanto, no requieren las técnicas empleadas por la subcapa MAC IEEE 802.

Las interfaces del router encapsulan el paquete en la trama apropiada. Se utiliza un método adecuado de control de acceso a los medios para acceder a cada enlace. En cualquier intercambio de paquetes de capas de red, puede haber muchas transiciones de medios y capa de enlace de datos.

En cada salto a lo largo de la ruta, un router realiza las siguientes funciones de Capa 2:

1. Aceptan una trama proveniente de un medio.
2. Desencapsulan la trama.
3. Vuelven a encapsular el paquete en una trama nueva.
4. Reenvían la nueva trama adecuada al medio de ese segmento de la red física.

Pulse Reproducir para ver la animación. El router de la figura tiene una interfaz Ethernet para conectarse a la LAN y una interfaz serial para conectarse a la WAN. A medida que el router procesa tramas, utilizará los servicios de la capa de enlace de datos para recibir la trama desde un medio, desencapsularlo en la PDU de la Capa 3, volver a encapsular la PDU en una trama nueva y colocar la trama en el medio del siguiente enlace de la red.



Esta animación ilustra cómo una trama de capa 2 se encapsula y se desencapsula a medida que viaja en una red. Un usuario envía una trama Ethernet al router de puerta de enlace predeterminado. Cuando el router recibe la trama, descapsulará la trama Ethernet para leer su contenido. Luego procesa el paquete de Capa 3 y toma una decisión de enrutamiento para elegir una interfaz serie como interfaz de salida a la dirección IP de salto siguiente. A continuación, el router vuelve a encapsular el paquete en una nueva trama de capa 2 y lo envía al siguiente router a través del enlace serie.

6.1.4

Estándares de la capa de enlace de datos

Los protocolos de capa de enlace de datos generalmente no están definidos por la Solicitud de comentarios (RFC), a diferencia de los protocolos de las capas superiores del conjunto TCP / IP. El Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para el conjunto de protocolos TCP / IP en las capas superiores, pero no definen las funciones y el funcionamiento de la capa de acceso a la red TCP / IP.

Las organizaciones de ingeniería que definen estándares abiertos y protocolos que se aplican a la capa de acceso a la red (es decir, las capas físicas y de enlace de datos OSI) incluyen lo siguiente:

- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Unión Internacional de Telecomunicaciones (ITU)
- Organización Internacional para la Estandarización (ISO)
- Instituto Nacional Estadounidense de Estándares (ANSI)

Los logotipos de estas organizaciones se muestran en la figura.

Logotipos de la organización de ingeniería

6.1.5

Compruebe su comprensión - Propósito de la capa de enlace de datos

Verifique su comprensión de la capa de enlace de datos eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La capa de vínculo de datos es la capa 2 del modelo OSI.
2. La capa de enlace de datos consta de dos subcapas. Estos son Control de vínculos lógicos (LLC) y Control de acceso a medios (MAC)
3. La subcapa MAC de la capa de enlace de datos es responsable de que las tramas entren y salgan de los medios.
4. Los routers realizan cuatro funciones en la Capa 2. Aceptan una trama de los medios, desencapsulan el paquete de una trama, vuelven a encapsular el paquete en una nueva trama y reenvía la nueva trama apropiada para el medio de ese segmento de la red física.
5. Los dos criterios para determinar el método de control de acceso a medios utilizados son el tipo de uso compartido de medios involucrados y la topología.
6. El IEEE define estándares para la capa de acceso de red TCP/IP, que son las capas físicas y de enlace de datos OSI.

Has tenido 6 respuestas correctas de 6.

1. ¿Cuál es otro nombre para la capa de enlace de datos OSI?

¡Lo tienes!

- ○ Capa 1
- ◉ Capa 2
- ○ Capa 3
- ○ Capa 6

2. ¿La capa de enlace de datos IEEE 802 LAN/MAN consta de dos subcapas? (Escoja dos.)

¡Lo tienes!

- ☐ protocolo de control de red
- ☑ control de enlace lógico
- ☑ Control de acceso a medios
- ☐ Protocolo de control de enlace

3. ¿Cuál es la responsabilidad de la subcapa MAC?

¡Lo tienes!

- ○ Agrega direcciones de capa 3 a la trama
- ○ Se comunica con la capa de red (Capa 3)
- ◉ Proporciona el método para obtener el fotograma dentro y fuera de los medios
- ○ Transmite los bits en los medios

4. ¿Qué función de capa 2 realiza un router? (Escoja tres.)

¡Lo tienes!

- [x] Aceptan una trama proveniente de un medio.
- [x] Desencapsulan la trama.
- [ ] Hace referencia a su tabla de enrutamiento de capa 3 para una red de destino coincidente
- [x] Vuelven a encapsular el paquete en una trama nueva.

5. ¿El método de control de acceso a los medios utilizado depende de qué dos criterios?

¡Lo tienes!

- [ ] Protocolo IP de capa 3
- [x] Uso compartido de multimedia
- [x] Topología
- [ ] Protocolo de la capa de transporte
- [ ] Tipo de datos

6. ¿Qué organización define estándares para la capa de acceso a la red (es decir, las capas físicas y de enlace de datos OSI)?

¡Lo tienes!

- ( ) Cisco
- ( ) IANA
- (•) IEEE
- ( ) IETF

Correct

You have successfully identified the correct answers.

1. The data link layer is Layer 2 of the OSI model.
2. The data link layer consists of two sublayers. These are Logical Link Control (LLC) and Media Access Control (MAC)
3. The MAC sublayer of the data link layer is responsible for getting frames on and off the media.
4. Routers perform four functions at Layer 2. They accept a frame from the media, de-encapsulate the packet from a frame, re-encapsulate the packet into a new frame, and forwards the new frame appropriate to the medium of that segment of the physical network.
5. The two criteria for determining the media access control method used are the type of media sharing involved and the topology.
6. The IEEE defines standards for the TCP/IP network access layer, which are the OSI physical and data link layers.

You got 6 out of 6 questions correct.

1. What is another name for the OSI data link layer?

You got it!

- ○ Layer 1
- ◉ Layer 2
- ○ Layer 3
- ○ Layer 6

2. The IEEE 802 LAN/MAN data link layer consists of which two sublayers? (Choose two.)

You got it!

- ☐ Network Control Protocol
- ☑ Logical Link Control
- ☑ Media Access Control
- ☐ Link Control Protocol

3. What is the responsibility of the MAC sublayer?

You got it!

- ○ Adds Layer 3 addresses to the frame
- ○ Communicates with the network layer (Layer 3)
- ◉ Provides the method to get the frame on and off the media
- ○ Transmits the bits on the media

4. What Layer 2 function does a router perform? (Choose three.)

You got it!

- ☑ Accepts a frame from a medium
- ☑ De-encapsulates the frame
- ☐ Refers to its Layer 3 routing table for a matching destination network
- ☑ Re-encapsulates the packet into a new frame

5. The media access control method used depends on which two criteria?

You got it!

- ☐ Layer 3 IP protocol
- ☑ Media sharing
- ☑ Topology
- ☐ Transport layer protocol
- ☐ Type of data

6. Which organization defines standards for the network access layer (i.e., the OSI physical and data link layers)?

You got it!

- ○ Cisco
- ○ IANA
- ◉ IEEE
- ○ IETF

Topologías

6.2.1

Topologías física y lógica

Como aprendió en el tema anterior, la capa de enlace de datos prepara los datos de red para la red física. Debe conocer la topología lógica de una red para poder determinar lo que se necesita para transferir tramas de un dispositivo a otro. En este tema se explican las formas en que la capa de vínculo de datos funciona con diferentes topologías de red lógicas.

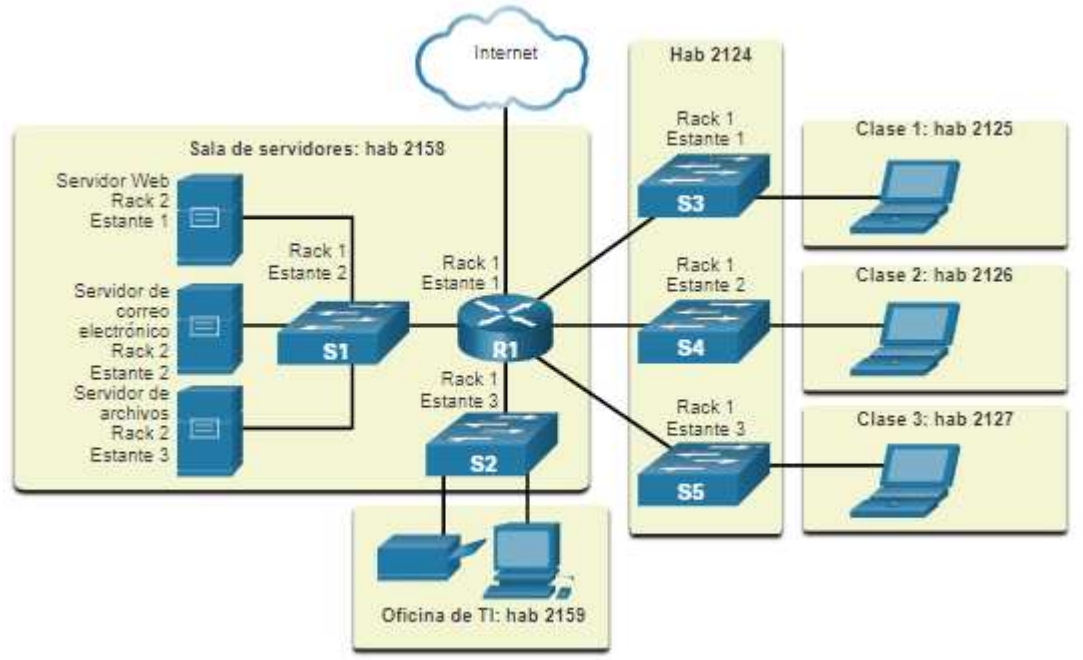
La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos.

Existen dos tipos de topologías utilizadas al describir redes LAN y WAN:

- **Topología física** – Identifica las conexiones físicas y cómo se interconectan los dispositivos finales y los dispositivos intermedios (es decir, routers, switches y puntos de acceso inalámbrico). La topología también puede incluir la ubicación específica del dispositivo, como el número de habitación y la ubicación en el rack del equipo. Las topologías físicas generalmente son punto a punto o en estrella.
- **Topología lógica** - Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta topología identifica las conexiones virtuales mediante interfaces de dispositivo y esquemas de direccionamiento IP de capa 3.

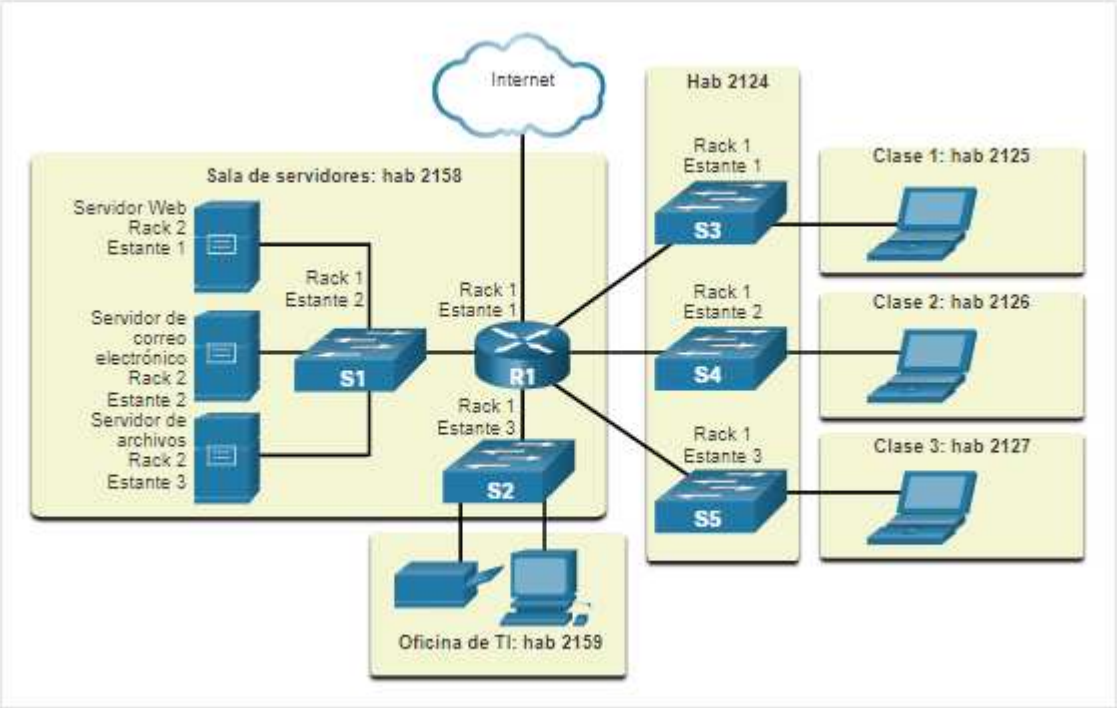
La capa de enlace de datos “ve” la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a los medios que se utilizan.

La figura muestra una topología **física** de ejemplo para una red de ejemplo pequeña.



La topología de red física muestra seis salas, cada una resaltada en una caja de color amarillo claro, con varios dispositivos de red y cableado. En el lado izquierdo está la sala de servidores etiquetada habitación 2158. Contiene un router etiquetado R1 montado en rack 1 estante 1 con seis conexiones de cable. Un cable en la parte superior se conecta a una nube etiquetada como Internet. Un cable a la izquierda se conecta a un switch etiquetado S1 montado en el estante 1 2. S1 está conectado a tres servidores: un servidor web montado en el rack 2 estante 1, un servidor de correo electrónico montado en el rack 2 estante 2 y un servidor de archivos montado en el rack 2 estante 3. Un cable conectado a la parte inferior de R1 se conecta a un switch etiquetado S2 montado en el rack 1 estante 3. S2 tiene dos conexiones que conducen a una impresora y un PC en la oficina de TI etiquetada habitación 2159. R1 tiene tres cables a la derecha conectados a tres switches ubicados en la sala 2124. El switch superior está etiquetado S3 y montado en el rack 1 estante 1. El switch central está etiquetado S4 y montado en el rack 1 estante 2. El switch inferior está etiquetado S5 y montado en el rack 1 estante 3. S3 tiene un cable a la izquierda conectado a un ordenador portátil en una habitación etiquetada clase 1 habitación 2125. S4 tiene un cable a la izquierda conectado a un ordenador portátil en una habitación etiquetada clase 2 habitación 2126. S5 tiene un cable a la izquierda conectado a un ordenador portátil en una habitación etiquetada clase 3 habitación 2127.

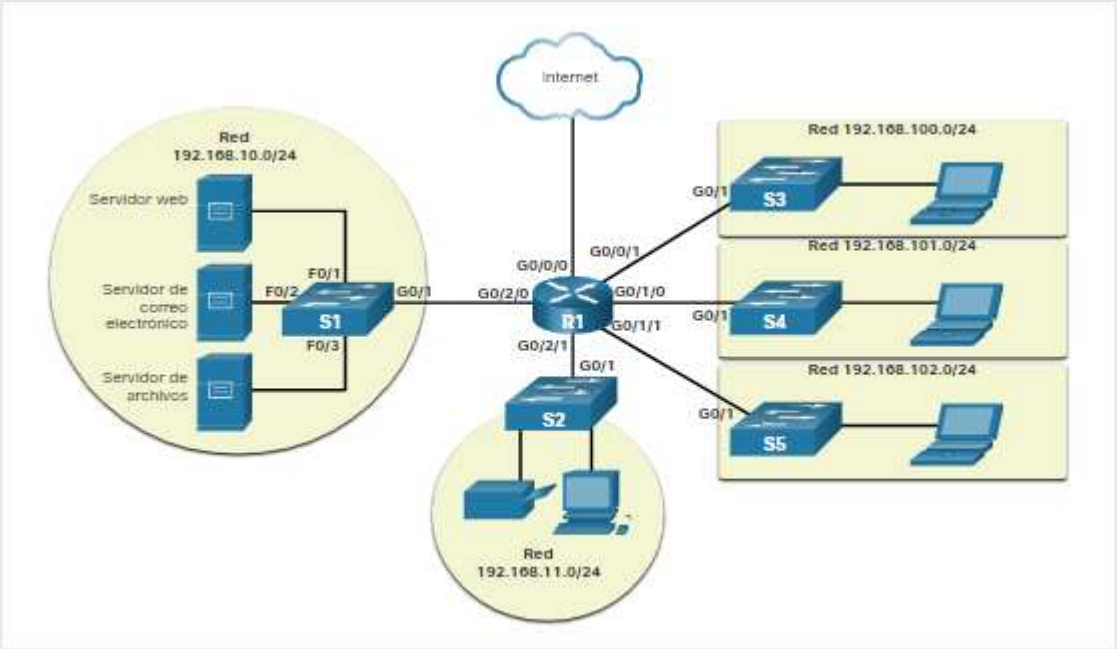
Topología física



La siguiente figura muestra una topología **lógica** de ejemplo para la misma red.

La topología de red lógica muestra los dispositivos, las etiquetas de puerto y el esquema de direccionamiento de red. En el medio de la imagen hay un router etiquetado R1. Un puerto etiquetado G0/0/0 se conecta a una nube en la parte superior de Internet. Un puerto etiquetado G0/2/0 se conecta a la izquierda con un switch etiquetado S1 en el puerto G0/1. S1 está conectado a tres servidores. S1 y los servidores se resaltan en un círculo amarillo claro con la red 192.168.10.0/24 escrita en la parte superior. El puerto F0/1 en S1 se conecta a un servidor web. El puerto F0/2 en S1 se conecta a un servidor de correo electrónico. El puerto F0/3 en S1 se conecta a un servidor de archivos. El puerto G0/0/1 en R1 se conecta en la parte inferior a un switch etiquetado S2. S2 se conecta a una impresora y una PC, todos los cuales se resaltan en un círculo amarillo claro con la red 192.168.11.0/24 escrita en la parte inferior. A la derecha de R1 hay tres conexiones adicionales, cada una de las cuales se conecta a un switch en el puerto G0/1 que luego se conecta a un portátil en el puerto F0/1. Cada switch y portátil se resaltan en amarillo y se muestra la dirección de red. El puerto G0/0/1 de R1 se conecta en la parte superior a un switch etiquetado S3 en la red 192.168.100.0. El puerto G0/1/0 de R1 se conecta en el medio a un switch etiquetado S4 en la red 192.169.101.0. El puerto G0/1/1 en R1 se conecta en la parte inferior a un switch etiquetado S5 en la red 192.168.102.0. R1 se conecta a Internet en la interfaz G0/0/0.

Topología lógica



6.2.2

Topologías de WAN

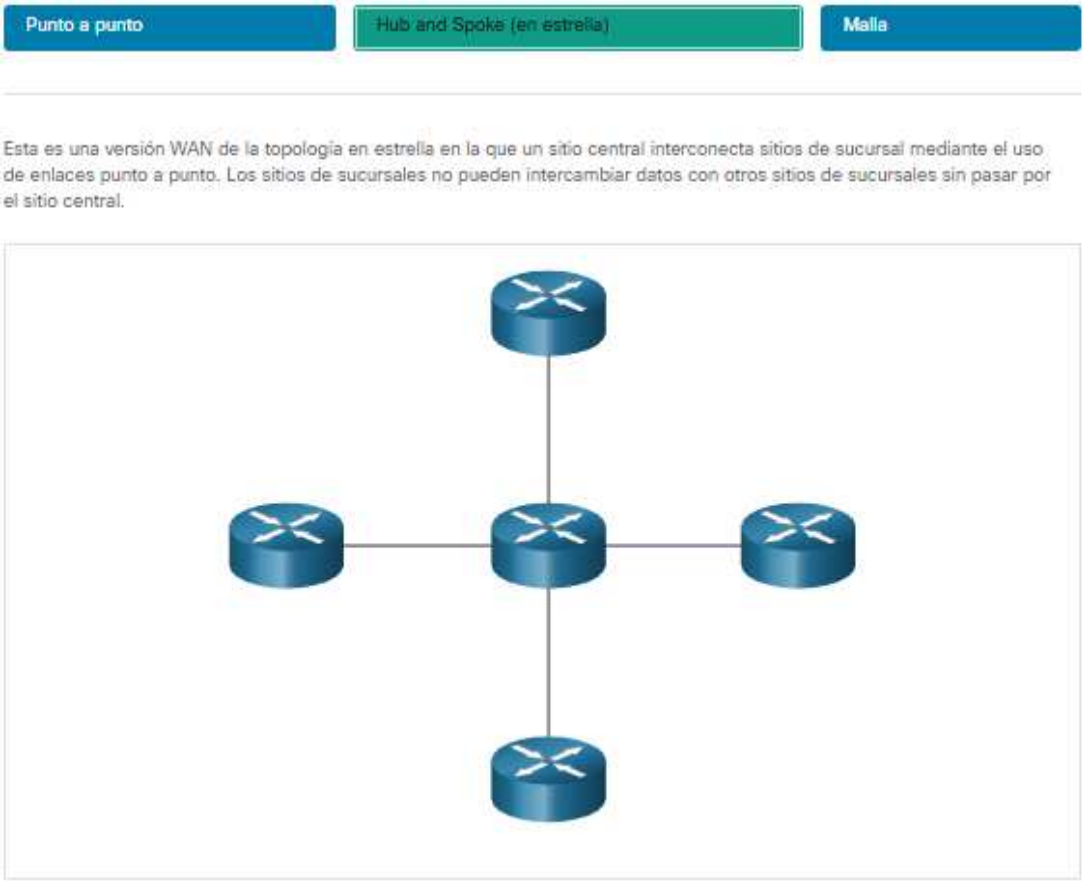
Las figuras ilustran cómo las WAN se interconectan comúnmente mediante tres topologías físicas comunes de WAN.

Haga clic en cada botón para obtener más información.

Punto a punto | Hub and Spoke (en estrella) | Malla

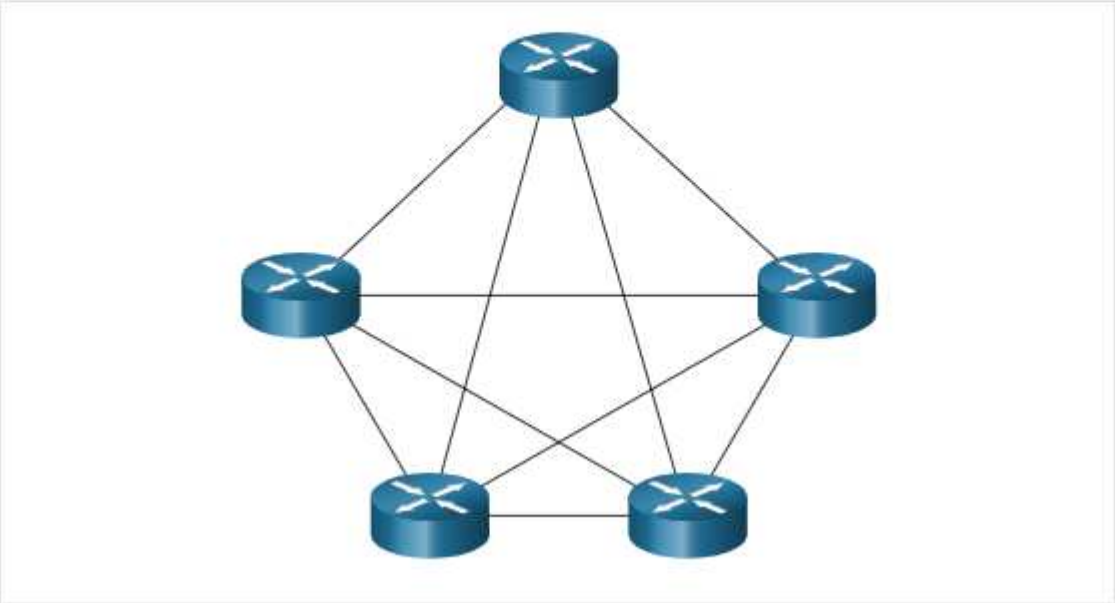
Esta es la topología WAN más simple y común. Es un enlace permanente entre dos terminales.

La imagen muestra dos routers con una sola línea, que representan un enlace, conectándolos.



Punto a punto | Hub and Spoke (en estrella) | Malla

Esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con cualquier otro sistema. Por lo tanto, los costos administrativos y físicos pueden ser importantes. Básicamente, cada enlace es un enlace punto a punto al otro nodo.



Un híbrido es una variación o combinación de cualquier topología. Por ejemplo, una malla parcial es una topología híbrida en la que algunos, pero no todos, los dispositivos finales están interconectados.

6.2.3

Topología WAN de punto a punto

Las topologías físicas punto a punto conectan dos nodos directamente, como se muestra en la figura. En esta disposición, los dos nodos no tienen que compartir los medios con otros hosts. Además, cuando se utiliza un protocolo de comunicaciones en serie, como el Protocolo punto a punto (PPP), un nodo no tiene que hacer ninguna determinación sobre si una trama entrante está destinada para él u otro nodo. Por lo tanto, los protocolos de enlace de datos lógicos pueden ser muy simples, dado que todas las tramas en los medios solo pueden transferirse entre los dos nodos. El nodo coloca las tramas en los medios en un extremo y esas tramas son tomadas de los medios por el nodo en el otro extremo del circuito punto a punto.

La imagen muestra un ejemplo de red punto a punto que consta de dos routers etiquetados como Nodo 1 y Nodo 2, cada uno conectado a una nube de red a través de vínculos WAN.

Las topologías punto a punto están limitadas a dos nodos.

Nota: Una conexión punto a punto a través de Ethernet requiere que el dispositivo determine si la trama entrante está destinada a este nodo.

Un nodo de origen y destino puede estar conectado indirectamente entre sí a través de cierta distancia geográfica utilizando múltiples dispositivos intermedios. Sin embargo, el uso de dispositivos físicos en la red no afecta la topología lógica, como se ilustra en la figura. En la figura, agregar conexiones físicas intermedias puede no cambiar la topología lógica. La conexión lógica punto a punto es la misma.

La imagen muestra un ejemplo de red punto a punto que consta de dos routers, denominados Nodo de origen y Nodo de destino, cada uno conectado a una nube de red a través de vínculos WAN. Los dos routers se muestran enviando tramas a la nube de red.

6.2.4

Topologías de LAN

En las LAN multiacceso, los dispositivos finales (es decir, nodos) están interconectados utilizando topologías estrella o estrella extendida, como se muestra en la figura. En este tipo de topología, los dispositivos finales están conectados a un dispositivo intermediario central, en este caso, un switch Ethernet. A **extended star** extiende esta topología interconectando varios switches Ethernet. La topología en estrella es fácil de instalar, muy escalable (es fácil agregar y quitar dispositivos finales) y de fácil para la resolución de problemas. Las primeras topologías en estrella interconectaban terminales mediante Ethernet hubs.

A veces, es posible que solo haya dos dispositivos conectados en la LAN Ethernet. Un ejemplo son dos routers interconectados. Este sería un ejemplo de Ethernet utilizado en una topología punto a punto.

Topologías LAN heredadas

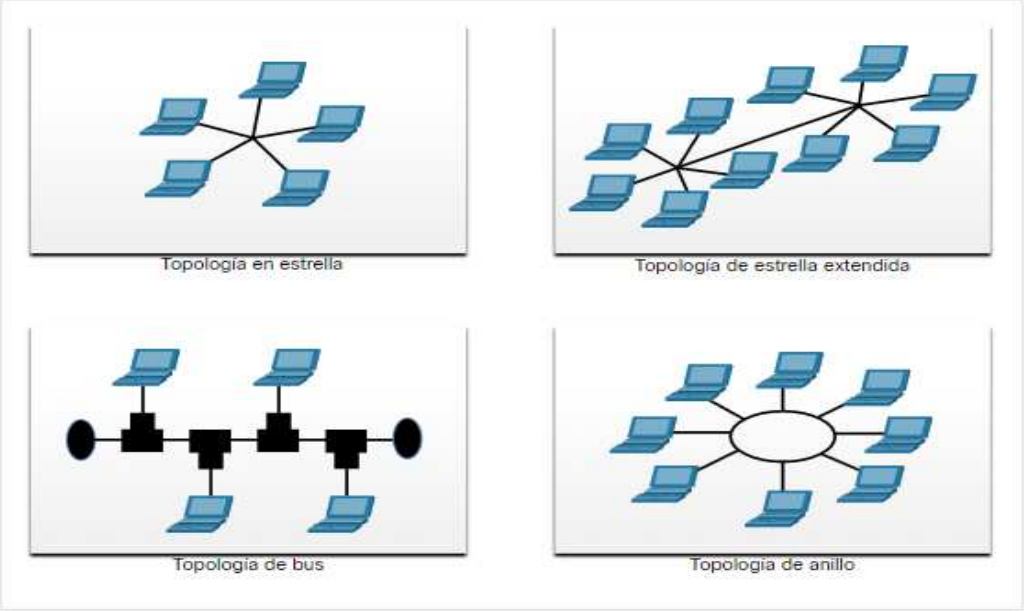
Las tecnologías antiguas Ethernet y Token Ring LAN heredadas incluían otros dos tipos de topologías:

- **Bus** - Todos los sistemas finales se encadenan entre sí y terminan de algún modo en cada extremo. No se requieren dispositivos de infraestructura, como switches, para interconectar los dispositivos finales. Las redes Ethernet heredadas a menudo eran topologías de bus que usaban cables coaxiales porque era económico y fácil de configurar.
- **Anillo** - Los sistemas finales se conectan a su respectivo vecino y forman un anillo. El anillo no necesita ser terminado, a diferencia de la topología del bus. La interfaz de datos distribuidos de fibra heredada (FDDI) y las redes Token Ring usaban topologías de anillo.

Las figuras ilustran cómo los dispositivos finales están interconectados en las LAN. Es común que una línea recta en un gráfico de redes represente una red LAN Ethernet que incluye una estrella simple y una estrella extendida.

Comparación de cuatro topologías físicas: estrella, estrella extendida, bus y anillo.

Topologías físicas



6.2.5

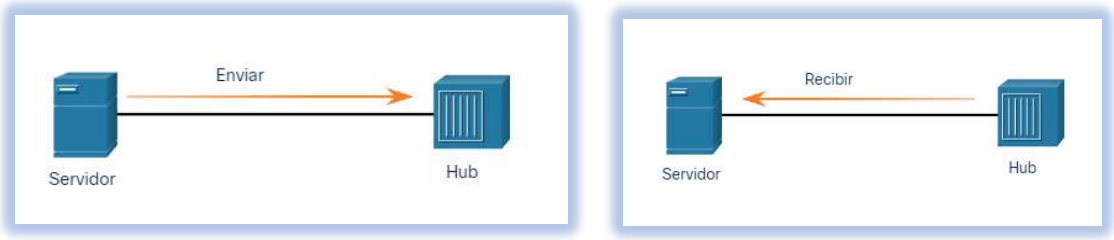
Comunicación Dúplex completo y semidúplex

Comprender la comunicación dúplex es importante cuando se habla de las topologías LAN, ya que se refiere a la dirección de la transmisión de datos entre dos dispositivos. Hay dos modos comunes de dúplex.

Comunicación Half-dúplex

Los dos dispositivos pueden transmitir y recibir en los medios, pero no pueden hacerlo simultáneamente. Las WLAN y las topologías de bus heredadas con swithes Ethernet utilizan el modo semidúplex. Half-dúplex permite que solo un dispositivo envíe o reciba a la vez en el medio compartido. Haga clic en Reproducir en la figura para ver la animación que muestra la comunicación semidúplex.

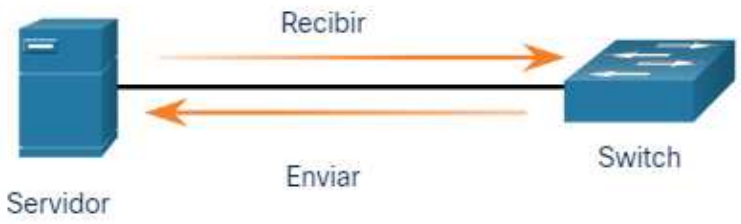
Comunicación Half-dúplex entre un servidor y un hub



Comunicación dúplex completa

Ambos dispositivos pueden transmitir y recibir simultáneamente en los medios compartidos. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Los switches Ethernet operan en el modo de dúplex completo de forma predeterminada, pero pueden funcionar en half-dúplex si se conectan a un dispositivo como un dispositivo externo. Haga clic en Reproducir en la figura para ver la animación que muestra la comunicación dúplex completo.

Comunicación dúplex completa entre un servidor y un hub



En resumen, las comunicaciones semidúplex restringen el intercambio de datos a una dirección a la vez. El dúplex completo permite el envío y la recepción de datos simultáneamente.

Es importante que dos interfaces interconectadas, como la NIC de un host y una interfaz en un switch Ethernet, operen con el mismo modo dúplex. De lo contrario, habrá incompatibilidad de dúplex y se generará ineficiencia y latencia en el enlace.

6.2.6

Métodos de control de acceso

Las LAN Ethernet y WLAN son un ejemplo de una red de accesos múltiples. Una red multiacceso es una red que puede tener dos o más dispositivos finales que intentan acceder a la red simultáneamente.

Algunas redes de acceso múltiple requieren reglas que rijan la forma de compartir los medios físicos. Hay dos métodos básicos de control de acceso al medio para medios compartidos:

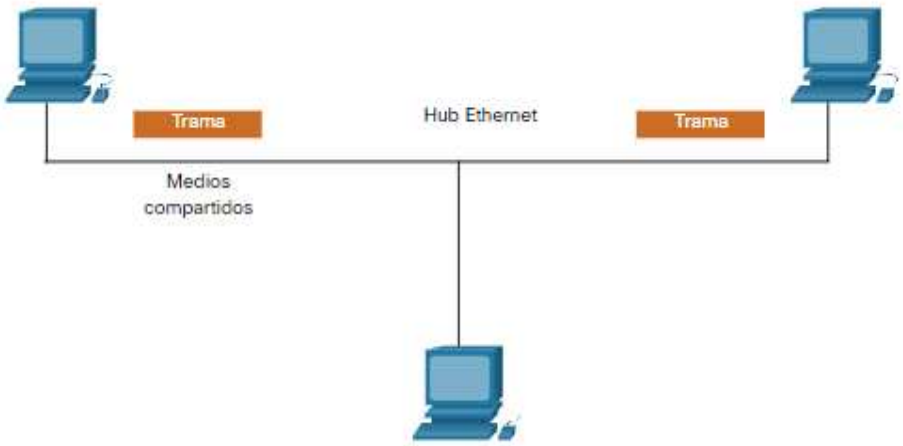
- Acceso por contienda
- Acceso controlado

Acceso basado en la contención

En las redes multiacceso basadas en contencion, todos los nodos operan en semidúplex, compitiendo por el uso del medio. Sin embargo, solo un dispositivo puede enviar a la vez. Por lo tanto, hay un proceso si más de un dispositivo transmite al mismo tiempo. Algunos ejemplos de métodos de acceso basados en contencion son los siguientes:

- Acceso múltiple con detección de colisiones (CSMA/CD) utilizado en LAN Ethernet de topología de bus heredada
- El operador detecta el acceso múltiple con prevención de colisiones (CSMA / CA) utilizado en LAN inalámbricas

La imagen muestra tres PC conectados a un hub Ethernet. Dos de los PCs están enviando tramas simultáneamente.



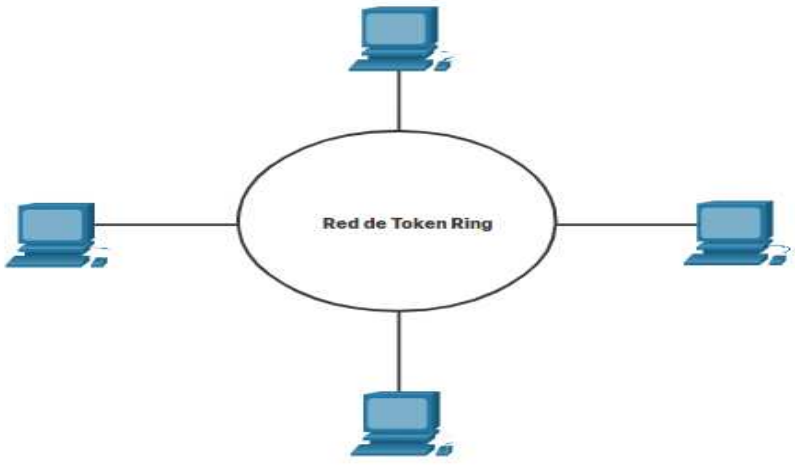
Acceso controlado

En una red de acceso múltiple basada en control, cada nodo tiene su propio tiempo para usar el medio. Estos tipos deterministas de redes no son eficientes porque un dispositivo debe aguardar su turno para acceder al medio. Algunos ejemplos de redes multiacceso que utilizan acceso controlado son los siguientes:

- Anillo de TokenLegacy
- ARCNETheredado

La imagen muestra cuatro PCs conectados a una red de Token Ring.

Red de Token Ring (cada nodo debe esperar su turno para acceder al medio de red)



Nota: Hoy en día, las redes Ethernet funcionan en dúplex completo y no requieren un método de acceso.

6.2.7

Acceso por contención: CSMA/CD

Entre los ejemplos de redes de acceso basadas en controversias se incluyen los siguientes:

- LAN inalámbrica (utiliza CSMA/CA)
- LAN Ethernet de topología de bus heredada (utiliza CSMA/CD)
- LAN Ethernet heredada con un hub (utiliza CSMA/CD)

Estas redes funcionan en modo semidúplex, lo que significa que solo un dispositivo puede enviar o recibir a la vez. Esto requiere un proceso para gestionar cuándo puede enviar un dispositivo y qué sucede cuando múltiples dispositivos envían al mismo tiempo.

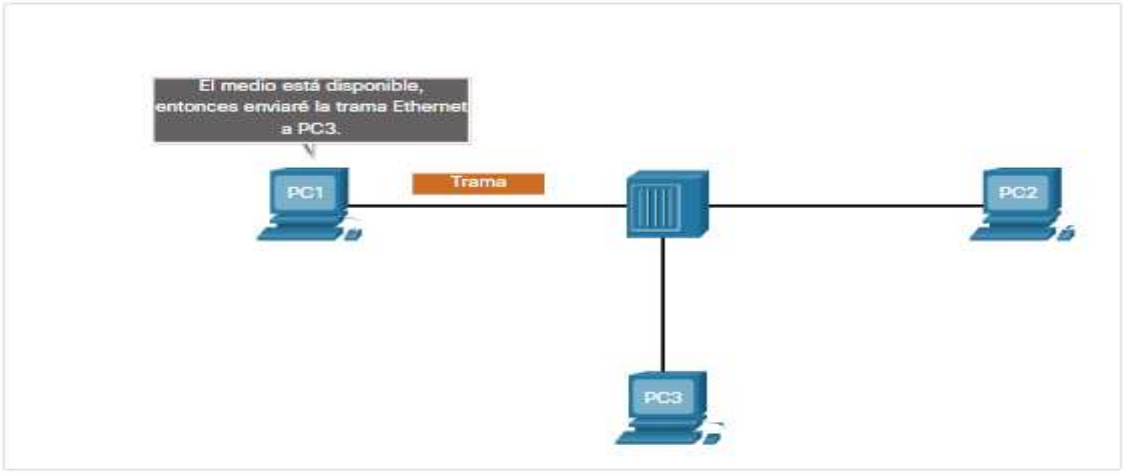
Si dos dispositivos transmiten al mismo tiempo, se produce una colisión. Para las LAN Ethernet heredadas, ambos dispositivos detectarán la colisión en la red. Esta es la parte de detección de colisiones (CD) de CSMA/CD. La NIC compara los datos transmitidos con los datos recibidos, o al reconocer que la amplitud de la señal es más alta de lo normal en los medios. Los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Haga clic en cada botón para obtener una imagen y una descripción del proceso CSMA/CD en LAN Ethernet heredadas que utilizan un hub.

PC1 envía una trama | El hub recibe la trama. | El Hub envía la trama

La PC1 tiene una trama que se debe enviar a la PC3. La NIC de PC1 necesita determinar si algún dispositivo está transmitiendo en el medio. Si no detecta un proveedor de señal, en otras palabras, si no recibe transmisiones de otro dispositivo, asumirá que la red está disponible para enviar.

La NIC PC1 envía la trama Ethernet cuando el medio está disponible, como se muestra en la figura.



La PC1 tiene una trama que se debe enviar a la PC3. La NIC de PC1 necesita determinar si algún dispositivo está transmitiendo en el medio. Si no detecta un proveedor de señal, en otras palabras, si no recibe transmisiones de otro dispositivo, asumirá que la red está disponible para enviar.

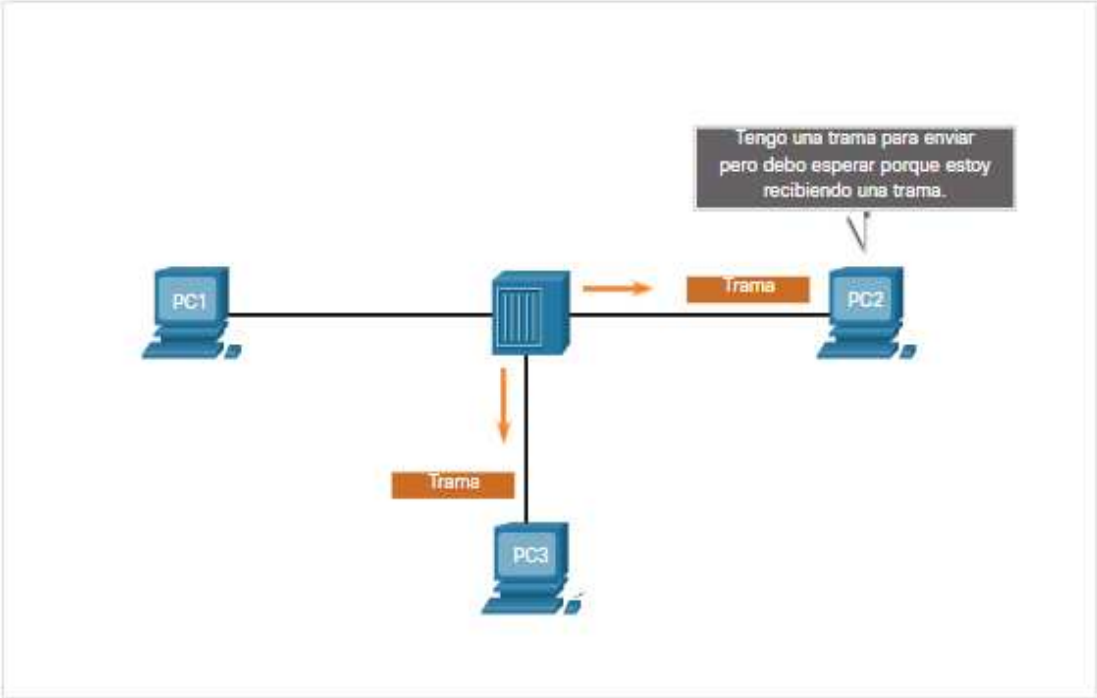
La NIC PC1 envía la trama Ethernet cuando el medio está disponible, como se muestra en la figura.

La imagen muestra tres PC (PC1, PC2 y PC3) conectados a un Ethernet hub. PC1 está enviando una trama. Un cuadro de texto sobre la PC1 dice: El medio está disponible, así que enviaré la trama de Ethernet a la PC3.

PC1 envía una trama | El hub recibe la trama. | El Hub envía la trama

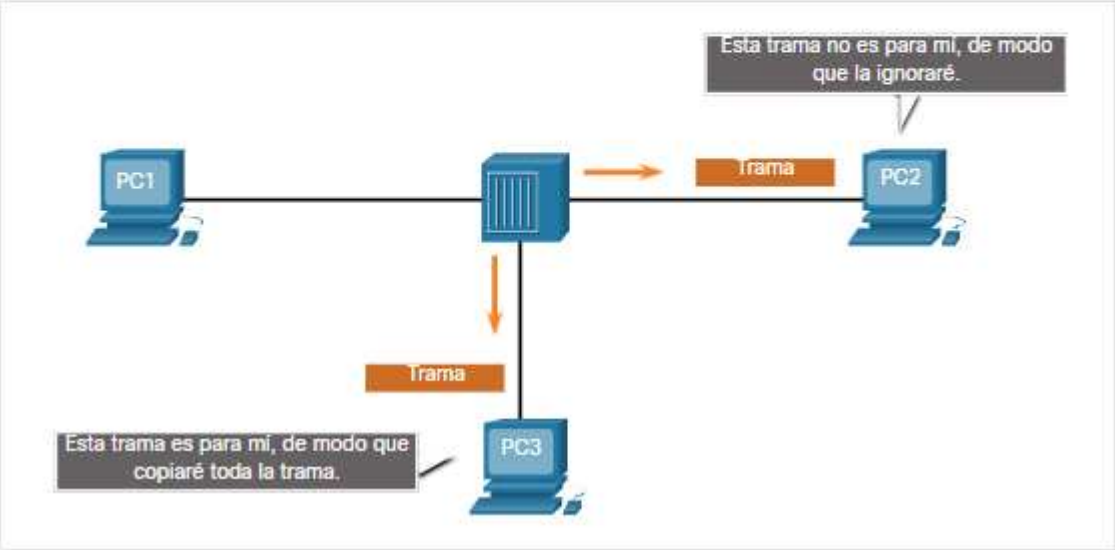
El hub Ethernet recibe y envía la trama. Un hub de Ethernet también se conoce como repetidor multipuerto. Todos los bits que se reciben de un puerto entrante se regeneran y envían a todos los demás puertos, como se indica en la figura.

Si otro dispositivo, como una PC2, quiere transmitir, pero está recibiendo una trama, deberá esperar hasta que el canal esté libre.



PC1 envía una trama | El hub recibe la trama. | El Hub envía la trama

Todos los dispositivos que están conectados al hub reciben la trama. Dado que la trama tiene una dirección destino de enlace de datos para la PC3, solo ese dispositivo aceptará y copiará toda la trama. Todas las demás NIC del dispositivo ignorarán la trama, como se muestra en la figura.



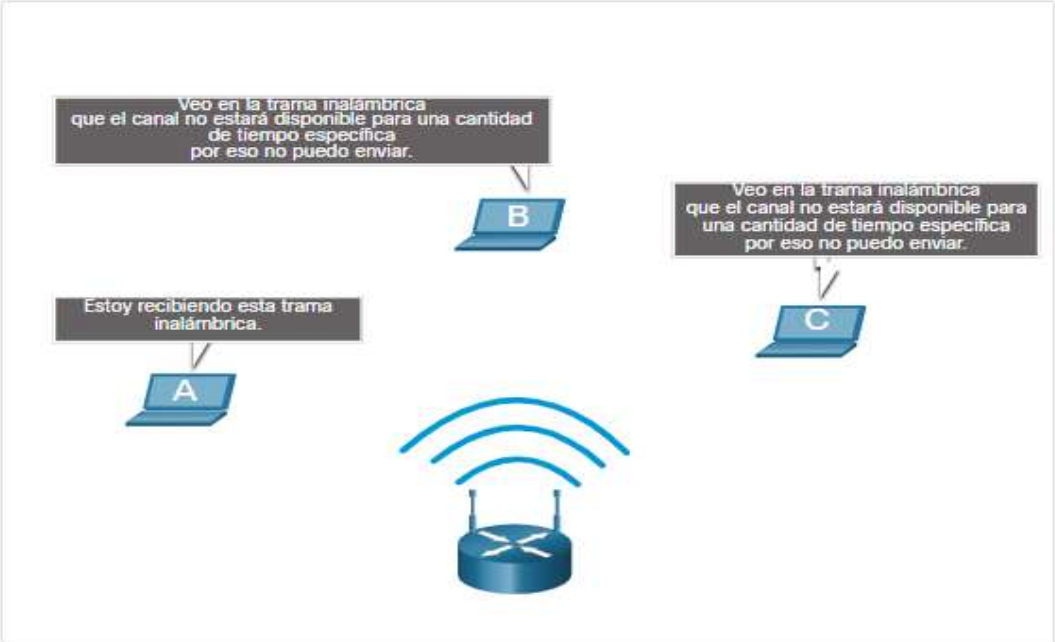
6.2.8

Acceso por contención: CSMA/CA

Otra forma de CSMA utilizada por las WLAN IEEE 802.11 es el acceso múltiple / detección de colisión de detección de portadora (CSMA / CA).

CSMA/CA utiliza un método similar a CSMA/CD para detectar si el medio está libre. CSMA/CA usa técnicas adicionales. En entornos inalámbricos, es posible que un dispositivo no detecte una colisión. CSMA/CA no detecta colisiones, pero intenta evitarlas ya que aguarda antes de transmitir. Cada dispositivo que transmite incluye la duración que necesita para la transmisión. Todos los demás dispositivos inalámbricos reciben esta información y saben durante cuánto tiempo el medio no estará disponible.

En la figura, si el host A recibe una trama inalámbrica desde el punto de acceso, los hosts B y C también verán la trama y cuánto tiempo el medio no estará disponible.



La imagen muestra una red inalámbrica que consta de un punto de acceso y tres computadoras portátiles, un portátil A, B y C. El portátil A tiene un cuadro de texto que dice: estoy recibiendo esta trama inalámbrica. La computadora portátil B tiene un cuadro de texto que dice: veo en la trama inalámbrica que el canal no está disponible durante un período de tiempo específico, por lo que no puedo enviarla. La computadora portátil C tiene un cuadro de texto que dice: veo en la trama inalámbrica que el canal no está disponible durante un período de tiempo específico, por lo que no puedo enviarla.

Luego de que un dispositivo inalámbrico envía una trama 802.11, el receptor devuelve un acuso de recibo para que el emisor sepa que se recibió la trama.

Ya sea que es una red LAN Ethernet con concentradores o una red WLAN, los sistemas por contención no escalan bien bajo un uso intensivo de los medios.

Nota: Las redes LAN Ethernet con switches no utilizan sistemas por contención porque el switch y la NIC de host operan en el modo de dúplex completo.

6.2.9

Compruebe su comprensión - Topologías

Verifique su comprensión de las topologías eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La topología lógica muestra las direcciones IP asignadas a las interfaces de dispositivo.
2. Las redes de área amplia (WAN) vienen en muchas topologías, que incluyen punto a punto, hub-and-spoke y malla.
3. La topología de estrella extendida se considera una topología híbrida porque combina varias topologías de estrella.
4. Las LAN inalámbricas (WLAN) solo admiten semidúplex porque solo un dispositivo puede acceder a los medios a la vez.
5. La detección de colisión / acceso múltiple por detección de portadora (CSMA / CD) es el método de control de acceso a medios utilizado en las LAN Ethernet heredadas.

Has tenido 5 respuestas correctas de 5.

1. ¿Qué topología muestra las direcciones IP de capa de dispositivo de red?

¡Lo tienes!

- topología aérea
- Topología de direcciones IP
- (•) Topología lógica
- Topología física

2. ¿Qué tipo de red utilizaría topologías punto a punto, hub y radio o malla?

¡Lo tienes!

- PAN
- LAN
- WLAN
- (•) WAN

3. ¿Qué topología LAN es una topología híbrida?

¡Lo tienes!

- Bus
- (•) Estrella extendida
- Anillo
- Estrella

4. ¿Qué método de comunicación dúplex se utiliza en las WLAN?

¡Lo tienes!

- dúplex completo
- Semidúplex
- Simplex

5. ¿Qué método de control de acceso a medios se utiliza en LAN Ethernet heredadas?

¡Lo tienes!

- operador detecta acceso múltiple / molestia de colisión
- operador detecta el acceso múltiple / evasión de colisión
- portador detecta el acceso múltiple / destrucción por colisión
- detección de colisión / acceso múltiple por detección de portadora

Correct

You have successfully identified the correct answers.

1. The logical topology shows the IP addresses assigned to device interfaces.
2. Wide Area Networks (WANs) come in many topologies, to include point-to-point, hub-and-spoke, and mesh.
3. The extended star topology is considered a hybrid topology because it combines multiple star topologies.
4. Wireless LANs (WLANs) only support half-duplex because only one device can access the media at a time.
5. Carrier sense multiple access /collision detection (CSMA/CD) is the media access control method used in legacy Ethernet LANs.

You got 5 out of 5 questions correct.

1. Which topology displays networking device layer IP addresses?

You got it!

- aerial topology
- IP address topology
- logical topology
- physical topology

2. What kind of network would use point-to-point, hub and spoke, or mesh topologies?

You got it!

- ○ PAN
- ○ LAN
- ○ WLAN
- ◉ WAN

3. Which LAN topology is a hybrid topology?

You got it!

- ○ bus
- ◉ extended star
- ○ ring
- ○ star

4. Which duplex communication method is used in WLANs?

You got it!

- ○ full-duplex
- ◉ half-duplex
- ○ simplex

5. Which media access control method is used in legacy Ethernet LANs?

You got it!

- ○ carrier sense multiple access/collision annoyance
- ○ carrier sense multiple access/collision avoidance
- ○ carrier sense multiple access/collision destruction
- ◉ carrier sense multiple access/collision detection

Capa de enlace de datos / Trama de enlace de datos

Trama de enlace de datos

6.3.1

La trama

En este tema se describe en detalle lo que sucede con la trama de vínculo de datos a medida que se mueve a través de una red. La información anexada a una trama está determinada por el protocolo que se está utilizando.

La capa de enlace de datos prepara los datos encapsulados (generalmente un paquete IPv4 o IPv6) para el transporte a través de los medios locales encapsulándolos con un encabezado y un trailer para crear una trama.

El protocolo de enlace de datos es responsable de las comunicaciones de NIC a NIC dentro de la misma red. Si bien existen muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene tres partes básicas:

- Encabezado
- Datos
- Tráiler

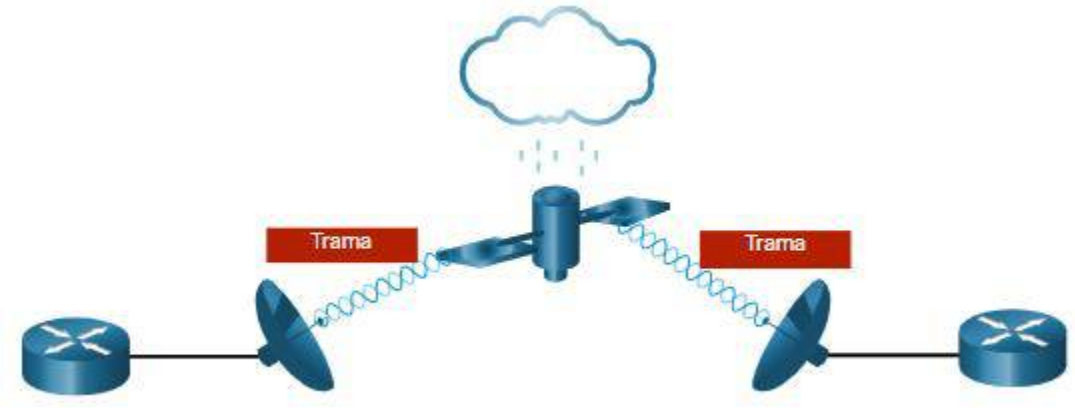
A diferencia de otros protocolos de encapsulación, la capa de enlace de datos agrega información en forma de trailer al final de la trama.

Todos los protocolos de capa de enlace de datos encapsulan los datos dentro del campo de datos de la trama. Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.

No hay una estructura de trama que cumpla con las necesidades de todos los transportes de datos a través de todos los tipos de medios. Según el entorno, la cantidad de información de control que se necesita en la trama varía para cumplir con los requisitos de control de acceso al medio de la topología lógica y de los medios. Por ejemplo, una trama WLAN debe incluir procedimientos para evitar colisiones y, por lo tanto, requiere información de control adicional en comparación con una trama Ethernet.

Como se muestra en la figura, en un entorno frágil, se necesitan más controles para garantizar la entrega. Los campos del encabezado y del tráiler son más grandes porque se necesita más información de control.

Dos routers que se comunican a través de una WAN inalámbrica a través de una conexión satelital.



Se necesitan mayores esfuerzos para garantizar la entrega. Esto significa una sobrecarga más alta y velocidades de transmisión más lentas.

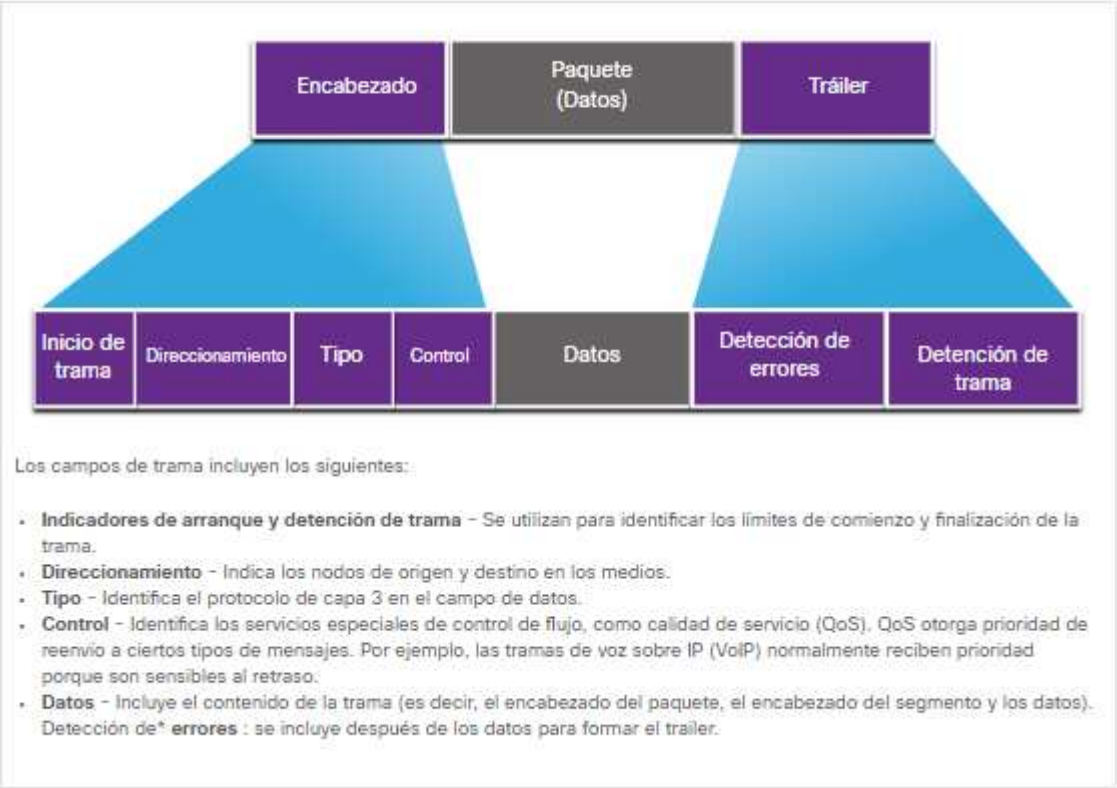
6.3.2

Campos de trama

El tramado rompe la transmisión en agrupaciones descifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato proporciona a las señales físicas una estructura reconocida por los nodos y decodificada en paquetes en el destino.

Los campos de trama genéricos se muestran en la figura. No todos los protocolos incluyen todos estos campos. Los estándares para un protocolo específico de enlace de datos definen el formato real de la trama.

La imagen muestra un paquete de datos encapsulado por un encabezado de enlace de datos y un trailer de enlace de datos. El encabezado del vínculo de datos se desglosa en para campos: Inicio de tramas, direccionamiento, tipo y control. El tráiler del enlace de datos se desglosa en dos campos: Detección de errores y parada de trama.



Los campos de trama incluyen los siguientes:

- **Indicadores de arranque y detención de trama** - Se utilizan para identificar los límites de comienzo y finalización de la trama.
- **Direccionamiento** - Indica los nodos de origen y destino en los medios.
- **Tipo** - Identifica el protocolo de capa 3 en el campo de datos.
- **Control** - Identifica los servicios especiales de control de flujo, como calidad de servicio (QoS). QoS otorga prioridad de reenvío a ciertos tipos de mensajes. Por ejemplo, las tramas de voz sobre IP (VoIP) normalmente reciben prioridad porque son sensibles al retraso.
- **Datos** - Incluye el contenido de la trama (es decir, el encabezado del paquete, el encabezado del segmento y los datos). Detección de* **errores** : se incluye después de los datos para formar el trailer.

Los protocolos de capa de enlace de datos agregan un tráiler al final de cada trama. En un proceso llamado detección de errores, el avance determina si la trama llegó sin error. Coloca un resumen lógico o matemático de los bits que componen la trama en el avance. La capa de enlace de datos agrega detección de errores porque las señales en los medios podrían estar sujetas a interferencia, distorsión o pérdida que cambiaría sustancialmente los valores de bits que representan esas señales.

Un nodo de transmisión crea un resumen lógico del contenido de la trama, conocido como el valor de comprobación de redundancia cíclica (CRC). Este valor se coloca en el campo Secuencia de Verificación de la Trama (FCS) para representar el contenido de la trama. En el tráiler Ethernet, el FCS proporciona un método para que el nodo receptor determine si la trama experimentó errores de transmisión.

6.3.3

Direcciones de Capa 2

La capa de enlace de datos proporciona el direccionamiento utilizado en el transporte de una trama a través de un medio local compartido. Las direcciones de dispositivo en esta capa se llaman direcciones físicas. El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local.

Normalmente se encuentra al principio de la trama, por lo que la NIC puede determinar rápidamente si coincide con su propia dirección de Capa 2 antes de aceptar el resto de la trama. El encabezado de la trama también puede contener la dirección de origen de la trama.

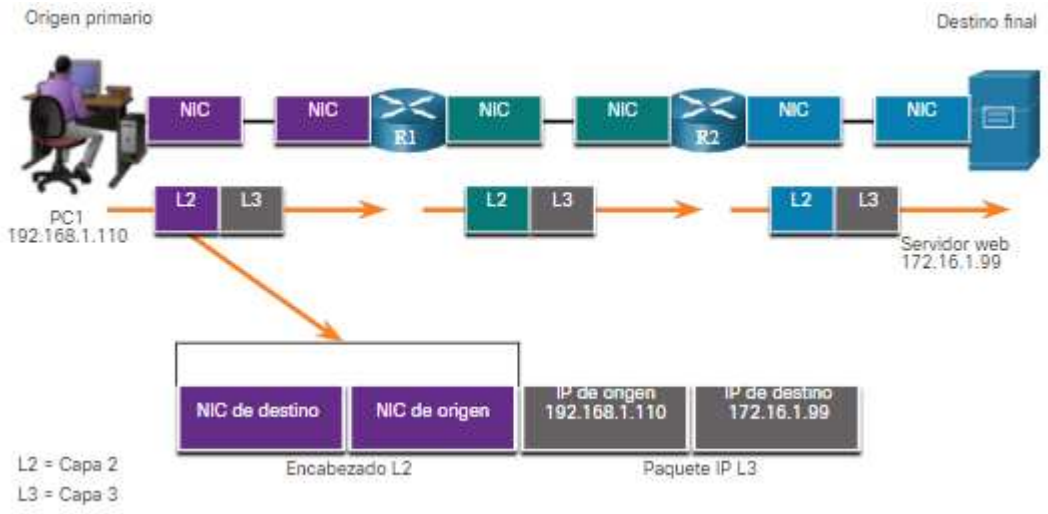
A diferencia de las direcciones lógicas de la Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo. En cambio, la dirección física es única para un dispositivo en particular. Un dispositivo seguirá funcionando con la misma dirección física de capa 2, incluso si el dispositivo se mueve a otra red o subred. Por lo tanto, las direcciones de capa 2 sólo se utilizan para conectar dispositivos dentro del mismo medio compartido, en la misma red IP.

Las figuras ilustran la función de las direcciones de Capa 2 y Capa 3. A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido. Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

Haga clic en cada botón para obtener más información.

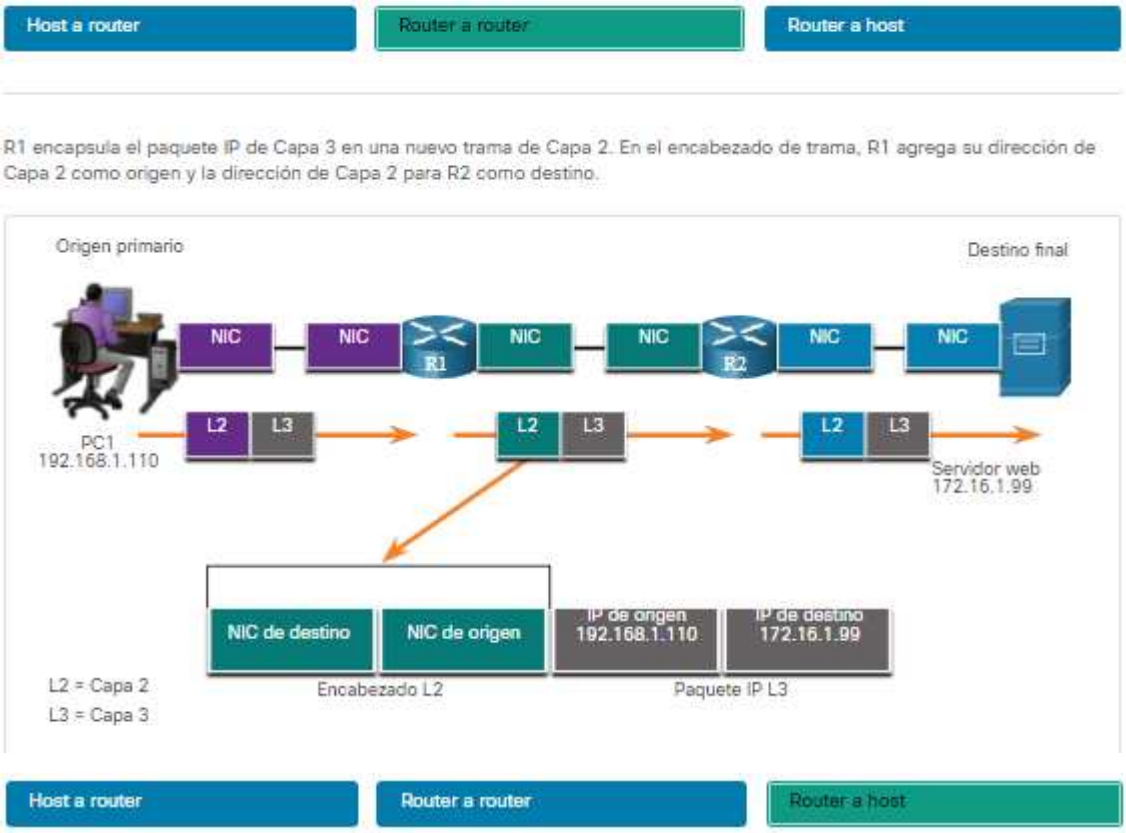
Host a router | Router a router | Router a host

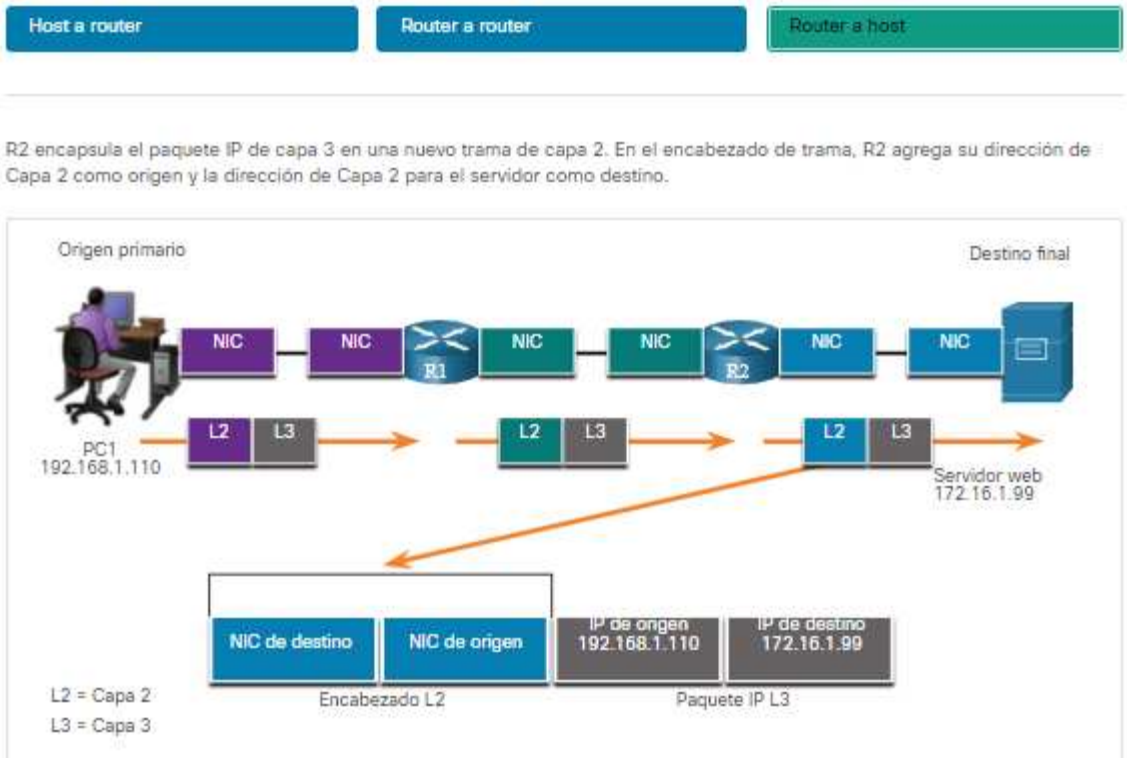
El host de origen encapsula el paquete IP de capa 3 en una trama de capa 2. En el encabezado de trama, el host agrega su dirección de Capa 2 como origen y la dirección de Capa 2 para R1 como destino.



La imagen muestra una red que consiste en un PC de origen, un router R1, un router R2 y un servidor web de destino final. Se muestra un cuadro de texto que representa la NIC de cada interfaz de dispositivo. PC1 tiene la dirección IP 192.168.1.100. El servidor tiene la dirección IP 172.16.1.99. PC1 está enviando una trama L2 con una dirección NIC de destino de R1 y

una dirección NIC de origen de su propia NIC. La trama está encapsulando un paquete IP L3 con una dirección IP de origen 192.168.1.110 y una dirección IP de destino 172.16.1.99.





La dirección de la capa de enlace de datos solo se usa para la entrega local. Las direcciones en esta capa no tienen significado más allá de la red local. Compare esto con la Capa 3, en donde las direcciones en el encabezado del paquete pasan del host de origen al host de destino, sin tener en cuenta la cantidad de saltos de redes a lo largo de la ruta.

Si los datos deben pasar a otro segmento de red, se necesita un dispositivo intermediario, como un router. El router debe aceptar la trama según la dirección física y desencapsularla para examinar la dirección jerárquica, o dirección IP. Usando la dirección IP, el router puede determinar la ubicación de red del dispositivo de destino y la mejor ruta para llegar a él. Una vez que sabe adónde reenviar el paquete, el router crea una nueva trama para el paquete, y la nueva trama se envía al segmento de red siguiente hacia el destino final.

6.3.4

Tramas LAN y WAN

Los protocolos Ethernet son utilizados por LAN cableadas. Las comunicaciones inalámbricas caen bajo los protocolos WLAN (IEEE 802.11). Estos protocolos fueron diseñados para redes multiacceso.

Tradicionalmente, los WAN utilizaban otros tipos de protocolos para varios tipos de topologías punto a punto, hub-spoke y de malla completa. Algunos de los protocolos WAN comunes a lo largo de los años han incluido:

- Protocolo punto a punto (PPP)
- Control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control)
- Frame Relay
- Modo de transferencia asíncrona (ATM)
- X.25

Estos protocolos de capa 2 ahora están siendo reemplazados en la WAN por Ethernet.

En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3. Sin embargo, el protocolo de capa 2 específico que se utilice depende de la topología lógica y de los medios físicos.

Cada protocolo realiza el control de acceso a los medios para las topologías lógicas de Capa 2 que se especifican. Esto significa que una cantidad de diferentes dispositivos de red puede actuar como nodos que operan en la capa de enlace de datos al implementar estos protocolos. Estos dispositivos incluyen las tarjetas de interfaz de red en PC, así como las interfaces en routers y en switches de la Capa 2.

El protocolo de la Capa 2 que se utiliza para una topología de red particular está determinado por la tecnología utilizada para implementar esa topología. La tecnología está, a su vez, determinada por el tamaño de la red, en términos de cantidad de hosts y alcance geográfico y los servicios que se proveerán a través de la red.

Una LAN generalmente usa una tecnología de alto ancho de banda capaz de soportar grandes cantidades de hosts. El área geográfica relativamente pequeña de una LAN (un solo edificio o un campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

Sin embargo, utilizar una tecnología de ancho de banda alto no es generalmente rentable para redes de área extensa que cubren grandes áreas geográficas (varias ciudades, por ejemplo). El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias, generalmente, ocasiona una menor capacidad de ancho de banda.

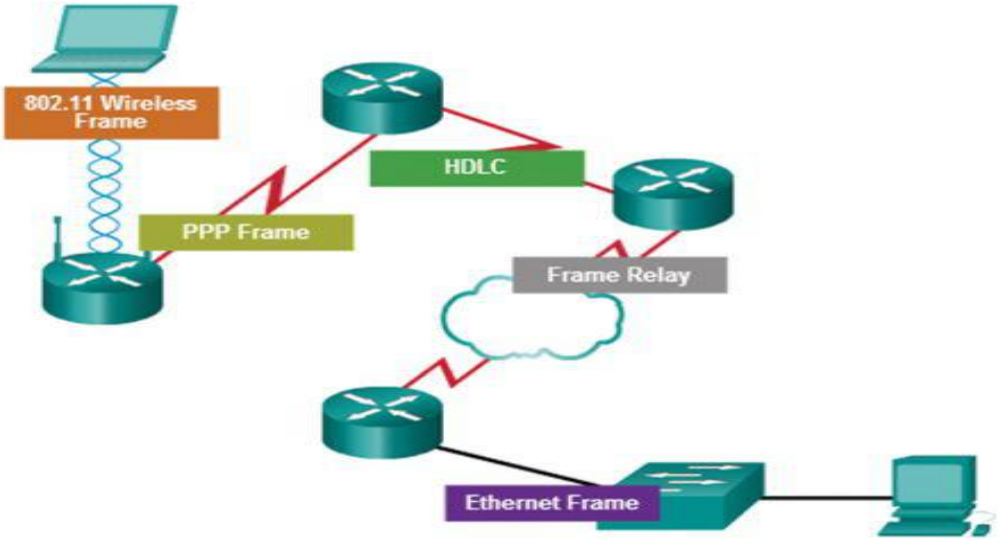
La diferencia de ancho de banda normalmente produce el uso de diferentes protocolos para las LAN y las WAN.

Los protocolos de la capa de enlace de datos incluyen:

- Ethernet
- 802.11 inalámbrico
- Protocolo punto a punto (PPP)
- Control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control)
- Frame Relay

Haga clic en el botón Reproducir para ver ejemplos de protocolos de capa 2.

Una representación de una red formada por LAN y WAN interconectadas



6.3.5

Compruebe su comprensión — Trama de enlace de datos

Verifique su comprensión de las topologías eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La capa de vínculo de datos agrega un encabezado que contiene la dirección de capa 2 de origen y destino y un trailer que contiene una secuencia de comprobación de trama (FCS).
2. El último campo dla trama de enlace de datos es la secuencia de comprobación de trama (FCS) que se utiliza para determinar si la trama ha experimentado errores de transmisión.
3. El orden correcto de los campos de dirección de capa 2 y capa 3 es: dirección NIC de destino, dirección NIC de origen, dirección IP de origen, dirección IP de destino
4. 802.11, Ethernet y PPP son protocolos de capa 2. IP es Capa 3 y UDP es Capa 4.

Has tenido 4 respuestas correctas de 4.

1. ¿Qué agrega la capa de enlace de datos a un paquete de capa 3 para crear una trama? (Escoja dos.)

¡Lo tienes!

- [ ] Señaladores
- [ ] número de secuencia
- [x] encabezado
- [x] Tráiler

2. ¿Cuál es la función del último campo en una trama de capa de enlace de datos?

¡Lo tienes!

- (•) Para determinar si la trama experimentó errores de transmisión
- ( ) Identificar servicios especiales de control de flujo, como la calidad de servicio (QoS)
- ( ) Para identificar los límites inicial y final dla trama
- ( ) Identifica el protocolo de capa 3 en el campo de datos.

3. ¿Qué enumera los campos de dirección de Capa 2 y Capa 3 en el orden correcto?

¡Lo tienes!

- (•) dirección NIC de destino, dirección NIC de origen, dirección IP de origen, dirección IP de destino
- ( ) dirección NIC de origen, dirección NIC de destino, dirección IP de origen, dirección IP de destino
- ( ) dirección NIC de destino, dirección NIC de origen, dirección IP de destino, dirección IP de origen
- ( ) dirección NIC de origen, dirección NIC de destino, dirección IP de destino, dirección IP de origen

4. ¿Cuáles de los siguientes son protocolos de capa de enlace de datos? (Elija tres)

¡Lo tienes!

- [x] 802.11
- [x] Ethernet
- [ ] IP
- [x] PPP
- [ ] UDP

Correct

You have successfully identified the correct answers.

1. The data link layer adds a header which contains the source and destination Layer 2 address and a trailer that contains a frame check sequence (FCS).
2. The last field in the data link frame is the frame check sequence (FCS) which is used to determine if the frame has experienced transmission errors.
3. The correct order of Layer 2 and Layer 3 address fields is: destination NIC address, source NIC address, source IP address, destination IP address
4. 802.11, Ethernet, and PPP are Layer 2 protocols. IP is Layer 3 and UDP is Layer 4.

You got 4 out of 4 questions correct.

1. What does the data link layer add to a Layer 3 packet to create a frame? (Choose two.)

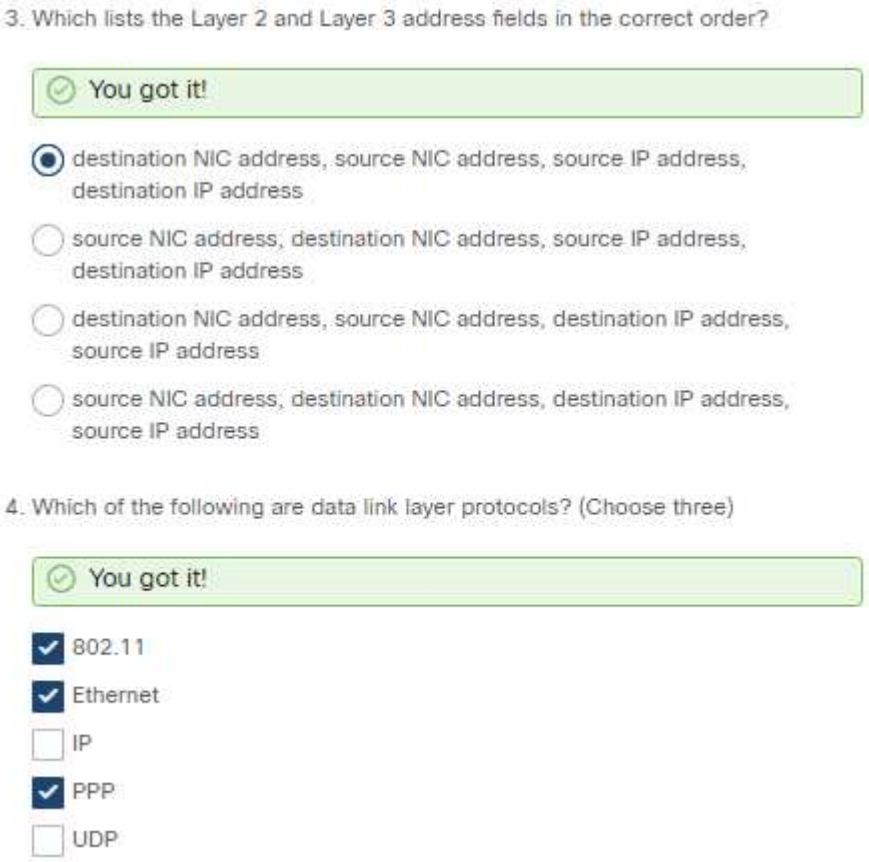
You got it!

- [ ] flags
- [ ] sequence number
- [x] header
- [x] trailer

2. What is the function of the last field in a data link layer frame?

You got it!

- (•) To determine whether the frame experienced transmission errors
- ( ) To identify special flow control services such as quality of service (QoS)
- ( ) To identify the beginning and end limits of the frame
- ( ) To identify the Layer 3 protocol in the data field



Módulo de Práctica y Prueba

6.4.1

¿Qué aprenderé en este módulo?

Propósito de la capa de enlace de datos

La capa de enlace de datos del modelo OSI (Capa 2) prepara los datos de la red para la red física. La capa de enlace de datos es responsable de las comunicaciones de tarjeta de interfaz de red (NIC) a tarjeta de interfaz de red. Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. La capa de enlace de datos IEEE 802 LAN/MAN consta de las dos subcapas siguientes: LLC y MAC. La subcapa MAC proporciona encapsulación de datos a través de la delimitación de tramas, direccionamiento y detección de errores. Las interfaces del router encapsulan el paquete en la trama apropiada.

Se utiliza un método adecuado de control de acceso a los medios para acceder a cada enlace. Las organizaciones de ingeniería que definen estándares abiertos y protocolos que se aplican a la capa de acceso a la red incluyen: IEEE, ITU, ISO y ANSI.

Topologías

Los dos tipos de topologías utilizadas en redes LAN y WAN son físicas y lógicas. La capa de enlace de datos "ve" la topología lógica de una red al controlar el acceso de datos a los medios. La topología lógica influye en el tipo de trama de red y el control de acceso a medios utilizado. Tres tipos comunes de topologías WAN físicas son: punto a punto, hub-spoke, y malla. Las topologías físicas punto a punto conectan directamente dos dispositivos finales (nodos). Agregar conexiones físicas intermedias puede no cambiar la topología lógica. En las LAN de acceso múltiple, los nodos están interconectados mediante topologías estrella o estrella extendida. En este tipo de topología, los nodos están conectados a un dispositivo intermediario central. Las topologías de LAN físicas incluyen: estrella, estrella extendida, bus y anillo. Las comunicaciones semidúplex intercambian datos en una dirección a la vez. Full-duplex envía y recibe datos simultáneamente. Dos interfaces interconectadas deben utilizar el mismo modo dúplex o habrá una falta de coincidencia dúplex que creará ineficiencia y latencia en el enlace. Las LAN Ethernet y WLAN son un ejemplo de una red de accesos múltiples. Una red de acceso múltiple es una red que puede tener varios nodos que acceden a la red simultáneamente. Algunas redes de acceso múltiple requieren reglas que rijan la forma de compartir los medios físicos. Existen dos métodos básicos de control de acceso para medios compartidos: el acceso basado en contencion y el acceso controlado. En redes multiacceso basadas en contencion, todos los nodos funcionan en semidúplex. Hay un proceso si más de un dispositivo transmite al mismo tiempo. Ejemplos de métodos de acceso basados en contencion incluyen: CSMA/CD para LAN Ethernet de topología de bus y CSMA/CA para WLAN.

Marco de enlace de datos

La capa de enlace de datos prepara los datos encapsulados (generalmente un paquete IPv4 o IPv6) para el transporte a través de los medios locales encapsulándolos con un encabezado y un trailer para crear una trama. El protocolo de enlace de datos es responsable de las comunicaciones de NIC a NIC dentro de la misma red. Existen muchos protocolos diferentes de capa de enlace de datos que describen marcos de capa de enlace de datos, cada tipo de marco tiene tres partes básicas: encabezado, datos y trailer. A diferencia de otros protocolos de encapsulación, la capa de enlace de datos anexa información en el tráiler. No hay una estructura de trama que cumpla con las necesidades de todos los transportes de datos a través de todos los tipos de medios. Según el entorno, la cantidad de información de control que se necesita en la trama varía para cumplir con los requisitos de control de acceso al medio de la topología lógica y de los medios. Los campos de trama incluyen: indicadores de inicio y parada de trama, direccionamiento, tipo, control, datos y detección de errores. La capa de enlace de datos proporciona direccionamiento utilizado para transportar un marco a través de medios locales compartidos. Las direcciones de dispositivo en esta capa son direcciones físicas. El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local. La dirección de la capa

de enlace de datos solo se usa para la entrega local. En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3. Sin embargo, el protocolo de capa 2 específico que se utilice depende de la topología lógica y de los medios físicos. Cada protocolo realiza el control de acceso a los medios para las topologías lógicas de Capa 2 que se especifican. El protocolo de la Capa 2 que se utiliza para una topología de red particular está determinado por la tecnología utilizada para implementar esa topología. Los protocolos de capa de enlace de datos incluyen: Ethernet, 802.11 Wireless, PPP, HDLC y Frame Relay.

6.4.2

Prueba del módulo — Capa de enlace de datos

Correct

You have successfully identified the correct answers.

Has tenido 14 respuestas correctas de 14.

1. ¿Qué identificador se utiliza en la capa de enlace de datos para identificar de forma única un dispositivo Ethernet?

Tema 6.3.0 - Las tramas Ethernet se identifican en la capa de enlace de datos por sus direcciones MAC, que son exclusivas de cada NIC. Las direcciones IP se utilizan en la capa de red y los números de puerto TCP y UDP se utilizan en la capa de transporte. Los números de secuencia son campos en encabezados TCP.

- ○ Dirección IP
- ◉ Dirección MAC
- ○ número de secuencia
- ○ Número de puerto TCP
- ○ Número de puerto UDP

2. ¿Qué dos organizaciones de ingeniería definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos? (Escoja dos.)

Tema 6.1.0 - La IANA es responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo. El EIA es una alianza internacional de estándares y comercio para organizaciones de electrónica, y es mejor conocido por sus estándares relacionados con el cableado eléctrico, los conectores y los racks de 19 pulgadas utilizados para montar equipos de red. El ISOC promueve el desarrollo abierto, la evolución y el uso de Internet en todo el mundo.

- ○ Organización Internacional para la Estandarización (ISO)
- ○ Autoridad de números asignados de Internet (IANA)
- ◉ Unión Internacional de Telecomunicaciones (ITU)
- ○ Asociación de Industrias Electrónicas (EIA)
- ○ Sociedad de Internet (ISOC)

3. ¿Qué capa del modelo OSI es responsable de especificar el método de encapsulación utilizado para tipos específicos de medios?

Tema 6.3.0 - La encapsulación es una función de la capa de enlace de datos. Los diferentes tipos de medios requieren una encapsulación de capa de enlace de datos diferente.

- [x] Aplicación
- [ ] Transporte
- [x] Enlace de datos
- [ ] Física
- [ ] Internet Society (ISOC)

4. ¿Qué es verdad con respecto a las topologías física y lógica?

Tema 6.2.0 - Las topologías físicas muestran la interconexión física de los dispositivos. Las topologías lógicas muestran la forma en que la red transfiere datos entre los nodos conectados.

- ( ) La topología lógica siempre es la misma que la topología física.
- ( ) Las topologías físicas se ocupan de cómo una red transmite las tramas.
- ( ) Las topologías físicas muestran el esquema de asignación de direcciones IP de cada red.
- (•) Las topologías lógicas se refieren a la forma en que una red transfiere datos entre dispositivos.

5. ¿Qué tipo de topología física se puede crear al conectar todos los cables de Ethernet a un dispositivo central?

Tema 6.2.0 - Los dispositivos conectados a la topología en estrella Ethernet se conectan a un hub o un switch.

- ( ) Bus
- ( ) Anillo
- (•) Estrella
- ( ) Malla

6. Se le pide a un técnico que cree una topología física para una red que proporcione un alto nivel de redundancia. ¿Qué topología física requiere que todos los nodos estén conectados a todos los demás nodos de la red?

Tema 6.2.0 - La topología de malla proporciona alta disponibilidad porque cada nodo está conectado a todos los demás nodos. Estas topologías se pueden encontrar en las WAN. También se puede utilizar una topología de malla parcial, en la que algunas terminales (no todas) se conectan entre sí.

- ( ) Bus
- ( ) Jerárquica
- (•) Malla
- ( ) Anillo
- ( ) Estrella

7. ¿Qué declaración describe el modo semidúplex de transmisión de datos?

Tema 6.2.0 - Los datos que se transmiten a través de la red pueden fluir utilizando uno de los tres modos:
- **Simplex** – Los datos sólo pueden fluir en una dirección.
- **Half-duplex** - Los datos fluyen en una dirección a la vez.
- **Full-duplex** - Los datos fluyen en ambas direcciones al mismo tiempo.

- ○ Los datos que se transmiten a través de la red solo pueden fluir en una dirección.
- ◉ Los datos que se transmiten a través de la red fluyen en una dirección a la vez.
- ○ Los datos que se transmiten a través de la red fluyen en una dirección a muchos destinos diferentes simultáneamente.
- ○ Los datos que se transmiten a través de la red fluyen en ambas direcciones al mismo tiempo.

8. ¿Cuál es una función de la subcapa de control de enlace lógico (LLC)?

Tema 6.1.0 - Definir los procesos de acceso a medios que realiza el hardware y proporcionar direccionamiento de capa de enlace de datos son funciones de la subcapa MAC. La capa de enlace de datos acepta paquetes de Capa 3 y los empaqueta en unidades de datos denominadas tramas.

- ○ definir los procesos de acceso a medios que realiza el hardware
- ○ proporcionar direccionamiento de la capa de enlace de datos.
- ◉ identificar qué protocolo de capa de red se está utilizando
- ○ aceptar segmentos y empaquetarlos en unidades de datos denominadas paquetes

9. ¿Qué método de control de acceso a medios de capa de enlace de datos utiliza Ethernet?

Tema 6.2.0 - CSMA/CD es utilizado por redes Ethernet.CSMA/CA es utilizado por redes inalámbricas basadas en 802.11.

- ◉ CSMA/CD
- ○ determinismo
- ○ toma de turno
- ○ paso de token

10. ¿Cuáles son las dos subcapas de la capa de enlace de datos del modelo OSI? (Escoja dos.)

Tema 6.1.0 - La capa de enlace de datos del modelo OSI se divide en dos subcapas: la subcapa Control de acceso al medio (MAC) y la subcapa Control de enlace lógico (LLC).

- [ ] Internet
- [ ] Física
- [x] LLC
- [ ] Transporte
- [x] MAC
- [ ] Acceso a la red

11. ¿Qué método se utiliza para administrar el acceso por contienda en una red inalámbrica?

Tema 6.2.0 - El acceso múltiple de detección de operador con prevención de colisión (CSMA / CA) se utiliza con tecnología de red inalámbrica para mediar en la contención de medios. El acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) se utiliza con la tecnología Ethernet por cable para mediar la contienda de medios. El orden de prioridad y el paso de tokens no se utilizan (o no son un método) para el control de acceso a medios.

- ( ) application
- ( ) Orden de prioridades
- (•) data link
- ( ) Paso de tokens

12. ¿Cuáles de los siguientes son dos servicios realizados por la capa de enlace de datos del modelo OSI? (Escoja dos.)

Tema 6.1.0 - La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de un medio de red físico. Específicamente, la capa de enlace de datos realiza estos dos servicios básicos:
- Acepta paquetes de Capa 3 y los encapsula en tramas.
- Controla el acceso al medio y realiza la detección de errores.

La determinación de rutas es un servicio que proporciona la capa 3. Un switch de capa 2 arma una tabla de direcciones MAC como parte de su operación, pero la capa de enlace de datos no proporciona el servicio de determinación de rutas.

- ( ) Encripta los paquetes de datos.
- ( ) Determina la ruta para reenviar los paquetes.
- (•) Acepta paquetes de capa 3 y los encapsula en tramas.
- ( ) Controla el acceso al medio y realiza la detección de errores.

13. ¿Qué hace un router después de desencapsular una trama recibida?

Tema 6.3.0 - Los routers son responsables de encapsular una trama con un formato adecuado para los medios de red físicos que conectan los routers. En cada salto a lo largo del camino, un router hace lo siguiente:
1. Aceptan una trama proveniente de un medio.
2. Desencapsulan la trama.
3. Determina la mejor ruta para reenviar el paquete
4. Vuelven a encapsular el paquete en una trama nueva.
5. Reenvían la nueva trama adecuada al medio de ese segmento de la red física.

- [ ] Determina la mejor ruta
- [ ] Desencapsulan la trama.
- [x] vuelve a encapsular el paquete en una nueva trama
- [x] reenvía la nueva trama al medio de red
- [ ] It monitors the Layer 2 communication by building a MAC address table.

14. ¿Qué atributo de una NIC lo colocaría en la capa de enlace de datos del modelo OSI?

Tema 6.3.0 - La capa de vínculo de datos describe el acceso a medios y el direccionamiento físico. La codificación de una dirección MAC en una NIC la coloca en esa capa. Los puertos y cables se colocan en la capa física del modelo OSI. Las direcciones IP se colocan en la capa de red. La pila de protocolos TCP/IP describe un modelo diferente.

- ( ) Conectar el cable de Ethernet.
- ( ) Dirección IP
- (•) Dirección MAC
- ( ) Puerto RJ-45
- ( ) Pila del protocolo TCP/IP

15. Aunque CSMA/CD sigue siendo una característica de Ethernet, ¿por qué ya no es necesario?

Tema 6.2.0 - El uso de switches de capa 2 que funcionan en modo dúplex completo elimina las colisiones, eliminando así la necesidad de CSMA/CD.

- ( ) la disponibilidad prácticamente ilimitada de direcciones IPv6
- ( ) el uso de CSMA/CA
- (•) el uso de switches de capa 2 con capacidad de dúplex completo
- ( ) el desarrollo de la operación de switch semidúplex
- ( ) el uso de velocidades Gigabit Ethernet

1. What identifier is used at the data link layer to uniquely identify an Ethernet device?

Topic 6.3.0 - Ethernet frames are identified at the data link layer by their MAC addresses, which are unique to each NIC. IP addresses are used at the network layer, and TCP and UDP port numbers are used at the transport layer. Sequence numbers are fields in TCP headers.

- ○ IP address
- ◉ MAC address
- ○ sequence number
- ○ TCP port number
- ○ UDP port number

2. What attribute of a NIC would place it at the data link layer of the OSI model?

Topic 6.3.0 - The data link layer describes media access and physical addressing. The encoding of a MAC address on a NIC places it at that layer. Ports and cables are placed at the physical layer of the OSI model. IP addresses are placed at the network layer. The TCP/IP protocol stack describes a different model.

- ○ attached Ethernet cable
- ○ IP address
- ◉ MAC address
- ○ RJ-45 port
- ○ TCP/IP protocol stack

3. Which two engineering organizations define open standards and protocols that apply to the data link layer? (Choose two.)

Topic 6.1.0 - The IANA is responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers. The EIA is an international standards and trade alliance for electronics organizations, and is best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment. IEEE defines open standards and protocols that apply to the network access layer.

- ☑ Institute of Electrical and Electronics Engineers (IEEE)
- ☐ Internet Assigned Numbers Authority (IANA)
- ☑ International Telecommunication Union (ITU)
- ☐ Electronic Industries Alliance (EIA)
- ☐ Internet Society (ISOC)

4. What is true concerning physical and logical topologies?

Topic 6.2.0 - Physical topologies show the physical interconnection of devices. Logical topologies show the way the network will transfer data between connected nodes.

- ○ The logical topology is always the same as the physical topology.
- ○ Physical topologies are concerned with how a network transfers frames.
- ○ Physical topologies display the IP addressing scheme of each network.
- ◉ Logical topologies refer to how a network transfers data between devices.

5. What method is used to manage contention-based access on a wireless network?

Topic 6.2.0 - Carrier sense multiple access with collision avoidance (CSMA/CA) is used with wireless networking technology to mediate media contention. Carrier sense multiple access with collision detection (CSMA/CD) is used with wired Ethernet technology to mediate media contention. Priority ordering and token passing are not used (or not a method) for media access control.

- ○ CSMA/CD
- ○ priority ordering
- ◉ CSMA/CA
- ○ token passing

6. A technician has been asked to develop a physical topology for a network that provides a high level of redundancy. Which physical topology requires that every node is attached to every other node on the network?

Topic 6.2.0 - The mesh topology provides high availability because every node is connected to all other nodes. Mesh topologies can be found in WANs. A partial mesh topology can also be used where some, but not all, end points connect to one another.

- ○ bus
- ○ hierarchical
- ◉ mesh
- ○ ring
- ○ star

7. Which statement describes the half-duplex mode of data transmission?

Topic 6.2.0 - The data that is transmitted over the network can flow using one of three modes:
- **Simplex** - Data can only flow in one direction.
- **Half-duplex** - Data flows in one direction at a time.
- **Full-duplex** - Data flows in both directions at the same time.

- ○ Data that is transmitted over the network can only flow in one direction.
- ◉ Data that is transmitted over the network flows in one direction at a time.
- ○ Data that is transmitted over the network flows in one direction to many different destinations simultaneously.
- ○ Data that is transmitted over the network flows in both directions at the same time.

8. Which is a function of the Logical Link Control (LLC) sublayer?

Topic 6.1.0 - Defining the media access processes that are performed by the hardware and providing data link layer addressing are functions of the MAC sublayer. The data link layer accepts Layer 3 packets and packages them into data units that are called frames.

- ○ to define the media access processes that are performed by the hardware
- ○ to provide data link layer addressing
- ◉ to identify which network layer protocol is being used
- ○ to accept segments and package them into data units that are called packets

9. Which data link layer media access control method does Ethernet use with legacy Ethernet hubs?

Topic 6.2.0 - CSMA/CD is used by Ethernet networks using legacy Ethernet hubs. CSMA/CA is used by 802.11-based wireless networks.

- ◉ CSMA/CD
- ○ determinism
- ○ turn taking
- ○ token passing

10. What are the two sublayers of the OSI model data link layer? (Choose two.)

Topic 6.1.0 - The data link layer of the OSI model is divided into two sublayers: the Media Access Control (MAC) sublayer and the Logical Link Control (LLC) sublayer.

- [ ] internet
- [ ] physical
- [x] LLC
- [ ] transport
- [x] MAC
- [ ] network access

11. Which layer of the OSI model is responsible for specifying the encapsulation method used for specific types of media?

Topic 6.3.0 - Encapsulation is a function of the data link layer. Different media types require different data link layer encapsulation.

- ( ) application
- ( ) transport
- (•) data link
- ( ) physical

12. What type of physical topology can be created by connecting all Ethernet cables to a central device?

Topic 6.2.0 - Devices connected to the Ethernet star topology connect to either a hub or a switch.

- ( ) bus
- ( ) ring
- (•) star
- ( ) mesh

13. What are two services performed by the data link layer of the OSI model? (Choose two.)

Topic 6.1.0 – The data link layer is responsible for the exchange of frames between nodes over a physical network media. Specifically the data link layer performs two basic services:
- It accepts Layer 3 packets and encapsulates them into frames.
- It provides media access control and performs error detection.

Path determination is a service provided at Layer 3. A Layer 2 switch builds a MAC address table as part of its operation, but path determination is not the service that is provided by the data link layer.

- [ ] It fragments data packets into the MTU size.
- [ ] It determines the path to forward packets.
- [x] It accepts Layer 3 packets and encapsulates them into frames.
- [x] It provides media access control and performs error detection.
- [ ] It monitors the Layer 2 communication by building a MAC address table.

14. Although CSMA/CD is still a feature of Ethernet, why is it no longer necessary?

Topic 6.2.0 – The use of Layer 2 switches operating in full-duplex mode eliminates collisions, thereby eliminating the need for CSMA/CD.

- ( ) the virtually unlimited availability of IPv6 addresses
- ( ) the use of CSMA/CA
- (•) the use of full-duplex capable Layer 2 switches
- ( ) the development of half-duplex switch operation
- ( ) the use of Gigabit Ethernet speeds

Capítulo 7_Switching Ethernet

Introducción

7.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Ethernet Switching!

Si planea convertirse en administrador de red o arquitecto de red, definitivamente necesitará saber acerca de la Ethernet Switching y Ethernet. Las dos tecnologías LAN más destacadas que se utilizan hoy en día son Ethernet y WLAN. Ethernet admite anchos de banda de hasta 100 Gbps, lo que explica su popularidad. Este módulo contiene un laboratorio que utiliza Wireshark en el que puede ver tramas Ethernet y otro laboratorio donde ver direcciones MAC

de dispositivos de red. También hay algunos vídeos instructivos para ayudarle a comprender mejor Ethernet. Para cuando haya terminado este módulo, usted también podría crear una red conmutada que use Ethernet.

7.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Switching Ethernet

Objetivos del módulo: Explique cómo funciona Ethernet en una red switched.

Título del tema	Objetivo del tema
Trama de Ethernet	Explique la forma en que las subcapas de Ethernet se relacionan con los campos de trama.
Dirección MAC de Ethernet	Describa la dirección MAC de Ethernet.
La tabla de direcciones MAC	Explique la forma en que un switch arma su tabla de direcciones MAC y reenvía las tramas.
Velocidades y métodos de reenvío del switch	Describa los métodos de reenvío de switch y la configuración de puertos disponibles para los puertos de switch en la capa 2 puertos de switch.

Switching Ethernet / Tramas de Ethernet

Tramas de Ethernet

7.1.1

Encapsulamiento de Ethernet

Este módulo comienza con una discusión de la tecnología Ethernet incluyendo una explicación de la subcapa MAC y los campos de trama Ethernet.

Ethernet es una de las dos tecnologías LAN utilizadas hoy en día, siendo la otra LAN inalámbricas (WLAN). Ethernet utiliza comunicaciones por cable, incluyendo pares trenzados, enlaces de fibra óptica y cables coaxiales.

Ethernet funciona en la capa de enlace de datos y en la capa física. Es una familia de tecnologías de red definidas en los estándares IEEE 802.2 y 802.3. Ethernet soporta los siguientes anchos de banda de datos:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10.000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

Como se muestra en la figura, los estándares de Ethernet definen tanto los protocolos de Capa 2 como las tecnologías de Capa 1.

Ethernet y el modelo OSI

Ethernet se define mediante protocolos de capa física y de capa de enlace de datos.

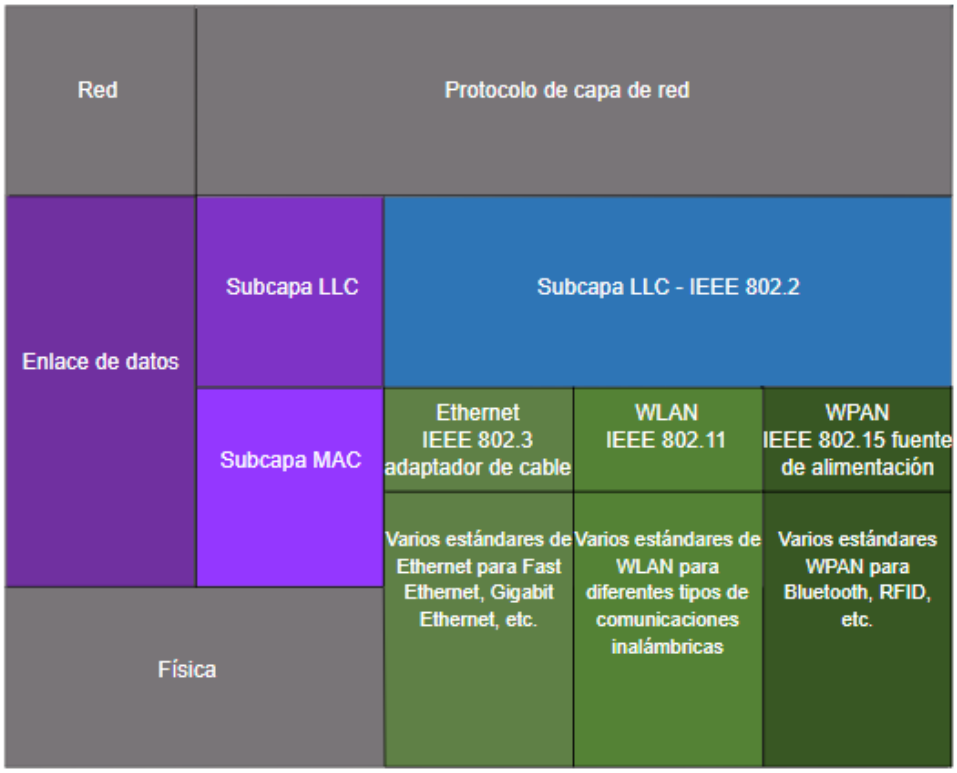
7.1.2

Subcapas de enlace de datos

Los protocolos IEEE 802 LAN/MAN, incluyendo Ethernet, utilizan las dos subcapas independientes siguientes de la capa de enlace de datos para operar. Son el Control de enlace lógico (LLC) y el Control de acceso a medios (MAC), como se muestra en la figura.

Recuerde que LLC y MAC tienen los siguientes roles en la capa de enlace de datos:

- **Subcapa LLC** - Esta subcapa IEEE 802.2 se comunica entre el software de red en las capas superiores y el hardware del dispositivo en las capas inferiores. Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que múltiples protocolos de Capa 3, como IPv4 e IPv6, utilicen la misma interfaz de red y medios.
- **Subcapa MAC** - Esta subcapa (IEEE 802.3, 802.11 o 802.15, por ejemplo) se implementa en hardware y es responsable de la encapsulación de datos y control de acceso a medios. Proporciona direccionamiento de capa de enlace de datos y está integrado con varias tecnologías de capa física.



El diagrama muestra la red OSI, el vínculo de datos y las capas físicas. También muestra las subcapas de capa de enlace de datos LLC y MAC y varios protocolos LAN/WAN. En la parte superior del diagrama se encuentra la capa de red y el protocolo de capa de red. Debajo de eso está la capa de enlace de datos y sus subcapas. La subcapa superior es la subcapa LLC como se especifica en IEEE 802.2. A continuación se muestra la subcapa MAC con tres columnas que representan diferentes tipos de tecnologías de red. La primera columna es Ethernet IEEE 802.3 en la parte superior de la subcapa MAC. Debajo de esto hay varios estándares Ethernet para Fast Ethernet, Gigabit Ethernet, etc. que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. La siguiente columna es WLAN IEEE 802.11 en la parte superior de la subcapa MAC. Debajo de esto se encuentran los diversos estándares WLAN para diferentes tipos de comunicaciones inalámbricas que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. La última columna es WPAN IEEE 802.15 en la parte superior de la subcapa MAC. Debajo de esto hay varios estándares WPAN para Bluetooth, RFID, etc. que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI.

7.1.3

Subcapa MAC

La subcapa MAC es responsable de la encapsulación de datos y el acceso a los medios.

Encapsulación de datos

La encapsulación de datos IEEE 802.3 incluye lo siguiente:

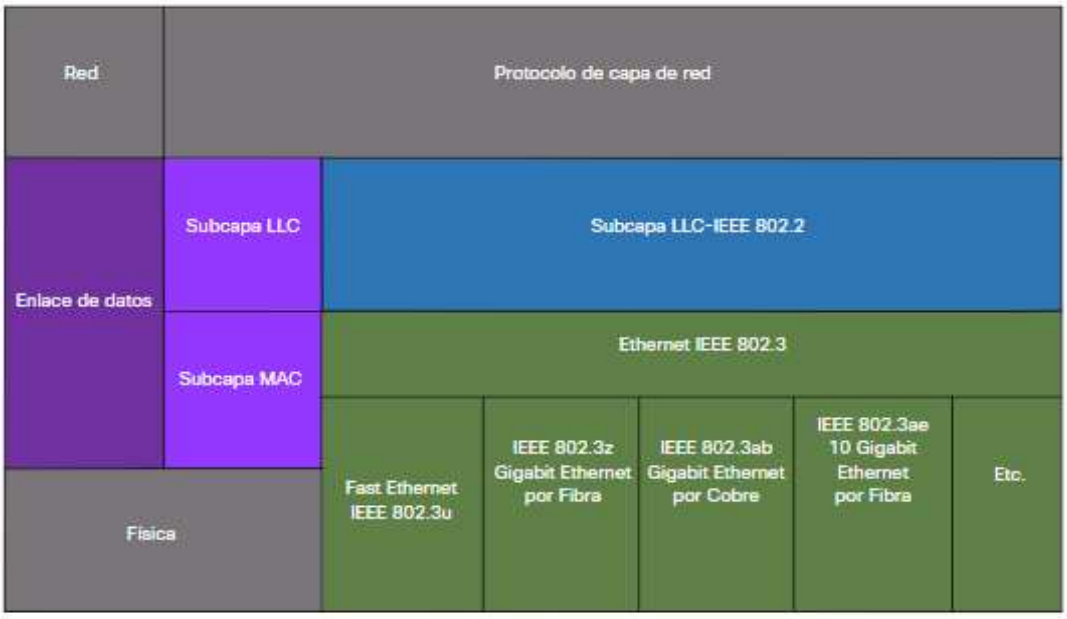
- **Trama de Ethernet** - Esta es la estructura interna de la trama Ethernet.
- **Direccionamiento Ethernet**: la trama Ethernet incluye una dirección MAC de origen y destino para entregar la trama Ethernet de NIC Ethernet a NIC Ethernet en la misma LAN.
- **Detección de errores Ethernet**: La trama Ethernet incluye un avance de secuencia de verificación de trama (FCS) utilizado para la detección de errores.

Accediendo a los medios

Como se muestra en la figura, la subcapa MAC IEEE 802.3 incluye las especificaciones para diferentes estándares de comunicaciones Ethernet sobre varios tipos de medios, incluyendo cobre y fibra.

El diagrama muestra varios estándares Ethernet en la subcapa MAC. En la parte superior del diagrama se encuentra la capa de red y el protocolo de capa de red. Debajo de eso está la capa de enlace de datos y sus subcapas. La subcapa superior es la subcapa IEEE 802.2 LLC. La siguiente es la subcapa MAC Ethernet IEEE 802.3. Debajo hay cinco columnas con varios estándares Ethernet y tipos de medios que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. De izquierda a derecha, las columnas son: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet sobre fibra; IEEE 802.ab Gigabit Ethernet sobre cobre; IEEE 802.3ae 10 Gigabit Ethernet sobre fibra; y Etc.

Estándares Ethernet en la subcapa MAC



Recuerde que Ethernet heredado utiliza una topología de bus o hubs, es un medio compartido, medio dúplex. Ethernet a través de un medio medio dúplex utiliza un método de acceso basado en contencion, detección de accesos múltiples/detección de colisiones (CSMA/CD) Esto garantiza que sólo un dispositivo esté transmitiendo a la vez. CSMA/CD permite que varios dispositivos compartan el mismo medio medio dúplex, detectando una colisión cuando más de un dispositivo intenta transmitir simultáneamente. También proporciona un algoritmo de retroceso para la retransmisión.

Las LAN Ethernet de hoy utilizan switches que funcionan en dúplex completo. Las comunicaciones dúplex completo con switches Ethernet no requieren control de acceso a través de CSMA/CD.

7.1.4

Campos de trama de Ethernet

El tamaño mínimo de trama de Ethernet es de 64 bytes, y el máximo es de 1518 bytes. Esto incluye todos los bytes del campo de dirección MAC de destino a través del campo de secuencia de verificación de trama (FCS). El campo preámbulo no se incluye al describir el tamaño de una trama.

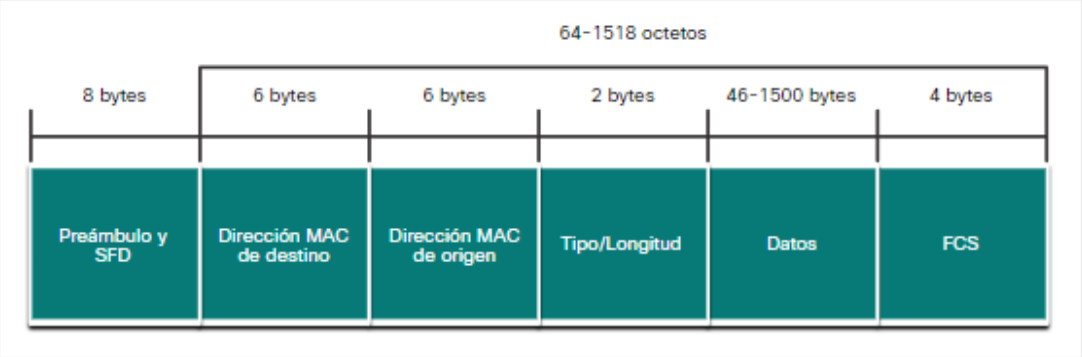
Cualquier trama de menos de 64 bytes de longitud se considera un fragmento de colisión o una trama corta, y es descartada automáticamente por las estaciones receptoras. Las tramas de más de 1500 bytes de datos se consideran "jumbos" o tramas bebés gigantes.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas. Ellas se consideran inválidas Las tramas jumbo suelen ser compatibles con la mayoría de los switches y NIC Fast Ethernet y Gigabit Ethernet.

La figura muestra cada campo en la trama Ethernet. Consulte la tabla para obtener más información sobre la función de cada campo.

El diagrama muestra los campos de una trama Ethernet. De izquierda a derecha, los campos y su longitud son: Preámbulo y SFD, 8 bytes; Dirección MAC de destino, 6 bytes; Dirección MAC de origen, 6 bytes; Tipo/longitud, 2 bytes; datos, 45 - 1500 bytes; y FCS, 4 bytes. Excluyendo el primer campo, el número total de bytes en los campos restantes está entre 64 y 1518.

Campos de trama de Ethernet



Detalle de campos de trama de Ethernet

Campo	Descripción
Campos Preámbulo y Delimitador de inicio de trama	El Preámbulo (7 bytes) y el Delimitador de tramas de inicio (SFD), también llamado Inicio de Trama (1 byte), los campos se utilizan para la sincronización entre el envío y recepción de dispositivos. Estos primeros ocho bytes de trama son utilizados para llamar la atención de los nodos receptores. Esencialmente, los primeros cuantos bytes le dicen a los receptores que se preparen para recibir una nueva trama.

Campo	Descripción
Campo Dirección MAC de destino	Este campo de 6 bytes es el identificador del destinatario deseado. Como usted recordará, esta dirección es utilizada por la capa 2 para ayudar a los dispositivos en determinar si una trama está dirigida a ellos. La dirección en la trama es comparada con la dirección MAC en el dispositivo. Si hay una coincidencia, el acepta la trama. Puede ser unicast, multicast o broadcast dirección.
Campo Dirección MAC de origen	Este campo de 6 bytes identifica la NIC o la interfaz de origen de la trama
Tipo/Longitud	Este campo de 2 bytes identifica el protocolo de capa superior encapsulado en la trama de Ethernet Los valores comunes son, en hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 y 0x806 para ARP. **Nota**: También puede ver este campo denominado como EtherType, Type o Length.
Campo de datos	Este campo (46 - 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU genérica de Capa 3, o más comúnmente, un IPv4 paquete. Todas las tramas deben tener, al menos, 64 bytes de longitud. Si un paquete pequeño es encapsulado, bits adicionales llamados pad se utilizan para aumentar el tamaño de la trama a este tamaño mínimo.
Campo Secuencia de verificación de trama	El campo Secuencia de verificación de trama (FCS) (4 bytes) se usa para detectar errores en una trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo de envío incluye los resultados de un CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar por errores. Si los cálculos coinciden, significa que no se produjo ningún error. Cálculos que no coinciden son una indicación de que los datos han cambiado; por lo tanto, la trama se descarta. Un cambio en los datos podría ser el resultado de una interrupción de las señales eléctricas que representan los bits.

7.1.5

Compruebe su comprensión - Ethernet Switching

Verifique su comprensión de las tramas de Ethernet eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Todas las tramas deben tener, al menos, 64 bytes de longitud. Los bits adicionales llamados "pad" se utilizan para aumentar el tamaño de de la trama al tamaño mínimo.
2. El campo FCS utiliza un CRC para detectar errores en una trama.
3. El campo EtherType identifica el protocolo de capa superior encapsulado en la trama de Ethernet.
4. Los primeros bytes del preámbulo informan al receptor de un nuevo trama.
5. La subcapa LLC es responsable de controlar la tarjeta de interfaz de red a través de controladores de software
6. La LLC trabaja con capas superiores para admitir protocolos de nivel superior.
7. La subcapa MAC comprueba si hay errores de bits, admite tecnologías Ethernet y controla el acceso a los medios.

Has tenido 7 respuestas correctas de 7.

1. ¿Qué parte de una trama Ethernet utiliza un pad para aumentar el campo de trama a al menos 64 bytes?

¡Lo tienes!

- EtherType
- Preámbulo
- Delimitador de inicio de trama
- (•) Campo de datos

2. ¿Qué parte de una trama Ethernet detecta errores en la trama?

¡Lo tienes!

- Preámbulo
- Delimitador de inicio de trama
- (•) Secuencia de verificación de trama

3. ¿Qué parte de una trama Ethernet describe el protocolo de capa superior encapsulado?

¡Lo tienes!

- (•) EtherType
- Preámbulo
- Delimitador de inicio de trama
- Secuencia de verificación de trama

4. ¿Qué parte de una trama Ethernet notifica al receptor que se prepare para una nueva trama?

¡Lo tienes!

- ( ) Delimitador de inicio de trama
- ( ) Secuencia de verificación de trama
- (•) Preámbulo
- ( ) Campo de datos

5. ¿Qué subcapa de enlace de datos controla la interfaz de red a través de controladores de software?

¡Lo tienes!

- ( ) MAC
- (•) LLC

6. ¿Qué subcapa de enlace de datos funciona con las capas superiores para agregar información de la aplicación para la entrega de datos a protocolos de nivel superior?

¡Lo tienes!

- ( ) MAC
- (•) LLC

7. ¿Qué es una función de la subcapa MAC? (Escoja tres).

¡Lo tienes!

- [x] Control de acceso a los medios
- [x] comprueba si hay errores en los bits recibidos
- [x] utiliza CSMA/CD o CSMA/CA para admitir la tecnología Ethernet
- [ ] se comunica entre el software en las capas superiores y el hardware del dispositivo en las capas inferiores
- [ ] permite que múltiples protocolos de Capa 3 utilicen la misma interfaz de red y medios

Correct

You have successfully identified the correct answers.

1. All frames must be at least 64 bytes long. Additional bits called a "pad" are used to increase the size of small frames to the minimum size.
2. The FCS field uses a CRC to detect errors in a frame.
3. The EtherType field identifies the upper layer protocol that is encapsulated in the Ethernet Frame.
4. The first few bytes of the preamble inform the receiver of a new frame.
5. The LLC sublayer is responsible for controlling the network interface card through software drivers
6. The LLC works with upper layers to support higher level protocols.
7. The MAC sublayer checks for bit errors, supports Ethernet technologies, and controls access to the media.

You got 7 out of 7 questions correct.

1. Which part of an Ethernet Frame uses a pad to increase the frame field to at least 64 bytes?

You got it!

- ○ EtherType
- ○ Preamble
- ○ Start of Frame Delimiter
- ◉ Data field

2. Which part of an Ethernet frame detects errors in the frame?

You got it!

- ○ Preamble
- ○ Start of Frame Delimiter
- ◉ Frame Check Sequence

3. Which part of an Ethernet Frame describes the higher-layer protocol that is encapsulated?

You got it!

- (●) EtherType
- ( ) Preamble
- ( ) Start of Frame Delimiter
- ( ) Frame Check Sequence

4. Which part of an Ethernet Frame notifies the receiver to get ready for a new frame?

You got it!

- ( ) Start of Frame Delimiter
- ( ) Frame Check Sequence
- (●) Preamble
- ( ) Data field

5. Which data link sublayer controls the network interface through software drivers?

You got it!

- ( ) MAC
- (●) LLC

6. Which data link sublayer works with the upper layers to add application information for delivery of data to higher level protocols?

You got it!

- ( ) MAC
- (●) LLC

7. What is a function of the MAC sublayer? (Choose three.)

You got it!

- [x] controls access to the media
- [x] checks for errors in received bits
- [x] uses CSMA/CD or CSMA/CA to support Ethernet technology
- [ ] communicates between software at the upper layers and the device hardware at the lower layers
- [ ] allows multiple Layer 3 protocols to use the same network interface and media

7.1.6

Lab - Utilizar Wireshark para examinar tramas de Ethernet

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Examinar los campos de encabezado de una trama de Ethernet II
- Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

Utilice Wireshark para examinar tramas de Ethernet

---

1. Switching Ethernet
2. Dirección MAC de Ethernet

Dirección MAC de Ethernet

7.2.1

Dirección MAC y hexadecimal

En redes, las direcciones IPv4 se representan utilizando el sistema de números de base decimal diez y el sistema de números base binaria 2. Las direcciones IPv6 y las direcciones Ethernet se representan utilizando el sistema de número hexadecimal de base dieciséis. Para entender hexadecimal, primero debe estar muy familiarizado con binario y decimal.

El sistema de numeración hexadecimal usa los números del 0 al 9 y las letras de la A a la F.

Una dirección MAC Ethernet consta de un valor binario de 48 bits. Hexadecimal se utiliza para identificar una dirección Ethernet porque un solo dígito hexadecimal representa cuatro bits binarios. Por lo tanto, una dirección MAC Ethernet de 48 bits se puede expresar utilizando sólo 12 valores hexadecimales.

La figura compara los valores decimales y hexadecimales equivalentes para el binario 0000 a 1111.

La figura es de tres columnas que muestran los equivalentes decimales y hexadecimales de los números binarios seleccionados de 4 bits. De izquierda a derecha, los encabezados de columna son: decimal, binario y hexadecimal. Cada columna tiene 16 filas debajo del encabezado.

Equivalentes decimales y binarios a los valores hexadecimales del 0 al F

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Dado que 8 bits (un byte) es un método de agrupación binaria común, los números binarios del 00000000 al 11111111 se pueden representar en hexadecimal como el rango del 00 al FF, como se muestra en la figura.

La figura es de tres columnas que muestran los equivalentes decimales y hexadecimales de los números binarios seleccionados de 8 bits. De izquierda a derecha, los encabezados de columna son: decimal, binario y hexadecimal. Cada columna tiene 18 filas debajo del encabezado.

Equivalentes decimales, binarios y hexadecimales seleccionados

Decimal	Binario	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Cuando se usa hexadecimal, los ceros iniciales siempre se muestran para completar la representación de 8 bits. Por ejemplo, en la tabla, el valor binario 0000 1010 se muestra en hexadecimal como 0A.

Los números hexadecimales suelen ser representados por el valor precedido por **0x** (por ejemplo, 0x73) para distinguir entre valores decimales y hexadecimales en la documentación.

El hexadecimal también puede estar representado por un subíndice 16, o el número hexadecimal seguido de una H (por ejemplo, 73H).

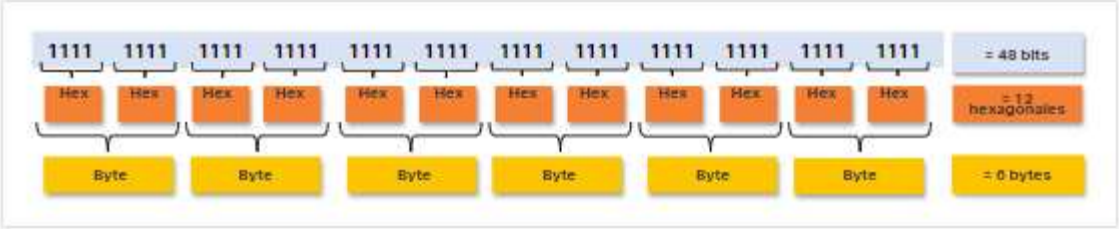
Es posible que tenga que convertir entre valores decimales y hexadecimales. Si es necesario realizar dichas conversiones, generalmente, es más fácil convertir el valor decimal o hexadecimal a un valor binario y, a continuación, convertir ese valor binario a un valor decimal o hexadecimal, según corresponda.

7.2.2

Dirección MAC de Ethernet

En una LAN Ethernet, cada dispositivo de red está conectado a los mismos medios compartidos. La dirección MAC se utiliza para identificar los dispositivos físicos de origen y destino (NIC) en el segmento de red local. El direccionamiento MAC proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI.

Una dirección MAC Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales, como se muestra en la figura. Debido a que un byte equivale a 8 bits, también podemos decir que una dirección MAC tiene 6 bytes de longitud.



El diagrama muestra que la dirección MAC se compone de 48 bits en total. Estos 48 bits se pueden dividir en doce grupos de 4 bits, o 12 dígitos hexadecimales. Combinando dos dígitos hexadecimales juntos hace un byte, por lo tanto, los 48 bits también son equivalentes a 6 bytes.

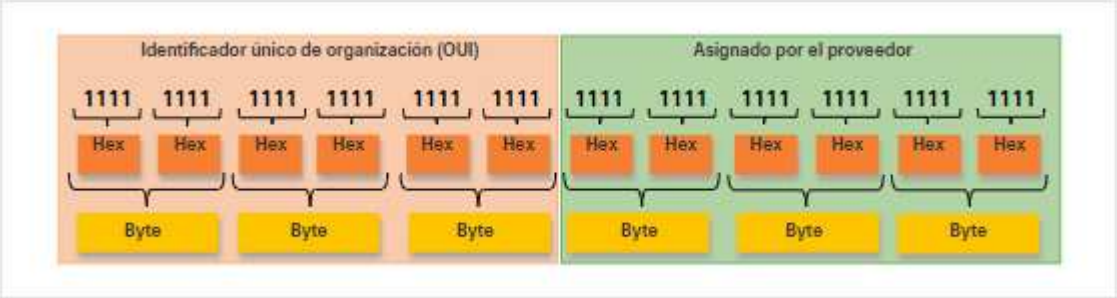
Todas las direcciones MAC deben ser únicas para el dispositivo Ethernet o la interfaz Ethernet. Para garantizar esto, todos los proveedores que venden dispositivos Ethernet deben registrarse con el IEEE para obtener un código hexadecimal único de 6 (es decir, 24 bits o 3 bytes) denominado identificador único de organización (OUI).

Cuando un proveedor asigna una dirección MAC a un dispositivo o interfaz Ethernet, el proveedor debe hacer lo siguiente:

- Utilice su OUI asignado como los primeros 6 dígitos hexadecimales.
- Asigne un valor único en los últimos 6 dígitos hexadecimales.

Por lo tanto, una dirección MAC Ethernet consiste en un código OUI de proveedor hexadecimal 6 seguido de un valor asignado por el proveedor hexadecimal 6, como se muestra en la figura.

Los primeros seis dígitos hexadecimales de una dirección MAC (también conocidos como los primeros 6 dígitos hexadecimales o los primeros 3 bytes) son el identificador único de la organización y los últimos seis dígitos hexadecimales están asignados por el proveedor.



Por ejemplo, suponga que Cisco necesita asignar una dirección MAC única a un nuevo dispositivo. El IEEE ha asignado a Cisco un OUI de **00-60-2F**. Cisco configuraría entonces el dispositivo con un código de proveedor único como **3A-07-BC**. Por lo tanto, la dirección MAC Ethernet de ese dispositivo sería **00-60-2F-3A-07-BC.**

Es responsabilidad del proveedor asegurarse de que ninguno de sus dispositivos tenga asignada la misma dirección MAC. Sin embargo, es posible que existan direcciones MAC duplicadas debido a errores cometidos durante la fabricación, errores cometidos en algunos métodos de implementación de máquinas virtuales o modificaciones realizadas con una de varias herramientas de software. En cualquier caso, será necesario modificar la dirección MAC con una nueva NIC o realizar modificaciones a través del software.

7.2.3

Procesamiento de tramas

A veces, la dirección MAC se conoce como una dirección grabada (BIA) porque la dirección está codificada en la memoria de solo lectura (ROM) en la NIC. Es decir que la dirección está codificada en el chip de la ROM de manera permanente.

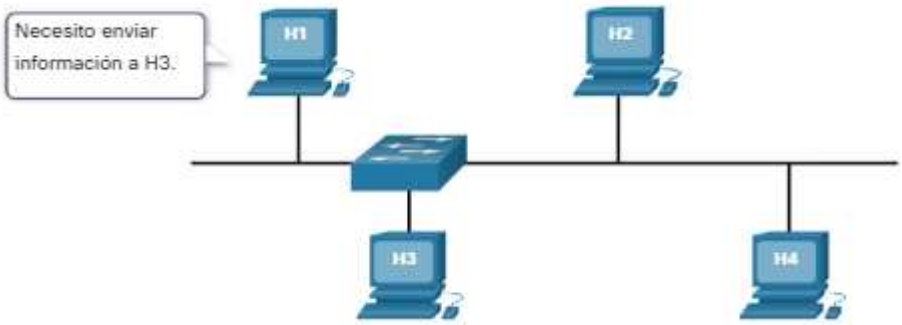
Nota: En los sistemas operativos de PC y NIC modernos, es posible cambiar la dirección MAC en el software. Esto es útil cuando se intenta acceder a una red filtrada por BIA. En consecuencia, el filtrado o el control de tráfico basado en la dirección MAC ya no son tan seguros.

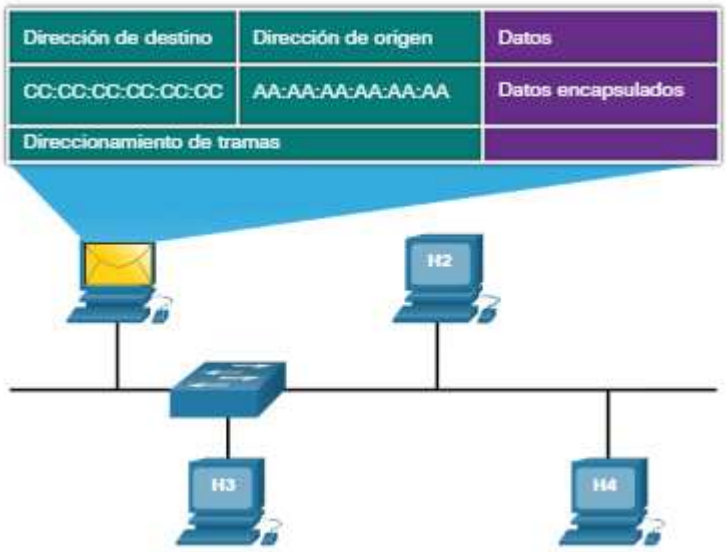
Cuando la computadora se inicia, la NIC copia su dirección MAC de la ROM a la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, el encabezado Ethernet incluye estos:

- **Dirección MAC de origen** - Esta es la dirección MAC de la NIC del dispositivo origen. Dirección MAC de **destino**: es la dirección MAC de la NIC del dispositivo de destino.

En la animación, haga clic en Reproducir para ver el proceso de reenvío de tramas.

La animación tiene una topología que consiste en un switch con vínculos a cuatro equipos host etiquetados, H1, H2, H3 y H4. H1 dice que necesito enviar información a H3. Aparece una trama en la pantalla de la PC y una vista ampliada dla trama aparece encima de la PC. la trama consiste en el direccionamiento de trama y los datos. La dirección de destino CC:CC:CC:CC:CC:CC, la dirección de origen AA:AA:AA:AA:AA:AA y la parte de datos de la trama está encapsulada. La trama de H1 se reenvía a el software. A continuación, el switch reenvía la trama fuera de cada interfaz, excepto la interfaz conectada a H1. Cuando H2 y H4 reciben la trama y dicen que esto no está dirigido a mí. Lo ignoraré. Cuando H3 recibe la trama, dice Esto es mío.

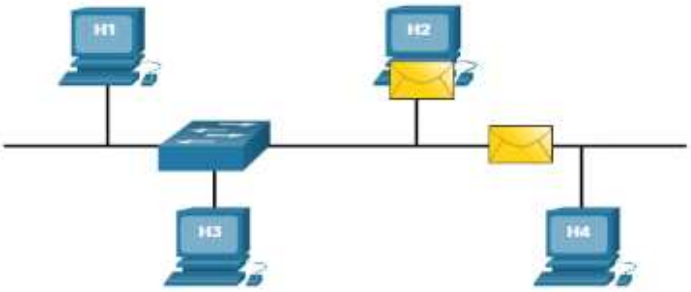


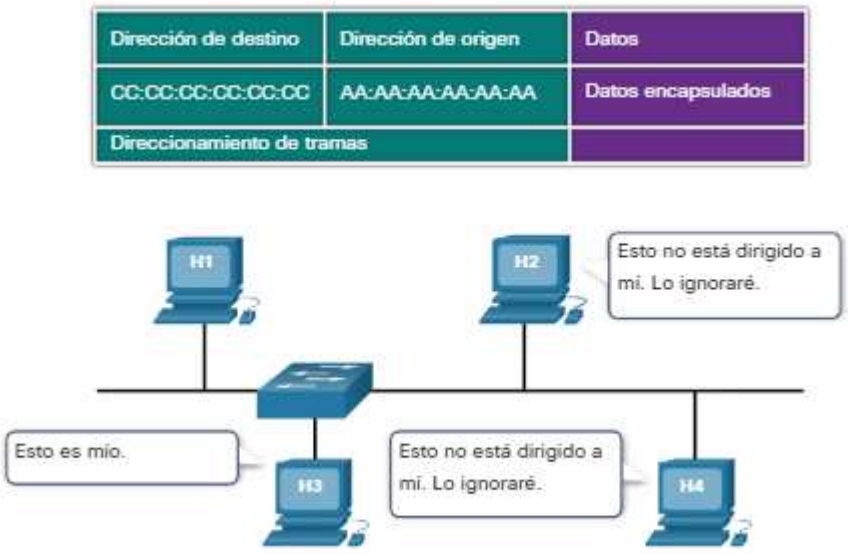


Dirección de destino	Dirección de origen	Datos
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Datos encapsulados
Direccionamiento de tramas		

Dirección de destino	Dirección de origen	Datos
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Datos encapsulados
Direccionamiento de tramas		

Dirección de destino	Dirección de origen	Datos
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Datos encapsulados
Direccionamiento de tramas		





Cuando una NIC recibe una trama de Ethernet, examina la dirección MAC de destino para ver si coincide con la dirección MAC física que está almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Si hay coincidencia, envía la trama a las capas OSI, donde ocurre el proceso de desencapsulamiento.

Nota: Las NIC de Ethernet también aceptarán tramas si la dirección MAC de destino es una transmisión o un grupo multicast del que es miembro el host.

Cualquier dispositivo que sea la origen o destino de una trama Ethernet, tendrá una NIC Ethernet y, por lo tanto, una dirección MAC. Esto incluye estaciones de trabajo, servidores, impresoras, dispositivos móviles y routers.

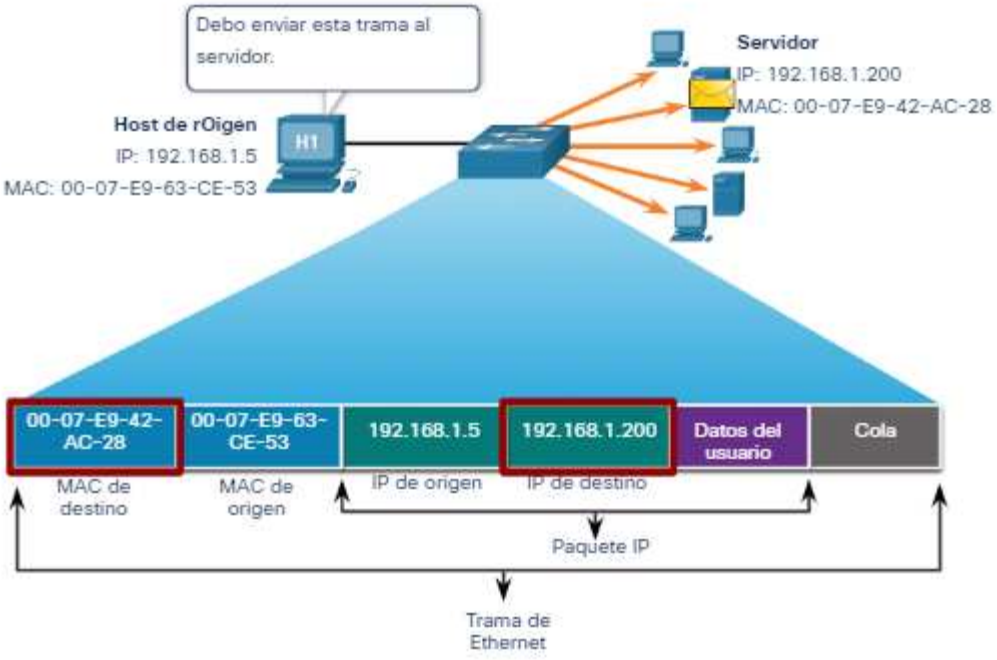
7.2.4

Dirección MAC de unicast

En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unicast, broadcast y multicast de capa 2.

Una dirección MAC de unicast es la dirección única que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino.

Haga clic en Reproducir en la animación para ver cómo se procesa una trama de unicast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son unicast.



La animación muestra un host con dirección IPv4 192.168.1.5 (origen) solicitando una página web de un servidor IPv4 unicast. dirección 192.168.1.200. La animación tiene una topología que consiste en un equipo host llamado H1 vinculado a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de un ethernet trama La trama consiste en el MAC 00-07-E9-42-AC-28 de destino, MAC 00-07-E9-63-CE-53 de origen, IP 192.168.1.5, dirección IP de destino 192.168.1.200, datos de usuario y remolque. La parte del paquete IP de la trama es la IP de origen, dirección IP de destino y datos del usuario. En la animación, H1 dice que necesito enviar la trama al servidor. Se envía una trama de H1 al switch. A continuación, el switch reenvía la trama al servidor con la IP y MAC que coinciden con la IP de destino y la dirección MAC.

En el ejemplo de la animación, un host con la dirección IPv4 192.168.1.5 (origen) solicita una página web del servidor en la dirección IPv4 unicast 192.168.1.200. Para que un paquete de unicast se envíe y se reciba, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la distribución de datos a un host de destino específico.

El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv4 se conoce como Protocolo de resolución de direcciones (ARP). El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv6 se conoce como Neighbor Discovery (ND).

Nota: La dirección MAC de origen siempre debe unicast.

7.2.5

Dirección MAC broadcast

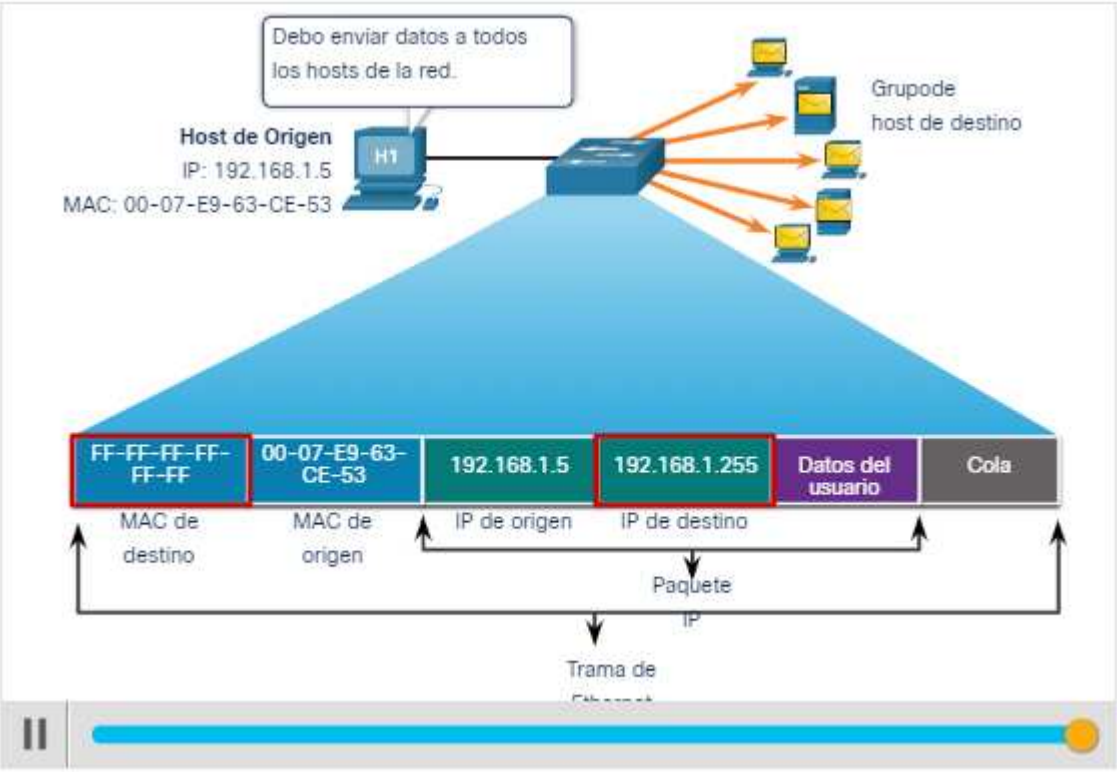
Cada dispositivo de la LAN Ethernet recibe y procesa una trama de broadcast Ethernet. Las características de una transmisión Ethernet son las siguientes:

- Tiene una dirección MAC de destino de FF-FF-FF-FF-FF-FF en hexadecimal (48 unidades en binario).
- Está inundado todos los puertos del switch Ethernet excepto el puerto entrante.
- No es reenviado por un router.

Si los datos encapsulados son un paquete broadcast IPv4, esto significa que el paquete contiene una dirección IPv4 de destino que tiene todos los (1s) en la parte del host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete.

Haga clic en Reproducir en la animación para ver cómo se procesa una trama de broadcast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son ambas broadcasts.

La animación muestra un host de origen que envía un paquete broadcast IPv4 a todos los dispositivos en su red. La animación tiene una topología que consiste en una PC host llamada H1 vinculada a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de una trama de ethernet. La trama consiste en el destino MAC FF-FF-FF-FF-FF-FF, origen MAC 00-07-E9-63-CE-53, origen IP 192.168.1.5, dirección IP de destino 192.168.1.255, usuario datos y tráiler. La parte del paquete IP de la trama es la IP de origen, la dirección IP de destino y los datos del usuario. En la animación, H1 dice que necesito enviar datos a todos los hosts en la red. Se envía una trama desde H1 al switch. El switch luego reenvía la trama a todas sus interfaces excepto la conectada a H1. Los otros tres hosts de PC y los dos servidores reciben las tramas.



Como se muestra en la animación, el host de origen envía un paquete broadcast IPv4 a todos los dispositivos de la red. La dirección IPv4 de destino es una dirección broadcast: 192.168.1.255. Cuando el paquete de broadcast IPv4 se encapsula en la trama de Ethernet, la dirección MAC de destino es la dirección MAC de difusión FF-FF-FF-FF-FF-FF en hexadecimal (48 números uno en binario).

DHCP para IPv4 es un ejemplo de protocolo que utiliza direcciones de broadcast Ethernet e IPv4.

Sin embargo, no todas las transmisiones Ethernet llevan un paquete de broadcast IPv4. Por ejemplo, las solicitudes ARP no utilizan IPv4, pero el mensaje ARP se envía como un broadcast Ethernet.

7.2.6

Dirección MAC de multicast

Una trama de multicast de Ethernet es recibida y procesada por un grupo de dispositivos en la LAN de Ethernet que pertenecen al mismo grupo de multicast. Las características de una multicast Ethernet son las siguientes:

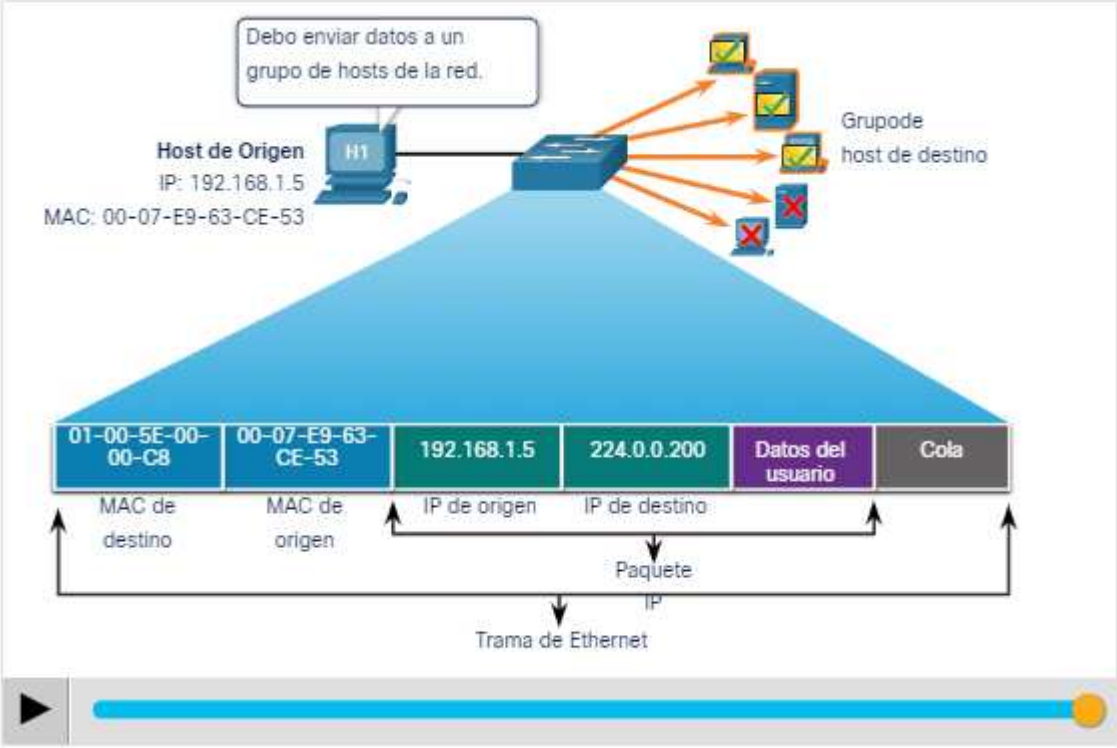
- Hay una dirección MAC de destino 01-00-5E cuando los datos encapsulados son un paquete de multicast IPv4 y una dirección MAC de destino de 33-33 cuando los datos encapsulados son un paquete de multicast IPv6.
- Existen otras direcciones MAC de destino de multicast reservadas para cuando los datos encapsulados no son IP, como Spanning Tree Protocol (STP) y Link Layer Discovery Protocol (LLDP).
- Se inundan todos los puertos del switch Ethernet excepto el puerto entrante, a menos que el switch esté configurado para la indagación de multicast. No* es reenviado por un router, a menos que el router esté configurado para enrutar paquetes de multicast.

Si los datos encapsulados son un paquete de multicast IP, a los dispositivos que pertenecen a un grupo de multicast se les asigna una dirección IP de grupo de multicast. El rango de direcciones de multicast IPv4 es 224.0.0.0 a 239.255.255.255. El rango de direcciones de multicast IPv6 comienza con ff00:: / 8. Debido a que las direcciones de multicast representan un grupo de direcciones (a veces denominado grupo de hosts), solo se pueden utilizar como el destino de un paquete. El origen siempre tiene una dirección de unicast.

Al igual que con las direcciones de unicast y broadcast, la dirección IP de multicast requiere una dirección MAC de multicast correspondiente para entregar tramas en una red local. La dirección MAC de multicast está asociada a la dirección de multicast IPv4 o IPv6 y utiliza la información de direccionamiento de dicha dirección.

Haga clic en Reproducir en la animación para ver cómo se procesa una trama de multicast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son ambas multicast.

La animación muestra un host de origen que envía una trama de multicast a los dispositivos que pertenecen al grupo de multicast. La animación tiene una topología que consiste en un equipo host llamado H1 vinculado a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de una trama de ethernet. La trama consiste en el destino MAC 01-00-5E-00-00-C8, origen MAC 00-07-E9-63-CE-53, origen IP 192.168.1.5, dirección IP de destino 224.0.0.200, usuario datos y tráiler. La parte del paquete IP de la trama es la IP de origen, la dirección IP de destino y los datos del usuario. En la animación, H1 dice que necesito enviar datos a todos los hosts en la red. Se envía una trama desde H1 al switch. El switch luego reenvía la trama a solo los dispositivos del grupo de multicast. Dos de los tres hosts de PC y un servidor reciben la trama de multicast.



Los protocolos de enrutamiento y otros protocolos de red utilizan direccionamiento multicast. Las aplicaciones como el software de vídeo e imágenes también pueden utilizar direccionamiento multicast, aunque las aplicaciones multicast no son tan comunes.

7.2.7

Lab - Ver las direcciones MAC del dispositivo de red

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Establecer la topología e inicializar los dispositivos
- Parte 2: Configurar los dispositivos y verificar la conectividad
- Parte 3: Mostrar, describir y analizar las direcciones MAC de Ethernet

Ver direcciones MAC de dispositivos de red

Switching Ethernet / Tabla de direcciones MAC

Tabla de direcciones MAC

7.3.1

Fundamentos de switches

Ahora que sabe todo acerca de las direcciones MAC Ethernet, es hora de hablar sobre cómo un switch utiliza estas direcciones para reenviar (o descartar) tramas a otros dispositivos de una red. Si un switch acaba de reenviar cada trama que recibió todos los puertos, su red estaría tan congestionada que probablemente se detendría por completo.

Un switch Ethernet de capa 2 usa direcciones MAC de capa 2 para tomar decisiones de reenvío. No tiene conocimiento de los datos (protocolo) que se transportan en la porción de datos de la trama, como un paquete IPv4, un mensaje ARP o un paquete IPv6 ND. El switch toma sus decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2.

Un switch Ethernet examina su tabla de direcciones MAC para tomar una decisión de reenvío para cada trama, a diferencia de los hubs Ethernet heredados que repiten bits en todos los puertos excepto el puerto entrante. En la ilustración, se acaba de encender el switch de cuatro puertos. La tabla muestra la tabla de direcciones MAC que aún no ha aprendido las direcciones MAC para las cuatro PC conectadas.

Nota: Las direcciones MAC se acortan a lo largo de este tema con fines de demostración.

El diagrama muestra cuatro hosts, junto con sus direcciones MAC asociadas, conectados a los puertos 1 - 4 de un switch. La tabla de direcciones MAC que asigna puertos a direcciones MAC está vacía actualmente.

La tabla de direcciones MAC del switch está vacía.

Nota: En ocasiones, la tabla de direcciones MAC se denomina tabla de memoria de contenido direccionable (CAM). Aunque el término "tabla CAM" es bastante común, en este curso nos referiremos a ella como "tabla de direcciones MAC".

7.3.2

Switch, Aprendiendo y Reenviando

El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

Haga clic en los botones Aprender y Reenviar para obtener una ilustración y una explicación de este proceso.

Aprender | Reenviar

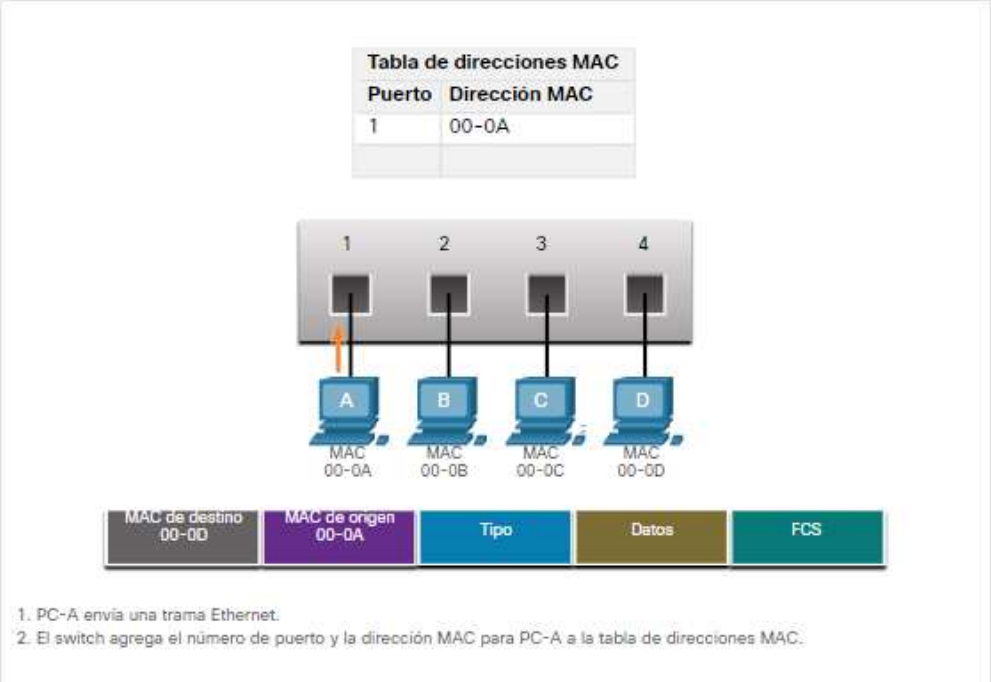
Examinar la dirección MAC de Origen

Se revisa cada trama que ingresa a un switch para obtener información nueva. Esto se realiza examinando la dirección MAC de origen de la trama y el número de puerto por el que ingresó al switch. Si la dirección MAC de origen no existe, se la agrega a la tabla, junto con el número de puerto de entrada. Si la dirección MAC de origen existe, el switch actualiza el temporizador de actualización para esa entrada. De manera predeterminada, la mayoría de los switches Ethernet guardan una entrada en la tabla durante cinco minutos.

En la figura, por ejemplo, la PC-A está enviando una trama Ethernet a la PC-D. La tabla muestra que el switch agrega la dirección MAC para PC-A a la tabla de direcciones MAC.

Nota: Si la dirección MAC de origen existe en la tabla, pero en un puerto diferente, el switch la trata como una entrada nueva. La entrada se reemplaza con la misma dirección MAC, pero con el número de puerto más actual.

Cuatro hosts, A - D, están conectados a un switch en los puertos 1 - 4. El host A con dirección MAC 00-0A (simplificado en este ejemplo) está conectado al switch en el puerto 1. El host A envía una trama con una dirección MAC de destino de 00-0D. La dirección MAC de origen de la trama es 00-0A, El switch asigna el puerto 1 a la dirección MAC 00-0A en su tabla de direcciones MAC.



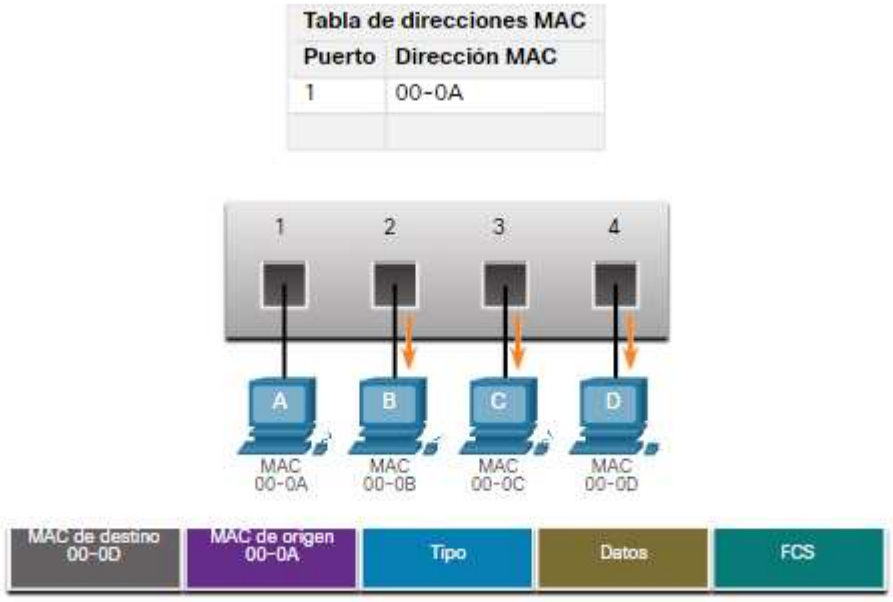
Aprender | Reenviar

Buscar dirección MAC de destino

Si la dirección MAC de destino es una dirección de unicast, el switch busca una coincidencia entre la dirección MAC de destino de la trama y una entrada en la tabla de direcciones MAC. Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado. Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada. Esto se conoce como unicast desconocida.

Como se muestra en la figura, el switch no tiene la dirección MAC de destino en su tabla para PC-D, por lo que envía la trama a todos los puertos excepto el puerto 1.

Nota: Si la dirección MAC de destino es de broadcast o de multicast, la trama también se envía por todos los puertos, excepto el de entrada.

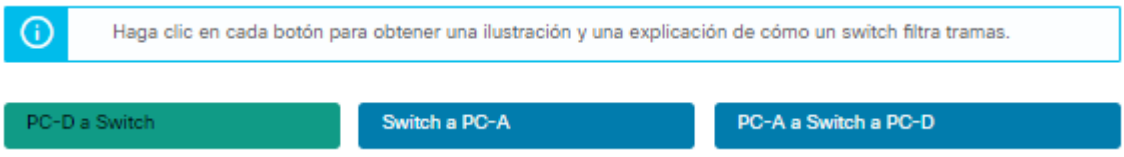


1. La dirección MAC de destino no está en la tabla.
2. El switch reenviará la trama a todos los puertos.

7.3.3

Filtrado de tramas

A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.



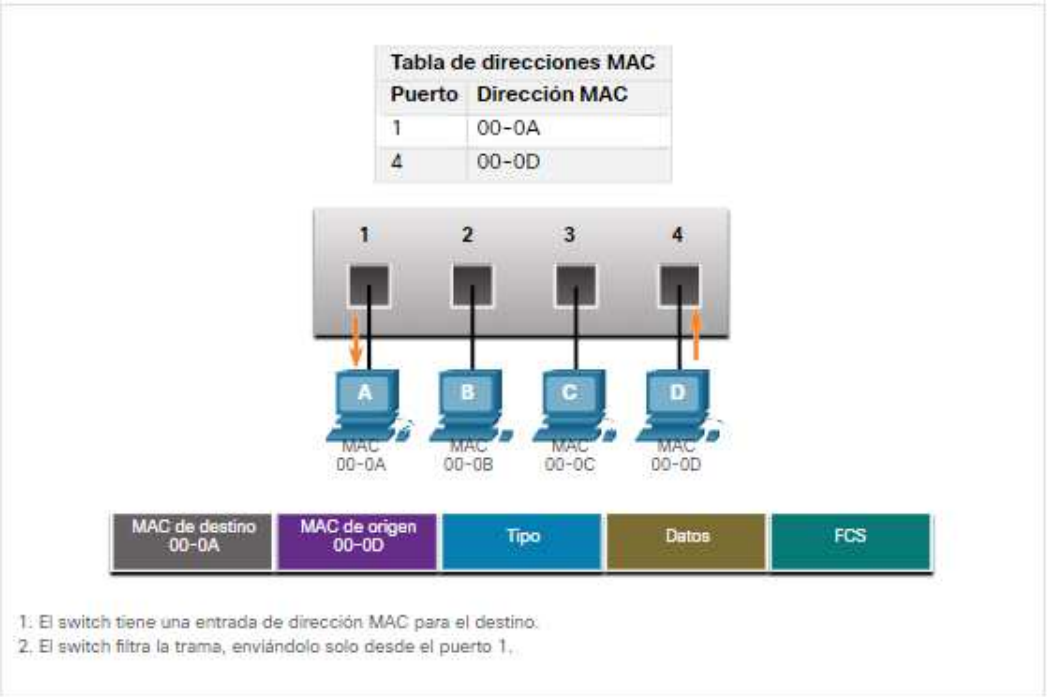
En la figura, PC-D responde a PC-A. El switch ve la dirección MAC de PC-D en la trama entrante en el puerto 4. A continuación, el switch coloca la dirección MAC de PC-D en la tabla de direcciones MAC asociada con el puerto 4.

Cuatro hosts, A - D, están conectados a un switch en los puertos 1 - 4. El host D con dirección MAC 00-0D está conectado al switch en el puerto 4. El host D envía una trama con una dirección MAC de destino de 00-0A y un MAC de origen de 00-0D. El switch asigna el puerto 4 a la dirección MAC 00-0D en su tabla de direcciones MAC.

El switch agrega el número de puerto y la dirección MAC para PC-D a su tabla de direcciones MAC.

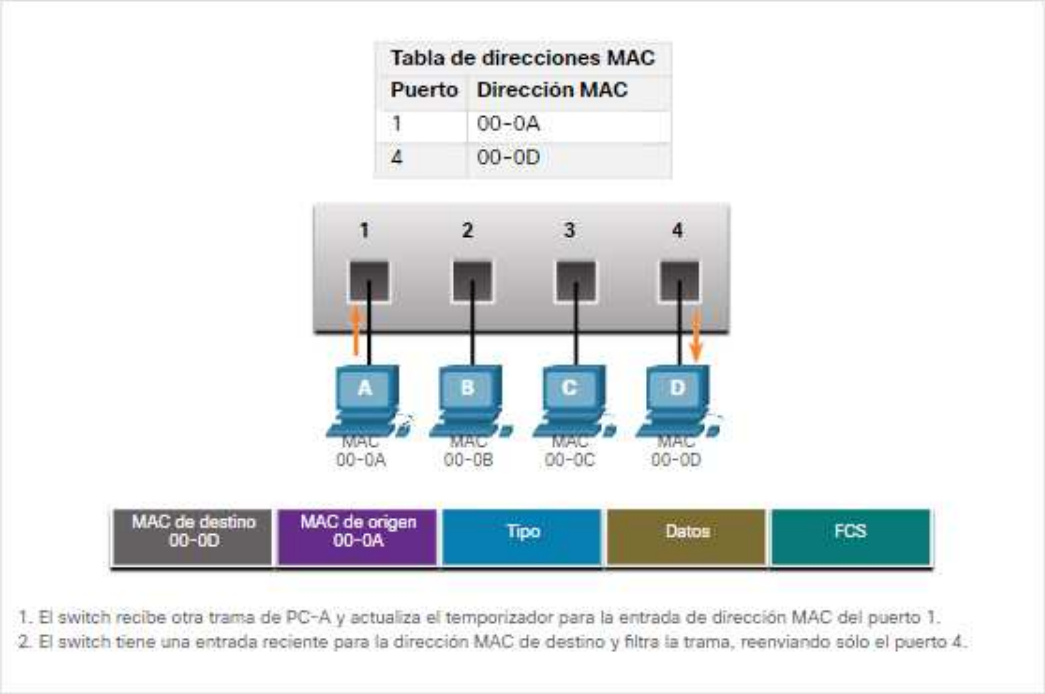
PC-D a Switch | Switch a PC-A | PC-A a Switch a PC-D

A continuación, dado que el switch tiene la dirección MAC de destino para la PC-A en la Tabla de direcciones MAC, enviará la trama solo al puerto 1, como se muestra en la figura.



PC-D a Switch | Switch a PC-A | PC-A a Switch a PC-D

A continuación, PC-A envía otra trama a PC-D como se muestra en la figura. La tabla de direcciones MAC ya contiene la dirección MAC para PC-A; por lo tanto, el temporizador de actualización de cinco minutos para esa entrada se restablece. Luego, debido a que la tabla de switch contiene la dirección MAC de destino para PC-D, envía la trama solo por el puerto 4.



7.3.4

Video: Tablas de direcciones MAC en switches conectados

Un switch puede tener muchas direcciones MAC asociadas a un solo puerto. Esto es común cuando el switch está conectado a otro switch. El switch tiene una entrada independiente en la tabla de direcciones MAC para cada trama recibida con una dirección MAC de origen diferente.

Haga clic en Reproducir en la figura para ver una demostración de cómo dos switches conectados crean tablas de direcciones MAC.

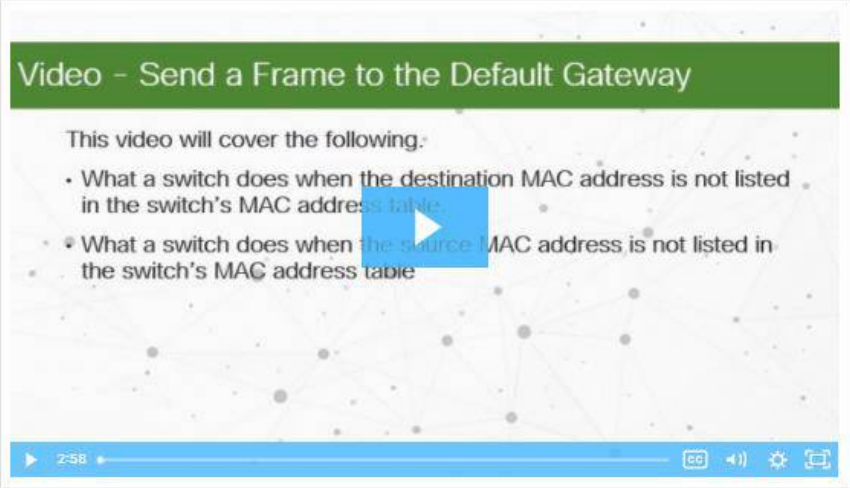
7.3.5

Video - Envío de una trama al gateway predeterminado

Cuando un dispositivo tiene una dirección IP ubicada en una red remota, la trama de Ethernet no se puede enviar directamente al dispositivo de destino. En cambio, la trama de Ethernet se envía a la dirección MAC del gateway predeterminado: el router.

En la ilustración, haga clic en Reproducir para ver una demostración de cómo la PC-A se comunica con el gateway predeterminado.

Nota: En el vídeo, el paquete IP que se envía de la PC-A al destino en una red remota tiene como dirección IP de origen la de la PC-A y como dirección IP de destino, la del host remoto. El paquete IP de retorno tiene la dirección IP de origen del host remoto, y la dirección IP de destino es la de la PC A.



7.3.6

Actividad: ¡El Switch!

Determine cómo el switch reenvía una trama en función de la dirección MAC de origen, la dirección MAC de destino y la información en la tabla MAC del switch. Responda las preguntas utilizando la información provista.

Correcto

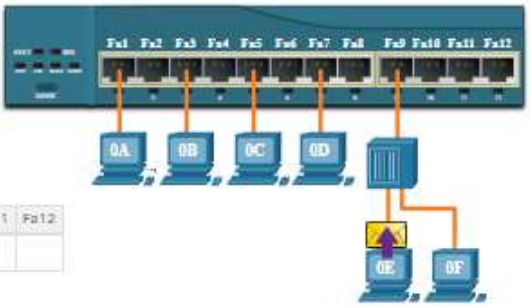
Respondió correctamente todas las preguntas según la información de la trama y la tabla MAC.

Trama

Preámbulo	Destino MAC	Origen MAC	Tipo/Longitud	Trama	Fin de Trama
	0B	0E			

Tabla MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
						0D		0E			



Pregunta 1 - ¿Adónde reenviará la trama el switch?

☑ Fa1 ☐ Fa2 ☑ Fa3 ☐ Fa4 ☑ Fa5 ☐ Fa6 ☑ Fa7 ☐ Fa8 ☐ Fa9 ☐ FA10 ☐ Fa11 ☐ Fa12

Pregunta 2 - ¿Cuáles de estas afirmaciones sobre el reenvío de una trama por parte del switch son verdaderas?

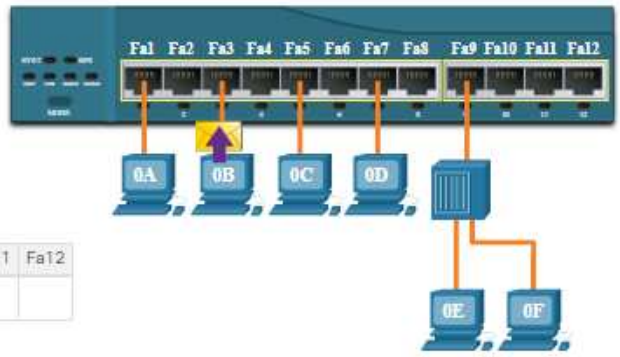
☐ Switch agrega la dirección MAC de origen que actualmente no está en la tabla de direcciones MAC.
☐ La trama es una trama broadcast y se reenvía a todos los puertos.
☐ La trama es una trama unicast y se reenvía solamente a un puerto específico.
☑ La trama es una trama unicast y se distribuye por saturación a todos los puertos.
☐ La trama es unicast, pero se descarta en el switch.

Frame

Preamble	Destination MAC	Source MAC	Type / Length	Frame	End of Frame
	0E	0B			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
				0C		0D		0F			



Question 1 - Where will the switch forward the frame?

☑ Fa1 ☐ Fa2 ☐ Fa3 ☐ Fa4 ☑ Fa5 ☐ Fa6 ☑ Fa7 ☐ Fa8 ☑ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

☑ Switch adds the source MAC address which is currently not in the MAC address table.
☐ Frame is a broadcast frame and will be forwarded to all ports.
☐ Frame is a unicast frame and will be sent to specific port only.
☑ Frame is a unicast frame and will be flooded to all ports.
☐ Frame is a unicast frame but it will be dropped at the switch.

7.3.7

Lab - Visualización de la tabla de direcciones MAC del switch

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Construcción y configuración de la red
- Parte 2: Examinar la tabla de direcciones MAC del switch

Ver la tabla de direcciones MAC del Switch

Velocidades y métodos de reenvío del switch

7.4.1

Métodos de reenvío de tramas de los switches Cisco

Como aprendió en el tema anterior, los modificadores utilizan sus tablas de direcciones MAC para determinar qué puerto utilizar para reenviar tramas. Con los switches Cisco, en realidad hay dos métodos de reenvío de tramas y hay buenas razones para usar uno en lugar del otro, dependiendo de la situación.

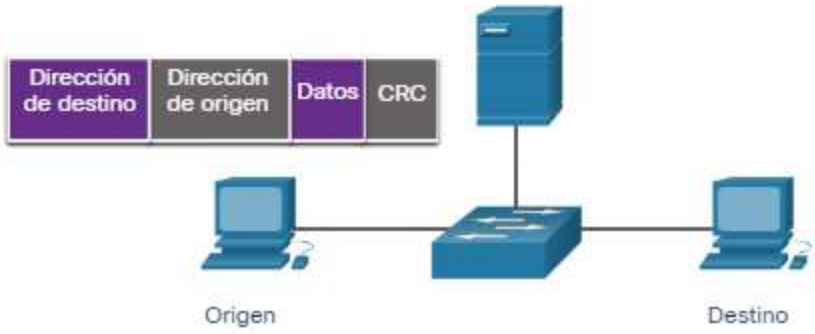
Los switches utilizan uno de los siguientes métodos de reenvío para el switching de datos entre puertos de la red:

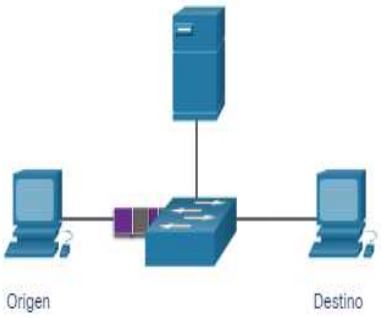
- **Store-and-forward switching** - Este método de reenvío de trama recibe la trama completa y calcula el CRC. La CRC utiliza una fórmula matemática basada en la cantidad de bits (números uno) de la trama para determinar si esta tiene algún error. Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida. Luego, la trama se reenvía desde el puerto correcto.
- **Cut-through switching** - Este método de reenvío de tramas reenvía la trama antes de que se reciba por completo. Como mínimo, se debe leer la dirección de destino para que la trama se pueda enviar.

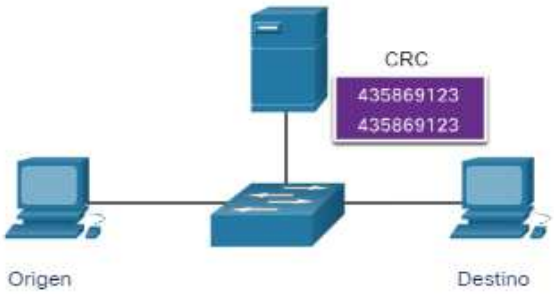
Una gran ventaja de store-and-forward switching, es que determina si una trama tiene errores antes de propagarla. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce el ancho de banda consumido por datos dañados. Store-and-forward switching se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo, los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de navegación web.

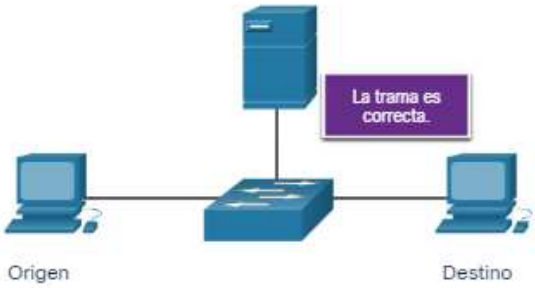
Haga clic en Reproducir en la animación para ver una demostración del proceso de store-and-forward

La animación se muestra como host de origen enviando una trama a un switch cut-through. La animación tiene una topología que consiste en un host de origen vinculado a un switch. El tiene un vínculo a un host de destino y un servidor. En la animación, el host de origen reenvía una trama al switch. El switch recibe la trama y mira su tabla de switching para determinar qué interfaz desea reenviar la trama. El switch luego envía la trama al host de destino.


Dirección de destino
Dirección de origen
Datos
CRC
Origen
Destino


Origen
Destino


CRC
435869123
435869123
Origen
Destino


La trama es correcta.
Origen
Destino

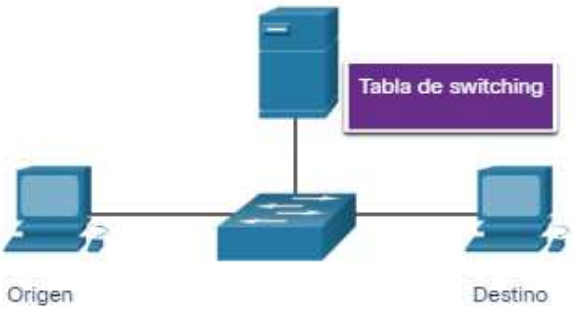
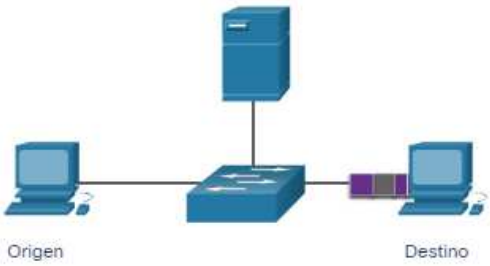


Tabla de switching
Origen
Destino


Origen
Destino

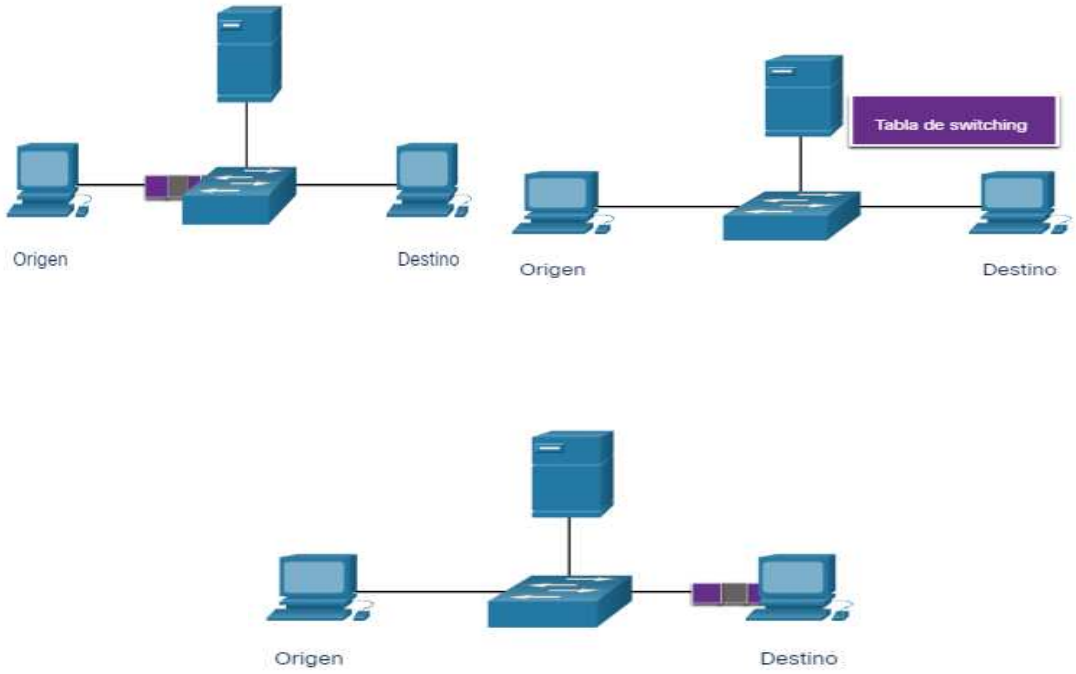
7.4.2

Switching por método de corte

En este tipo de switching, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se completó. El switch almacena la cantidad suficiente de trama como para leer la dirección MAC de destino para que pueda determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo. El switch busca la dirección MAC de destino en la tabla de switching, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado. El switch no lleva a cabo ninguna verificación de errores en la trama.

Reproduzca la animación para ver una demostración del proceso cut-through switching.

La animación se muestra como host de origen enviando una trama a un switch de store-and-forward. El switch calcula el CRC y, si es válido envía la trama al host de destino. La animación tiene una topología que consiste en un host de origen vinculado a un switch. El switch tiene un vínculo a un host de destino y un servidor. En la animación, el host de origen muestra el contenido de la trama consistente en una dirección de destino, dirección de origen, datos y CRC. La trama se reenvía al switch desde el host de origen. El switch recibe la trama y calcula el CRC en la trama. El CRC en el paquete es 435869123 y el CRC calculado es 435869123, ambos coincidentes. El switch dice que la Trama es buena y luego mira su tabla de switching para determinar a qué interfaz reenvíar la trama. A continuación, el switch envía la trama al host de destino.



A continuación, se presentan dos variantes del cut-through switching:

- **Fast-forward switching -** Este método ofrece el nivel de latencia más bajo. Fast-forward switching reenvía el paquete inmediatamente después de leer la dirección de destino. Como el fast-forward switching comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. Esto ocurre con poca frecuencia y la NIC de destino descarta el paquete defectuoso al recibirlo. En el modo de fast-forward, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El fast-forward switching es el método de corte típico.
- **Fragment-free switching -** En este método, el switch almacena los primeros 64 bytes de la trama antes de reenviarla. El fragment-free switching se puede ver como un punto medio entre el store-and-forward switching y el fast-forward switching. El motivo por el que el fragment-free switching almacena solamente los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El fragment-free switching intenta mejorar el fast-forward switching al realizar una pequeña verificación de errores en los 64 bytes de la trama para asegurar que no haya ocurrido una colisión antes de reenviarla. Este método de fragment-free switching es un punto medio entre la alta latencia y la alta integridad del store-and-forward switching, y la baja latencia y la baja integridad del fast-forward switching.

Algunos switches están configurados para realizar el cut-through switching en cada puerto hasta alcanzar un umbral de errores definido por el usuario y, luego, cambiar automáticamente al store-and-forward. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente al cut-through switching.

7.4.3

Almacenamiento en búfer de memoria en los switches

Un switch Ethernet puede usar una técnica de almacenamiento en búfer para almacenar tramas antes de enviarlas. También se puede utilizar el almacenamiento en búfer cuando el puerto de destino está ocupado debido a la congestión. El switch almacena la trama hasta que se pueda transmitir.

Como se muestra en la tabla, hay dos métodos de almacenamiento en memoria intermedia:

Método de almacenamiento en búfer de memoria

Método	Descripción
Memoria basada en puerto	Las tramas se almacenan en colas que se enlazan a puertos específicos de entrada y puertos de salida.

Método	Descripción
	Una trama se transmite al puerto de salida sólo cuando todas las tramas en la cola se han transmitido correctamente. Es posible que una sola trama retrase la transmisión de todas las tramas en memoria debido a un puerto de destino ocupado. Esta demora se produce aunque las demás tramas se puedan transmitir a puertos de destino abiertos.
Memoria compartida	Deposita todas las tramas en un búfer de memoria común compartido por todos los switches y la cantidad de memoria intermedia requerida por un puerto es asignada dinámicamente. Las tramas que están en el búfer se enlazan de forma dinámica al puerto de destino. que permite recibir un paquete en un puerto y, a continuación, transmitido en otro puerto, sin moverlo a una cola diferente.

El almacenamiento en búfer de memoria compartida también da como resultado la capacidad de almacenar tramas más grandes con potencialmente menos tramas descartadas. Esto es importante con la conmutación asimétrica, que permite diferentes velocidades de datos en diferentes puertos, como cuando se conecta un servidor a un puerto de switch de 10 Gbps y PC a puertos de 1 Gbps.

7.4.4

Configuración de dúplex y velocidad

Dos de las configuraciones más básicas en un switch son el ancho de banda (a veces denominado "velocidad") y la configuración dúplex para cada puerto de switch individual. Es fundamental que los parámetros de dúplex y de ancho de banda coincidan entre el puerto de switch y los dispositivos conectados, como una computadora u otro switch.

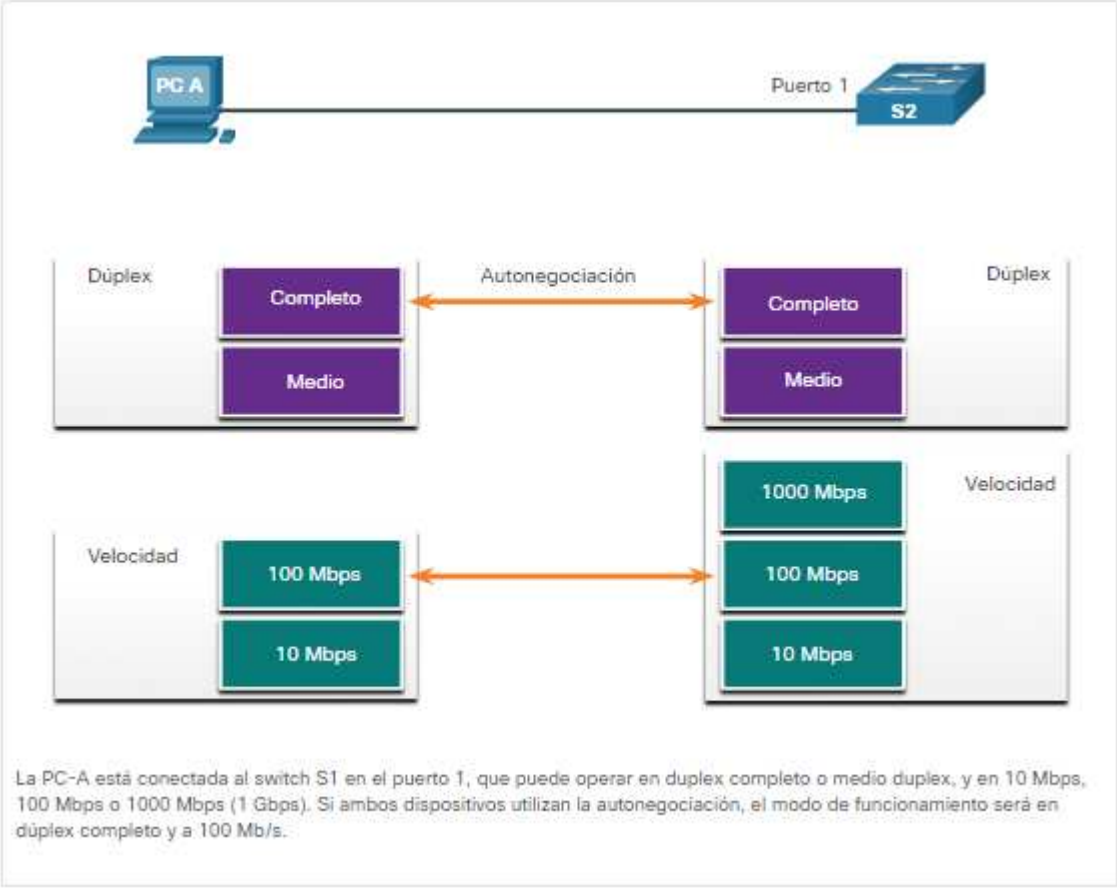
Se utilizan dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet:

- **Full-duplex** - Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Half-duplex** - Solo uno de los extremos de la conexión puede enviar datos por vez.

La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NICs. Permite que dos dispositivos negocien automáticamente las mejores

capacidades de velocidad y dúplex. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto.

En la figura, la NIC Ethernet para PC-A puede funcionar en dúplex completo o medio dúplex, y en 10 Mbps o 100 Mbps.

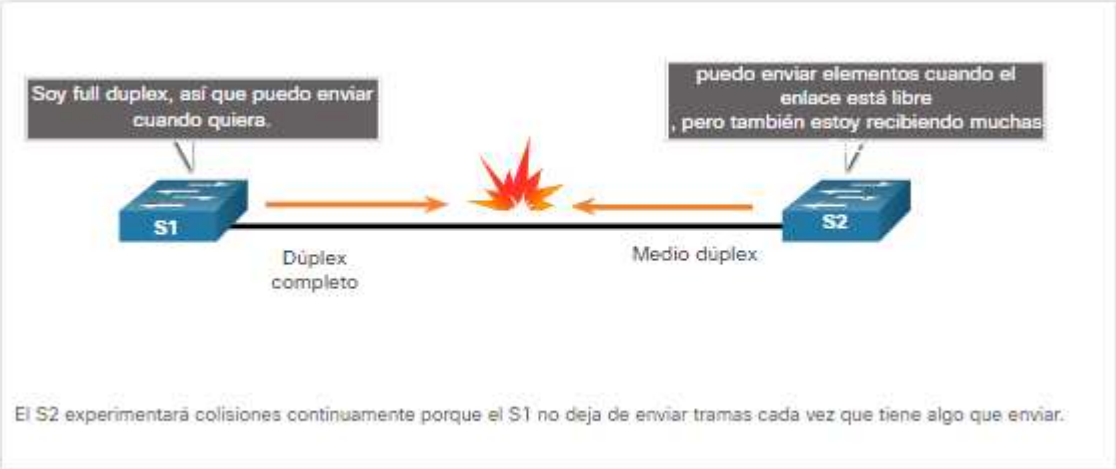


La PC-A está conectada al switch S1 en el puerto 1, que puede operar en duplex completo o medio duplex, y en 10 Mbps, 100 Mbps o 1000 Mbps (1 Gbps). Si ambos dispositivos utilizan la autonegociación, el modo de funcionamiento será en dúplex completo y a 100 Mb/s.

Nota: La mayoría de los switches de Cisco y las NIC de Ethernet tienen por defecto la negociación automática para velocidad y dúplex. Los puertos Gigabit Ethernet solamente funcionan en dúplex completo.

La falta de coincidencia dúplex es una de las causas más comunes de problemas de rendimiento en enlaces Ethernet de 10/100 Mbps. Ocurre cuando un puerto en el enlace opera en medio duplex mientras que el otro puerto opera en duplex completo, como se muestra en la figura.

El switch S1 está conectado al switch S2. S1 funciona en dúplex completo y S2 funciona en medio dúplex. Un texto sobre S1 dice: dice: Yo soy dúplex completo para que pueda enviar cuando quiera. Un texto sobre S2: Yo soy medio dúplex, así que solo puedo enviar cuando el enlace está despejado, ¡pero también estoy recibiendo muchas colisiones! El gráfico muestra ambos switches que envían datos al mismo tiempo que han dado lugar a una colisión.



La falta de coincidencia dúplex se produce cuando se restablecen uno o ambos puertos en un enlace, y el proceso de negociación automática no da como resultado que ambos socios del enlace tengan la misma configuración. También puede ocurrir cuando los usuarios reconfiguran un lado del enlace y olvidan reconfigurar el otro. Ambos lados de un enlace deben tener activada la autonegociación, o bien ambos deben tenerla desactivada. La práctica recomendada es configurar ambos puertos del switch Ethernet como dúplex completo.

7.4.5

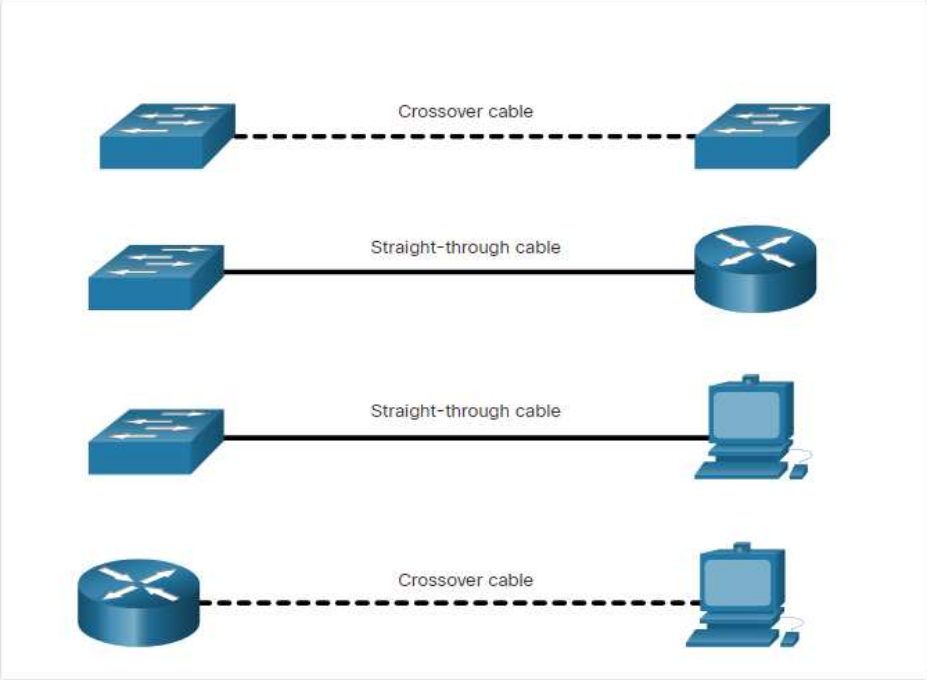
Auto-MDIX (MDIX automático)

Las conexiones entre dispositivos requerían el uso de un cable cruzado o directo. El tipo de cable requerido dependía del tipo de dispositivos de interconexión.

Por ejemplo, la figura identifica el tipo de cable correcto necesario para interconectar dispositivos de switch a switch, switch a router, switch a host o router a host. Se utiliza un cable cruzado cuando se conectan dispositivos similares, y un cable directo para conectarse a dispositivos diferentes.

Nota: Una conexión directa entre un router y un host requiere una conexión cruzada.

El diagrama muestra el tipo de cable correcto que se debe utilizar al conectar varios tipos de dispositivos de red juntos. De arriba a abajo, los dispositivos y tipos de cable son: switch a switch es un cable cruzado; switch a router es un cable directo; switch a host es un cable directo; y router a host es un cable cruzado.



Actualmente, la mayor parte de los dispositivos admiten la característica interfaz cruzada automática dependiente del medio (auto-MDIX). Cuando está habilitado, el switch detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia. Por lo tanto, se puede utilizar un cable directo o cruzado para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que esté en el otro extremo de la conexión.

La función auto-MDIX está habilitada de manera predeterminada en los switches que ejecutan Cisco IOS Release 12.2 (18) SE o posterior. Sin embargo, la característica podría estar deshabilitada. Por esta razón, siempre debe utilizar el tipo de cable correcto y no confiar en la función Auto-MDIX. Auto-MDIX se puede volver a habilitar mediante el comando **mdix auto** de configuración de interfaz.

7.4.6

Compruebe su comprensión — Cambiar velocidades y métodos de reenvío

Verifique su comprensión de las velocidades de cambio y los métodos de reenvío eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Los dos métodos de switching de datos entre puertos de un switch son cut-through switching y store-and-forward switching.
2. Cut-through switching se implementa mediante fast-forward switching o fragment-free switching.
3. Los switches utilizan dos técnicas de almacenamiento en búfer de memoria: almacenamiento en búfer de memoria basada en puerto y almacenamiento en búfer de memoria compartida.
4. La negociación automática es una tecnología que negocia automáticamente la velocidad y el dúplex entre dos dispositivos conectados.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuáles son dos métodos para cambiar datos entre puertos de un switch? (Escoja dos).

¡Lo tienes!

- [ ] conmutación de corte
- [x] Switching por método de corte
- [x] Switching de almacenamiento y envío
- [ ] conmutación de almacenamiento y suministro
- [ ] store-and-forward switching

2. ¿Qué método de switching se puede implementar mediante fast-forward switching o fragment-free switching?

¡Lo tienes!

- ( ) conmutación de corte
- (•) Switching por método de corte
- ( ) Switching de almacenamiento y envío
- ( ) store-and-forward switching

3. ¿Qué dos tipos de técnicas de almacenamiento en búfer de memoria utilizan los switches? (Escoja dos).

¡Lo tienes!

- [ ] almacenamiento en búfer de memoria a largo plazo
- [x] Búfer de memoria basada en puerto
- [x] Búfer de memoria compartida
- [ ] almacenamiento en búfer de memoria a corto plazo

4. ¿Qué función negocia automáticamente la mejor velocidad y configuración dúplex entre dispositivos de interconexión?

¡Lo tienes!

- MDIX automático
- Autobots
- autonegociación
- autotune

Correct

You have successfully identified the correct answers.

1. The two methods for switching data between ports on a switch are cut-through switching and store-and-forward switching.
2. Cut-through switching is implemented using either fast-forward switching or fragment-free switching.
3. Switches use two memory buffering techniques: Port-based memory buffering and shared memory buffering.
4. Autonegotiation is a technology that automatically negotiates the speed and duplex between two connected devices.

You got 4 out of 4 questions correct.

1. What are two methods for switching data between ports on a switch? (Choose two.)

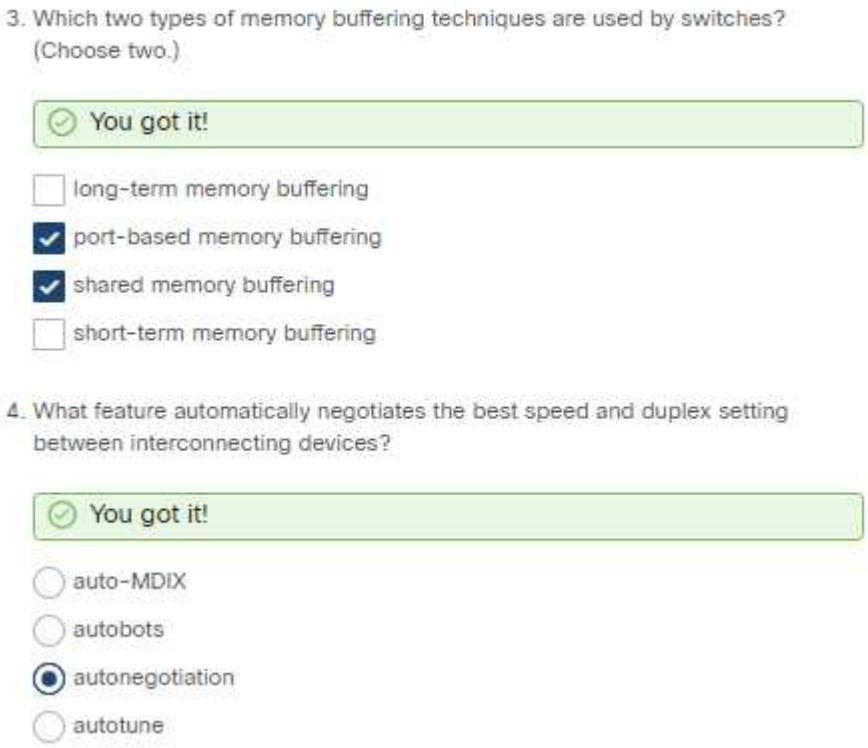
You got it!

- [ ] cut-off switching
- [x] cut-through switching
- [x] store-and-forward switching
- [ ] store-and-supply switching
- [ ] store-and-restore switching

2. Which switching method can be implemented using fast-forward switching or fragment-free switching?

You got it!

- cut-off switching
- cut-through switching
- store-and-forward switching
- store-and-restore switching



Módulo de Práctica y Prueba

7.5.1

¿Qué aprendió en este módulo?

Trama Ethernet

Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares de Ethernet definen los protocolos de capa 2 y las tecnologías de capa 1. Ethernet utiliza las subcapas LLC y MAC de la capa de enlace de datos para operar. La encapsulación de datos incluye lo siguiente: trama Ethernet, direccionamiento Ethernet y detección de errores Ethernet. Las LAN Ethernet utilizan switches que funcionan en dúplex completo. Los campos de trama Ethernet son: delimitador de trama de preámbulo y inicio, dirección MAC de destino, dirección MAC de origen, EtherType, datos y FCS.

Dirección MAC Ethernet

El sistema de números binarios usa los dígitos 0 y 1. Decimal usa de 0 a 9. Hexadecimal utiliza de 0 a 9 y las letras A a F. La dirección MAC se utiliza para identificar los dispositivos físicos de origen y destino (NIC) en el segmento de red local. El direccionamiento MAC proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI. Una dirección MAC de Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales o 6 bytes. Una dirección MAC Ethernet consta de un código OUI de proveedor hexadecimal 6 seguido de un valor asignado de proveedor hexadecimal 6. Cuando un dispositivo reenvía un mensaje a una red Ethernet, el encabezado Ethernet incluye las direcciones MAC de origen y destino. En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unicast, broadcast y multicast de capa 2.

La tabla de direcciones MAC

Un switch Ethernet de capa 2 toma sus decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2. El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC. A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

Métodos de reenvío y velocidad del switch

Los switches utilizan uno de los siguientes métodos de reenvío para cambiar datos entre puertos de red: store-and-forward switching o cut-through switching. Dos variantes de cut-through switching son fast-forward y fragment-free. Dos métodos de almacenamiento en búfer de memoria son la memoria basada en puertos y la memoria compartida. Hay dos tipos de configuraciones dúplex utilizadas para las comunicaciones en una red Ethernet: dúplex completo y medio dúplex. La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NICs. Permite que dos dispositivos negocien automáticamente las mejores capacidades de velocidad y dúplex. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto. Actualmente, la mayor parte de los dispositivos admiten la característica interfaz cruzada automática dependiente del medio (auto-MDIX). Cuando está habilitado, el switch detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia.

7.5.2

Prueba de módulo- Ethernet Switching

Correcto

Identificó bien las respuestas correctas.

Has tenido 14 respuestas correctas de 14.

1. ¿Qué dispositivo de red toma decisiones de reenvío sobre la base de la dirección MAC de destino incluida en la trama?

Tema 7.3.0 - Los switches son el punto de conexión central para una LAN y mantienen una tabla de direcciones MAC. En la tabla de direcciones MAC, hay un número de puerto asociado a una dirección MAC para cada dispositivo. El switch inspecciona una trama para encontrar la dirección MAC de destino. Luego, el switch busca en su tabla de direcciones MAC y, si encuentra esa dirección, reenvía los datos al puerto asociado con esa dirección MAC específica.

- ○ repetidor
- ○ Concentrador
- ◉ Switch
- ○ Router

2. ¿Qué dispositivo de red tiene la función principal para enviar datos a un destino específico en función de la información que se encuentra en la tabla de direcciones MAC?

Tema 7.3.0 - Si se encuentra una dirección MAC en la tabla de direcciones MAC, los datos se envían al puerto del switch asociado. Si la dirección MAC no se encuentra en la tabla de direcciones MAC, los datos se envían a todos los puertos del switch que tienen dispositivos conectados a la misma red.

- ○ Concentrador
- ○ Router
- ◉ Switch
- ○ módem

3. ¿Qué función u operación es realizada por la subcapa LLC?

Tema 7.1.0 - La subcapa Ethernet LLC tiene la responsabilidad de manejar la comunicación entre las capas superiores y las capas inferiores de la pila de protocolos. La LLC se implementa en software y se comunica con las capas superiores de la aplicación para hacer la transición del paquete a las capas inferiores para la entrega.

- ( ) Realiza la encapsulación de datos.
- (•) Se comunica con las capas de protocolo superiores.
- ( ) Es responsable del control de acceso a los medios.
- ( ) Agrega un encabezado y un remolque a un paquete para formar una PDU OSI de capa 2.

4. ¿Qué declaración es verdadera acerca de las direcciones MAC?

Tema 7.2.0 - Una dirección MAC se compone de 6 bytes. Los primeros 3 bytes se utilizan para la identificación del proveedor y a los últimos 3 bytes se les debe asignar un valor único dentro del mismo OUI. Las direcciones MAC se implementan en el hardware. Una NIC necesita una dirección MAC para comunicarse a través de la LAN. El IEEE regula las direcciones MAC.

- ( ) Las direcciones MAC son implementadas por el software.
- ( ) Una NIC solo necesita una dirección MAC si está conectada a una WAN.
- (•) Los tres primeros bytes son utilizados por el proveedor asignado OUI.
- ( ) La ISO es responsable de las regulaciones MAC.

5. ¿Qué sucede con las tramas cortas que recibe un switch Ethernet Cisco?

Tema 7.1.0 - En un intento de ahorrar ancho de banda y no reenviar tramas inútiles, los dispositivos Ethernet descartan las tramas que se consideran tramas cortas (de menos de 64 bytes) o jumbos (de más de 1500 bytes).

- (•) La trama se descarta.
- ( ) La trama se devuelve al dispositivo de red de origen.
- ( ) La trama se transmite por broadcast a todos los demás dispositivos de la misma red.
- ( ) La trama se envía al gateway predeterminado.

6. ¿Cuáles son los dos tamaños (mínimo y máximo) de una trama de Ethernet? (Escoja dos).

Tema 7.1.0 - El tamaño mínimo de una trama de Ethernet es de 64 bytes. El tamaño máximo de una trama de Ethernet es de 1518 bytes. Un técnico de redes debe conocer los tamaños de trama mínimo y máximo para reconocer tramas cortas y jumbos.

- [ ] 56 bytes
- [x] 64 bytes
- [ ] 128 bytes
- [ ] 1024 bytes
- [x] 1518 bytes

7. ¿Qué información de direccionamiento registra un switch para armar su tabla de direcciones MAC?

Tema 7.3.0 - Un switch arma una tabla de direcciones MAC por medio de la inspección de las tramas de capa 2 entrantes y del registro de la dirección MAC de origen que se encuentra en el encabezado de las tramas. A continuación, la dirección MAC obtenida y registrada se asocia con el puerto que se utilizó para recibir la trama.

- ○ la dirección de capa 3 de destino de sus paquetes entrantes
- ○ la dirección de capa 2 de destino de sus tramas salientes
- ○ la dirección de capa 3 de destino de sus paquetes salientes
- ◉ la dirección de capa 2 de destino de sus tramas entrantes

8. ¿Cuáles dos características describen la tecnología Ethernet? (Escoja dos).

Tema 7.1.0 - El estándar 802.3 Ethernet especifica que una red implementa el método de control de acceso CSMA/CD.

- ☑ Es compatible con los estándares IEEE 802.3.
- ☐ Es compatible con los estándares IEEE 802.5.
- ☐ Normalmente utiliza un promedio de 16 MB/s para velocidades de transferencia de datos.
- ☑ Utiliza el método de control de acceso CSMA/CD.
- ☐ Utiliza una topología de anillo.

9. ¿Cuál de estas afirmaciones describe una característica de las direcciones MAC?

Tema 7.2.0 – Cualquier proveedor de dispositivos Ethernet debe registrarse en el IEEE para asegurarse de que se le asigne un código de 24 bits único, que se convierte en los primeros 24 bits de la dirección MAC. Los últimos 24 bits de la dirección MAC se generan por cada dispositivo de hardware. Esto permite asegurar que cada dispositivo Ethernet tenga una dirección globalmente única.

- ◉ Deben ser globalmente únicas.
- ○ Solo son enrutables dentro de la red privada.
- ○ Se agregan como parte de una PDU de capa 3.
- ○ Tienen un valor binario de 32 bits.

10. ¿Cuál es el valor especial asignado a los primeros 24 bits de una dirección MAC de multicast?

Tema 7.2.0 – Al igual que con las direcciones IP de multicast, hay un valor asignado especial para las direcciones MAC de multicast. Los primeros 24 bits se establecen en hexadecimal en: 01-00-5E. Los 6 dígitos hexadecimales restantes se derivan de los 23 bits inferiores de la IP de multicast.

- ○ 01-5E-00
- ○ FF-00-5E
- ○ FF-FF-FF
- ◉ 01-00-5E

11. ¿Qué hará un host en una red Ethernet si recibe una trama con una dirección MAC de destino que no coincide con su propia dirección MAC?

Tema 7.3.0 - En una red Ethernet, cada NIC de la red comprueba cada trama que llega para ver si la dirección MAC de destino de la trama coincide con su propia dirección MAC. Si no hay coincidencia, el dispositivo descarta la trama. Si hay una coincidencia, la NIC pasa la trama a la siguiente capa OSI.

- (●) Se descartará la trama.
- ( ) Reenviará la trama al siguiente host.
- ( ) Eliminará la trama del medio.
- ( ) Se quitará la trama de enlace de datos para comprobar la dirección IP de destino.

12. ¿Qué es auto-MDIX?

Tema 7.4.0 - Auto-MDIX es una característica que está habilitada en los switches Cisco más recientes y permite que el switch detecte y utilice cualquier tipo de cable que se conecte a un puerto específico.

- ( ) Un tipo de switch Cisco
- ( ) Un tipo de conector Ethernet
- ( ) Un tipo de puerto en un switch Cisco
- (●) Una característica que permite detectar el tipo de cable Ethernet

13. ¿Qué dos funciones u operaciones realiza la subcapa MAC? (Escoja dos).

Tema 7.1.0 - La subcapa MAC es la inferior de las dos subcapas de vínculos de datos y está más cerca de la capa física. Las dos funciones principales de la subcapa MAC son encapsular los datos de los protocolos de capa superior y controlar el acceso a los medios.

- [x] Es responsable del Control de Acceso a Medios.
- [ ] Realiza la función de software de controlador NIC.
- [x] Agrega un encabezado y un trailer para formar una PDU OSI de capa 2.
- [ ] Maneja la comunicación entre las capas superior e inferior.
- [ ] Agrega información de control a los datos de capa de protocolo de red.

14. ¿Qué tipo de dirección es 01-00-5E-0A-00-02?

Tema 7.2.0 -La dirección MAC de multicast es un valor especial que comienza con 01-00-5E en hexadecimal. Permite que un dispositivo origen envíe un paquete a un grupo de dispositivos.

- ( ) una dirección que llega a cada host dentro de una subred local
- ( ) una dirección que llega a un host específico
- ( ) una dirección que llega a todos los hosts de la red
- (●) una dirección que llega a un grupo específico de hosts

Correct

You have successfully identified the correct answers.

You got 14 out of 14 questions correct.

1. Which two characteristics describe Ethernet technology? (Choose two.)

Topic 7.1.0 - The 802.3 Ethernet standard specifies that a network implement the CSMA/CD access control method. Each node on the network has a unique MAC address for communication purposes.

- [x] It is supported by IEEE 802.3 standards.
- [ ] It is supported by IEEE 802.5 standards.
- [ ] It typically uses an average of 16 Mbps for data transfer rates.
- [x] It uses unique MAC addresses to ensure that data is sent to the appropriate destination.
- [ ] It uses a ring topology.

2. What statement describes a characteristic of MAC addresses?

Topic 7.2.0 - Any vendor selling Ethernet devices must register with the IEEE to ensure the vendor is assigned a unique 24-bit code, which becomes the first 24 bits of the MAC address. The last 24 bits of the MAC address are generated per hardware device. This helps to ensure globally unique addresses for each Ethernet device.

- (•) They must be globally unique.
- ( ) They are only routable within the private network.
- ( ) They are added as part of a Layer 3 PDU.
- ( ) They have a 32-bit binary value.

3. What is the special value assigned to the first 24 bits of a multicast MAC address transporting an IPv4 packet?

Topic 7.2.0 - Just as with multicast IP addresses, there is a special assigned value for multicast MAC addresses. The first 24 bits are set in hex to: 01-00-5E. The remaining 6 hex digits are derived from the lower 23 bits of the IP multicast.

- ( ) 01-5E-00
- ( ) FF-00-5E
- ( ) FF-FF-FF
- (•) 01-00-5E

4. What will a host on an Ethernet network do if it receives a frame with a unicast destination MAC address that does not match its own MAC address?

Topic 7.3.0 - In an Ethernet network, each NIC in the network checks every arriving frame to see if the destination MAC address in the frame matches its own MAC address. If there is no match, the device discards the frame. If there is a match, the NIC passes the frame up to the next OSI layer.

- (●) It will discard the frame.
- ( ) It will forward the frame to the next host.
- ( ) It will remove the frame from the media.
- ( ) It will strip off the data-link frame to check the destination IP address.

5. Which network device makes forwarding decisions based on the destination MAC address that is contained in the frame?

Topic 7.3.0 - Switches are the central connection point for a LAN and they maintain a MAC address table. The MAC address table has a port number associated with a MAC address for each particular device. The switch inspects a frame to look at the destination MAC address. The switch then looks in its MAC address table and if that MAC address is found, the switch forwards the data to the port that is associated with that particular MAC address.

- ( ) repeater
- ( ) hub
- (●) switch
- ( ) router

6. Which network device has the primary function to send data to a specific destination based on the information found in the MAC address table?

Topic 7.3.0 - If a MAC address is found in the MAC address table, then data is sent to the associated switch port. If the MAC address is not found in the MAC address table, the data is sent to all switch ports that have devices attached to the same network.

- ( ) hub
- ( ) router
- (●) switch
- ( ) modem

7. Which function or operation is performed by the LLC sublayer?

Topic 7.1.0 - The Ethernet LLC sublayer has the responsibility to handle communication between the upper layers and the lower layers of the protocol stack. The LLC is implemented in software and communicates with the upper layers of the application to transition the packet to the lower layers for delivery.

- It performs data encapsulation.
- (•) It communicates with upper protocol layers.
- It is responsible for media access control.
- It adds a header and trailer to a packet to form an OSI Layer 2 PDU.

8. What happens to runt frames received by a Cisco Ethernet switch?

Topic 7.1.0 - In an attempt to conserve bandwidth and not forward useless frames, Ethernet devices drop frames that are considered to be runt (less than 64 bytes) or jumbo (greater than 1500 bytes) frames.

- (•) The frame is dropped.
- The frame is returned to the originating network device.
- The frame is broadcast to all other devices on the same network.
- The frame is sent to the default gateway.

9. What addressing information is recorded by a switch to build its MAC address table?

Topic 7.3.0 - A switch builds a MAC address table by inspecting incoming Layer 2 frames and recording the source MAC address found in the frame header. The discovered and recorded MAC address is then associated with the port used to receive the frame.

- the destination Layer 3 address of incoming packets
- the destination Layer 2 address of outgoing frames
- the source Layer 3 address of outgoing packets
- (•) the source Layer 2 address of incoming frames

10. What is auto-MDIX?

Topic 7.4.0 - Auto-MDIX is a feature that is enabled on the latest Cisco switches and that allows the switch to detect and use whatever type of cable is attached to a specific port.

- ○ a type of Cisco switch
- ○ an Ethernet connector type
- ○ a feature to automatically determine speed and duplex
- ◉ a feature that detects Ethernet cable type

11. What type of address is 01-00-5E-0A-00-02?

Topic 7.2.0 - The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal. It allows a source device to send a packet to a group of devices.

- ○ an address that reaches every host inside a local subnet
- ○ an address that reaches one specific host
- ○ an address that reaches every host in the network
- ◉ an address that reaches a specific group of hosts

12. Which statement is true about MAC addresses?

Topic 7.2.0 - A MAC address is composed of 6 bytes. The first 3 bytes are used for vendor identification and the last 3 bytes must be assigned a unique value within the same OUI. MAC addresses are implemented in hardware. A NIC needs a MAC address to communicate over the LAN. The IEEE regulates the MAC addresses.

- ○ MAC addresses are implemented by software.
- ○ A NIC only needs a MAC address if connected to a WAN.
- ◉ The first three bytes are used by the vendor assigned OUI.
- ○ The ISO is responsible for MAC addresses regulations.

13. What are the two sizes (minimum and expected maximum) of an Ethernet frame? (Choose two.)

Topic 7.1.0 - The minimum Ethernet frame is 64 bytes. The maximum expected Ethernet frame is 1518 bytes. A network technician must know the minimum and expected maximum frame size in order to recognize runt and jumbo frames.

- ☐ 56 bytes
- ☑ 64 bytes
- ☐ 128 bytes
- ☐ 1024 bytes
- ☑ 1518 bytes

14. Which two functions or operations are performed by the MAC sublayer? (Choose two.)

Topic 7.1.0 - The MAC sublayer is the lower of the two data link sublayers and is closest to the physical layer. The two primary functions of the MAC sublayer are to encapsulate the data from the upper layer protocols and to control access to the media.

- ☑ It is responsible for Media Access Control.
- ☐ It performs the function of NIC driver software.
- ☑ It adds a header and trailer to form an OSI Layer 2 PDU.
- ☐ It handles communication between upper and lower layers.
- ☐ It adds control information to network protocol layer data.

Capítulo 8_Capa de red

Introducción

8.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Capa de red!

Por ahora puede haber notado que los módulos en este curso están progresando de abajo hacia arriba a través de las capas del modelo OSI. En la capa de red del modelo OSI, le presentamos protocolos de comunicación y protocolos de enrutamiento. Supongamos que desea enviar un correo electrónico a un amigo que vive en otra ciudad, o incluso en otro país. Esta persona no está en la misma red que usted. Una simple red conmutada no puede recibir su mensaje más allá del final de su propia red. Necesitas ayuda para mantener este mensaje en movimiento a lo largo del camino hacia el dispositivo final de tu amigo. Para enviar un correo electrónico (un video, un archivo, etc.) a cualquier persona que no esté en su red local, debe tener acceso a routers. Para acceder a los routers, debe usar protocolos de capa de red. Para ayudarle a visualizar estos procesos, este módulo contiene dos actividades Wireshark. ¡Disfrute!

8.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Capa de red

Objetivos del módulo: Explique cómo los routers utilizan los protocolos y los servicios de capa de red para habilitar la conectividad integral.

Título del tema	Objetivo del tema
Características de la capa de red	Explique cómo la capa de red utiliza los protocolos IP para una confiabilidad de comunicaciones.
Paquete IPv4	Explique la función de los principales campos de encabezado en el paquete IPv4.
Paquete IPv6	Explique la función de los principales campos de encabezado en el paquete IPv6.

Título del tema	Objetivo del tema
Cómo arma las rutas un host	Explique cómo los dispositivos de red usan tablas de enrutamiento para dirigir paquetes a un red de destino.
Tablas de enrutamiento de router	Explique la función de los campos en la tabla de enrutamiento de un router.

Capa de red / Características de la capa de red

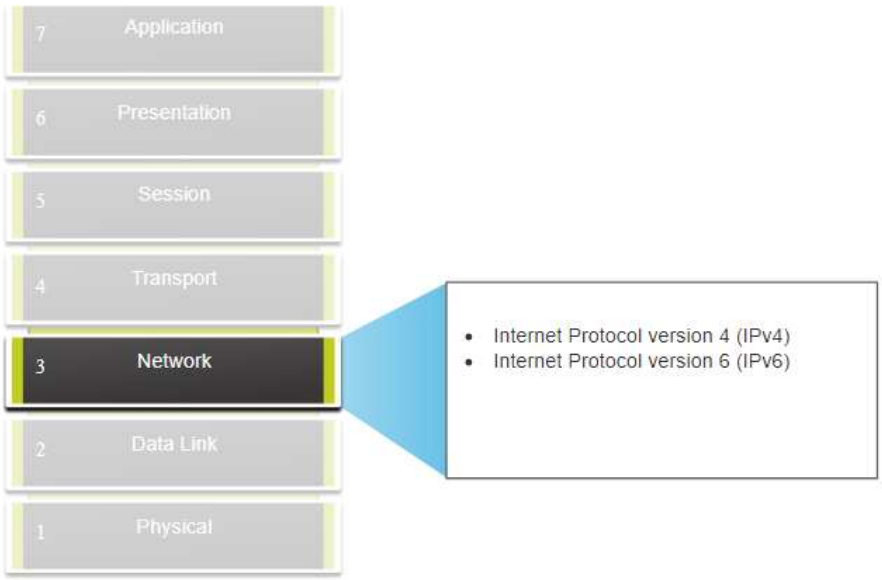
Características de la capa de red

8.1.1

La capa de red

La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. Como se muestra en la figura, IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red. Otros protocolos de capa de red incluyen protocolos de enrutamiento como Open Shortest Path First (OSPF) y protocolos de mensajería como Internet Control Message Protocol (ICMP).

Protocolos de capa de red

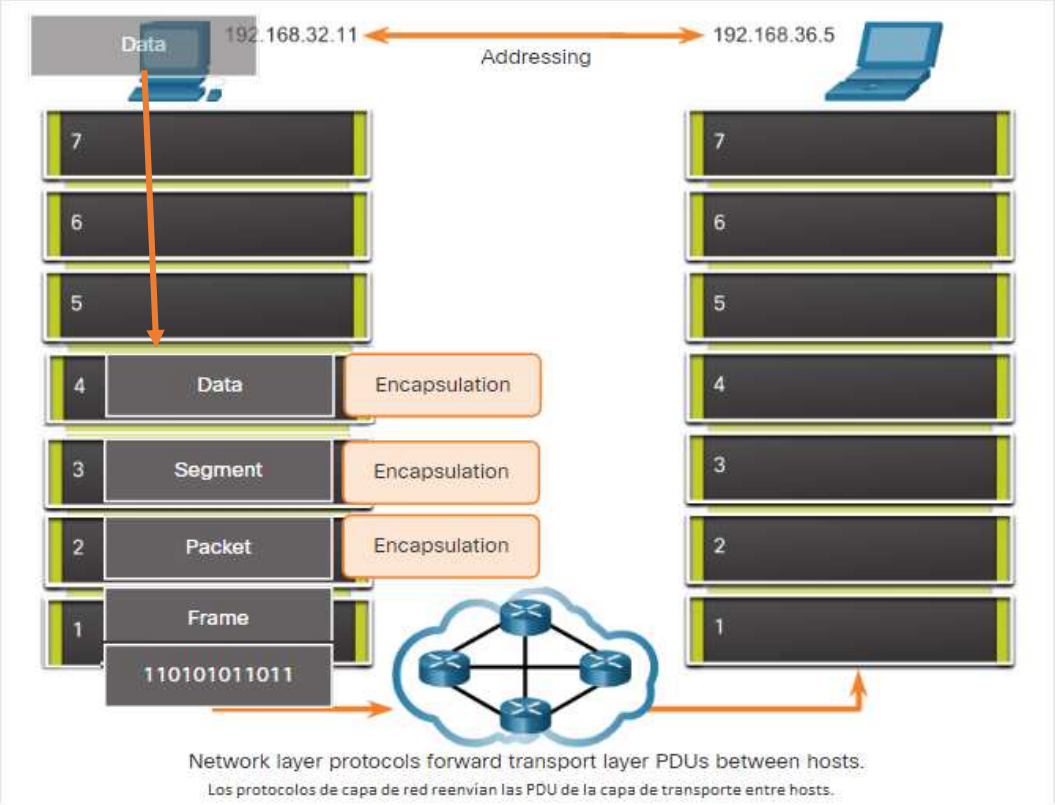


Para lograr comunicaciones end-to-end a través de los límites de la red, los protocolos de capa de red realizan cuatro operaciones básicas:

- **Direccionamiento de dispositivos finales**: los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.
- **Encapsulación:** La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores). El proceso de encapsulación lo realiza el origen del paquete IP.
- **Enrutamiento:** La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento". Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.
- **Desencapsulación:** Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte. El proceso de desencapsulación lo realiza el host de destino del paquete IP.

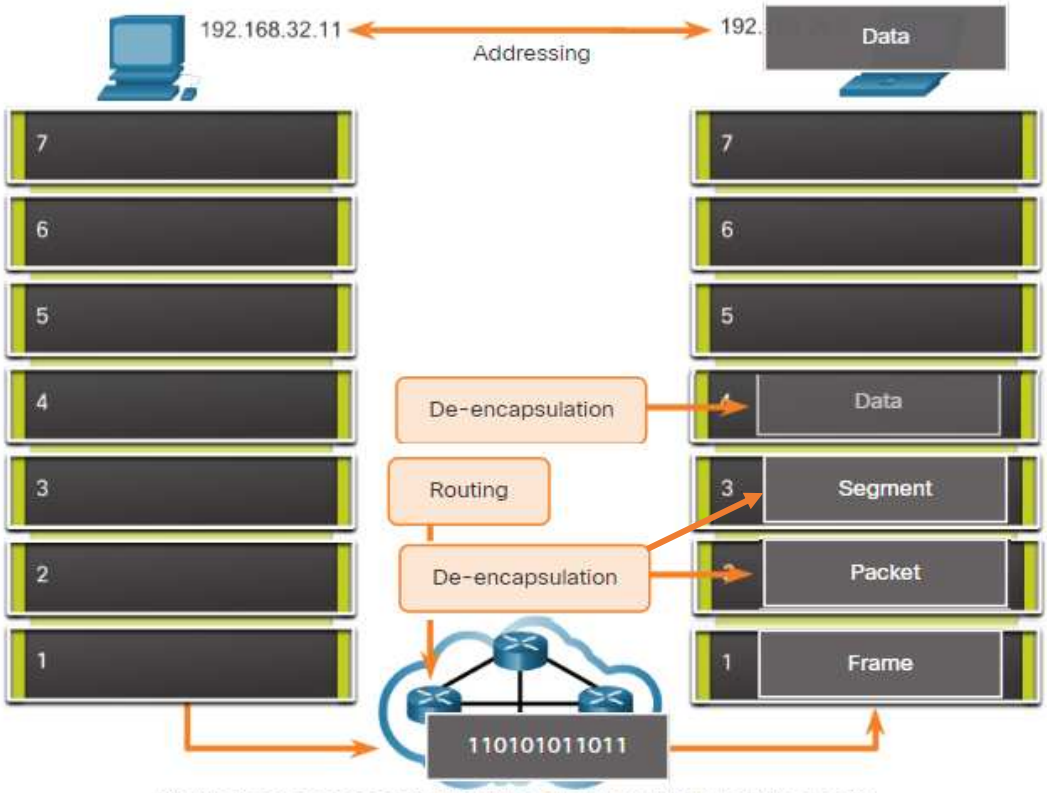
A diferencia de la capa de transporte (Capa OSI 4), que gestiona el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de comunicación de la capa de red (es decir, IPv4 e IPv6) especifican la estructura de paquetes y el procesamiento utilizado para transportar los datos de un host a otro host. La capa de red puede transportar paquetes de varios tipos de comunicación entre varios hosts porque funciona sin tener en cuenta los datos que contiene cada paquete.

Haga clic en Reproducir en la ilustración para ver una animación sobre el intercambio de datos.



Network layer protocols forward transport layer PDUs between hosts.

Los protocolos de capa de red reenvían las PDU de la capa de transporte entre hosts.



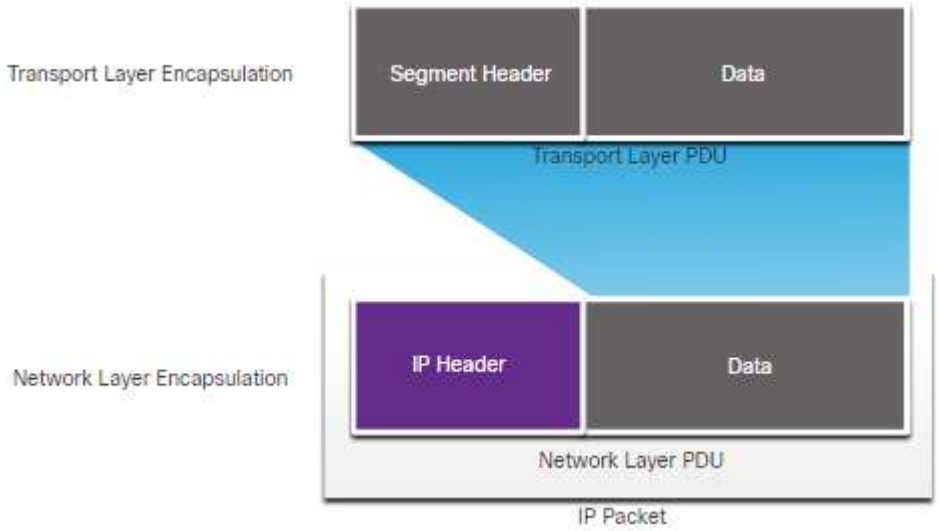
Network layer protocols forward transport layer PDUs between hosts.

8.1.2

Encapsulación IP

IP encapsula el segmento de la capa de transporte (la capa justo por encima de la capa de red) u otros datos agregando un encabezado IP. El encabezado IP se usa para entregar el paquete al host de destino.

La figura ilustra cómo la PDU de la capa de transporte es encapsulada por la PDU de la capa de red para crear un paquete IP.



La ilustración muestra la PDU de la capa de transporte encapsulada en un paquete IP. En la parte superior del gráfico está la encapsulación de la capa de transporte. Muestra el encabezado del segmento seguido de los datos. Esto comprende la PDU de capa de transporte. Esto se pasa a la capa de red para su posterior encapsulación y se convierte en la parte de datos de la PDU de capa de red. Se agrega un encabezado IP delante de los datos para crear el paquete IP.

El proceso de encapsulamiento de datos capa por capa permite que se desarrollen y se escalen los servicios en las diferentes capas sin afectar a las otras capas. Esto significa que IPv4 o IPv6 o cualquier protocolo nuevo que se desarrolle en el futuro puede armar sin inconvenientes un paquete con los segmentos de capa de transporte.

El encabezado IP es examinado por dispositivos de Capa 3 (es decir, routers y switches de Capa 3) a medida que viaja a través de una red a su destino. Es importante tener en cuenta que la información de direccionamiento IP permanece igual desde el momento en que el paquete sale del host de origen hasta que llega al host de destino, excepto cuando se traduce por el dispositivo que realiza la traducción de direcciones de red (NAT) para IPv4.

Nota: NAT se discute en módulos posteriores.

Los routers implementan protocolos de enrutamiento para enrutar paquetes entre redes. El enrutamiento realizado por estos dispositivos intermediarios examina el direccionamiento de la capa de red en el encabezado del paquete. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada u otros datos, permanece sin cambios durante los procesos de la capa de red.

8.1.3

Características de IP

IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.

Estas son las características básicas de la propiedad intelectual:

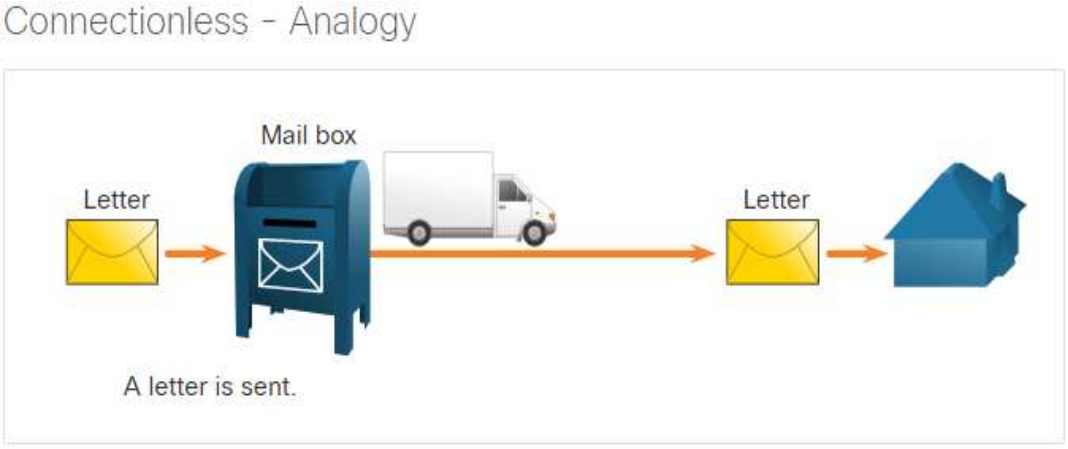
- **Sin conexión:** - no hay conexión con el destino establecido antes de enviar paquetes de datos.
- **Mejor esfuerzo:** - la IP es inherentemente poco confiable porque no se garantiza la entrega de paquetes.
- **Medios independientes:** - Medios independientes: la operación es independiente del medio (es decir, cobre, fibra óptica o inalámbrico) que transporta los datos.

8.1.4

Sin conexión

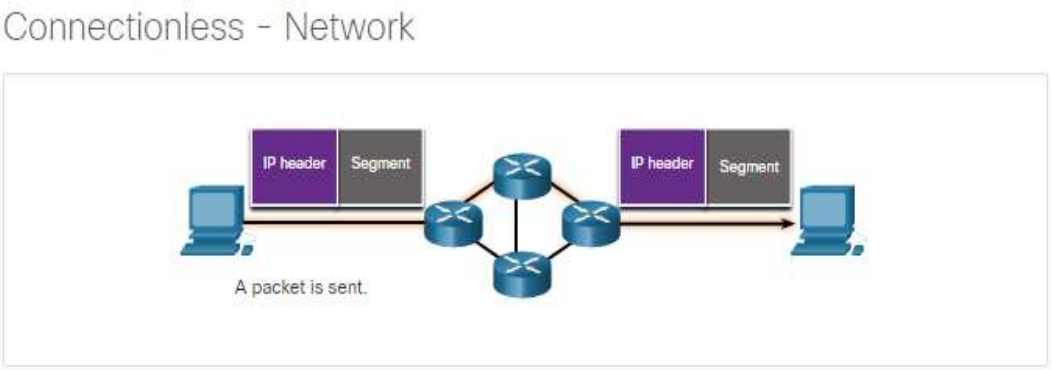
IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. La comunicación sin conexión es conceptualmente similar a enviar una carta a alguien sin notificar al destinatario por adelantado. La figura resume este punto clave.

un paquete, que consiste en un encabezado y un segmento IP, se envía desde un origen de una red a un destino de otra red



Se envía una carta.

Las comunicaciones de datos sin conexión funcionan con el mismo principio. Como se muestra en la figura, IP no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que se reenvíen los paquetes.



Se envía un paquete.

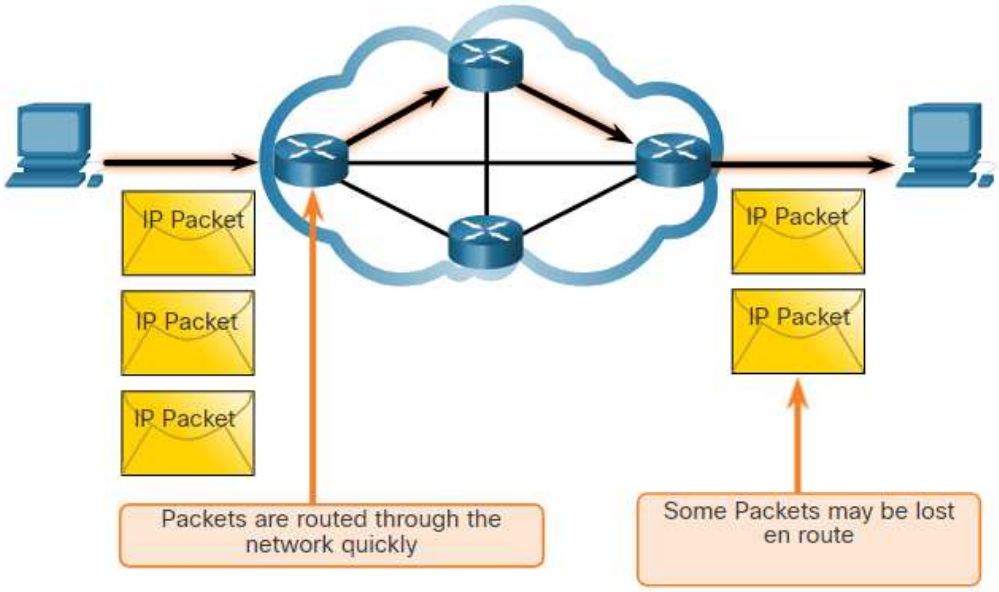
8.1.5

Servicio mínimo

La IP tampoco necesita campos adicionales en el encabezado para mantener una conexión establecida. Este proceso reduce en gran medida la sobrecarga del protocolo IP. Sin embargo, sin una conexión completa preestablecida, los remitentes no saben si los dispositivos de destino están presentes y en funcionamiento cuando envían paquetes, ni tampoco si el destinatario recibe el paquete o si puede acceder al paquete y leerlo.

El protocolo IP no garantiza que todos los paquetes que se envían, de hecho, se reciban. En la ilustración, se muestran las características de entrega de mejor esfuerzo o poco confiable del protocolo IP.

El diagrama muestra un origen en una red y un destino en otra red. Entre los dos hosts hay una nube que consta de cuatro routers en una topología de malla. Tres paquetes IP salen del host de origen, pero sólo dos llegan al host de destino. El texto del gráfico dice: Los paquetes se enrutan rápidamente a través de la red; Algunos paquetes pueden perderse en el camino.



Los paquetes se enrutan a través de la red rápidamente. Algunos paquetes pueden perderse en la ruta.

Dado que es un protocolo de capa de red no confiable, IP no garantiza que se reciban todos los paquetes enviados. Otros protocolos administran el proceso de seguimiento de paquetes y de aseguramiento de entrega.

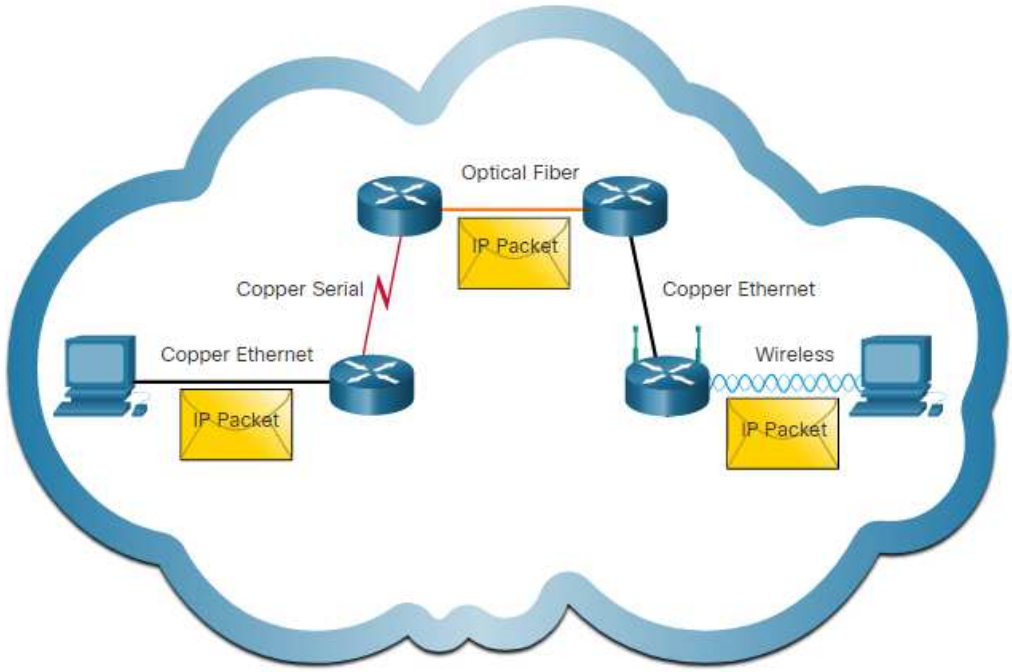
8.1.6

Independiente de los medios

Que sea poco confiable significa que IP no tiene la funcionalidad para administrar o recuperar paquetes no recibidos o dañados. Esto se debe a que, si bien los paquetes IP se envían con información sobre la ubicación de la entrega, no contienen información que pueda procesarse para informar al remitente si la entrega fue exitosa. Es posible que los paquetes lleguen dañados o fuera de secuencia al destino o que no lleguen en absoluto. IP no tiene la funcionalidad de retransmitir paquetes si se producen errores.

Las aplicaciones que utilizan los datos o los servicios de capas superiores deben solucionar problemas como el envío de paquetes fuera de orden o la pérdida de paquetes. Esta característica permite que IP funcione de manera muy eficaz. En el conjunto de protocolos TCP / IP, la confiabilidad es la función del protocolo TCP en la capa de transporte.

IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. Como se muestra en la ilustración, los paquetes IP pueden ser señales electrónicas que se transmiten por cables de cobre, señales ópticas que se transmiten por fibra óptica o señales de radio inalámbricas.



IP packets can travel over different media.

Los paquetes IP pueden trasladarse a través de diferentes medios.

El diagrama muestra una topología de red dentro de una nube con un paquete que viaja a través de varios tipos de medios entre dos hosts. Se muestra un paquete IP moviéndose entre un host y un router a través de una conexión Ethernet de cobre. El primer router está conectado al segundo router a través de una conexión en serie de cobre. Se muestra un paquete IP moviéndose entre el segundo router y el tercer router a través de una conexión de fibra óptica. El tercer router está conectado a un cuarto router, que es un router inalámbrico. Se muestra un paquete IP moviéndose entre el cuarto router y un host a través de una conexión inalámbrica.

La capa de enlace de datos OSI es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicación. Esto significa que la entrega de paquetes IP no se limita a ningún medio en particular.

Sin embargo, la capa de red tiene en cuenta una de las características más importantes del medio, que es el tamaño máximo de PDU que cada medio puede transportar. Esta característica se conoce como "unidad de transmisión máxima" (MTU). Parte del control de la comunicación entre la capa de enlace de datos y la capa de red consiste en establecer el

tamaño máximo del paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. La capa de red luego determina qué tamaño pueden tener los paquetes.

En algunos casos, un dispositivo intermedio, generalmente un router, debe dividir un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña. Este proceso se denomina "fragmentación de paquetes" o "fragmentación". La fragmentación provoca latencia. El router no puede fragmentar los paquetes IPv6.

8.1.7

Verifique su comprensión - Características de IP

Compruebe su comprensión de las características de la capa de red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correct

You have successfully identified the correct answers.

1. **Transport layer** PDUs, called segments, are encapsulated at the network layer by IPv4 and IPv6 into packets.
2. The **data link layer** receives IP packets from the network layer and encapsulates them for transmission over the medium.
3. **Fragmentation** is the process of splitting up IP packets to travel over a medium with a smaller MTU.
4. **Best effort** delivery does not guarantee packets will be delivered to the destination.

You got 4 out of 4 questions correct.

Correcto

Identificó bien las respuestas correctas.

1. Las PDU de la capa de transporte, denominadas segmentos, se encapsulan en la capa de red mediante IPv4 e IPv6 en paquetes.
2. La capa de enlace de datos recibe paquetes IP de la capa de red y los encapsula para su transmisión a través del medio.
3. La fragmentación es el proceso de división de paquetes IP para viajar a través de un medio con una MTU más pequeña.
4. La entrega del mejor esfuerzo no garantiza que los paquetes se entreguen al destino.

Has tenido 4 respuestas correctas de 4.

1. Which OSI layer sends segments to be encapsulated in an IPv4 or IPv6 packet?

You got it!

- ○ data link layer
- ○ network layer
- ◉ transport layer
- ○ session layer

2. Which layer is responsible for taking an IP packet and preparing it for transmission over the communications medium?

You got it!

- ○ physical layer
- ○ network layer
- ◉ data link layer
- ○ transport layer

2. Which layer is responsible for taking an IP packet and preparing it for transmission over the communications medium?

You got it!

- ○ physical layer
- ○ network layer
- ◉ data link layer
- ○ transport layer

3. What is the term for splitting up an IP packet when forwarding it from one medium to another medium with a smaller MTU?

You got it!

- ○ encapsulation
- ◉ fragmentation
- ○ segmentation
- ○ serialization

4. Which delivery method does not guarantee that the packet will be delivered fully without errors?

You got it!

- ○ connectionless
- ◉ best effort
- ○ media independent

1. ¿Qué capa OSI envía segmentos para ser encapsulados en un paquete IPv4 o IPv6?

¡Lo tienes!

- Capa de enlace de datos
- Capa de red
- (•) Capa de transporte
- Capa de sesión

2. ¿Qué capa es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicación?

¡Lo tienes!

- capa física
- Capa de red
- (•) Capa de enlace de datos
- Capa de transporte

3. ¿Cuál es el término para dividir un paquete IP al reenviarlo de un medio a otro medio con una MTU más pequeña?

¡Lo tienes!

- encapsulación
- (•) fragmentación
- segmentación
- serialización

4. ¿Qué método de entrega no garantiza que el paquete se entregará completamente sin errores?

¡Lo tienes!

- sin conexión
- (•) mejor esfuerzo
- independiente de los medios

Capa de red / Paquete IPv4

Paquete IPv4

8.2.1

Encabezado de paquetes IPv4

IPv4 es uno de los protocolos de comunicación de la capa de red principal. El encabezado del paquete IPv4 se utiliza para garantizar que este paquete se entrega en su siguiente parada en el camino a su dispositivo final de destino.

El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3.

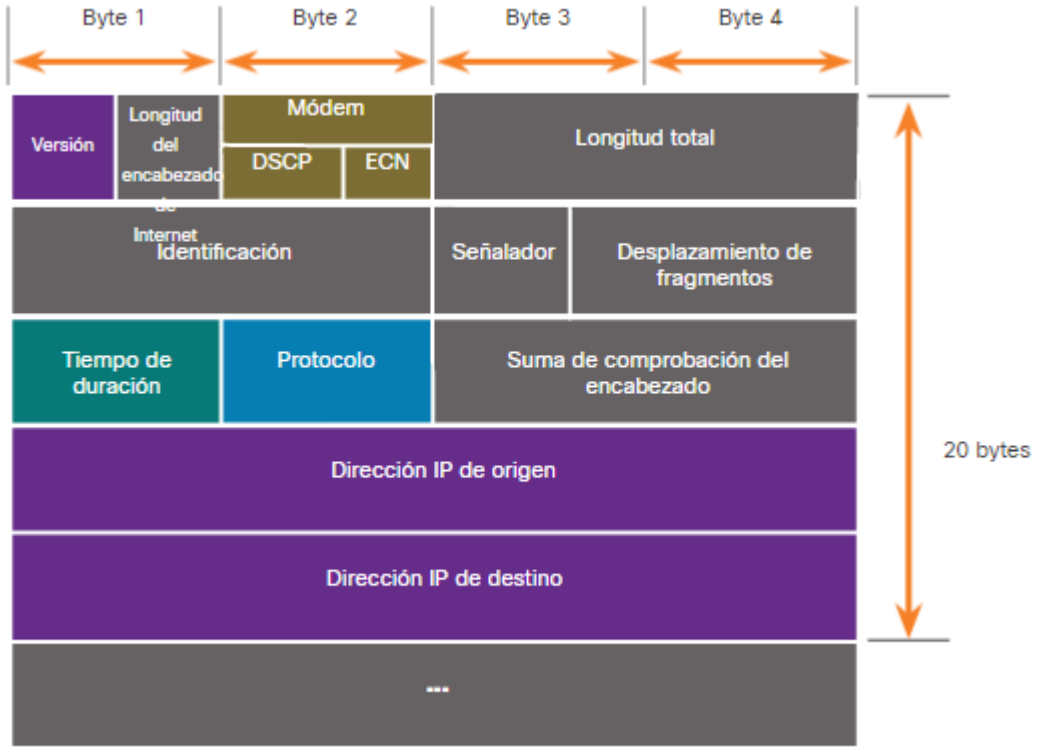
8.2.2

Campos de encabezado de paquete IPv4

Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo, proporcionan una representación visual de consulta al analizar los campos de protocolo. El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv4.

Nombres y longitud de bits de los campos en un encabezado de paquete IPv4.

Campos del encabezado de paquetes IPv4



Los campos significativos en el encabezado IPv4 incluyen lo siguiente:

- **Versión -** Contiene un valor binario de 4 bits establecido en 0100 que identifica esto como un paquete IPv4.
- **Servicios diferenciados o DiffServ (DS):** Anteriormente llamado campo de tipo de servicio (ToS), el campo DS es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los seis bits más significativos del campo DiffServ son los bits de punto de código de servicios diferenciados (DSCP) y los dos últimos bits son los bits de notificación de congestión explícita (ECN).
- **Suma de comprobación deencabezado:** se utiliza para detectar daños en el encabezado IPv4.
- **Tiempo de duración (Time to Live, TTL):** TTL contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del paquete IPv4 establece el valor TTL inicial. Se reduce en uno cada vez que el paquete es procesado por un router. Si el campo TTL llega a cero, el router descarta el paquete y envía a la dirección IP de origen un mensaje de tiempo superado del protocolo de mensajes de control de Internet (ICMP). Debido a que el router disminuye el TTL de cada paquete, el router también debe volver a calcular la suma de comprobación de encabezado.
- **Protocolo:** Este campo se utiliza para identificar el protocolo de siguiente nivel. Este valor binario de 8 bits indica el tipo de carga de datos que lleva el paquete, lo que permite que la capa de red transmita los datos al protocolo de capa superior apropiado. ICMP (1), TCP (6) y UDP (17) son algunos valores comunes.
- **Dirección IPv4 de origen:** Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen siempre es una dirección de unidifusión.
- **Dirección IPv4 de destino:** Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección de unidifusión, de multidifusión o de difusión.

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino En estos campos, se identifica de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian mientras se viaja desde el origen hasta el destino.

Para identificar y validar el paquete, se usan los campos de longitud del encabezado de Internet (IHL), longitud total y el encabezado checksum.

Para reordenar un paquete fragmentado, se usan otros campos. Específicamente, el paquete IPv4 utiliza los campos de identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña.

Los campos Opciones y Relleno rara vez se usan y están fuera del alcance de este módulo.

8.2.3

Video: ejemplos de encabezados IPv4 en Wireshark

Haga clic en Reproducir en la ilustración para ver una demostración de una revisión de encabezados IPv4 en una captura de Wireshark.

8.2.4

Verifique su comprensión - Paquete IPv4

Verifique su comprensión del paquete IPv4 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Los campos de encabezado IP que identifican dónde se originó el paquete y hacia dónde se dirige son Dirección IP de origen y Dirección IP de destino.
2. Las direcciones IP de origen y destino del paquete IP no cambian en la ruta de origen a destino.
3. El campo Suma de comprobación de encabezado en un encabezado IPv4 se utiliza para detectar paquetes corruptos.
4. El campo de protocolo identifica el protocolo de capa superior que se transporta dentro del paquete IP. Los protocolos comunes son TCP, UDP e ICMP.

Has tenido 4 respuestas correctas de 4.

Correct

You have successfully identified the correct answers.

1. The IP header fields that identify where the packet originated and where it is going are **Source IP Address** and **Destination IP Address**.
2. **The source and destination IP addresses in the IP packet do not change** in route from source to destination.
3. The **Header Checksum** field in an IPv4 header is used to detect corrupt packets.
4. The **protocol** field identifies the upper layer protocol that is carried inside the IP packet. Common protocols are TCP, UDP, and ICMP.

You got 4 out of 4 questions correct.

1. ¿Cuáles son los dos campos a los que se hace referencia más comúnmente en un encabezado de paquete IPv4 que indican de dónde viene el paquete y hacia dónde va? (Escoja dos opciones).

¡Lo tienes!

- [x] Dirección IP de destino
- [ ] protocolo
- [ ] Duración
- [x] Dirección IP de origen
- [ ] Servicios diferenciados (DS)

2. ¿Qué declaración es correcta acerca de los campos de encabezado de paquetes IPv4?

¡Lo tienes!

- (•) Las direcciones IPv4 de origen y destino siguen siendo las mismas mientras se viaja de origen a destino.
- ( ) El campo Tiempo de vida se utiliza para determinar la prioridad de cada paquete.
- ( ) Los campos Longitud total y Suma de comprobación de encabezado se utilizan para reordenar un paquete fragmentado.
- ( ) El campo Versión identifica el protocolo de siguiente nivel.

3. ¿Qué campo se utiliza para detectar daños en el encabezado IPv4?

¡Lo tienes!

- (•) Suma de comprobación del encabezado
- ( ) Duración
- ( ) Protocolo
- ( ) Servicios diferenciados (DS)

4. ¿Qué campo incluye valores comunes como ICMP (1), TCP (6) y UDP (17)?

¡Lo tienes!

- ○ Suma de comprobación del encabezado
- ○ Duración
- ◉ Protocolo
- ○ Servicios diferenciados (DS)

1. What are the two most commonly referenced fields in an IPv4 packet header that indicate where the packet is coming from and where it is going? (Choose two.)

You got it!

- ☑ destination IP address
- ☐ protocol
- ☐ Time to Live
- ☑ source IP address
- ☐ Differentiated Services (DS)

2. Which statement is correct about IPv4 packet header fields?

You got it!

- ◉ The source and destination IPv4 addresses remain the same while travelling from source to destination.
- ○ The Time to Live field is used to determine the priority of each packet.
- ○ The Total Length and Header Checksum fields are used to reorder a fragmented packet.
- ○ The Version field identifies the next level protocol.

3. Which field is used to detect corruption in the IPv4 header?

You got it!

- ◉ Header Checksum
- ○ Time to Live
- ○ Protocol
- ○ Differentiated Services (DS)

4. Which field includes common values such as ICMP (1), TCP (6), and UDP (17)?

You got it!

- ○ Header Checksum
- ○ Time to Live
- ◉ Protocol
- ○ Differentiated Services (DS)

Paquete IPv6

8.3.1

Limitaciones de IPv4

IPv4 todavía está en uso hoy en día. Este tema trata sobre IPv6, que eventualmente reemplazará a IPv4. Para comprender mejor por qué necesita conocer el protocolo IPv6, ayuda a conocer las limitaciones de IPv4 y las ventajas de IPv6.

A lo largo de los años, se han elaborado protocolos y procesos adicionales para hacer frente a los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de la dirección IPv4:** IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
- **Falta de conectividad de extremo a extremo:** La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4. NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
- **Mayor complejidad de la red**: mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6. NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.

8.3.2

Información general sobre IPv6

A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de trabajo de ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo. Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.

Las mejoras que ofrece IPv6 incluyen las siguientes:

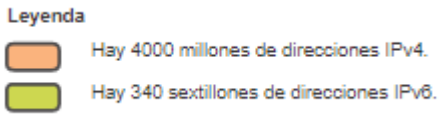
- **Manejo de paquetes mejorado:** - las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en lugar de IPv4 con 32 bits.
- **Mejor manejo de paquetes** - Manejo de paquetes mejorado: el encabezado IPv6 se ha simplificado con menos campos.
- **Elimina la necesidad de NAT:** - Elimina la necesidad de NAT: con una cantidad tan grande de direcciones IPv6 públicas, no se necesita NAT entre una dirección IPv4 privada y una IPv4 pública. Esto evita algunos de los problemas inducidos por NAT que experimentan las aplicaciones que requieren conectividad de extremo a extremo.

El espacio de las direcciones IPv4 de 32 bits ofrece aproximadamente 4.294.967.296 direcciones únicas. El espacio de direcciones IPv6 proporciona 340,282,366,920,938,463,463,374,607,431,768,211,456, o 340 undecillones de direcciones. Esto es aproximadamente equivalente a cada grano de arena en la Tierra.

En la ilustración, se puede ver una comparación entre el espacio de direcciones IPv4 e IPv6.

Comparación del espacio de direcciones IPv4 e IPv6

Nombre del número	Notación científica	Cantidad de ceros
Mil	10^3	1000
1 millón	10^6	1 000000
1000 millones	10^9	1000000000
1 billón	10^12	1000000000000
1000 billones	10^15	1000000000000000
1 trillón	10^18	1000000000000000000
1000 trillones	10^21	10000000000000000000000
1 cuatrillón	10^24	100000000000000000000000
1000 cuatrillones	10^27	1000000000000000000000000000
1 quintillón	10^30	10000000000000000000000000000
1000 quintillones	10^33	100000000000000000000000000000000
1 sextillón	10^36	1000000000000000000000000000000000



8.3.3

Campos de encabezado de paquete IPv4 en el encabezado de paquete IPv6

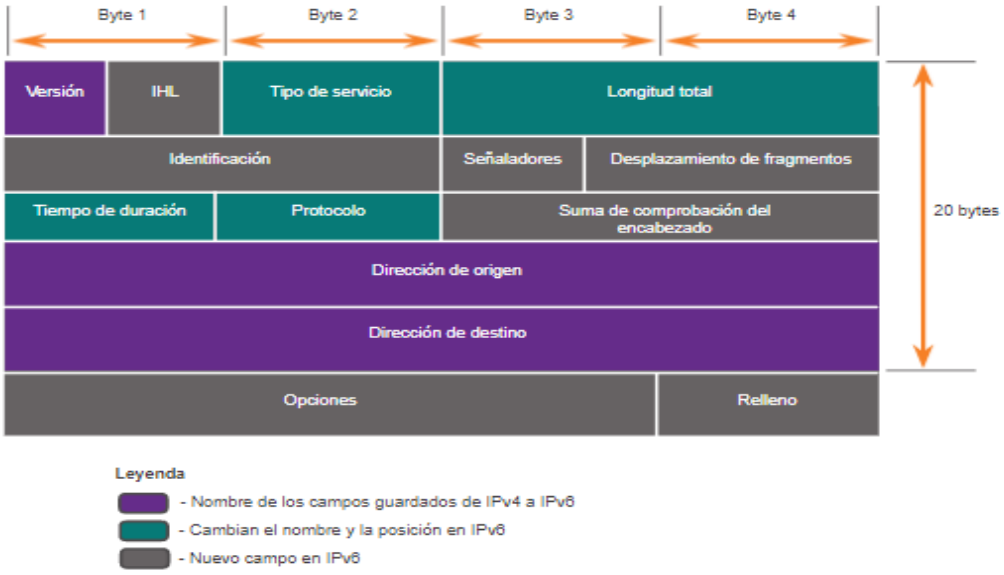
Uno de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6.

Por ejemplo, el encabezado IPv4 consiste en un encabezado de longitud variable de 20 octetos (hasta 60 bytes si se usa el campo Opciones) y 12 campos de encabezado básicos, sin incluir el campo Opciones y el campo Relleno.

Para IPv6, algunos campos se han mantenido igual, algunos campos han cambiado de nombre y posición, y algunos campos de IPv4 ya no son necesarios, como se destaca en la figura.

El diagrama muestra un encabezado de paquete IPv4 e indica qué campos mantenían el mismo nombre, qué campos cambiaron nombres y posición y qué campos no se mantuvieron en IPv6. Los campos que mantienen el mismo nombre son: versión, dirección de origen y dirección de destino. Los campos que cambiaron los nombres y la posición son: tipo de servicio, duración total, tiempo de vida y protocolo. Los campos que no se mantuvieron en IPv6 son: IHL, identificación, indicadores, desplazamiento de fragmentos, suma de comprobación de encabezado, opciones y relleno.

Encabezado de paquetes IPv4



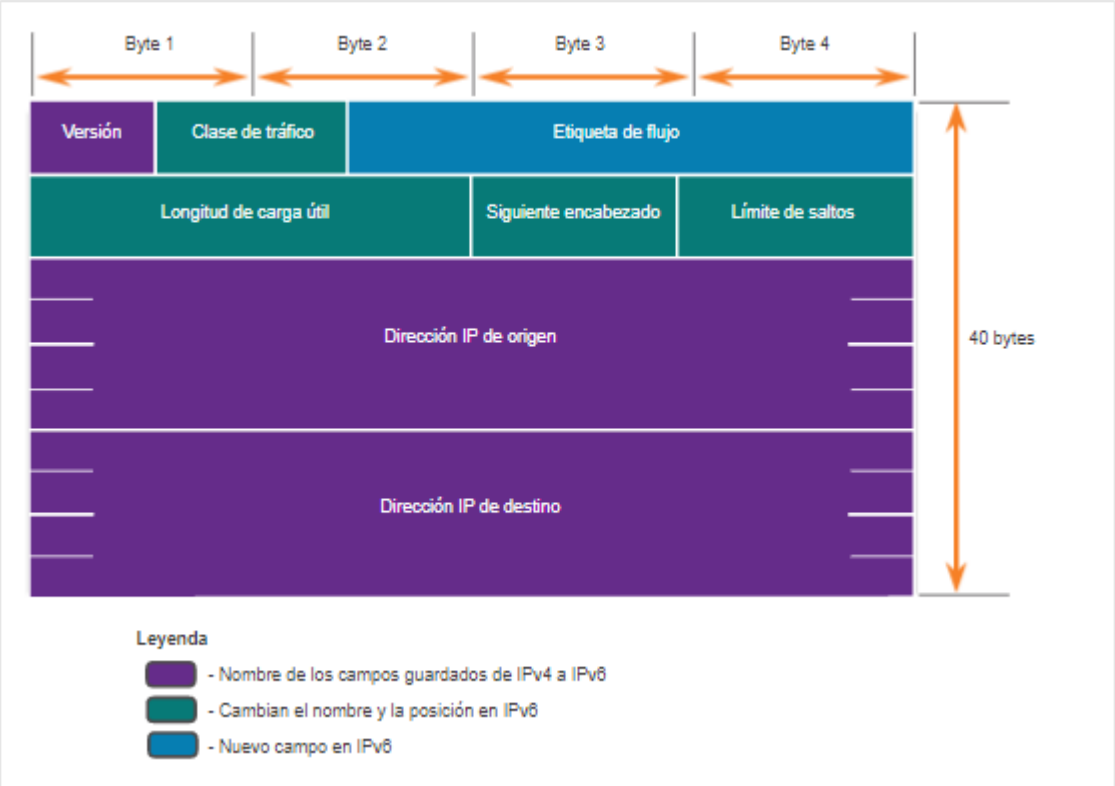
La figura muestra los campos de encabezado de paquete IPv4 que se mantuvieron, movieron, cambiaron, así como aquellos que no se mantuvieron en el encabezado de paquete IPv6.

En contraste, el encabezado IPv6 simplificado que se muestra en la siguiente figura consiste en un encabezado de longitud fija de 40 octetos (en gran parte debido a la longitud de las direcciones IPv6 de origen y destino).

El encabezado simplificado IPv6 permite un procesamiento más eficiente de encabezados IPv6.

El diagrama muestra un encabezado de paquete IPv6 e indica qué campos mantenían el mismo nombre de IPv4 a IPv6, qué campos cambiaron nombres y posición en IPv6, qué campos no se guardaban en IPv6 y nuevos campos en IPv6. Los nombres de campo que se mantuvieron iguales son: versión, dirección IP de origen y dirección IP de destino. Los campos que cambiaron los nombres y la posición en IPv6 son: clase de tráfico, longitud de carga útil, encabezado siguiente y límite de salto. El campo que es NUEVO para IPv6 es la etiqueta de flujo.

Encabezado de paquetes IPv6



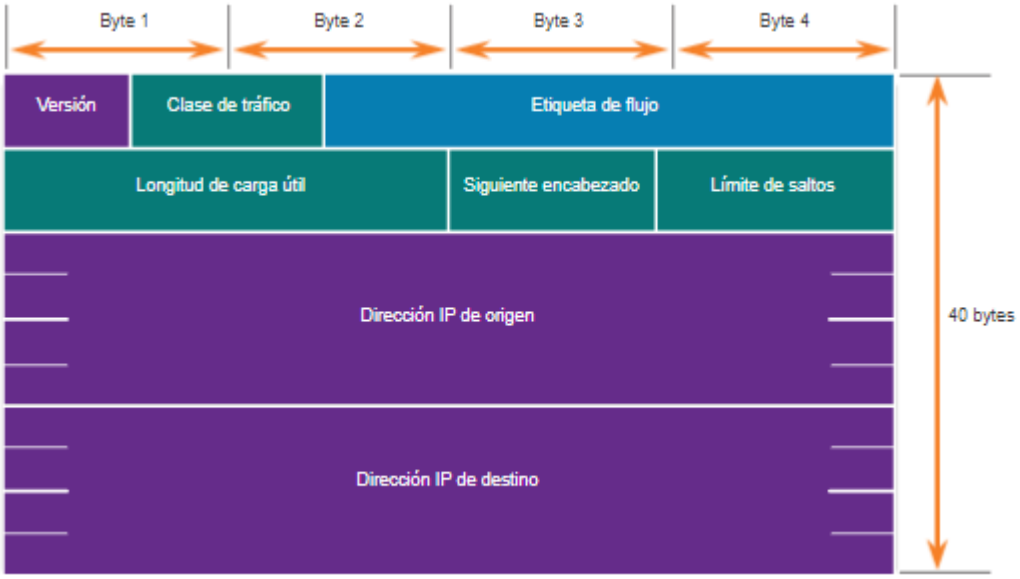
La figura muestra los campos de encabezado de paquetes IPv4 que se mantuvieron o movieron junto con los nuevos campos de encabezado de paquetes IPv6.

8.3.4

Encabezado de paquetes IPv6

El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv6.

Campos del encabezado de paquetes IPv6



Nombres y longitud de bits de los campos en un encabezado IPv6

Los campos en el encabezado del paquete IPv6 incluyen lo siguiente:

- **Versión -** Este campo contiene un valor binario de 4 bits establecido en 0110 que identifica esto como un paquete IP versión 6.
- **Clase de tráfico:** Este campo de 8 bits es equivalente al campo de Servicios diferenciados (DS) IPv4.
- **Etiqueta de flujo:** Este campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo por routers.
- **Longitud de carga útil -** Este campo de 16 bits indica la longitud de la porción de datos o carga útil del paquete IPv6. Esto no incluye la longitud del encabezado IPv6, que es un encabezado fijo de 40 bytes.
- **Encabezado siguiente:** Este campo de 8 bits es equivalente al campo de Protocolo IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de salto**: este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje ICMPv6 Tiempo excedido al host emisor. Esto indica que el paquete no llegó a su destino porque se excedió el límite de saltos. A diferencia de IPv4, IPv6 no incluye una suma de comprobación de encabezado IPv6, ya que esta función se realiza tanto en las capas inferior como superior. Esto significa que la suma de comprobación no necesita ser recalculada por cada router cuando disminuye el campo Límite de saltos, lo que también mejora el rendimiento de la red.
- **Dirección IPv6 de origen -** Este campo de 128 bits identifica la dirección IPv6 del host emisor.
- **Dirección IPv6 de destino:** Este campo de 128 bits identifica la dirección IPv6 del host receptor.

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están

ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.

A diferencia de IPv4, los routers no fragmentan de los paquetes IPv6 enrutados.

8.3.5

Video: ejemplos de encabezados IPv6 en Wireshark

Haga clic en Reproducir en la ilustración para ver una demostración de una revisión de encabezados IPv6 en una captura de Wireshark.

8.3.6

Verifique su comprensión - Paquete IPv6

Verifique su comprensión del paquete IPv6 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. IPv4 se estandarizó en la década de 1980 y tiene varias limitaciones tecnológicas, como la falta de conectividad de extremo a extremo y un espacio de direcciones agotado.
2. Hay varias mejoras técnicas realizadas en IPv6, dos de las cuales son un grupo de direcciones IP mucho más grande y un encabezado de protocolo simplificado.
3. El encabezado IPv6 tiene una longitud fija de 40 octetos y contiene 8 campos de encabezado.
4. Varios campos del encabezado IPv6 reemplazaron los campos del encabezado IPv4. Por ejemplo, el campo Límite de saltos reemplazó al campo Tiempo de vida del encabezado IPv4.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuáles son las tres opciones principales problemas asociados con IPv4? (Escoja tres opciones).

¡Lo tienes!

- [x] Agotamiento de direcciones IP
- [x] mayor complejidad de la red y expansión de la tabla de enrutamiento de Internet
- [ ] siempre en conexiones
- [x] falta de conectividad de extremo a extremo
- [ ] fronteras mundiales y políticas
- [ ] demasiadas direcciones IPv4 disponibles

2. ¿Cuáles dos opciones son mejoras proporcionadas por IPv6 en comparación con IPv4? (Escoja dos opciones).

¡Lo tienes!

- [ ] admite campos adicionales para paquetes complejos
- [x] aumentó el espacio de la dirección IP
- [ ] estandariza el uso de NAT
- [ ] admite redes basadas en clases
- [x] utiliza un encabezado más simple para proporcionar un manejo mejorado de paquetes

3. ¿Cuál es el verdadero del encabezado IPv6?

¡Lo tienes!

- [ ] consta de 20 octetos.
- [x] consta de 40 octetos.
- [x] contiene 8 campos de encabezado.
- [ ] contiene 12 campos de encabezado.

4. ¿Cuál es el verdadero del encabezado del paquete IPv6?

¡Lo tienes!

- (•) El campo Límite de salto reemplaza el campo Tiempo de vida IPv4.
- ( ) Las direcciones IPv6 de origen y destino cambian mientras se viaja de origen a destino.
- ( ) El campo Tiempo de vida reemplaza al campo DiffServ.
- ( ) El campo Versión identifica el siguiente encabezado.

Correct

You have successfully identified the correct answers.

1. IPv4 was standardized in the 1980s and has several technological limitations, such as lack of end-to-end connectivity and a depleted address space.
2. There are several technical improvements made to IPv6, two of which are a vastly larger IP address pool and a simplified protocol header.
3. The IPv6 header is a fixed length of 40 octets and contains 8 header fields.
4. Several fields in the IPv6 header replaced fields in the IPv4 header. For example, the Hop Limit field replaced the IPv4 header Time to Live field.

You got 4 out of 4 questions correct.

1. Which three options are major issues associated with IPv4? (Choose three.)

You got it!

- [x] IP address depletion
- [x] increased network complexity and Internet routing table expansion
- [ ] always on connections
- [x] lack of end-to-end connectivity
- [ ] global and political boundaries
- [ ] too many IPv4 addresses available

2. Which two options are improvements provided by IPv6 as compared to IPv4? (Choose two.)

You got it!

- [ ] header supports additional fields for complex packets
- [x] increased the IP address space
- [ ] standardizes the use of NAT
- [ ] supports class-based networks
- [x] uses a simpler header to provide improved packet handling

3. Which is true of the IPv6 header?

You got it!

- [ ] it consists of 20 octets.
- [x] it consists of 40 octets.
- [x] it contains 8 header fields.
- [ ] it contains 12 header fields.

4. Which is true of the IPv6 packet header?

You got it!

- (•) The Hop Limit field replaces the IPv4 Time to Live field.
- ( ) The Source and Destination IPv6 addresses change while travelling from source to destination.
- ( ) The Time to Live field replaces the DiffServ field.
- ( ) The Version field identifies the next header.

Capa de red / ¿Cómo arma las rutas el host?

¿Cómo arma las rutas el host?

8.4.1

La decisión de reenvío de host

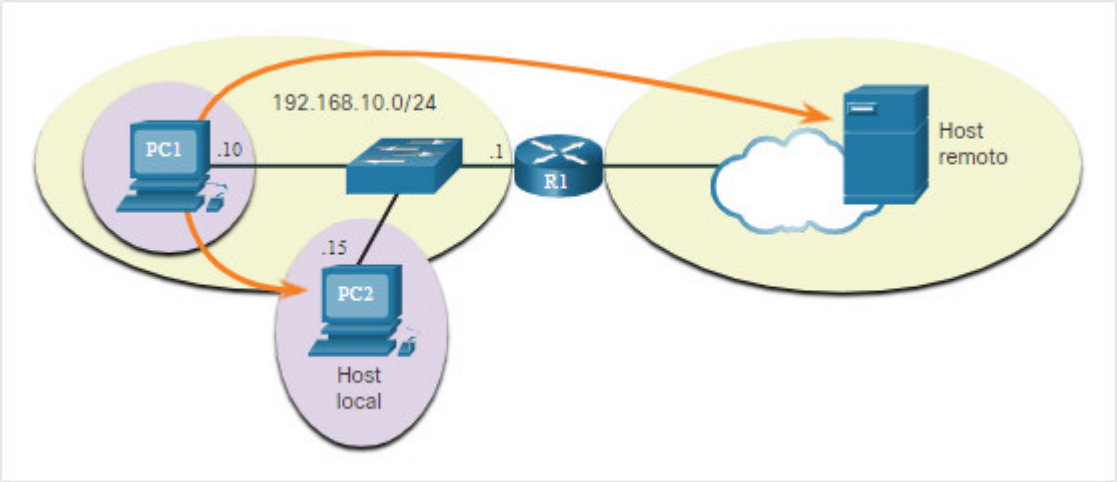
Con IPv4 e IPv6, los paquetes siempre se crean en el host de origen. El host de origen debe poder dirigir el paquete al host de destino. Para ello, los dispositivos finales de host crean su propia tabla de enrutamiento. En este tema se explica cómo los dispositivos finales utilizan las tablas de enrutamiento.

Otra función de la capa de red es dirigir los paquetes entre hosts. Un host puede enviar un paquete de la forma siguiente:

- **Itself** - Un host puede hacer ping a sí mismo enviando un paquete a una dirección IPv4 especial de 127.0.0.1 o una dirección IPv6 ::1, que se conoce como la interfaz de bucle invertido. El hacer ping a la interfaz de bucle invertido, pone a prueba la pila del protocolo TCP/IP en el host.
- **Host local \:** - este es un host de destino que se encuentra en la misma red local que el host emisor. Los hosts de origen y destino comparten la misma dirección de red.

- **Host remoto \:** este es un host de destino en una red remota. Los hosts de origen y destino no comparten la misma dirección de red.

La figura ilustra la conexión de PC1 a un host local en la misma red y a un host remoto ubicado en otra red.



El diagrama muestra un host, PC1, que se conecta a un host local, PC2, en la misma red y a un host remoto, un servidor, en otra red. PC1 y PC2 están conectados a un switch en la red 192.168.10.0/24. PC1 tiene una dirección de.10 y PC2 tiene una dirección de.15. El switch está conectado a un router, R1, en la dirección .1. En el otro lado de la R1 hay una conexión a la nube donde reside el host remoto.

El dispositivo final de origen determina si un paquete está destinado a un host local o a un host remoto. El dispositivo final de origen determina si la dirección IP de destino está en la misma red en la que está el propio dispositivo de origen. El método de determinación varía según la versión IP:

- **En IPv4**: el dispositivo de origen utiliza su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para realizar esta determinación.
- **En IPv6**: el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red.

En una red doméstica o comercial, puede tener varios dispositivos cableados e inalámbricos interconectados mediante un dispositivo intermediario, como un switch LAN o un punto de acceso inalámbrico (WAP). Este dispositivo intermediario proporciona interconexiones entre hosts locales en la red local. Los hosts locales pueden conectarse y compartir información sin la necesidad de dispositivos adicionales. Si un host está enviando un paquete a un dispositivo que está configurado con la misma red IP que el dispositivo host, el paquete simplemente se reenvía desde la interfaz del host, a través del dispositivo intermediario, y directamente al dispositivo de destino.

Por supuesto, en la mayoría de las situaciones queremos que nuestros dispositivos puedan conectarse más allá del segmento de red local, como a otros hogares, negocios e Internet.

Los dispositivos que no están en el segmento de red local se denominan "módulo remoto de E/S". Cuando un dispositivo de origen envía un paquete a un dispositivo de destino remoto, se necesita la ayuda de los routers y del enrutamiento. El enrutamiento es el proceso de identificación de la mejor ruta para llegar a un destino. El router conectado al segmento de red local se denomina gateway predeterminado.

8.4.2

Gateway predeterminado

La puerta de enlace predeterminada es el dispositivo de red (es decir, el router o el switch de capa 3) que puede enrutar el tráfico a otras redes. Si se piensa en una red como si fuera una habitación, el gateway predeterminado es como la puerta. Si desea ingresar a otra habitación o red, debe encontrar la puerta.

En una red, una puerta de enlace predeterminada suele ser un router con estas características:

- Tiene una dirección IP local en el mismo rango de direcciones que otros hosts en la red local.
- Puede aceptar datos en la red local y reenviar datos fuera de la red local.
- Enruta el tráfico a otras redes.

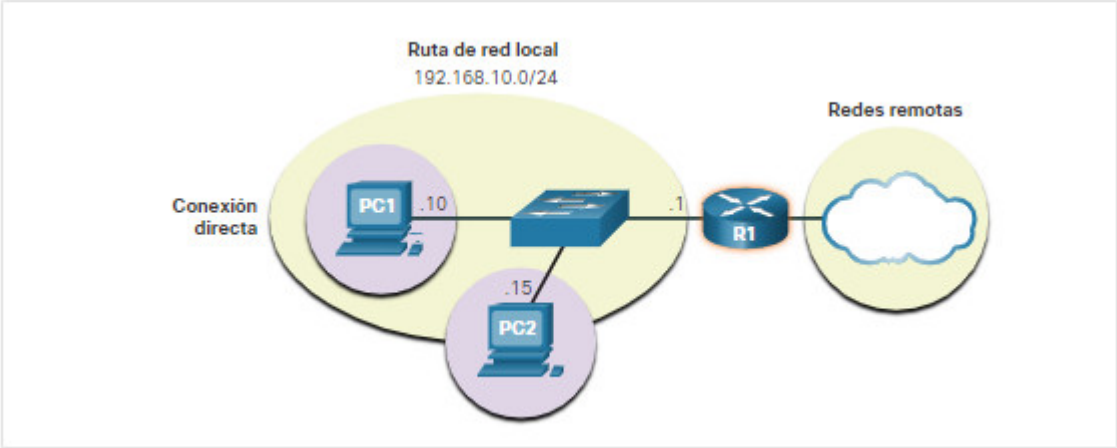
Se requiere una puerta de enlace predeterminada para enviar tráfico fuera de la red local. El tráfico no se puede reenviar fuera de la red local si no hay una puerta de enlace predeterminada, la dirección de la puerta de enlace predeterminada no está configurada o la puerta de enlace predeterminada está desactivada.

8.4.3

Un host enruta a la puerta de enlace predeterminada

Una tabla de enrutamiento de host generalmente incluirá una puerta de enlace predeterminada. En IPv4, el host recibe la dirección IPv4 de la puerta de enlace predeterminada, ya sea dinámicamente desde el Protocolo de configuración dinámica de host (DHCP) o configurado manualmente. En IPv6, el router anuncia la dirección de la puerta de enlace predeterminada o el host se puede configurar manualmente.

En la figura, PC1 y PC2 están configuradas con la dirección IPv4 de 192.168.10.1 como la puerta de enlace predeterminada.



El diagrama muestra dos hosts, PC1 y PC2, conectados a un switch en la red 192.168.10.0/24, la ruta de red local. El switch está conectado a un router, R1, que luego se conecta a la nube que representa redes remotas. PC1 tiene una dirección de.10, PC2 tiene una dirección de.15 y la interfaz del router a la que está conectado el switch tiene una dirección de .1. Las PC, el switch y la interfaz del router tienen una conexión directa.

La configuración de un gateway predeterminado genera una ruta predeterminada en la tabla de enrutamiento de la PC. Una ruta predeterminada es la ruta o camino que la PC utiliza cuando intenta conectarse a la red remota.

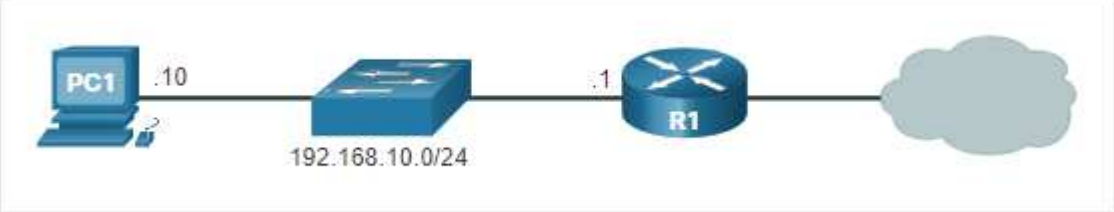
Tanto la PC1 como la PC2 tendrán una ruta predeterminada para enviar todo el tráfico destinado a las redes remotas al R1.

8.4.4

Tablas de enrutamiento de host

En un host de Windows, el comando **route print** o **netstat -r** se puede usar para mostrar la tabla de enrutamiento del host. Los dos comandos generan el mismo resultado. Al principio, los resultados pueden parecer abrumadores, pero son bastante fáciles de entender.

La figura muestra una topología de ejemplo y la salida generada por el comando **netstat –r**.



El diagrama muestra una topología de red que consiste en un host, PC1, conectado a un switch en la red 192.168.10.0/24. El switch está conectado a un router, R1, que luego se conecta a la nube. PC1 tiene una dirección de.10 y la interfaz del router a la que está conectado el switch tiene una dirección de .1.

Tabla de enrutamiento IPv4 para la PC1

```
C:\Users\PC1 > netstat -r
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
          0.0.0.0 0.0.0.0 192.168.10.1 192.168.10.10 25
        127.0.0.0 255.0.0.0 On-link 127.0.0.1 306
        127.0.0.1 255.255.255.255 On-link 127.0.0.1 306
  127.255.255.255 255.255.255.255 On-link 127.0.0.1 306
     192.168.10.0 255.255.255.0 On-link 192.168.10.10 281
    192.168.10.10 255.255.255.255 On-link 192.168.10.10 281
   192.168.10.255 255.255.255.255 On-link 192.168.10.10 281
        224.0.0.0 240.0.0.0 On-link 127.0.0.1 306
        224.0.0.0 240.0.0.0 On-link 192.168.10.10 281
  255.255.255.255 255.255.255.255 On-link 127.0.0.1 306
  255.255.255.255 255.255.255.255 On-link 192.168.10.10 281
```

Nota: La salida sólo muestra la tabla de rutas IPv4.

Al ingresar el comando **netstat -r** o el comando equivalente **route print,** se muestran tres secciones relacionadas con las conexiones de red TCP / IP actuales:

- **Lista de interfaces: -** enumera la dirección de control de acceso a medios (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
- **Tabla de rutas IPv4: -** enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, la red local y las rutas locales predeterminadas.
- **Tabla de rutas IPv6: -** Tabla de rutas IPv6: enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, la red local y las rutas locales predeterminadas.

8.4.5

Compruebe su comprensión - Cómo enruta un host

Verifique su comprensión de cómo un host enruta eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. No se necesita un router para reenviar paquetes entre hosts locales de la red.
2. La puerta de enlace predeterminada es la dirección IP de un router en la red local.
3. Los comandos **netstat -r** y **route print** mostrarán la tabla de enrutamiento de un host de Windows.

Has tenido 3 respuestas correctas de 3.

1. ¿Qué declaración sobre las decisiones de reenvío de host es verdadera?

¡Lo tienes!

- ( ) Un host no puede hacer ping a sí mismo.
- ( ) Un host de destino remoto está en la misma red local que el host de envío.
- (•) Los hosts locales pueden llegar entre sí sin la necesidad de un router.
- ( ) El enrutamiento está habilitado en los switches para descubrir la mejor ruta a un destino.

2. ¿Qué declaración de puerta de enlace predeterminada es verdadera?

¡Lo tienes!

- ( ) Se requiere una puerta de enlace predeterminada para enviar paquetes a otros hosts de la red local.
- ( ) La dirección de puerta de enlace predeterminada es la dirección IP de un switch en una red remota.
- (•) La dirección de puerta de enlace predeterminada es la dirección IP del router en la red local.
- ( ) El tráfico sólo se puede reenviar fuera de la red local si no hay una puerta de enlace predeterminada.

3. ¿Qué dos comandos se pueden introducir en un host de Windows para ver su tabla de enrutamiento IPv4 e IPv6? (Escoja dos opciones).

¡Lo tienes!

- [ ] ruta de red -l
- [x] **netstat -r**
- [ ] ruta de impresión
- [x] **route print**
- [ ] red de impresión

Correct

You have successfully identified the correct answers.

1. A router is not needed to forward packets between local hosts on the network.
2. The default gateway is the IP address of a router on the local network.
3. The commands **netstat -r** and **route print** will display the routing table of a Windows host.

You got 3 out of 3 questions correct.

1. Which statement about host forwarding decisions is true?

You got it!

- ○ A host cannot ping itself.
- ○ A remote destination host is on the same local network as the sending host.
- ◉ Local hosts can reach each other without the need of a router.
- ○ Routing is enabled on switches to discover the best path to a destination.

2. Which default gateway statement is true?

You got it!

- ○ A default gateway is required to send packets to other hosts on the local network.
- ○ The default gateway address is the IP address of a switch on a remote network.
- ◉ The default gateway address is the IP address of the router on the local network.
- ○ Traffic can only be forwarded outside the local network if there is no default gateway.

3. Which two commands could be entered on a Windows host to view its IPv4 and IPv6 routing table? (Choose two.)

You got it!

- ☐ **netroute -l**
- ☑ **netstat -r**
- ☐ **print route**
- ☑ **route print**
- ☐ **print net**

Capa de red / Introducción al enrutamiento

Introducción al enrutamiento

8.5.1

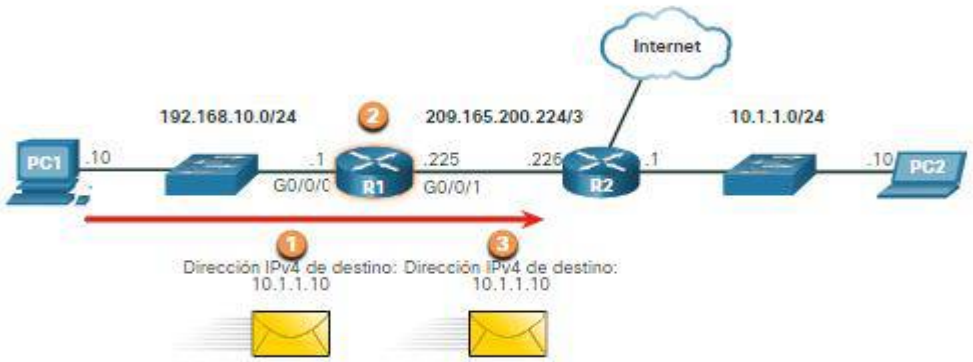
Decisión de envío de paquetes del router

En el tema anterior se discutieron las tablas de enrutamiento de host. La mayoría de las redes también contienen routers, que son dispositivos intermediarios. Los routers también contienen tablas de enrutamiento. En este tema se tratan las operaciones del router en la capa de red. Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la puerta de enlace predeterminada, que generalmente es el router local.

¿Qué sucede cuando llega un paquete a la interfaz de un router?

El router examina la dirección IP de destino del paquete y busca en su tabla de enrutamiento para determinar dónde reenviar el paquete. La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete. Estas entradas se conocen como entradas de ruta o rutas. El router reenviará el paquete utilizando la mejor entrada de ruta que coincida (más larga).

El diagrama es una topología de red que muestra lo que sucede con un paquete IPv4 a medida que se enruta entre redes. El host PC1, con una dirección de.10, está conectado a un switch en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del router R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro router, R2 en la dirección .226. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 tambien tiene una conexión a la nube de Internet. Se envía un paquete con la dirección IPv4 de destino 10.1.1.10 desde PC1 a R1. R1 envía el paquete con la dirección IPv4 de destino 10.1.1.10 a R2.



1. El paquete llega a la interfaz Gigabit Ethernet 0/0/0 del router R1. R1 desencapsula el encabezado Ethernet de Capa 2 y el remolque.
2. El router R1 examina la dirección IPv4 de destino del paquete y busca la mejor coincidencia en su tabla de enrutamiento IPv4. La entrada de ruta indica que este paquete se reenviará al router R2.
3. El router R1 encapsula el paquete en un nuevo encabezado Ethernet y remolque, y reenvía el paquete al siguiente router de salto R2.

La siguiente tabla muestra la información pertinente de la tabla de ruteo R1.

Tabla de enrutamiento del R1

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Default Route 0.0.0.0/0	via R2

8.5.2

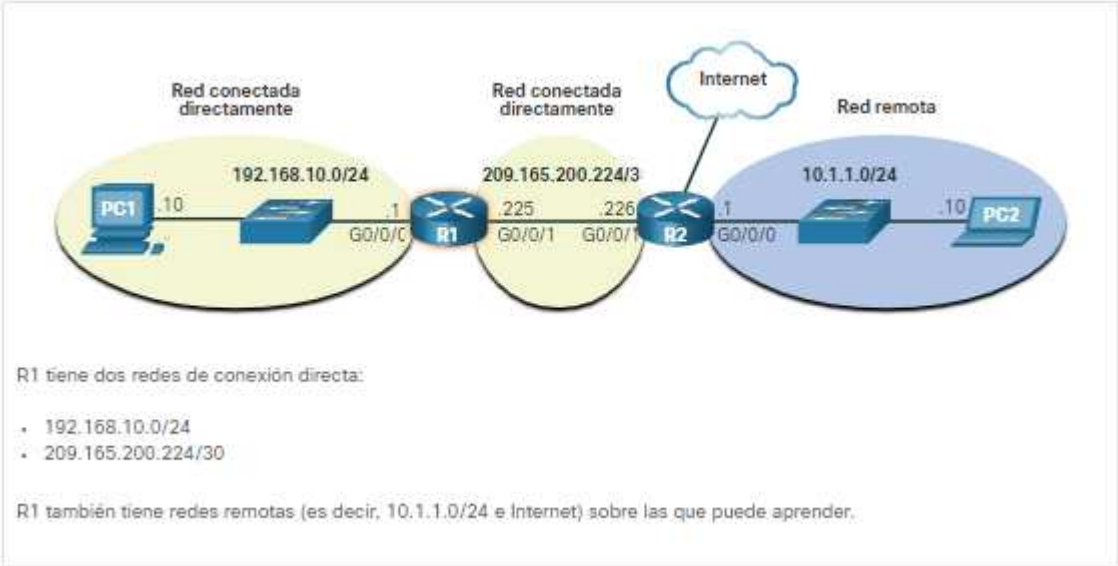
Tabla de enrutamiento IP del router

La tabla de enrutamiento del router contiene entradas de ruta de red que enumeran todos los posibles destinos de red conocidos.

La tabla de enrutamiento almacena tres tipos de entradas de ruta:

- **Redes conectadas directamente:** estas entradas de ruta de red son interfaces de router activas. Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una dirección IP y se activa. Cada interfaz de router está conectada a un segmento de red diferente. En la figura, las redes conectadas directamente en la tabla de enrutamiento IPv4 R1 serían 192.168.10.0/24 y 209.165.200.224/30.
- **Redes remotas:** estas entradas de ruta de red están conectadas a otros routers. Los routers aprenden acerca de las redes remotas ya sea mediante la configuración explícita de un administrador o mediante el intercambio de información de ruta mediante un protocolo de enrutamiento dinámico. En la figura, la red remota en la tabla de enrutamiento IPv4 R1 sería 10.1.1.0/24.
- Ruta **predeterminada**: al igual que un host, la mayoría de los routers también incluyen una entrada de ruta predeterminada, una puerta de enlace de último recurso. La ruta predeterminada se utiliza cuando no hay una mejor coincidencia (más larga) en la tabla de enrutamiento IP. En la figura, la tabla de enrutamiento IPv4 R1 probablemente incluiría una ruta predeterminada para reenviar todos los paquetes al router R2.

La figura identifica las redes directamente conectadas y remotas del router R1.



El diagrama es una topología de red que identifica las redes conectadas directamente y las redes remotas de un router. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro router, R2 en la dirección .226 en G0/0/1. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 tambien tiene una conexión a la nube de Internet. Las redes 192.168.10.0/24 y 209.165.200.224/30 se muestran como redes conectadas directamente a R1 y a la red 10.1.2.0/24 (¿debería ser 10.1.1.0/24?) se muestra como una red remota a R2.

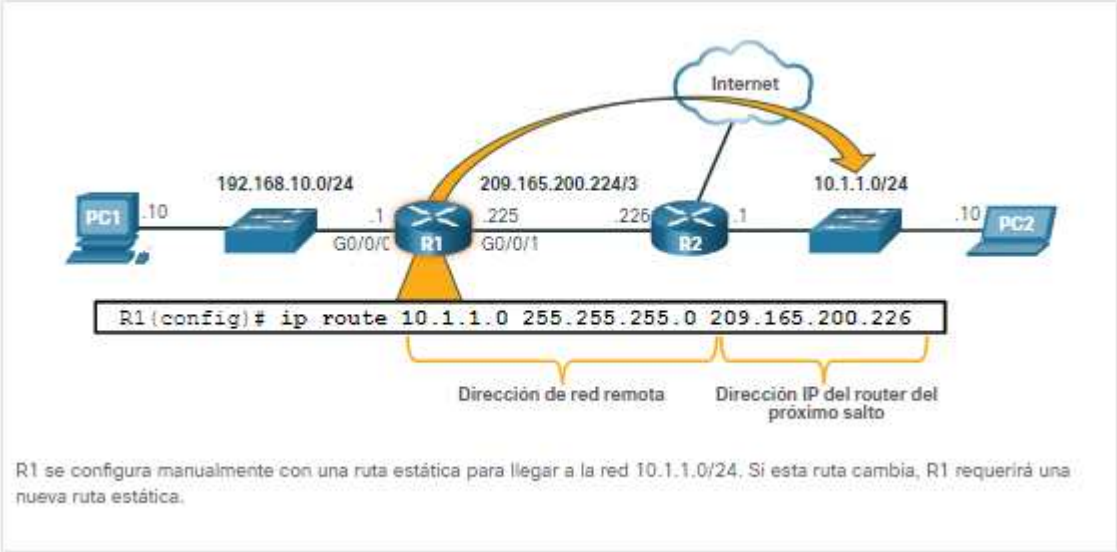
Un router puede descubrir redes remotas de dos maneras:

- **Manualmente:** - Manualmente: las redes remotas se ingresan manualmente en la tabla de rutas mediante rutas estáticas.
- **Dinámicamente \:** Dinámicamente \: las rutas remotas se aprenden automáticamente mediante un protocolo de enrutamiento dinámico.

8.5.3

Enrutamiento estático

Las rutas estáticas son entradas de ruta que se configuran manualmente. La figura muestra un ejemplo de una ruta estática que se configuró manualmente en el router R1. La ruta estática incluye la dirección de red remota y la dirección IP del router de salto siguiente.

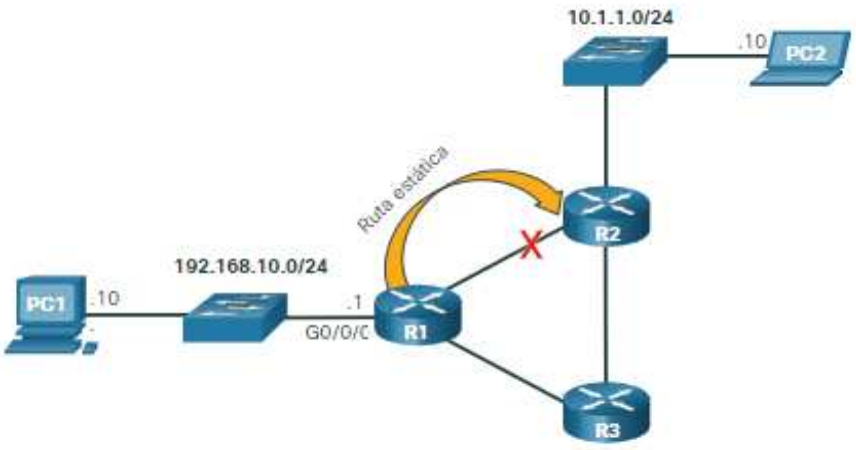


R1 se configura manualmente con una ruta estática para llegar a la red 10.1.1.0/24. Si esta ruta cambia, R1 requerirá una nueva ruta estática.

El diagrama es una topología de red que muestra una configuración de ruta estática para llegar a una red remota. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro enrutador, R2 en la dirección .226. R2 tiene una interfaz con la dirección .1 conectada a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, la dirección .10. R2 tambien tiene una conexión a la nube de Internet. Una configuración de ruta estática en R1 a la red 10.1.1.0/24 dice: R1(config)#IP route 10.1.1.0 255.255.255.0 209.165.200.226. En la configuración, 10.1.1.0 255.255.0 está etiquetado como red remota y 209.165.200.226 como dirección IP del router de salto siguiente.

Si hay un cambio en la topología de la red, la ruta estática no se actualiza automáticamente y debe reconfigurarse manualmente. Por ejemplo, en la figura R1 tiene una ruta estática para llegar a la red 10.1.1.0/24 a través de R2. Si esa ruta ya no está disponible, R1 tendría que reconfigurarse con una nueva ruta estática a la red 10.1.1.0/24 a través de R3. Por lo tanto, el router R3 necesitaría tener una entrada de ruta en su tabla de enrutamiento para enviar paquetes destinados a 10.1.1.0/24 a R2.

El diagrama es una topología de red que muestra un vínculo fallido en una ruta estática. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. R1 está conectado al router R2 y al router R3 que también se dirigen conectados. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. Se ha configurado una ruta estática en R1 que apunta a R2 como el salto siguiente. Una X roja indica que este enlace ha fallado.



Si la ruta desde R1 a R2 ya no está disponible, debería configurarse una nueva ruta estática a través de R3. Una ruta estática no se ajusta automáticamente para los cambios de topología.

El enrutamiento estático tiene las siguientes características:

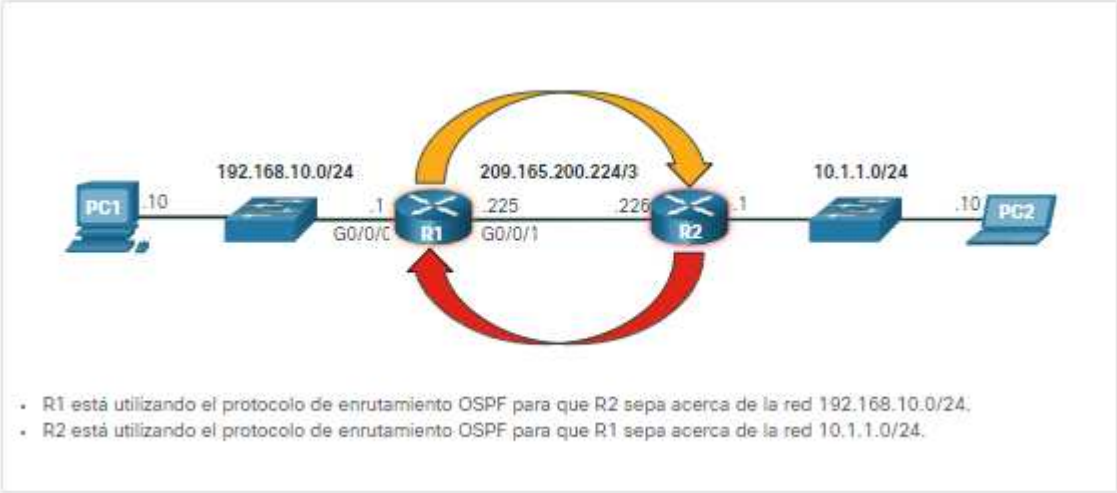
- Una ruta estática debe configurarse manualmente.
- El administrador necesita volver a configurar una ruta estática si hay un cambio en la topología y la ruta estática ya no es viable.
- Una ruta estática es apropiada para una red pequeña y cuando hay pocos o ninguno de los enlaces redundantes.
- Una ruta estática se usa comúnmente con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada.

8.5.4

Enrutamiento dinámico

Un protocolo de enrutamiento dinámico permite a los routers aprender automáticamente sobre redes remotas, incluida una ruta predeterminada, de otros routers. Los routers que usan protocolos de enrutamiento dinámico comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin que sea necesaria la participación del administrador de la red. Si se produce un cambio en la topología de red, los routers comparten esta información mediante el protocolo de enrutamiento dinámico y actualizan automáticamente sus tablas de enrutamiento.

Los protocolos de enrutamiento dinámico incluyen OSPF y Enhanced Interior Gateway Routing Protocol (EIGRP). La figura muestra un ejemplo de routers R1 y R2 que comparten automáticamente información de red mediante el protocolo de enrutamiento OSPF.

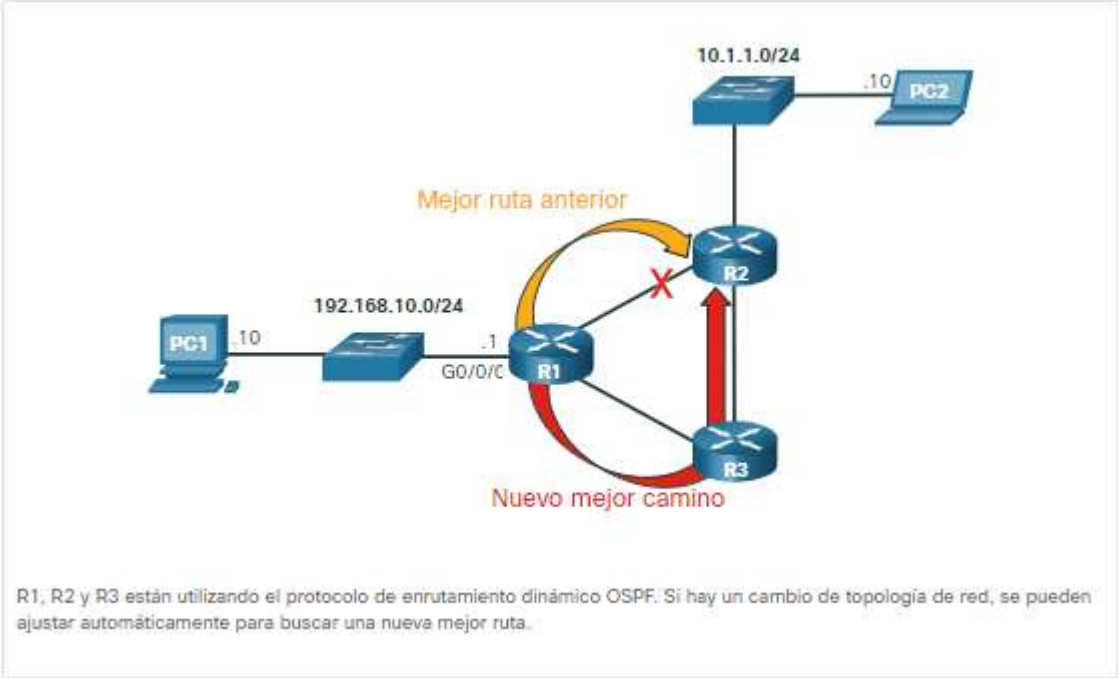


El diagrama es una topología de red que muestra los routers que utilizan protocolos de enrutamiento dinámico para intercambiar información. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro enrutador, R2 en la dirección .226. R2 tiene una interfaz con la dirección .1 conectada a un switch en la red 10.1.1.0/24 a la que está conectada la PC2 host, dirección .10. Las flechas muestran R1 y R2 compartiendo información entre sí.

La configuración básica sólo requiere que el administrador de red habilite las redes conectadas directamente dentro del protocolo de enrutamiento dinámico. El protocolo de enrutamiento dinámico hará automáticamente lo siguiente:

- Detectar redes remotas.
- Mantener información de enrutamiento actualizada.
- Elija el mejor camino hacia las redes de destino
- Intente encontrar una nueva mejor ruta si la ruta actual ya no está disponible

Cuando un router se configura manualmente con una ruta estática o aprende acerca de una red remota dinámicamente mediante un protocolo de enrutamiento dinámico, la dirección de red remota y la dirección de salto siguiente se introducen en la tabla de enrutamiento IP. Como se muestra en la figura, si hay un cambio en la topología de red, los routers se ajustarán automáticamente e intentarán encontrar una nueva mejor ruta.



R1, R2 y R3 están utilizando el protocolo de enrutamiento dinámico OSPF. Si hay un cambio de topología de red, se pueden ajustar automáticamente para buscar una nueva mejor ruta.

El diagrama muestra una topología de red en la que los routers que utilizan protocolos de enrutamiento dinámico están ajustando las mejores rutas después de un cambio de topología. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. R1 está conectado al router R2 y al router R3 que también se dirigen conectados. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. Una X roja indica que el enlace entre R1 y R2, etiquetado como la mejor ruta anterior, ha fallado. Se muestra un nuevo mejor camino que va de R1 a R3 a R2.

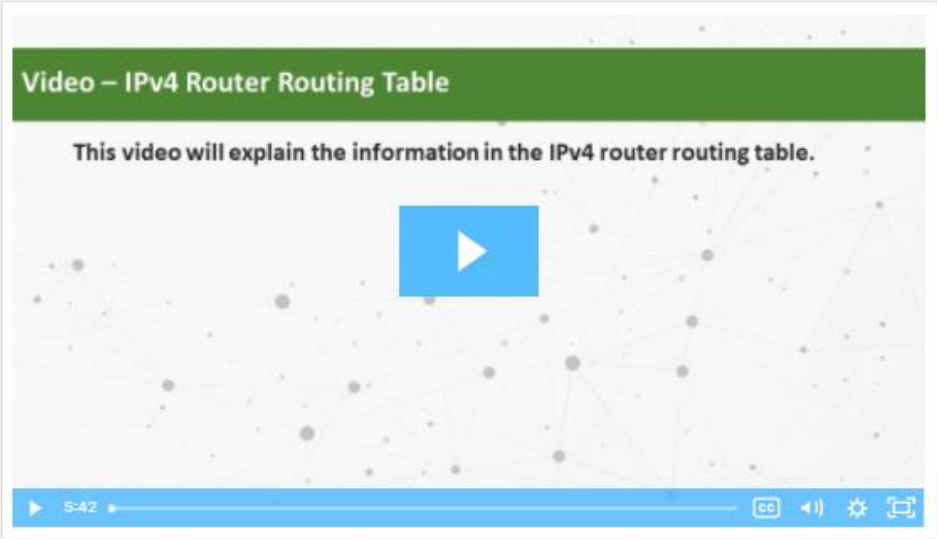
Nota: Es común que algunos routers usen una combinación de rutas estáticas y un protocolo de enrutamiento dinámico.

8.5.5

Video- Tablas de enrutamiento de router IPv4

A diferencia de una tabla de enrutamiento de la computadora host, no hay encabezados de columna que identifiquen la información contenida en la tabla de enrutamiento de un router. Es importante aprender el significado de los diferentes elementos presentes en cada tabla de enrutamiento.

Haga clic en Reproducir en la ilustración para ver una introducción a la tabla de enrutamiento IPv4.

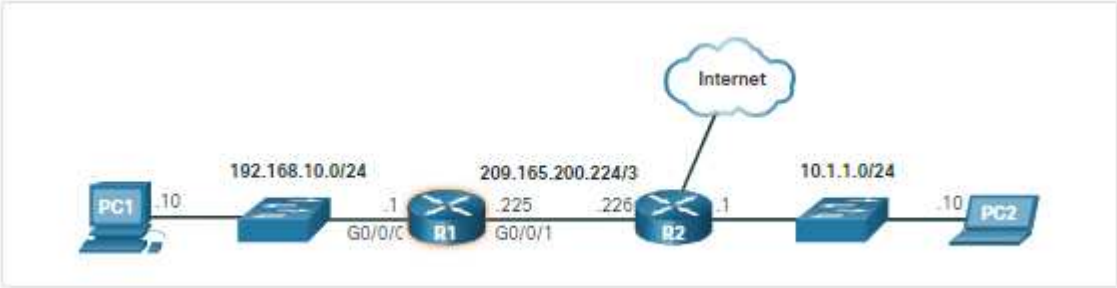


8.5.6

Introducción a una tabla de enrutamiento IPv4

Observe en la figura que R2 está conectado a Internet. Por lo tanto, el administrador configuró R1 con una ruta estática predeterminada que envía paquetes a R2 cuando no hay ninguna entrada específica en la tabla de enrutamiento que coincida con la dirección IP de destino. R1 y R2 también están utilizando el enrutamiento OSPF para anunciar redes conectadas directamente.

El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro enrutador, R2 en la dirección .226. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 también tiene una conexión a la nube de Internet.



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0 S* 0.0.0.0/0 [1/0] via 209.165.200.226,
GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O 10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

El comando **show ip route** de EXEC mode privilegiado se utiliza para ver la tabla de enrutamiento IPv4 en un router Cisco IOS. El ejemplo muestra la tabla de enrutamiento IPv4 del router R1. Al principio de cada entrada de tabla de enrutamiento hay un código que se utiliza para identificar el tipo de ruta o cómo se aprendió la ruta. Entre las fuentes de ruta comunes (códigos) se incluyen las siguientes:

- **L** - Dirección IP de interfaz local conectada directamente
- **C** – Red conectada directamente
- **S** — La ruta estática fue configurada manualmente por un administrador
- **O** - OSPF
- **D** - EIGRP

La tabla de enrutamiento muestra todas las rutas de destino IPv4 conocidas para R1.

Una ruta conectada directamente se crea automáticamente cuando se configura una interfaz de router con información de dirección IP y se activa. El router añade dos entradas de ruta con los códigos C (es decir, la red conectada) y L (es decir, la dirección IP de la interfaz local de la red conectada). Las entradas de ruta también identifican la interfaz de salida que se utilizará para llegar a la red. Las dos redes conectadas directamente en este ejemplo son 192.168.10.0/24 y 209.165.200.224/30.

Los routers R1 y R2 también están utilizando el protocolo de enrutamiento dinámico OSPF para intercambiar información de router. En la tabla de enrutamiento de ejemplo, R1 tiene una entrada de ruta para la red 10.1.1.0/24 que aprendió dinámicamente del router R2 a través del protocolo de enrutamiento OSPF.

Una ruta predeterminada tiene una dirección de red de todos los ceros. Por ejemplo, la dirección de red IPv4 es 0.0.0.0. Una entrada de ruta estática en la tabla de enrutamiento comienza con un código de S\ *, como se resalta en el ejemplo.

8.5.7

Verifique su comprensión - Introducción al enrutamiento

Verifique su comprensión de la introducción al enrutamiento eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El **show ip route** comando se utiliza para ver la tabla de enrutamiento en un router Cisco.
2. Los códigos al principio de cada entrada de la tabla de enrutamiento se utilizan para identificar el tipo de ruta o cómo se aprendió la ruta. Un código de "O" indica que la ruta se aprendió de OSPF.
3. Una ruta predeterminada también se conoce como puerta de acceso de último recurso.
4. Las rutas estáticas se configuran manualmente y no se ajustan a los cambios en la topología de red y no se anuncian a los routers vecinos.
5. La respuesta correcta es verdadero. Los routers se pueden configurar con rutas estáticas y con un protocolo de enrutamiento dinámico.

Has tenido 5 respuestas correctas de 5.

1. ¿Cuál es el comando utilizado en un router Cisco IOS para ver la tabla de enrutamiento?

¡Lo tienes!

- netstart -r
- route print
- **show ip route**
- mostrar tablade enrutamiento

2. ¿Qué indica un código de «O» junto a una ruta en la tabla de enrutamiento?

¡Lo tienes!

- una ruta directamente conectada
- una ruta con una distancia administrativa de 0
- una puerta de entrada de último recurso
- una ruta aprendida dinámicamente de OSPF

3. Este tipo de ruta también se conoce como una puerta de entrada de último recurso.

¡Lo tienes!

- Ruta estática
- ruta remota
- Ruta predeterminada
- Ruta conectada directamente

4. ¿Cuál es una característica de las rutas estáticas?

¡Lo tienes!

- (•) Ellos se configuran manualmente.
- ( ) Se anuncian a los vecinos directamente conectados.
- ( ) Son apropiados cuando hay muchos enlaces redundantes.
- ( ) Se ajustan automáticamente a un cambio en la topología de red.

5. ¿Verdadero o falso? Un router se puede configurar con una combinación de rutas estáticas y un protocolo de enrutamiento dinámico.

¡Lo tienes!

- (•) Verdadero
- ( ) Falso

Correct

You have successfully identified the correct answers.

1. The **show ip route** command is used to view the routing table on a Cisco router.
2. Codes at the beginning of each routing table entry are used to identify the type of route or how the route was learned. A code of "O" indicates the route was learned from OSPF.
3. A default route is also known as a gateway of last resort.
4. Static routes are manually configured and do not adjust to changes in the network topology and are not advertised to neighboring routers.
5. The correct answer is True. Routers can be configured with static routes and with a dynamic routing protocol.

You got 5 out of 5 questions correct.

1. What is the command used on a Cisco IOS router to view the routing table?

You got it!

- ( ) **netstart -r**
- ( ) **route print**
- (•) **show ip route**
- ( ) **show routing table**

2. What does a code of "O" indicate next to a route in the routing table?

You got it!

- ○ a directly connected route
- ○ a route with an administrative distance of 0
- ○ a gateway of last resort
- ◉ a route learned dynamically from OSPF

3. This type of route is also known as a gateway of last resort.

You got it!

- ○ static route
- ○ remote route
- ◉ default route
- ○ directly connected route

4. Which is a characteristic of static routes?

You got it!

- ◉ They are manually configured.
- ○ They are advertised to directly connected neighbors.
- ○ They are appropriate when there are many redundant links.
- ○ They automatically adjust to a change in network topology.

5. True or False? A router can be configured with a combination of both static routes and a dynamic routing protocol.

You got it!

- ◉ True
- ○ False

Capa de red / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

8.6.1

¿Qué aprenderé en este módulo?

Network Layer Characteristics

La capa de red (Capa OSI 3) proporciona servicios para permitir que los dispositivos finales intercambien datos a través de las redes. IPv4 e IPv6 son los principales protocolos de comunicación de la capa de red. La capa de red también incluye el protocolo de enrutamiento OSPF y protocolos de mensajería como ICMP. Los protocolos de capa de red realizan cuatro operaciones básicas: direccionamiento de dispositivos finales, encapsulación, enrutamiento y desencapsulación. IPv4 e IPv6 especifican la estructura de paquetes y el procesamiento utilizado para transportar los datos de un host a otro. IP encapsula el segmento de la capa de transporte agregando un encabezado IP, que se utiliza para entregar el paquete al host de destino. El encabezado IP es examinado por los dispositivos de Capa 3 (es decir, routers) a medida que viaja a través de una red a su destino. Las características de la IP son que es sin conexión, el mejor esfuerzo e independiente de los medios de comunicación. IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. El protocolo IP no garantiza que todos los paquetes que se envían, de hecho, se reciban. Esta es la definición de la característica poco confiable, o mejor esfuerzo. IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos.

IPv4 Packet

Un encabezado de paquete IPv4 consta de campos que contienen información sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3. Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los campos significativos del encabezado IPv6 incluyen: versión, DS, suma de comprobación de encabezado, TTL, protocolo y direcciones IPv4 de origen y destino.

IPv6 Packet

IPv6 está diseñado para superar las limitaciones de IPv4, entre ellas: agotamiento de direcciones IPv4, falta de conectividad de extremo a extremo y mayor complejidad de la red. IPv6 aumenta el espacio de direcciones disponible, mejora el manejo de paquetes y elimina la necesidad de NAT. Los campos en el encabezado del paquete IPv6 incluyen: versión, clase de tráfico, etiqueta de flujo, longitud de la carga útil, siguiente encabezado, límite de salto y las direcciones IPv6 de origen y destino.

How a Host Routes

Un host puede enviar un paquete a sí mismo, a otro host local y a un host remoto. En IPv4, el dispositivo de origen utiliza su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para determinar si el host de destino está en la misma red. En IPv6, el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red, para realizar esta determinación. La puerta de enlace predeterminada es el dispositivo de red (es decir, el router) que puede enrutar el tráfico a otras redes. En una red, una puerta de enlace predeterminada suele ser un router que tiene una dirección IP local en el mismo rango de direcciones que otros hosts de la red local, puede aceptar datos en la red local y reenviar datos fuera de la red local, y enrutar el tráfico a otras redes. Una tabla de enrutamiento de host generalmente incluirá una puerta de enlace predeterminada. En IPv4, el host recibe la dirección IPv4 de la puerta de enlace predeterminada de forma dinámica a través de DHCP o se configura manualmente. En IPv6, el router anuncia la dirección de la puerta de enlace predeterminada o el host se puede configurar manualmente. En un host de Windows, el comando **route print** o **netstat -r** se puede usar para mostrar la tabla de enrutamiento del host.

Introduction to Routing

Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la puerta de enlace predeterminada, que generalmente es el router local. ¿Qué sucede cuando llega un paquete a la interfaz de un enrutador? El router examina la dirección IP de destino del paquete y busca en su tabla de enrutamiento para determinar dónde reenviar el paquete. La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete. Estas entradas se conocen como entradas de ruta o rutas. El router reenviará el paquete utilizando la mejor entrada de ruta que coincida (más larga). La tabla de enrutamiento de un router almacena tres tipos de entradas de ruta: redes conectadas directamente, redes remotas y una ruta predeterminada. Los routers aprenden sobre redes remotas de forma manual o dinámica utilizando un protocolo de enrutamiento dinámico. Las rutas estáticas son entradas de ruta que se configuran manualmente. Las rutas estáticas incluyen la dirección de red remota y la dirección IP del router de salto siguiente. OSPF y EIGRP son dos protocolos de enrutamiento dinámico. El comando modo EXEC privilegiado **show ip route,** se utiliza para ver la tabla de enrutamiento IPv4 en un router Cisco IOS. Al principio de una tabla de enrutamiento IPv4, hay un código que se utiliza para identificar el tipo de ruta o cómo se aprendió la ruta. Las fuentes de ruta comunes (códigos) incluyen:

L - Dirección IP de interfaz local conectada directamente

C - Red conectada directamente

S - La ruta estática fue configurada manualmente por un administrador

O - Open Shortest Path First (OSPF)

D - Enhanced Interior Gateway Routing Protocol (EIGRP)

8.6.2

Módulo Quiz - Capa de red

Correcto

Identificó bien las respuestas correctas.

Has tenido 14 respuestas correctas de 14.

1. ¿Qué información utilizan los routers para reenviar un paquete de datos hacia su destino?

Tema 8.4.0: la dirección IP de destino es la dirección IP del dispositivo receptor. Esta dirección IP es utilizada por los routers para reenviar el paquete a su destino.

- Dirección IP de origen
- dirección IP de destino
- Dirección de origen
- Dirección de destino

2. Un equipo tiene que enviar un paquete a un host de destino en la misma LAN. ¿Cómo se enviará el paquete?

Tema 8.4.0 - Si el host de destino está en la misma LAN que el host de origen, no hay necesidad de una puerta de enlace predeterminada. Se necesita una puerta de enlace predeterminada si se necesita enviar un paquete fuera de la LAN.

- El paquete se enviará primero a la puerta de enlace predeterminada y, a continuación, dependiendo de la respuesta de la puerta de enlace, se puede enviar al host de destino.
- El paquete se enviará directamente al host de destino.
- El paquete se enviará primero a la puerta de enlace predeterminada y, a continuación, desde la puerta de enlace predeterminada, se enviará directamente al host de destino.
- El paquete se enviará sólo a la puerta de enlace predeterminada.

3. Un router recibe un paquete de la interfaz Gigabit 0/0 y determina que el paquete necesita ser reenviado desde la interfaz Gigabit 0/1. ¿Qué hará el router a continuación?

Tema 8.5.0 - Una vez que un router recibe un paquete y mira dentro del encabezado para determinar la red de destino, el router compara la red de destino con la tabla de enrutamiento para determinar si el paquete se va a enrutar o quitar. Si se enruta, el router conecta un nuevo encabezado de capa 2 basado en la tecnología que utiliza el puerto de salida que se utiliza. A continuación, el paquete se enruta hacia fuera del puerto de destino según lo designado por la tabla de enrutamiento. La caché ARP se utiliza para hacer coincidir una dirección IP con una dirección MAC.

- ○ enrutar el paquete hacia fuera de la interfaz Gigabit 0/1
- ◉ crear un nuevo marco Ethernet de Capa 2 para ser enviado al destino
- ○ buscar en la memoria caché ARP para determinar la dirección IP de destino
- ○ busque en la tabla de enrutamiento para determinar si la red de destino está en la tabla de enrutamiento

4. ¿Qué direcciones IPv4 puede usar un host para hacerle ping a la interfaz de bucle invertido?

Tema 8.4.0: un host puede hacer ping en la interfaz de bucle de retorno enviando un paquete a una dirección IPv4 especial dentro de la red 127.0.0.0/8.

- ○ 126.0.0.1
- ○ 127.0.0.0
- ○ 126.0.0.0
- ◉ 127.0.0.1

5. Cuando un protocolo sin conexión está en uso en una capa inferior del modelo OSI, ¿cómo se detectan y se retransmiten, si es necesario, los datos faltantes?

Tema 8.1.0: cuando se utilizan protocolos sin conexión en una capa inferior del modelo OSI, los protocolos de nivel superior pueden necesitar trabajar juntos en los hosts de envío y recepción para dar cuenta y retransmitir los datos perdidos. En algunos casos, esto no es necesario porque algunas aplicaciones toleran cierto nivel de pérdida de datos.

- ○ Se utilizan acuses de recibo sin conexión para solicitar la retransmisión.
- ◉ Los protocolos de capa superior orientados a la conexión hacen un seguimiento de los datos recibidos y pueden solicitar la retransmisión desde los protocolos de capa superior del host emisor.
- ○ Los protocolos IP de la capa de red administran las sesiones de comunicación si no están disponibles los servicios de transporte orientados a la conexión.
- ○ El proceso de distribución de servicio mínimo garantiza que todos los paquetes se envíen y se reciban.

6. ¿Cuál es el motivo para la creación e implementación de IPv6?

Tema 8.3.0: el espacio de direccionamiento IPv4 se agota por el rápido crecimiento de Internet y los dispositivos conectados a Internet. IPv6 extiende el espacio de direcciones IP porque aumenta la longitud de una dirección de 32 a 128 bits, lo que debería proporcionar suficientes direcciones para el crecimiento futuro de Internet durante muchos años.

- ○ Facilitar la lectura de direcciones de 32 bits
- ◉ Evitar que se agoten la direcciones IPv4
- ○ Proporcionar más espacio de direcciones en el Registro de nombres de Internet
- ○ Permitir la compatibilidad NAT para la asignación de direcciones privadas

7. ¿Qué enunciado describe con precisión una característica de IPv4?

Tema 8.2.0 - IPv4 tiene un espacio de direcciones de 32 bits, que proporciona 4.294.967.296 direcciones únicas, pero solo se pueden asignar 3.700 millones, un límite debido a la reserva de direcciones para multidifusión y pruebas.IPv4 no proporciona soporte nativo para IPSec.IPv6 tiene un encabezado simplificado con menos campos que IPv4.

- ( ) Todas las direcciones IPv4 se pueden asignar a hosts.
- (•) IPv4 tiene un espacio de direcciones de 32 bits.
- ( ) Un encabezado IPv4 tiene menos campos que un encabezado IPv6.
- ( ) IPv4 admite de forma nativa IPSec.

8. ¿Qué campo de un encabezado de paquete IPv4 normalmente permanece igual durante su transmisión?

Tema 8.1.0 - El valor del campo Dirección de destino de un encabezado IPv4 seguirá siendo el mismo durante su transmisión. Las otras opciones pueden cambiar durante su transmisión.

- ( ) Señalador
- ( ) Tiempo de duración
- ( ) Longitud del paquete
- (•) Dirección de destino

9. Cuando un router recibe un paquete, ¿qué información debe analizarse para que el paquete se envíe a un destino remoto?

Tema 8.4.0: cuando un router recibe un paquete, examina la dirección de destino del paquete y utiliza la tabla de enrutamiento para buscar la mejor ruta a esa red.

- ( ) Dirección MAC de destino
- ( ) Dirección IP de origen
- (•) dirección IP de destino
- ( ) Dirección MAC de origen

10. ¿Qué campo de un paquete IPv6 utiliza el router para determinar si un paquete ha caducado y debe descartarse?

Tema 8.3.0: ICMPv6, como IPv4, envía un mensaje de Tiempo excedido si el router no puede reenviar un paquete IPv6 porque el paquete ha expirado. Sin embargo, el paquete IPv6 no tiene un campo TTL, por lo que utiliza el campo de límite de saltos para determinar si el paquete caducó.

- ( ) TTL
- (•) Límite de saltos
- ( ) No se puede alcanzar la dirección
- ( ) no hay ruta para el destino.

11. ¿Qué comando se puede usar en un host de Windows para mostrar la tabla de enrutamiento?

Tema 8.4.0: en un host de Windows, se pueden usar los comandos **route print** o **netstat -r** para mostrar la tabla de enrutamiento del host. El **show ip route** comando se utiliza en un router para mostrar su tabla de enrutamiento. El **netstat -s** comando se utiliza para mostrar estadísticas por protocolo. El **tracert** comando se utiliza para mostrar la ruta que un paquete viaja a su destino.

- ( ) **netstat –s**
- ( ) **show ip route**
- (•) **netstat –r**
- ( ) **tracert**

12. ¿Qué información se agrega durante el encapsulamiento en la capa 3 del modelo OSI?

Tema 8.1.0: IP es un protocolo de capa 3. Los dispositivos de capa 3 pueden abrir el encabezado de dicha capa para inspeccionar la información relacionada con IP que contiene, incluidas las direcciones IP de origen y de destino.

- ○ Dirección MAC de origen y destino
- ○ Protocolo de aplicaciones de origen y destino
- ○ Número de puertos de origen y destino
- ◉ Dirección IP de origen y destino

13. ¿Cómo utiliza la capa de red el valor de MTU?

Tema 8.1.0: la capa de enlace de datos indica a la capa de red la MTU para el medio que se está utilizando. La capa de red utiliza esa información para determinar qué tan grande puede ser el paquete cuando se reenvía. Cuando los paquetes se reciben en un medio y se reenvían a otro con una MTU más pequeña, el dispositivo de capa de red puede fragmentar el paquete para adaptarse al tamaño más pequeño.

- ○ La capa de red depende de las capas de niveles superiores para determinar la MTU.
- ○ La capa de red depende de la capa de enlace de datos para establecer la MTU y ajusta la velocidad de transmisión para admitirla.
- ◉ La capa de enlace de datos pasa la MTU a la capa de red.
- ○ Para aumentar la velocidad de entrega, la capa de red ignora la MTU.

14. ¿Qué característica distingue una mejora de IPv6 respecto de IPv4?

Tema 8.3.0: las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits, y el encabezado IPv6 se ha simplificado con menos campos, lo que mejora el manejo de paquetes. IPv6 admite funcionalidades de autenticación y privacidad de manera nativa, mientras que IPv4 requiere características adicionales para admitirlas. El espacio de direcciones IPv6 es muchas veces mayor que el espacio de direcciones IPv4.

- ○ Las direcciones IPv6 se basan en direccionamiento plano de 128 bits, mientras que IPv4 se basa en direccionamiento jerárquico de 32 bits.
- ◉ El encabezado de IPv6 es más sencillo que el de IPv4, lo que mejora el manejo de paquetes.
- ○ Tanto IPv4 como IPv6 admiten la autenticación, pero solamente IPv6 admite las funcionalidades de privacidad.
- ○ El espacio de direcciones IPv6 es cuatro veces mayor que el espacio de direcciones IPv4.

Correct

You have successfully identified the correct answers.

You got 13 out of 13 questions correct.

1. Which command can be used on a Windows host to display the routing table?

Topic 8.4.0 - On a Windows host, either the **route print** or **netstat -r** commands can be used to display the host routing table. The **show ip route** command is used on a router to display its routing table. The **netstat -s** command is used to display per-protocol statistics. The **tracert** command is used to display the path that a packet travels to its destination.

- **netstat -s**
- **show ip route**
- **netstat -r**
- **tracert**

2. What information is added during encapsulation at OSI Layer 3?

Topic 8.1.0 - IP is a Layer 3 protocol. Layer 3 devices can open the Layer 3 header to inspect the Layer 3 header which contains IP-related information including the source and destination IP addresses.

- source and destination MAC
- source and destination application protocol
- source and destination port number
- source and destination IP address

3. How does the network layer use the MTU value?

Topic 8.1.0 - The data link layer indicates to the network layer the MTU for the medium that is being used. The network layer uses that information to determine how large the packet can be when it is forwarded. When packets are received on one medium and forwarded on a medium with a smaller MTU, the network layer device can fragment the packet to accommodate the smaller size.

- The network layer depends on the higher level layers to determine the MTU.
- The network layer depends on the data link layer to set the MTU, and adjusts the speed of transmission to accommodate it.
- The MTU is passed to the network layer by the data link layer.
- To increase speed of delivery, the network layer ignores the MTU.

4. Which characteristic describes an IPv6 enhancement over IPv4?

Topic 8.3.0 - IPv6 addresses are based on 128-bit hierarchical addressing, and the IPv6 header has been simplified with fewer fields, improving packet handling. IPv6 natively supports authentication and privacy capabilities as opposed to IPv4 that needs additional features to support those. The IPv6 address space is many times bigger than IPv4 address space.

- ○ IPv6 addresses are based on 128-bit flat addressing as opposed to IPv4 which is based on 32-bit hierarchical addressing.
- ◉ The IPv6 header is simpler than the IPv4 header is, which improves packet handling.
- ○ Both IPv4 and IPv6 support authentication, but only IPv6 supports privacy capabilities.
- ○ The IPv6 address space is four times bigger than the IPv4 address space.

5. Which statement accurately describes a characteristic of IPv4?

Topic 8.2.0 - IPv4 has a 32-bit address space, providing 4,294,967,296 unique addresses, but only 3.7 billion are assignable, a limit due to address reservation for multicasting and testing. IPv4 does not provide native support for IPsec. IPv6 has a simplified header with fewer fields than IPv4 has.

- ○ All IPv4 addresses are assignable to hosts.
- ◉ IPv4 has a 32-bit address space.
- ○ An IPv4 header has fewer fields than an IPv6 header has.
- ○ IPv4 natively supports IPsec.

6. When a router receives a packet, what information must be examined in order for the packet to be forwarded to a remote destination?

Topic 8.4.0 - When a router receives a packet, it examines the destination address of the packet and uses the routing table to search for the best path to that network.

- ○ destination MAC address
- ○ source IP address
- ◉ destination IP address
- ○ source MAC address

7. A computer has to send a packet to a destination host in the same LAN. How will the packet be sent?

Topic 8.4.0 - If the destination host is in the same LAN as the source host, there is no need for a default gateway. A default gateway is needed if a packet needs to be sent outside the LAN.

- ○ The packet will be sent to the default gateway first, and then, depending on the response from the gateway, it may be sent to the destination host.
- ◉ The packet will be sent directly to the destination host.
- ○ The packet will first be sent to the default gateway, and then from the default gateway it will be sent directly to the destination host.
- ○ The packet will be sent only to the default gateway.

8. Which IPv4 address can a host use to ping the loopback interface?

Topic 8.4.0 - A host can ping the loopback interface by sending a packet to a special IPv4 address within the network 127.0.0.0/8.

- ○ 126.0.0.1
- ○ 127.0.0.0
- ○ 126.0.0.0
- ◉ 127.0.0.1

9. When a connectionless protocol is in use at a lower layer of the OSI model, how is missing data detected and retransmitted if necessary?

Topic 8.1.0 - When connectionless protocols are in use at a lower layer of the OSI model, upper-level protocols may need to work together on the sending and receiving hosts to account for and retransmit lost data. In some cases, this is not necessary, because for some applications a certain amount of data loss is tolerable.

- ○ Connectionless acknowledgements are used to request retransmission.
- ◉ Upper-layer connection-oriented protocols keep track of the data received and can request retransmission from the upper-level protocols on the sending host.
- ○ Network layer IP protocols manage the communication sessions if connection-oriented transport services are not available.
- ○ The best-effort delivery process guarantees that all packets that are sent are received.

10. What was the reason for the creation and implementation of IPv6?

Topic 8.3.0 - IPv4 addressing space is exhausted by the rapid growth of the Internet and the devices connected to the Internet. IPv6 expands the IP addressing space by increasing the address length from the 32 bits to 128 bits, which should provide sufficient addresses for future Internet growth needs for many years to come.

- ○ to make reading a 32-bit address easier
- ◉ to relieve IPv4 address depletion
- ○ to provide more address space in the Internet Names Registry
- ○ to allow NAT support for private addressing

11. Which information is used by routers to forward a data packet toward its destination?

Topic 8.4.0 - The destination IP address is the IP address for the receiving device. This IP address is used by routers to forward the packet to its destination.

- ○ source IP address
- ◉ destination IP address
- ○ source data-link address
- ○ destination data-link address

12. Which field in an IPv4 packet header will typically stay the same during its transmission?

Topic 8.1.0 - The value in the Destination Address field in an IPv4 header will stay the same during its transmission. The other options might change during its transmission.

- ○ Flag
- ○ Time-to-Live
- ○ Packet Length
- ◉ Destination Address

13. Which field in an IPv6 packet is used by the router to determine if a packet has expired and should be dropped?

Topic 8.3.0 – ICMPv6, like IPv4, sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired. However, the IPv6 packet does not have a TTL field. Instead, it uses the Hop Limit field to determine if the packet has expired.

- ○ TTL
- ◉ Hop Limit
- ○ Address Unreachable
- ○ No Route to Destination

Capítulo 9_Resolución de direcciones

Introducción

9.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Resolución de Direcciones!

Tanto los hosts como los routers crean tablas de enrutamiento para garantizar que pueden enviar y recibir datos a través de las redes. Entonces, ¿cómo se crea esta información en una tabla de enrutamiento? Como administrador de red, puede introducir estas direcciones MAC e IP manualmente. Pero eso llevaría mucho tiempo y la probabilidad de cometer algunos errores es grande. ¿Está pensando que debe haber alguna manera de que esto pueda hacerse automáticamente, por los propios hosts y routers? ¡Por supuesto, tiene razón! Y aunque sea automático, debe entender cómo funciona esto, porque puede que tenga que solucionar un problema o, peor aún, su red podría ser amenazada por un atacante. ¿Está listo para obtener información sobre la resolución de direcciones? Este módulo tiene varios videos muy buenos para ayudar a explicar los conceptos, así como tres actividades Packet Tracer para consolidar su comprensión. ¿Por qué esperar?

9.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Resolución de dirección

Objetivos del módulo: Explique cómo ARP y ND permiten la comunicación en una red.

Título del tema	Objetivo del tema
MAC e IP	Compare las funciones de la dirección MAC y de la dirección IP.
ARP	Describa el propósito de ARP.
detección de vecinos	Describa el funcionamiento de la detección de vecinos IPv6.

Resolución de dirección / MAC e IP

MAC e IP

9.1.1

Destino en la misma red

A veces, un host debe enviar un mensaje, pero solo conoce la dirección IP del dispositivo de destino. El host necesita saber la dirección MAC de ese dispositivo, pero ¿cómo se puede descubrir? Ahí es donde la resolución de direcciones se vuelve crítica.

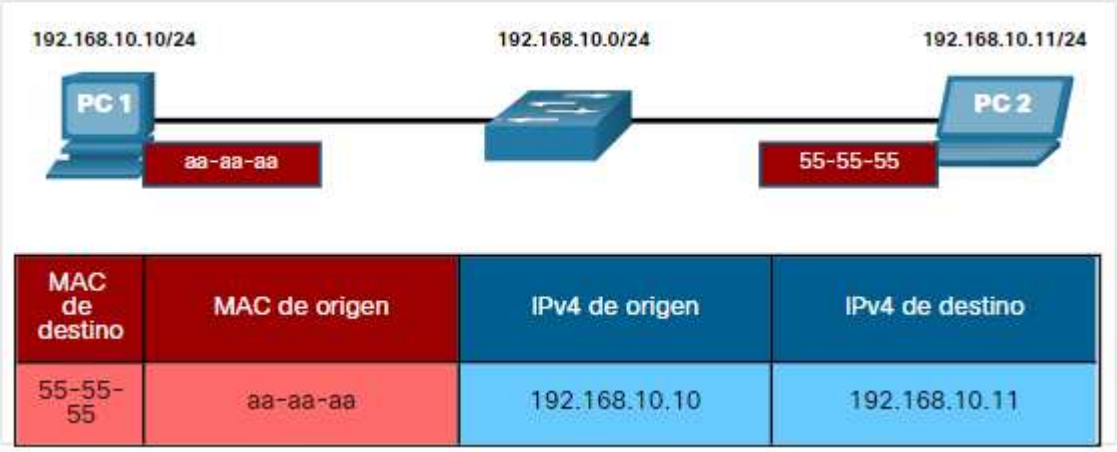
Hay dos direcciones primarias asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física (la dirección MAC)** – Se utiliza para comunicaciones NIC a NIC en la misma red Ethernet.
- **Dirección lógica (la dirección IP)** – Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino. La dirección IP de destino puede estar en la misma red IP que la de origen o en una red remota.

Las direcciones físicas de capa 2 (es decir, las direcciones MAC de Ethernet) se utilizan para entregar la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra NIC que está en la misma red. Si la dirección IP de destino está en la misma red, la dirección MAC de destino es la del dispositivo de destino.

Considere el siguiente ejemplo utilizando representaciones de direcciones MAC simplificadas.

La imagen es un diagrama de red con PC 1 en IP 192.168.10.10/24 con MAC simplificado aa-aa-aa, conectado a un switch en IP 192.168.10.0/24, conectado a PC 2 en IP 192.168.10.11/24 con MAC simplificado 55-55. Debajo del diagrama hay cuatro cuadros que leen de izquierda a derecha: Destino MAC 55-55, MAC de origen aa-aa-aa, IPv4 192.168.10.10 y Destino IPv4 192.168.10.11.



En este ejemplo, PC1 desea enviar un paquete a PC2. La figura muestra las direcciones MAC de origen y destino de Capa 2 y el direccionamiento IPv4 de Capa 3 que se incluirían en el paquete enviado desde PC1.

La trama Ethernet de capa 2 contiene lo siguiente:

Dirección MAC de ***destino****: esta es la dirección MAC simplificada de PC2, 55-55. Dirección MAC de* **origen**: es la dirección MAC simplificada de la NIC Ethernet en PC1, aa-aa-aa.

El paquete IP de capa 3 contiene lo siguiente:

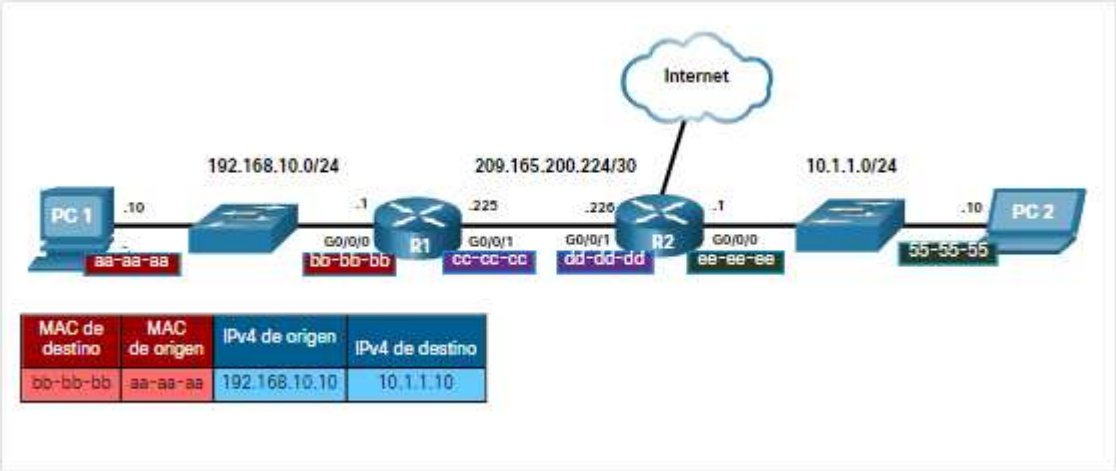
Dirección IPv4 de ***origen****: esta es la dirección IPv4 de PC1, 192.168.10.10. Dirección IPv4 de* **destino**: esta es la dirección IPv4 de PC2, 192.168.10.11.

9.1.2

Destino en una red remota

Cuando la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino será la dirección de gateway predeterminada del host (es decir, la interfaz del router).

Considere el siguiente ejemplo utilizando una representación de dirección MAC simplificada.

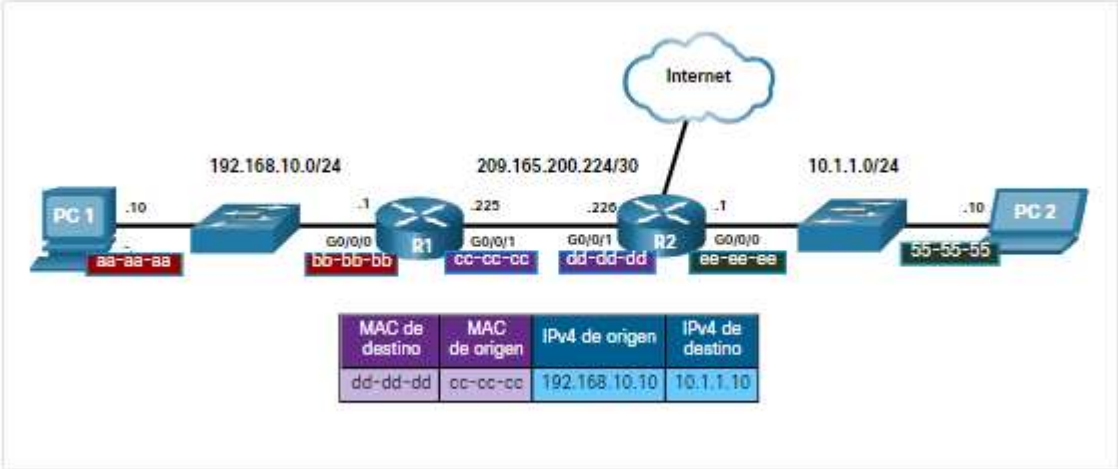


La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino para el primer salto cuando la información se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de 209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en la red 192.168.10.0/24 hay cuatro cuadros que leen de izquierda a derecha: MAC de destino bb-bb-bb, MAC de origen aa-aa-aa, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10.

En este ejemplo, PC1 desea enviar un paquete a PC2. PC2 se encuentra en una red remota. Dado que la dirección IPv4 de destino no está en la misma red local que PC1, la dirección MAC de destino es la del gateway predeterminado local en el router.

Los routers examinan la dirección IPv4 de destino para determinar la mejor ruta para reenviar el paquete IPv4. Cuando el router recibe una trama de Ethernet, desencapsula la información de capa 2. Por medio de la dirección IP de destino, determina el dispositivo del siguiente salto y desencapsula el paquete IP en una nueva trama de enlace de datos para la interfaz de salida.

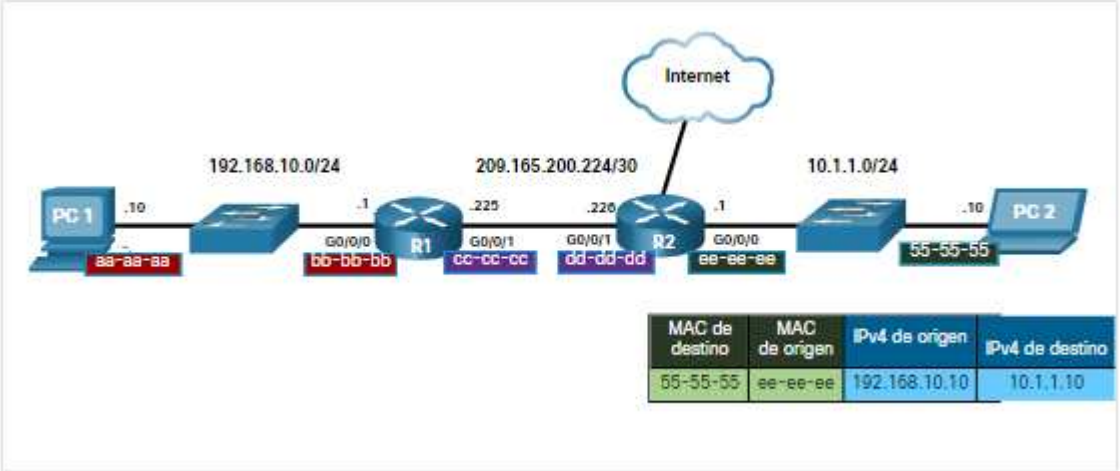
En nuestro ejemplo, R1 ahora encapsularía el paquete con la nueva información de dirección de Capa 2 como se muestra en la figura.



La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino cuando la información se pasa entre dos routers a medida que se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de 209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en red 209.165.200.224/30 hay cuatro cuadros que leen de izquierda a derecha: Destino MAC dd-dd-dd, MAC de origen cc-cc-cc, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10.

La nueva dirección MAC de destino sería la de la interfaz R2 G0/0/1 y la nueva dirección MAC de origen sería la de la interfaz R1 G0/0/1.

A lo largo de cada enlace de una ruta, un paquete IP se encapsula en una trama. La trama, es específica de la tecnología de enlace de datos asociada a ese vínculo, como Ethernet. Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino será la del NIC de Ethernet del dispositivo, como se muestra en la figura.



La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino cuando la información sale de un router al destino final a medida que se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de 209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en la red 10.1.1.0/24 hay cuatro cuadros que leen de izquierda a derecha: Destino MAC 55-55, MAC de origen ee-ee-ee, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10.

¿Cómo se asocian las direcciones IP de los paquetes IP en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Para los paquetes IPv4, esto se realiza a través de un proceso llamado Protocolo de resolución de direcciones (ARP). Para los paquetes IPv6, el proceso es ICMPv6 Neighbor Discovery (ND).

9.1.3

Packet Tracer: Identificación de direcciones MAC y direcciones IP

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Recopilar información de PDU para la comunicación de red local
- Recopilar información de PDU para la comunicación de red remota

Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Reunirá información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

Identificación de direcciones MAC y direcciones IP

Identificación de direcciones MAC y direcciones IP

9.1.4

Verifique su comprensión: MAC e IP

Verifique su comprensión del direccionamiento MAC e IP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Al enviar una trama a otro dispositivo en la misma red local, el dispositivo que envía la trama utilizará la dirección MAC del dispositivo de destino.
2. Al enviar una trama a otro dispositivo en una red remota, el dispositivo que envía la trama utilizará la dirección MAC de la interfaz del router local, que es el gateway predeterminado.
3. El Protocolo de resolución de direcciones (ARP) se utiliza para determinar la dirección MAC del dispositivo de una dirección IPv4 de un dispositivo de destino conocido. Detección de vecinos (ND) se utiliza para determinar la dirección MAC de una dirección IPv6 de dispositivo de destino conocida.

Has tenido 3 respuestas correctas de 3.

Correct

You have successfully identified the correct answers.

1. When sending a frame to another device on the same local network, the device sending the frame will use the MAC address of the destination device.
2. When sending a frame to another device on a remote network, the device sending the frame will use the MAC address of the local router interface, which is the default gateway.
3. Address Resolution Protocol (ARP) is used to determine the device MAC address of a known destination device IPv4 address. Neighbor Discovery (ND) is used to determine the MAC address of a known destination device IPv6 address.

You got 3 out of 3 questions correct.

1. ¿Qué dirección MAC de destino se incluiría en una trama enviada desde un dispositivo de origen a un dispositivo de destino en la misma red local?

¡Lo tienes!

- ○ Dirección MAC broadcast de FF-FF-FF-FF-FF-FF.
- ◉ La dirección MAC del dispositivo de destino.
- ○ La dirección MAC de la interfaz del router local.

2. ¿Qué dirección MAC de destino se incluiría en una trama enviada desde un dispositivo de origen a un dispositivo de destino en una red local remota?

¡Lo tienes!

- ○ Dirección MAC broadcast de FF-FF-FF-FF-FF-FF.
- ○ La dirección MAC del dispositivo de destino.
- ◉ La dirección MAC de la interfaz del router local.

3. ¿Qué dos protocolos se utilizan para determinar la dirección MAC de una dirección IP de un dispositivo de destino conocido (IPv4 e IPv6)?

¡Lo tienes!

- ☐ DHCP
- ☑ ARP
- ☐ DNS
- ☑ ND

1. What destination MAC address would be included in a frame sent from a source device to a destination device on the same local network?

You got it!

- ○ A broadcast MAC address of FF-FF-FF-FF-FF-FF.
- ◉ The MAC address of the destination device.
- ○ The MAC address of the local router interface.

2. What destination MAC address would be included in a frame sent from a source device to a destination device on a remote local network?

You got it!

- ○ A broadcast MAC address of FF-FF-FF-FF-FF-FF.
- ○ The MAC address of the destination device.
- ◉ The MAC address of the local router interface.

3. What two protocols are used to determine the MAC address of a known destination device IP address (IPv4 and IPv6)?

You got it!

- ☐ DHCP
- ☑ ARP
- ☐ DNS
- ☑ ND

Resolución de direcciones / ARP

ARP

9.2.1

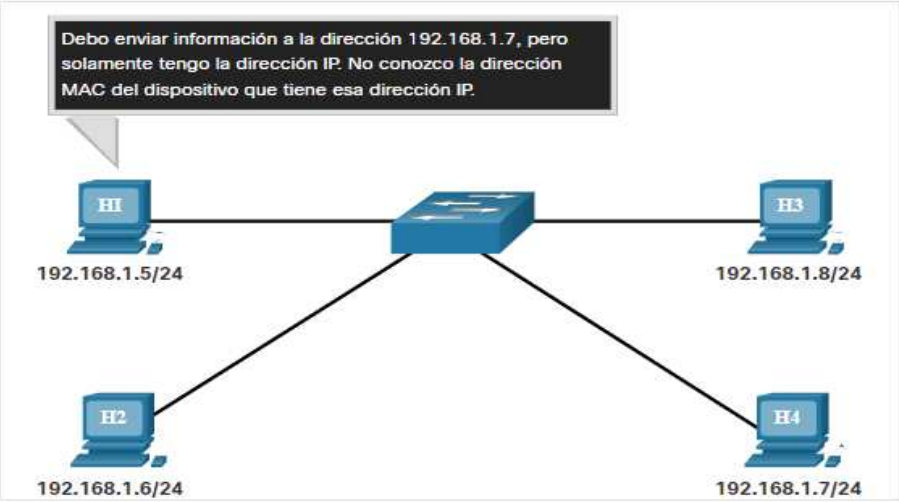
Descripción general de ARP

Si su red utiliza el protocolo de comunicaciones IPv4, el protocolo de resolución de direcciones o ARP es lo que necesita para asignar direcciones IPv4 a direcciones MAC. En este tema se explica cómo funciona ARP.

Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet única. Cuando un dispositivo envía una trama de capa 2 de Ethernet, contiene estas dos direcciones:

- **Dirección MAC de destino** - La dirección MAC Ethernet del dispositivo de destino en el mismo segmento de red local. Si el host de destino está en otra red, entonces la dirección de destino en la trama sería la del gateway predeterminado (es decir, router).
- **Dirección MAC de origen** - La dirección MAC de la NIC de Ethernet en el host de origen.

La figura ilustra el problema al enviar una trama a otro host en el mismo segmento en una red IPv4.



Cuatro hosts, H1, H2, H3 y H4, están conectados al mismo switch. H1 tiene una IP de 192.168.1.5/24, H2 tiene una IP de 192.168.1.6/24, H3 tiene una IP de 192.168.1.8/24 y H4 tiene una IP de 192.168.1.7/24. H1 tiene un enunciado que dice: Necesito enviar información a 192.168.1.7, pero solo tengo la dirección IP. No conozco la dirección MAC del dispositivo que tiene esa dirección IP.

Para enviar un paquete a otro host en la misma red IPv4 local, un host debe conocer la dirección IPv4 y la dirección MAC del dispositivo de destino. Las direcciones IPv4 de destino del dispositivo se conocen o se resuelven por el nombre del dispositivo. Sin embargo, las direcciones MAC deben ser descubiertas.

Un dispositivo utiliza el Protocolo de resolución de direcciones (ARP) para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantener una tabla de asignaciones de direcciones IPv4 a MAC

9.2.2

Funciones del ARP

Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4. Esta tabla se almacena temporalmente en la memoria RAM y se denomina tabla ARP o caché ARP.

El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

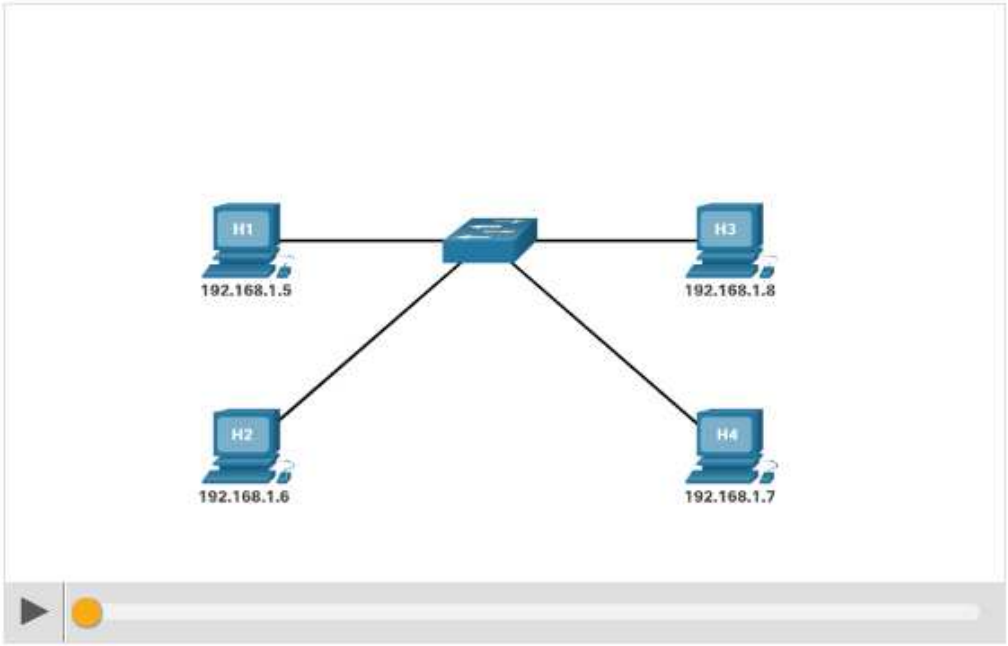
- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
- Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

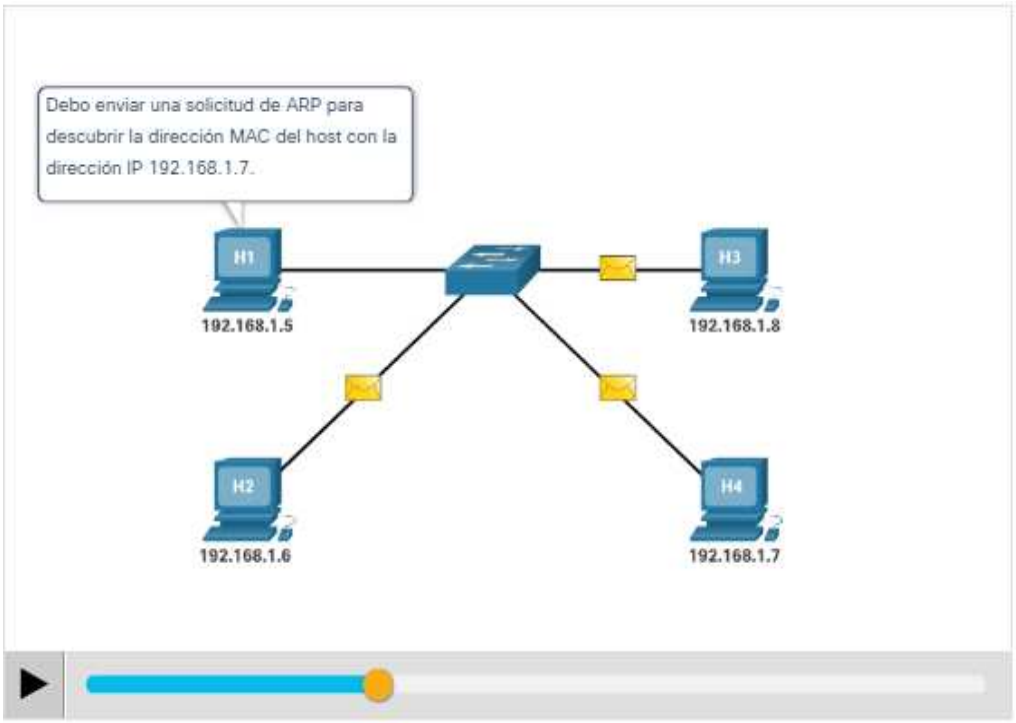
En ambos casos, se realiza una búsqueda de la dirección IPv4 y la dirección MAC correspondiente para el dispositivo.

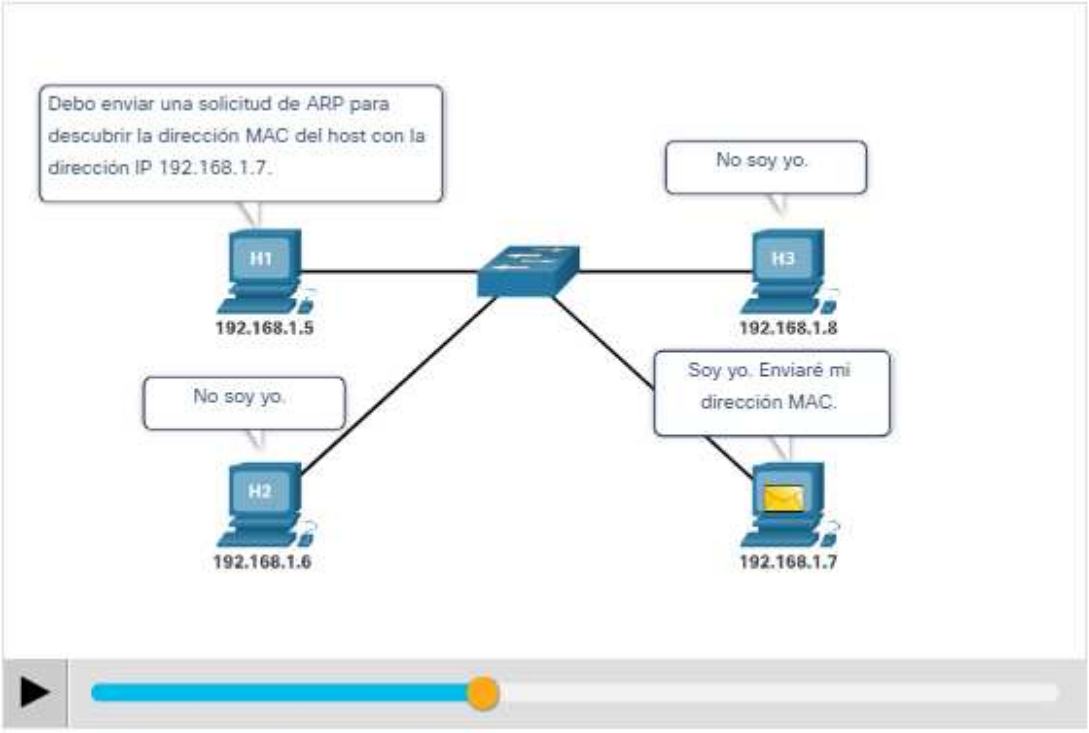
En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. Llamamos a la relación entre los dos valores un mapa. Esto solamente significa que es posible buscar una dirección IPv4 en la tabla y encontrar la dirección MAC correspondiente. La tabla ARP almacena temporalmente (en caché) la asignación para los dispositivos de la LAN.

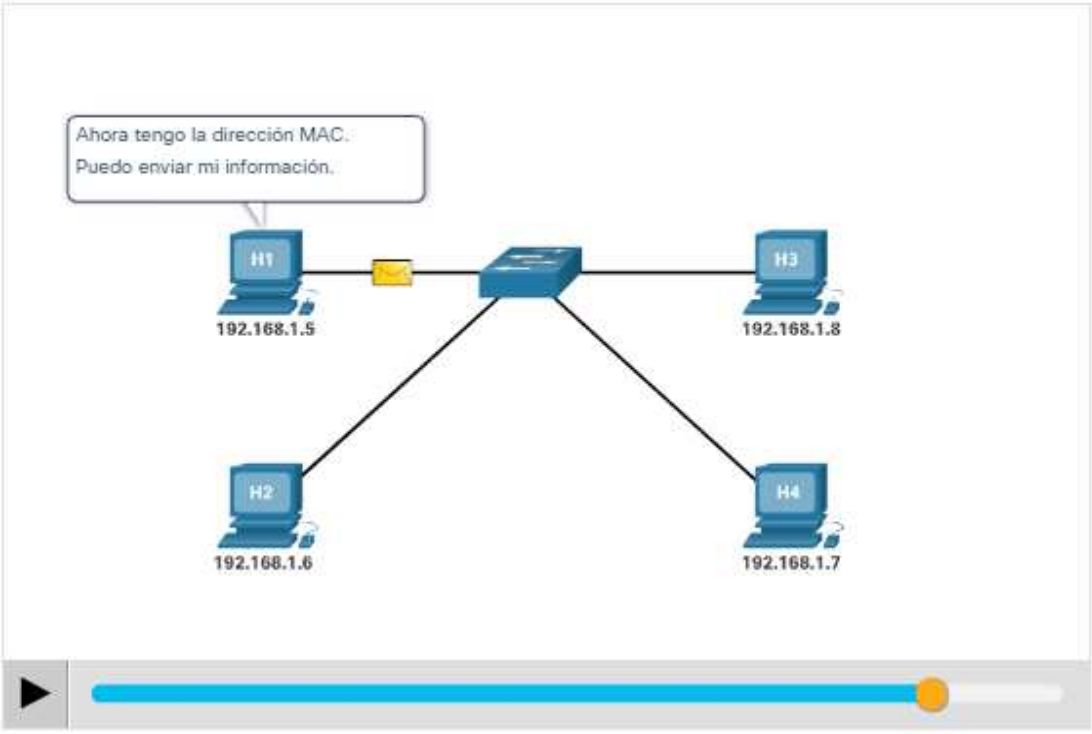
Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.

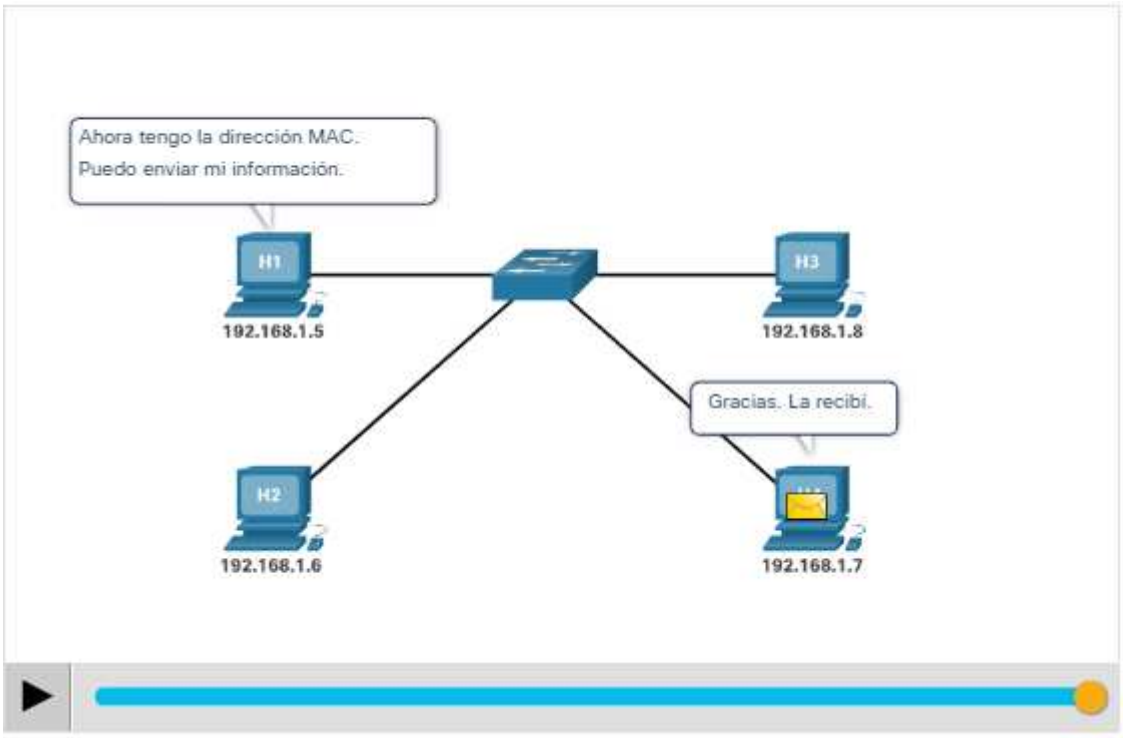
Haga clic en Reproducir en la figura para ver una animación de la función ARP.


H1
192.168.1.5
H3
192.168.1.8
H2
192.168.1.6
H4
192.168.1.7


Debo enviar una solicitud de ARP para descubrir la dirección MAC del host con la dirección IP 192.168.1.7.
H1
192.168.1.5
H3
192.168.1.8
H2
192.168.1.6
H4
192.168.1.7


Debo enviar una solicitud de ARP para descubrir la dirección MAC del host con la dirección IP 192.168.1.7.
No soy yo.
H1
H3
192.168.1.5
192.168.1.8
No soy yo.
Soy yo. Enviaré mi dirección MAC.
H2
192.168.1.6
192.168.1.7


Ahora tengo la dirección MAC.
Puedo enviar mi información.
H1
H3
192.168.1.5
192.168.1.8
H2
H4
192.168.1.6
192.168.1.7



Esta animación ilustra cómo un host utilizará ARP para descubrir la dirección MAC de una dirección IP conocida. El host H1 necesita enviar cierta información a un host con dirección IP 192.168.1.7. Sin embargo, H1 no tiene la dirección MAC para esa dirección. Por lo tanto, envía una solicitud ARP a la dirección IP 192.168.1.7. Todos los hosts en la red recibirán la solicitud ARP. Sin embargo, sólo el host H4 con dirección IP 192.168.1.7 enviará una respuesta ARP que contenga su dirección MAC.

9.2.3

Video - Solicitud de ARP

Se envía una solicitud ARP cuando un dispositivo necesita determinar la dirección MAC que está asociada con una dirección IPv4, y no tiene una entrada para la dirección IPv4 en su tabla ARP.

Los mensajes de ARP se encapsulan directamente dentro de una trama de Ethernet. No se utiliza un encabezado de IPv4. La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

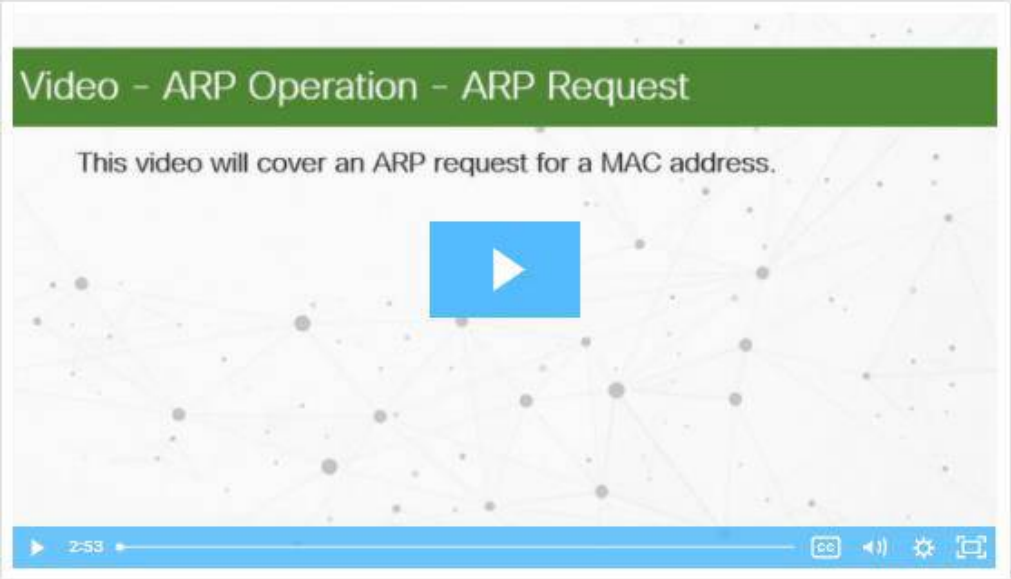
- **Dirección MAC de destino** – esta es una dirección broadcast que requiere que todas las NIC Ethernet de la LAN acepten y procesen la solicitud de ARP.
- **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la solicitud ARP.

- **Tipo** - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Como las solicitudes de ARP son de broadcast, el switch las envía por todos los puertos, excepto el de recepción. Todas las NIC Ethernet de la LAN procesan transmisiones y deben entregar la solicitud ARP a su sistema operativo para su procesamiento. Cada dispositivo debe procesar la solicitud de ARP para ver si la dirección IPv4 objetivo coincide con la suya. Un router no reenvía broadcasts por otras interfaces.

Sólo un dispositivo de la LAN tiene la dirección IPv4 que coincide con la dirección IPv4 objetivo de la solicitud de ARP. Todos los demás dispositivos no envían una respuesta.

Haga clic en Reproducir para ver una demostración de una solicitud de ARP para una dirección IPv4 de destino que está en la red local.



9.2.4

Vídeo - Funcionamiento de ARP - Respuesta de ARP

Solo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP. La respuesta de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- **Dirección MAC de destino** – Es la dirección MAC del remitente de la solicitud de ARP.

- **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la respuesta ARP.
- **Tipo** - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Solamente el dispositivo que envió inicialmente la solicitud de ARP recibe la respuesta de ARP de unicast. Una vez que recibe la respuesta de ARP, el dispositivo agrega la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP. A partir de ese momento, los paquetes destinados para esa dirección IPv4 se pueden encapsular en las tramas con su dirección MAC correspondiente.

Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no se puede crear una trama.

Las entradas de la tabla ARP tienen marcas de tiempo. Si un dispositivo no recibe una trama de un dispositivo en particular antes de que caduque la marca de tiempo, la entrada para este dispositivo se elimina de la tabla ARP.

Además, se pueden introducir entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y se deben eliminar de forma manual.

Nota: IPv6 utiliza un proceso similar a ARP para IPv4, conocido como ICMPv6 Neighbour Discovery (ND). IPv6 utiliza mensajes de solicitud de vecino y de anuncio de vecino similares a las solicitudes y respuestas de ARP de IPv4.

Haga clic en Reproducir en la ilustración para ver una demostración de una respuesta de ARP.

9.2.5

Video - Rol ARP en Comunicaciones Remotas

Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado. Esta es la interfaz del router local. Cuando un dispositivo de origen tiene un paquete con una dirección IPv4 de otra red, lo encapsula en una trama con la dirección MAC de destino del router.

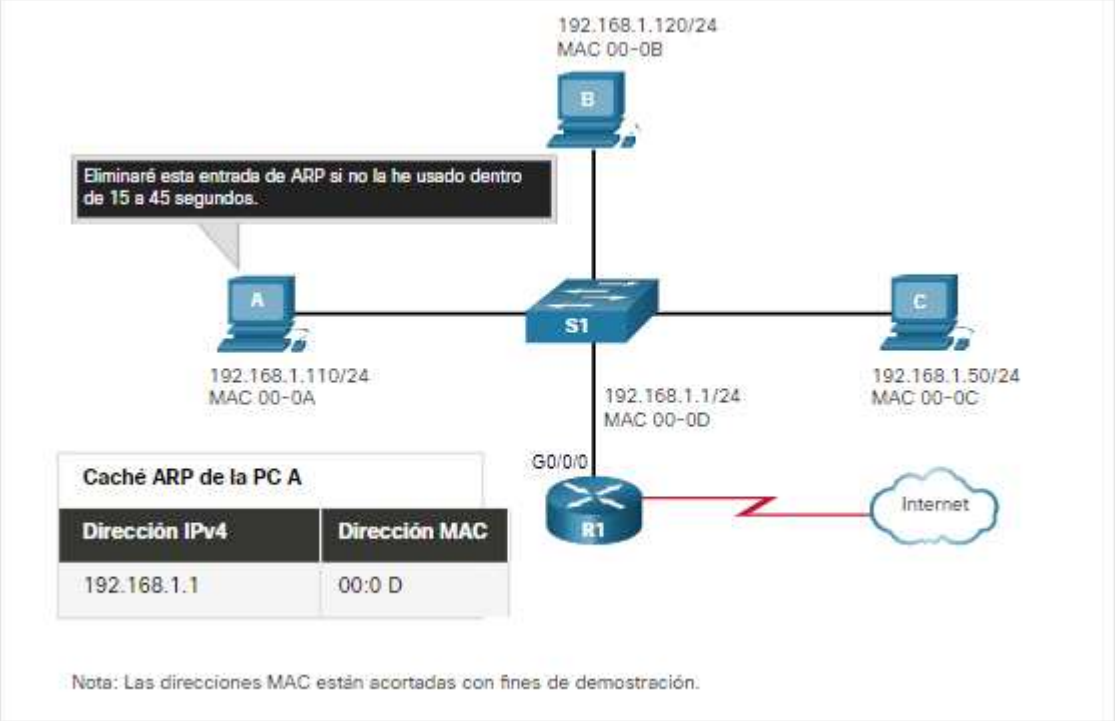
La dirección IPv4 de la dirección del gateway predeterminado se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino con la propia para determinar si ambas están ubicadas en la misma red de capa 3. Si el host de destino no está en la misma red, el origen busca en la tabla ARP una entrada que contenga la dirección IPv4 del gateway predeterminado. Si no existe una entrada, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.

Haga clic en Reproducir para ver una demostración de una solicitud de ARP y una respuesta de ARP asociadas con el gateway predeterminado.

9.2.6

Eliminación de entradas de una tabla ARP

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los tiempos varían según el sistema operativo del dispositivo. Por ejemplo, los sistemas operativos Windows más recientes almacenan entradas de tabla ARP entre 15 y 45 segundos, como se ilustra en la figura:



Los comandos también se pueden usar para eliminar manualmente algunas o todas las entradas de la tabla ARP. Después de eliminar una entrada, el proceso de envío de una solicitud de ARP y de recepción de una respuesta de ARP debe ocurrir nuevamente para que se introduzca la asignación en la tabla ARP.

9.2.7

Tablas ARP en dispositivos de red

En un router Cisco, el comando **show ip arp,** se utiliza para mostrar la tabla ARP, como se muestra en la figura:

```
R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabiteThernet0/0/0
Internet 209.165.200.225 - a0e0.af0d.e141 ARPA GigabiteThernet0/0/1
Internet 209.165.200.226 1 a03d.6fe1.9d91 ARPA GigabiteThernet0/0/1
R1#
```

En una PC con Windows 10, el **arp –a** comando se usa para mostrar la tabla ARP, como se muestra en la figura:

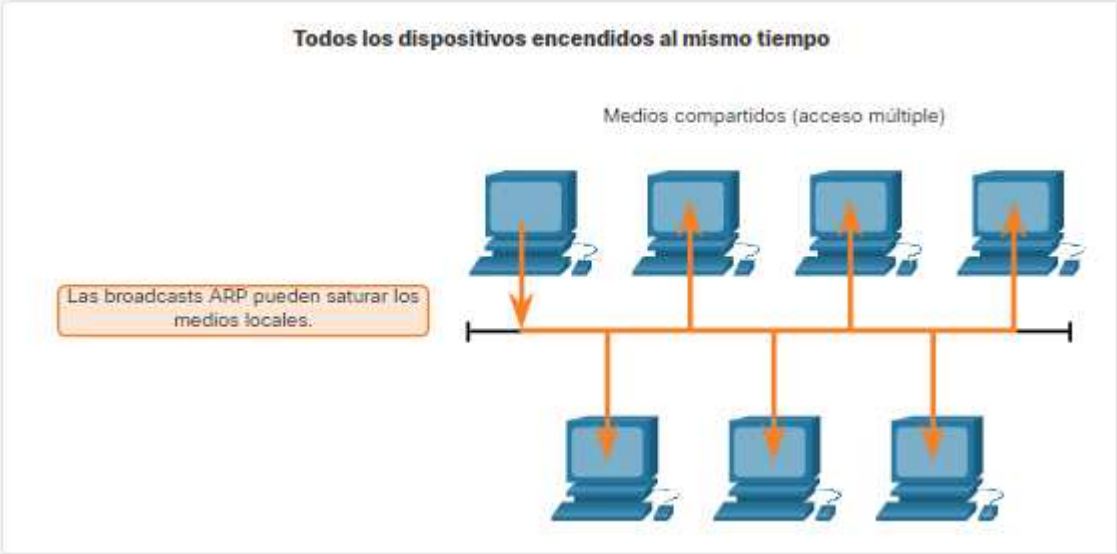
```
C:\Users\PC > arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address Physical Address Type
  192.168.1.1 c8-d7-19-cc-a0-86 dynamic
  192.168.1.101 08-3e-0c-f5-f7-77 dynamic
  192.168.1.110 08-3e-0c-f5-f7-56 dynamic
  192.168.1.112 ac-b3-13-4a-bd-d0 dynamic
  192.168.1.117 08-3e-0c-f5-f7-5c dynamic
  192.168.1.126 24-77-03-45-5d-c4 dynamic
  192.168.1.146 94-57-a5-0c-5b-02 dynamic
  192.168.1.255 ff-ff-ff-ff-ff-ff static
  224.0.0.22 01-00-5e-00-00-16 static
  224.0.0.22 01-00-5e-00-00-16 static
  239.255.255.250 01-00-5e-7f-ff-fa static
  255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\PC >
```

9.2.8

Problemas de ARP: Broadcasts ARP y ARP Spoofing

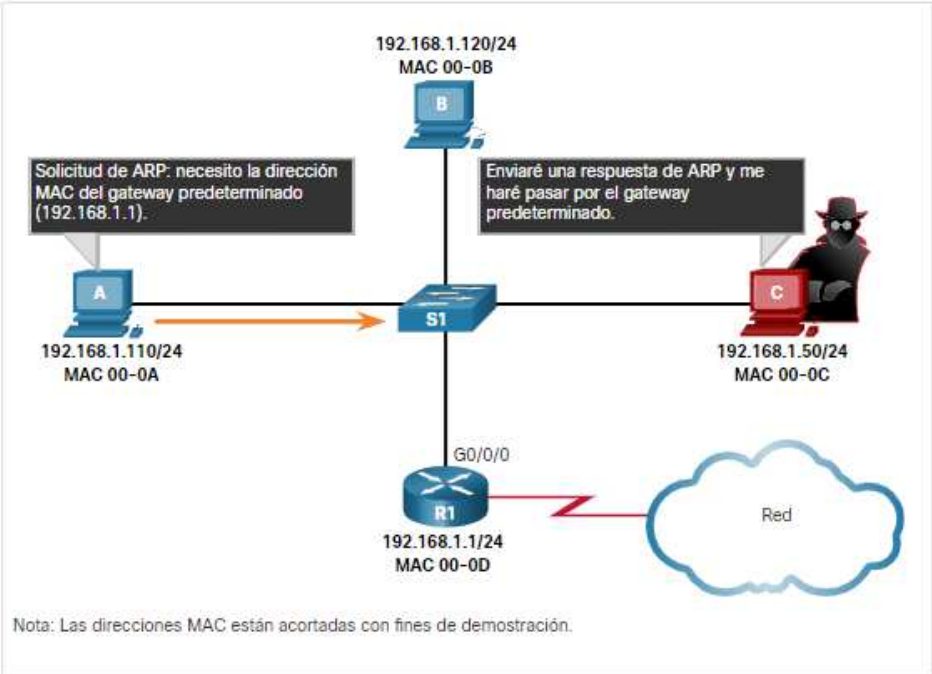
Como trama broadcast, todos los dispositivos de la red local reciben y procesan una solicitud ARP. En una red comercial típica, estos broadcasts tendrían, probablemente, un efecto mínimo en el rendimiento de la red. Sin embargo, si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período, como se muestra en la figura. Después de que los dispositivos envían los broadcasts ARP iniciales y obtienen las direcciones MAC necesarias, se minimiza cualquier efecto en la red.

El diagrama muestra siete dispositivos en medios compartidos (acceso múltiple) todos encendidos al mismo tiempo. Un cuadro de texto dice: los broadcasts ARP pueden inundar los medios locales.



En algunos casos, el uso de ARP puede conducir a un riesgo potencial de seguridad. Un atacante puede usar la ARP spoofing para realizar un ataque de ARP poisoning. Esta es una técnica utilizada por un atacante para responder a una solicitud de ARP de una dirección IPv4 que pertenece a otro dispositivo, como el gateway predeterminado, como se muestra en la ilustración. El atacante envía una respuesta de ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante.

Los switches de nivel empresarial incluyen técnicas de mitigación conocidas como "inspección dinámica de ARP (DAI)". DAI está más allá del alcance de este curso.



La imagen es un diagrama de red que muestra dos hosts, Host A con IP 192.168.1.110/24 y MAC 00-0A y Host B con IP 192.168.1.120/24 y MAC 00-0B, conectados al switch S1 que está conectado al router R1 en el puerto G0/0/0 (la gateway predeterminado con IP 192.168.1.1/24 y MAC 00-0D) que está conectado a Internet nube. También está conectado a S1 un atacante en el host C con IP 192.168.1.50/24 y MAC 00-0C. El host A tiene un enunciado que dice: Solicitud ARP: Necesito la dirección MAC del gateway predeterminado, 192.168.1.1. El atacante anfitrión C tiene un enunciado que dice: ¡Enviaré una respuesta ARP y fingiré ser la gateway predeterminado! Nota: Las direcciones MAC están acortadas con fines de demostración.

9.2.9

Packet Tracer: Examinar la tabla ARP

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Examinar una solicitud de ARP
- Examinar una tabla de direcciones MAC del switch
- Examinar el proceso ARP en comunicaciones remotas

Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Reunirá información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

Revisión de la tabla ARP

Revisión de la tabla ARP

9.2.10

Verifique su comprensión - ARP

Verifique su comprensión de ARP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. ARP tiene dos funciones principales: mantener una tabla de asignaciones de direcciones IPv4 a MAC y determinar las direcciones MAC de direcciones IPv4 conocidas.
2. La tabla ARP se almacena en caché temporalmente en la RAM.
3. La tabla ARP se almacena en caché temporalmente en la RAM.
4. El comando **show ip arp** se utiliza en routers Cisco para ver la tabla ARP.
5. Dos problemas de seguridad con las solicitudes ARP son que los mensajes ARP se envían como broadcast y se pueden suplantar.

Has tenido 5 respuestas correctas de 5.

1. ¿Qué dos funciones proporciona ARP? (Escoja dos.)

¡Lo tienes!

- [ ] Mantiene una tabla de direcciones IPv4 a los nombres de dominio
- [x] Mantiene una tabla de asignaciones de direcciones IPv4 a MAC
- [ ] Mantiene una tabla de asignaciones de direcciones IPv6 a MAC
- [ ] Resuelve direcciones IPv4 a nombres de dominio
- [x] Resuelve direcciones IPv4 a direcciones MAC
- [ ] Resuelve direcciones IPv6 a direcciones MAC

2. ¿Dónde se almacena la tabla ARP en un dispositivo?

¡Lo tienes!

- ( ) ROM
- ( ) Memoria flash
- ( ) NVRAM
- (•) RAM

3. ¿Qué afirmación es verdadera sobre ARP?

¡Lo tienes!

- ( ) No se puede eliminar manualmente una memoria caché ARP.
- ( ) Las entradas ARP se almacenan en caché de forma permanente.
- (•) Las entradas ARP se almacenan en caché temporalmente.

4. ¿Qué comando se podría usar en un router Cisco para ver su tabla ARP?

¡Lo tienes!

- arp -a
- arp -d
- mostrar tablaarp
- **show ip arp**

5. ¿Qué es un ataque usando ARP?

¡Lo tienes!

- broadcasts ARP
- ataques ARP hopping
- Envenenamiento ARP
- La inanición de ARP

Correct

You have successfully identified the correct answers.

1. ARP has two primary functions: maintain a table of IPv4 to MAC address mappings and determine the MAC addresses of known IPv4 addresses.
2. The ARP table is cached temporarily in RAM.
3. The ARP table is cached temporarily in RAM.
4. The command **show ip arp** is used on Cisco routers to view the ARP table.
5. Two security issues with ARP Requests are that ARP messages are sent as broadcasts and can be spoofed.

You got 5 out of 5 questions correct.

1. What two functions are provided by ARP? (Choose two.)

You got it!

- [ ] Maintains a table of IPv4 address to domain names
- [x] Maintains a table of IPv4 to MAC address mappings
- [ ] Maintains a table of IPv6 to MAC address mappings
- [ ] Resolves IPv4 addresses to domain names
- [x] Resolves IPv4 addresses to MAC addresses
- [ ] Resolves IPv6 addresses to MAC addresses

2. Where is the ARP table stored on a device?

You got it!

- ROM
- flash
- NVRAM
- RAM

3. Which statement is true about ARP?

You got it!

- An ARP cache cannot be manually deleted.
- ARP entries are cached permanently.
- ARP entries are cached temporarily.

4. Which command could be used on a Cisco router to view its ARP table?

You got it!

- **arp -a**
- **arp -d**
- **show arp table**
- **show ip arp**

5. What is an attack using ARP?

You got it!

- ARP broadcasts
- ARP hopping attacks
- ARP poisoning
- ARP starvation

Resolución de dirección / Detección de vecinos IPv6

Detección de vecinos IPv6

9.3.1

Video - Detección de vecinos IPv6

Si su red utiliza el protocolo de comunicaciones IPv6, el protocolo de detección de vecinos o ND es lo que necesita para hacer coincidir las direcciones IPv6 con las direcciones MAC. En este tema se explica cómo funciona ND.

Haga clic en Reproducir en la figura para ver una demostración de Descubrimiento de vecinos IPv6.

9.3.2

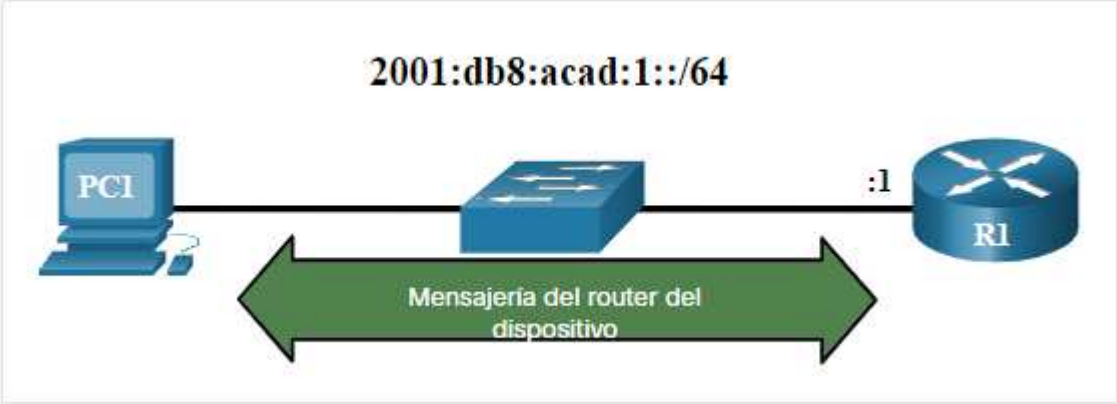
Mensajes de descubrimiento de vecinos IPv6

El protocolo IPv6 descubrimiento de vecinos se conoce a veces como ND o NDP. En este curso, nos referiremos a él como ND. ND proporciona servicios de resolución de direcciones, detección de routers y redirección para IPv6 mediante ICMPv6. ICMPv6 ND utiliza cinco mensajes ICMPv6 para realizar estos servicios:

- NS: Mensajes de solicitud de vecinos.
- NA: Mensaje de anuncio de vecino
- RS: Mensaje de solicitud del router
- RA: Mensajes de anuncio del router. Mensaje de* redirección

Los mensajes de solicitud de vecino y anuncio de vecino se utilizan para la mensajería de dispositivo a dispositivo, como la resolución de direcciones (similar a ARP para IPv4). Los dispositivos incluyen tanto equipos host como routers.

Los mensajes de solicitud de router y anuncio de router son para mensajes entre dispositivos y routers. Normalmente, la detección de routers se utiliza para la asignación dinámica de direcciones y la configuración automática de direcciones sin estado (SLAAC).



Nota: El quinto mensaje ICMPv6 ND es un mensaje de redirección que se utiliza para una mejor selección de siguiente salto. Esto está fuera del alcance de este curso.

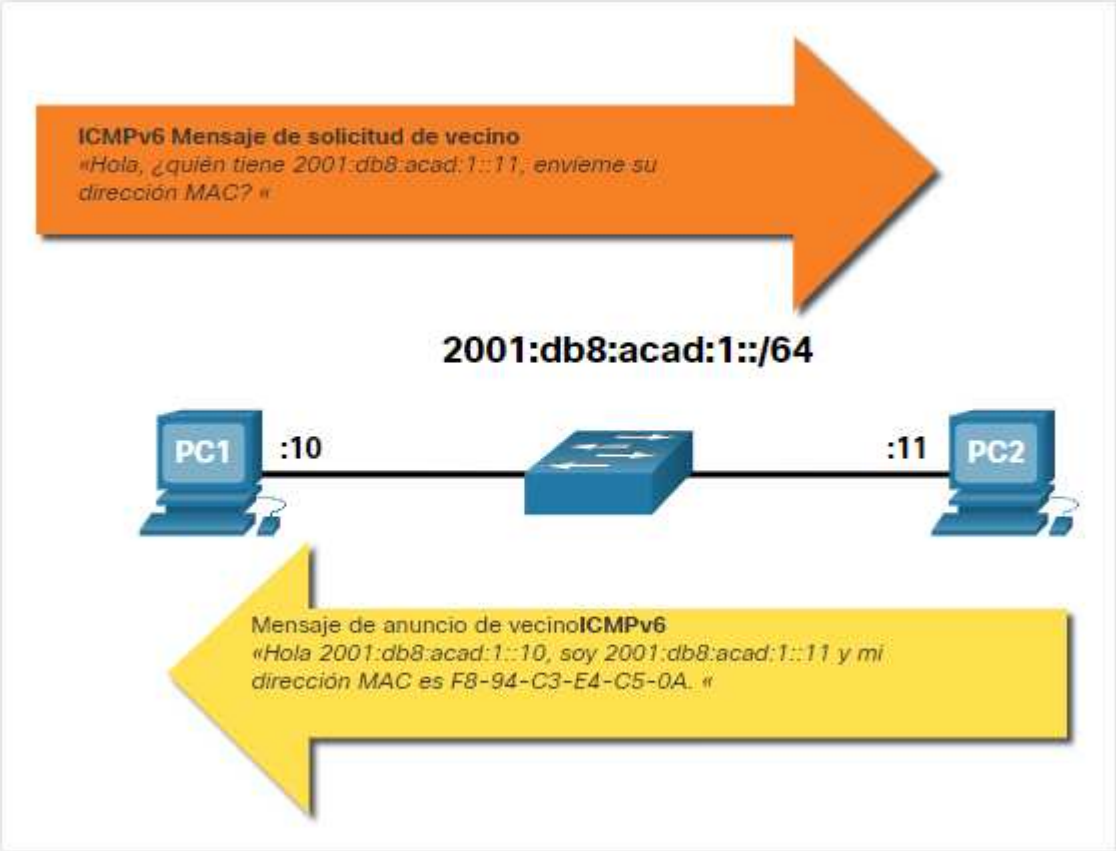
IPv6 ND se define en IETF RFC 4861.

9.3.3

Descubrimiento de vecinos IPv6: resolución de direcciones

Al igual que ARP para IPv4, los dispositivos IPv6 utilizan IPv6 ND para determinar la dirección MAC de un dispositivo que tiene una dirección IPv6 conocida.

Los mensajes ICMPv6 Solicitud de vecino y Anuncio de vecino se utilizan para la resolución de la dirección MAC. Esto es similar a las solicitudes ARP y las respuestas ARP utilizadas por ARP para IPv4. Por ejemplo, supongamos que PC1 desea hacer ping a PC2 en la dirección IPv6 2001:db8:acad: :11. Para determinar la dirección MAC de la dirección IPv6 conocida, PC1 envía un mensaje de solicitud de vecino ICMPv6 como se ilustra en la figura.



El diagrama muestra PC1 y PC2 conectados al mismo switch en la red 2001:db8:acad:1: :/64. PC1 tiene una dirección IPv6 2001:db8:acad:1: :10 y PC2 tiene una dirección IPv6 2001:db8:acad:1: :11. PC1 está enviando un mensaje de solicitud de vecino ICMPv6 que dice: Hola, ¿quién tiene 2001: db8: acad: 1:: 11, envíeme su dirección MAC? PC2 está respondiendo con un mensaje de anuncio de vecino ICMPv6 que dice: Hola 2001:db8:acad:1::10, soy 2001:db8:acad:1::11 y mi dirección MAC es F8-94-C3-E4-C5-0A.

Los mensajes de solicitud de vecinos ICMPv6 se envían utilizando direcciones multibroadcast Ethernet e IPv6 especiales. Esto permite que la NIC Ethernet del dispositivo receptor determine si el mensaje de solicitud de vecino es para sí mismo sin tener que enviarlo al sistema operativo para su procesamiento.

PC2 responde a la solicitud con un mensaje ICMPv6 Neighbor Advertisement que incluye su dirección MAC.

9.3.4

Packet Tracer - Detección de vecinos IPv6

Para que un dispositivo se comunique con otro dispositivo, se debe conocer la dirección MAC del dispositivo de destino. Con IPv6, un proceso denominado Neighbor Discovery es responsable de determinar la dirección MAC de destino. Recopilará información de PDU en modo de simulación para comprender mejor el proceso. No hay puntuación de Packet Tracer para esta actividad.

Descubrimiento de vecinos IPv6

Descubrimiento de vecinos IPv6

9.3.5

Compruebe su comprensión - Detección de vecinos

Verifique su comprensión eligiendo la MEJOR respuesta a las siguientes preguntas:

Correcto

Identificó bien las respuestas correctas.

1. Los dos mensajes ICMPv6 utilizados en SLAAC son la solicitud del router y el anuncio del router.
2. Los dos mensajes ICMPv6 utilizados para determinar la dirección MAC de una dirección IPv6 conocida son la solicitud de vecino y el anuncio de vecino.
3. Los mensajes de solicitud de vecino ICMPv6 se envían como multicast.

Has tenido 3 respuestas correctas de 3.

Correct

You have successfully identified the correct answers.

1. The two ICMPv6 messages used in SLAAC are the router solicitation and the router advertisement.
2. The two ICMPv6 messages used in determining the MAC address of a known IPv6 address are the neighbor solicitation and the neighbor advertisement.
3. ICMPv6 neighbor solicitation messages are sent as a multicast.

You got 3 out of 3 questions correct.

1. ¿Qué dos mensajes ICMPv6 se utilizan en SLAAC?

¡Lo tienes!

- [ ] Anuncio de vecino
- [ ] Solicitud de vecino
- [x] Anuncio de router
- [x] Solicitud de router

2. ¿En qué dos mensajes ICMPv6 se utilizan para determinar la dirección MAC de una dirección IPv6 conocida?

¡Lo tienes!

- [x] Anuncio de vecino
- [x] Solicitud de vecino
- [ ] Anuncio de router
- [ ] Solicitud de router

3. ¿A qué tipo de dirección se envían los mensajes de solicitud de vecino ICMPv6?

¡Lo tienes!

- ( ) Unidifusión
- (•) Multidifusión
- ( ) Difusión

1. Which two ICMPv6 messages are used in SLAAC?

You got it!

- [ ] Neighbor Advertisement
- [ ] Neighbor Solicitation
- [x] Router Advertisement
- [x] Router Solicitation

2. Which two ICMPv6 messages are used in to determine the MAC address of a known IPv6 address?

You got it!

- [x] Neighbor Advertisement
- [x] Neighbor Solicitation
- [ ] Router Advertisement
- [ ] Router Solicitation

3. To what type of address are ICMPv6 neighbor solicitation messages sent?

You got it!

- ( ) unicast
- (•) multicast
- ( ) broadcast

Módulo de Práctica y Prueba

9.4.1

¿Qué aprendió en este módulo?

MAC and IP

Las direcciones físicas de capa 2 (es decir, las direcciones MAC de Ethernet) se utilizan para entregar la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra NIC que está en la misma red. Si la dirección IP de destino está en la misma red, la dirección MAC de destino es la del dispositivo de destino. Cuando la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino será la dirección de gateway predeterminada del host (es decir, la interfaz del router). A lo largo de cada enlace de una ruta, un paquete IP se encapsula en una trama. La trama, es específica de la tecnología de enlace de datos asociada a ese vínculo, como Ethernet. Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino es la de la NIC Ethernet del dispositivo. ¿Cómo se asocian las direcciones IP de los paquetes IP en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Para los paquetes IPv4, esto se realiza a través de un proceso llamado ARP. Para los paquetes IPv6, el proceso es ICMPv6 ND.

ARP

Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet única. Cuando un dispositivo envía una trama de capa 2 de Ethernet, contiene estas dos direcciones: dirección MAC de destino y dirección MAC de origen. Un dispositivo utiliza ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4. ARP proporciona dos funciones básicas: resolver direcciones IPv4 a direcciones MAC y mantener una tabla de asignaciones de direcciones IPv4 a MAC. La solicitud ARP se encapsula en una trama Ethernet utilizando esta información de encabezado: direcciones MAC de origen y destino y tipo. Solo un dispositivo de la LAN tiene la dirección IPv4 que coincide con la dirección IPv4 objetivo de la solicitud de ARP. Todos los demás dispositivos no envían una respuesta. La respuesta ARP contiene los mismos campos de encabezado que la solicitud. Solamente el dispositivo que envió inicialmente la solicitud de ARP recibe la respuesta de ARP de unicast. Una vez que recibe la respuesta de ARP, el dispositivo agrega la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP. Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado. Esta es la interfaz del router local. Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los comandos también se pueden usar para eliminar manualmente algunas o todas las entradas de la tabla ARP. Como una trama de difusión, todos los dispositivos de la red local reciben y procesan una solicitud ARP, lo que

podría hacer que la red se desacelere. Un atacante puede usar la ARP spoofing para realizar un ataque de ARP poisoning.

Neighbor Discovery

IPv6 no utiliza ARP, utiliza el protocolo ND para resolver direcciones MAC. ND proporciona servicios de resolución de direcciones, detección de routers y redirección para IPv6 mediante ICMPv6. ICMPv6 ND utiliza cinco mensajes ICMPv6 para realizar estos servicios: solicitud de vecino, anuncio de vecino, solicitud de router, anuncio de router y redirección. Al igual que ARP para IPv4, los dispositivos IPv6 utilizan IPv6 ND para resolver la dirección MAC de un dispositivo en una dirección IPv6 conocida.

9.4.2

Prueba de módulo - Resolución de direcciones

1. Cuando se envía un paquete IP a un host en una red remota, ¿qué información proporciona ARP?

Tema 9.1.0 – Cuando un host envía un paquete IP a un destino en una red diferente, la trama Ethernet no se puede enviar directamente al host de destino porque no se puede acceder directamente al host en la misma red. La trama de Ethernet se debe enviar a otro dispositivo conocido como router o gateway predeterminado para reenviar el paquete IP. ARP se utiliza para descubrir la dirección MAC del router (o gateway predeterminado) y utilizarlo como dirección MAC de destino en el encabezado de trama.

- ( ) la dirección IP del host de destino
- ( ) La dirección IP del gateway predeterminado
- (•) la dirección MAC de la interfaz del router más cercana al host de envío
- ( ) la dirección MAC del puerto del switch que se conecta al host de envío

2. ¿Cómo utiliza el proceso ARP una dirección IP?

Tema 9.1.0 – El proceso ARP se utiliza para completar la asignación necesaria de direcciones IP y MAC que se almacenan en la tabla ARP que mantiene cada nodo en una LAN. Cuando el dispositivo de destino no está en la misma red que el dispositivo de origen, se detecta la dirección MAC del dispositivo de capa 3 de la red de origen y se agrega a la tabla ARP del nodo de origen.

- ( ) para determinar la dirección MAC del host de destino remoto
- (•) para determinar la dirección MAC de un dispositivo en la misma red
- ( ) para determinar la cantidad de tiempo que tarda un paquete al viajar de origen a destino
- ( ) para determinar el número de red basado en el número de bits en la dirección IP

3. La tabla ARP en un switch asigna qué dos tipos de direcciones juntos?

Tema 9.2.0 - La tabla ARP del switch mantiene una asignación de direcciones MAC de Capa 2 a direcciones IP de Capa 3. Estas asignaciones pueden ser aprendidas por el switch dinámicamente a través de ARP o estáticamente a través de la configuración manual.

- (●) Dirección de capa 3 a una dirección de capa 2
- ( ) Dirección de capa 3 a una dirección de capa 4
- ( ) Dirección de capa 4 a una dirección de capa 2
- ( ) Dirección de capa 2 a una dirección de capa 4

4. ¿Cuál es la función del protocolo ARP?

Tema 9.2.0 - Las dos funciones principales del protocolo ARP son resolver una dirección IPv4 en una dirección MAC y mantener una tabla ARP, que enumera los pares resueltos de dirección IPv4 y dirección MAC. Un dispositivo obtiene automáticamente una dirección IP a través de DHCP. Las funciones de DNS incluyen resolver (o asignar) un nombre de dominio con su dirección IP y mantener una tabla para los pares de nombres de dominio/IP.

- ( ) obtener una dirección IP automáticamente
- ( ) mapear un nombre de dominio a su dirección IP
- (●) resolver una dirección IPv4 a una dirección MAC
- ( ) mantener una tabla de nombres de dominio con sus direcciones IP resueltas

5. ¿Qué componente del router contiene la tabla de enrutamiento, la memoria caché ARP y el archivo de configuración en ejecución?

Tema 9.2.0 - La tabla de enrutamiento, la memoria caché ARP y el archivo de configuración en ejecución se almacenan en RAM volátil.

- (●) RAM
- ( ) Memoria flash
- ( ) NVRAM
- ( ) ROM

6. ¿Qué tipo de información se incluye en una tabla de ARP?

Tema 9.2.0 - Las tablas ARP se utilizan para almacenar asignaciones de direcciones IP a direcciones MAC. Cuando un dispositivo de red debe reenviar un paquete, el dispositivo solo conoce la dirección IP. Para enviar el paquete en una red Ethernet, se necesita una dirección MAC. ARP resuelve la dirección MAC y la almacena en una tabla de ARP.

- ( ) Puertos de switch asociados con las direcciones MAC de destino
- ( ) Asignaciones de nombres de dominio a direcciones IP
- ( ) Rutas para llegar a las redes de destino
- (●) Asignación de direcciones IP a direcciones MAC

7. Un PC está configurado para obtener automáticamente una dirección IP de la red 192.168.1.0/24. El administrador de red emite el **arp -a** comando y observa una entrada de 192.168.1.255 ff-ff-ff-ff-ff-ff. ¿Qué enunciado describe esta entrada?

Tema 9.2.0 - La dirección IP de 192.168.1.255 en la red 192.168.1.0/24 es la dirección de broadcast, que está asignada estáticamente a ff-ff-ff-ff-ff-ff en la tabla ARP.

- (●) Esta es una entrada de mapa estática.
- ( ) Esta es una entrada de mapa dinámica.
- ( ) Esta entrada se refiere a la propia PC.
- ( ) Esta entrada se asigna a la gateway predeterminado.

8. Un analista especializado en ciberseguridad considera que un atacante está falsificando la dirección MAC del gateway predeterminado para lanzar un ataque man-in-the-middle. ¿Qué comando debe usar el analista para ver la dirección MAC que usa un host para llegar al gateway predeterminado?

Tema 9.2.0 - ARP es un protocolo utilizado con IPv4 para asignar una dirección MAC a una dirección IP específica asociada. El comando**arp -a** mostrará la tabla de direcciones MAC en una PC con Windows.

- ( ) **ipconfig /all**
- ( ) **route print**
- ( ) **netstat -r**
- (●) **arp -a**

9. ¿Cuál es la función de ARP?

Tema 9.2.0 - Resolver direcciones IPv4 en direcciones MAC es una función de ARP. ARP también es responsable del mantenimiento de la tabla ARP.

- ( ) la resolución de direcciones MAC a direcciones IPv4
- ( ) la resolución de direcciones de puerto de direcciones MAC
- ( ) la resolución de direcciones MAC a direcciones de puerto
- (●) la resolución de direcciones IPv4 a direcciones MAC

10. ¿Cuál es el propósito de ARP en una red IPv4?

Tema 9.2.0 - ARP realiza dos funciones:
- Para obtener una dirección MAC específica cuando se conoce una dirección IP, mediante la broadcast de un mensaje de solicitud ARP a todos los dispositivos de una red Ethernet determinada
- Para utilizar la información recopilada para crear una tabla visible de direcciones IP a asignaciones de direcciones MAC

- ( ) para reenviar datos en función de la dirección IP de destino
- (●) para obtener una dirección MAC específica cuando se conoce una dirección IP
- ( ) para reenviar datos en función de la dirección MAC de destino.
- ( ) para construir la tabla de direcciones MAC en un switch a partir de la información recopilada

11. ¿Qué acción realiza un switch de Capa 2 cuando recibe un fotograma de broadcast de Capa 2?

Tema 9.2.0 - Cuando un switch de capa 2 recibe una trama con una dirección de destino de broadcast, inunda la trama en todos los puertos excepto en el puerto en el que recibió la trama.

- descarta la trama.
- (•) Envía la trama a todos los puertos excepto el puerto en el que recibió la trama.
- Envía la trama a todos los puertos registrados para reenviar transmisiones.
- Envía el trama a todos los puertos.

12. ¿Qué dirección de destino se utiliza en una trama de solicitud ARP?

Tema 9.2.0 - El propósito de una solicitud ARP es encontrar la dirección MAC del host de destino en una LAN Ethernet. El proceso ARP envía un broadcast de Capa 2 a todos los dispositivos de la LAN Ethernet. La trama contiene la dirección IP del destino y la dirección MAC de broadcast, FFFF.FF.FFFF.

- 0.0.0.0
- 255.255.255.255
- (•) FFFF.FFFF.FFFF
- 127.0.0.1
- 01-00-5E-00-AA-23

13. ¿Qué direcciones asigna ARP?

Tema 9.2.0 - ARP, o el Protocolo de resolución de direcciones, funciona asignando una dirección MAC de destino a una dirección IPv4 de destino. El host conoce la dirección IPv4 de destino y utiliza ARP para resolver la dirección MAC de destino correspondiente.

- (•) Una dirección MAC de destino a una dirección IPv4 de destino
- Una dirección IPv4 de destino a la dirección MAC de origen
- Una dirección IPv4 de destino al nombre de host de destino
- Una dirección MAC de destino a una dirección IPv4 de origen

14. ¿Qué hará un switch de capa 2 cuando la dirección MAC de destino de una trama recibida no está en la tabla MAC?

Tema 9.2.0 - Un switch de capa 2 determina cómo manejar tramas entrantes mediante su tabla de direcciones MAC. Cuando una trama entrante contiene una dirección MAC de destino que no está en la tabla, el switch reenvía la trama a todos los puertos, excepto el puerto en el que se recibió.

- Inicia una solicitud ARP.
- Emite el fotograma fuera de todos los puertos del switch.
- Notifica al host de envío que la trama no se puede entregar.
- (•) Reenvía la trama de todos los puertos excepto el puerto en el que se recibió la trama.

15. ¿Qué dos mensajes ICMPv6 se utilizan durante el proceso de resolución de direcciones MAC Ethernet? (Escoja dos.)

Tema 9.3.0 - IPv6 utiliza mensajes ICMPv6 de solicitud de vecino (NS) y anuncio de vecino (NA) para la resolución de direcciones MAC.

- [ ] solicitud de router
- [ ] anuncio de router
- [x] solicitud de vecino (NS)
- [x] Anuncio de vecino (NA)
- [ ] Solicitud echo

Correct

You have successfully identified the correct answers.

You got 14 out of 14 questions correct.

1. Which router component holds the routing table, ARP cache, and running configuration file?

Topic 9.2.0 - The routing table, ARP cache, and running configuration file are stored in volatile RAM.

- (•) RAM
- ( ) Flash
- ( ) NVRAM
- ( ) ROM

2. What type of information is contained in an ARP table?

Topic 9.2.0 - ARP tables are used to store mappings of IPv4 addresses to MAC addresses. When a network device needs to forward a packet, the device knows only the IPv4 address. To deliver the packet on an Ethernet network, a MAC address is needed. ARP resolves the MAC address and stores it in an ARP table.

- ( ) switch ports associated with destination MAC addresses
- ( ) domain name to IPv4 address mappings
- ( ) routes to reach destination networks
- (•) IPv4 address to MAC address mappings

3. A PC is configured to obtain an IPv4 address automatically from network 192.168.1.0/24. The network administrator issues the **arp -a** command and notices an entry of 192.168.1.255 ff-ff-ff-ff-ff-ff. Which statement describes this entry?

Topic 9.2.0 - The IPv4 address of 192.168.1.255 on the 192.168.1.0/24 network is the broadcast address, which is statically mapped to ff-ff-ff-ff-ff-ff in the ARP table.

- (●) This is a static map entry.
- ( ) This is a dynamic map entry.
- ( ) This entry refers to the PC itself.
- ( ) This entry maps to the default gateway.

4. A cybersecurity analyst believes an attacker is spoofing the MAC address of the default gateway to perform a man-in-the-middle attack. Which command should the analyst use to view the MAC address a host is using to reach the default gateway?

Topic 9.2.0 - ARP is a protocol used with IPv4 to map a MAC address to an associated specific IP address. The command **arp -a** will display the MAC address table on a Windows PC.

- ( ) **ipconfig /all**
- ( ) **route print**
- ( ) **netstat -r**
- (●) **arp -a**

5. What will a Layer 2 switch do when the destination MAC address of a received frame is not in the MAC table?

Topic 9.2.0 - A Layer 2 switch determines how to handle incoming frames by using its MAC address table. When an incoming frame contains a destination MAC address that is not in the table, the switch forwards the frame out all ports, except for the port on which it was received.

- ( ) It initiates an ARP request.
- ( ) It broadcasts the frame out of all ports on the switch.
- ( ) It notifies the sending host that the frame cannot be delivered.
- (●) It forwards the frame out of all ports except for the port at which the frame was received.

6. Which two ICMPv6 messages are used during the Ethernet MAC address resolution process? (Choose two.)

Topic 9.3.0 - IPv6 uses neighbor solicitation (NS) and neighbor advertisement (NA) ICMPv6 messages for MAC address resolution.

- [ ] router solicitation
- [ ] router advertisement
- [x] neighbor solicitation
- [x] neighbor advertisement
- [ ] echo request

7. How does the ARP process use an IPv4 address?

Topic 9.1.0 - The ARP process is used to complete the necessary mapping of IPv4 and MAC addresses that are stored in the ARP table that is maintained by each node on a LAN. When the destination device is not on the same network as the source device, the MAC address of the Layer 3 device on the the source network is discovered and added to the ARP table of the source node.

- ( ) to determine the MAC address of the remote destination host
- (•) to determine the MAC address of a device on the same network
- ( ) to determine the amount of time a packet takes when traveling from source to destination
- ( ) to determine the network number based on the number of bits in the IPv4 address

8. What is one function of the ARP protocol?

Topic 9.2.0 - The two main functions of the ARP protocol are to resolve an IPv4 address to a MAC address and to maintain an ARP table, which lists the resolved pairs of IPv4 address and MAC address. A device automatically obtains an IP address through DHCP. The functions of DNS include resolving (or mapping) a domain name with its IP address and maintaining a table for the domain name/IP pairs.

- ( ) obtaining an IPv4 address automatically
- ( ) mapping a domain name to its IP address
- (•) resolving an IPv4 address to a MAC address
- ( ) maintaining a table of domain names with their resolved IP addresses

9. Which action is taken by a Layer 2 switch when it receives a Layer 2 broadcast frame?

Topic 9.2.0 - When a Layer 2 switch receives a frame with a broadcast destination address, it floods the frame to all ports except the port on which it received the frame.

- It drops the frame.
- (•) It sends the frame to all ports except the port on which it received the frame.
- It sends the frame to all ports that are registered to forward broadcasts.
- It sends the frame to all ports.

10. What addresses are mapped by ARP?

Topic 9.2.0 - ARP, or the Address Resolution Protocol, works by mapping the IPv4 address to a destination MAC address. The host knows the destination IPv4 address and uses ARP to resolve the corresponding destination MAC address.

- (•) IPv4 address to a destination MAC address
- destination IPv4 address to the source MAC address
- destination IPv4 address to the destination host name
- destination MAC address to the source IPv4 address

11. When an IPv4 packet is sent to a host on a remote network, what information is provided by ARP?

Topic 9.1.0 - When a host sends an IPv4 packet to a destination on a different network, the Ethernet frame cannot be sent directly to the destination host because the host is not directly reachable in the same network. The Ethernet frame must be sent to another device known as the router or default gateway in order to forward the IPv4 packet. ARP is used to discover the MAC address of the router (or default gateway) and use it as the destination MAC address in the frame header.

- the IPv4 address of the destination host
- the IPv4 address of the default gateway
- (•) the MAC address of the router interface closest to the sending host
- the MAC address of the switch port that connects to the sending host

12. The ARP table in a switch maps which two types of address together?

Topic 9.2.0 - The switch ARP table keeps a mapping of Layer 2 MAC addresses to Layer 3 IP addresses. These mappings can be learned by the switch dynamically through ARP or statically through manual configuration.

- (●) Layer 3 address to a Layer 2 address
- ( ) Layer 3 address to a Layer 4 address
- ( ) Layer 4 address to a Layer 2 address
- ( ) Layer 2 address to a Layer 4 address

13. What is the purpose of ARP in an IPv4 network?

Topic 9.2.0 - ARP performs two functions:
- To obtain a specific MAC address when an IP address is known, by broadcasting an ARP request message to all devices on a particular Ethernet network
- To use the gathered information to create a viewable table of IP address to MAC address mappings

- ( ) to forward data onward based on the destination IP address
- (●) to obtain a specific MAC address when an IP address is known
- ( ) to forward data onward based on the destination MAC address.
- ( ) to build the MAC address table in a switch from the information that is gathered

14. Which destination address is used in an ARP request frame?

Topic 9.2.0 - The purpose of an ARP request is to find the MAC address of the destination host on an Ethernet LAN. The ARP process sends a Layer 2 broadcast to all devices on the Ethernet LAN. The frame contains the IP address of the destination and the broadcast MAC address, FFFF.FFFF.FFFF.

- ( ) 0.0.0.0
- ( ) 255.255.255.255
- (●) FFFF.FFFF.FFFF
- ( ) 127.0.0.1
- ( ) 01-00-5E-00-AA-23

Capítulo 10_Configuración básica de un router

Introducción

10.0.1

¿Por qué debería tomar este módulo?

Bienvenido a la Configuración básica de un router!

¿Alguna vez has hecho un relevo? La primera persona corre la primera etapa de la carrera y entrega la batuta al siguiente corredor, que continúa hacia adelante en la segunda etapa de la carrera y entrega la batuta al tercer corredor, y sigue adelante. El enrutamiento de paquetes es muy similar a un relé. Pero si el primer corredor no sabe dónde encontrar al segundo corredor, o deja caer la batuta en la primera etapa, entonces ese equipo de relevos seguramente perderá la carrera.

El enrutamiento de paquetes es muy similar a un relé. Como sabe, los enrutadores crean y utilizan tablas de enrutamiento para reenviar paquetes desde sus redes locales a otras redes. Pero un router no puede crear una tabla de enrutamiento ni reenviar ningún paquete hasta que se haya configurado. Si planea convertirse en administrador de red, definitivamente debe saber cómo hacerlo. ¿Las buenas noticias? ¡Es fácil! Este módulo tiene actividades de Comprobador de sintaxis para que pueda practicar los comandos de configuración y ver el resultado. También hay algunas actividades de Packet Tracer para comenzar. ¡Adelante!

10.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Configuración básica de un router

Objetivos del módulo: Implemente la configuración inicial en un router y terminales.

Título del tema	Objetivo del tema
Configuración de los parámetros iniciales del router	Configure los parámetros iniciales en un router con IOS de Cisco.
Configuración de interfaces	Configure dos interfaces activas en un router con Cisco IOS.
Configuración del gateway predeterminado	Configure dispositivos para utilizar el gateway predeterminado.

Configuración de los parámetros iniciales del router

10.1.1

Pasos básicos en la configuración de un router

Las siguientes tareas deben completarse al configurar la configuración inicial en un enrutador.

1. Configure the device name.

```
Router(config)# hostname hostname
```

2. Secure privileged EXEC mode.

```
Router(config)# enable secret password
```

3. Secure user EXEC mode.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

4. Secure remote Telnet / SSH access.

```
Router(config-line)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

5. Secure all passwords in the config file.

```
Router(config-line)# exit
Router(config)# service password-encryption
```

6. Provide legal notification.

```
Router(config)# banner motd delimiter message delimiter
```

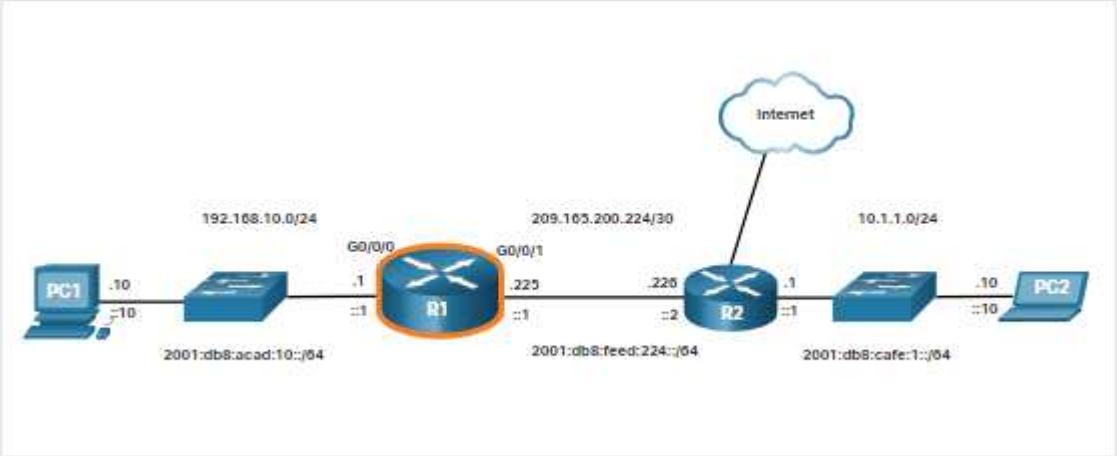
7. Save the configuration.

```
Router(config)# end
Router# copy running-config startup-config
```

10.1.2

Configuración básica de un router

En este ejemplo, el router R1 del diagrama de topología se configurará con la configuración inicial.



Para configurar el nombre del dispositivo para R1, utilice los siguientes comandos:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Nota: Observe cómo el indicador del enrutador muestra ahora el nombre de host del enrutador.

Todo el acceso al router debe estar asegurado. El modo EXEC privilegiado proporciona al usuario acceso completo al dispositivo y su configuración. Por lo tanto, es el modo más importante para asegurar.

Los siguientes comandos aseguran el modo EXEC privilegiado y el modo EXEC de usuario, habilitan el acceso remoto Telnet y SSH y cifran todas las contraseñas de texto sin formato (es decir, EXEC de usuario y línea VTY).

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# Inicio de sesión
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# Inicio de sesión
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# cifrado de contraseña de servicio
R1(config)#
```

La notificación legal advierte a los usuarios que solo deben acceder al dispositivo los usuarios permitidos. La notificación legal se configura de la siguiente manera.

```
R1(config)# banner motd #
Escriba un mensaje de texto. Termina con una nueva línea y el #
**********************************************  WARNING: Unauthorized access is prohibited!
********************************************** #
R1(config)#
```

Si se configuraron los comandos anteriores y el router perdió energía accidentalmente, se perderían todos los comandos configurados. Por esta razón, es importante guardar la configuración cuando se implementen los cambios. Los siguientes comandos guardan la configuración en ejecución en la NVRAM.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

10.1.3

Comprobador de sintaxis - Configurar los ajustes iniciales del enrutador

Utilice este comprobador de sintaxis para practicar la configuración inicial en un router.

- Configure el nombre del dispositivo.
- Proteger el modo EXEC con privilegios
- Proteger el acceso remoto por Telnet y SSH
- Cifre todas las contraseñas de texto.
- Proporcione una notificación legal.

Enter global configuration mode to configure the name of the router as “R1”.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
```

Configure 'class' as the secret password.

```
R1(config)#enable secret class
```

Configure 'cisco' as the console line password, require users to login, and return to global configuration mode.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

For vty line 0 through 4, configure 'cisco' as the password, require users to login, enable SSH and Telnet access, and return to global configuration mode.

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config-line)#transport input ssh telnet
R1(config-line)#exit
```

Encrypt all clear text passwords.

```
R1(config)#service password-encryption
```

Enter the banner 'Authorized Access Only!' and use # as the delimiting character.

```
R1(config)#banner motd #Authorized Access Only!#
```

Exit global configuration mode.

```
R1(config)#exit
R1#
```

You have successfully configured the initial settings on router R1.

10.1.4

Packet Tracer: Configuración inicial del router

En esta actividad, configurará los parámetros básicos del router. Protegerá el acceso seguro a la CLI y al puerto de consola con contraseñas cifradas y de texto no cifrado. También configurará los mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten a los usuarios no autorizados que el acceso está prohibido. Por último, verificará y guardará la configuración en ejecución.

Configuración inicial del router

Configuración inicial del router

Configuración básica de un router / Configuración de interfaces

Configuración de interfaces

10.2.1

Configurar interfaces de routers

En este punto, los routers tienen sus configuraciones básicas. El siguiente paso es configurar sus interfaces. Esto se debe a que los dispositivos finales no pueden acceder a los enrutadores hasta que se configuran las interfaces. Existen muchos tipos diferentes de interfaces para los routers Cisco. Por ejemplo, el router Cisco ISR 4321 está equipado con dos interfaces Gigabit Ethernet:

- **GigabitEthernet 0/0/0 (G0/0/0)**
- **GigabitEthernet 0/0/1 (G0/0/1)**

La tarea de configurar una interfaz de enrutador es muy similar a un SVI de administración en un conmutador. Específicamente, incluye la emisión de los siguientes comandos:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

Nota: Cuando se habilita una interfaz de enrutador, se deben mostrar mensajes de información confirmando el vínculo habilitado.

Aunque el comando **description** no es necesario para habilitar una interfaz, es una buena práctica usarlo. Puede ser útil para solucionar problemas en redes de producción proporcionando información sobre el tipo de red conectada. Si la interfaz se conecta a un ISP o a un proveedor de servicios de telefonía móvil, **description** resulta útil introducir la información de contacto y de conexión de dichos terceros.

Nota: El texto de la descripción tiene un límite de 240 caracteres.

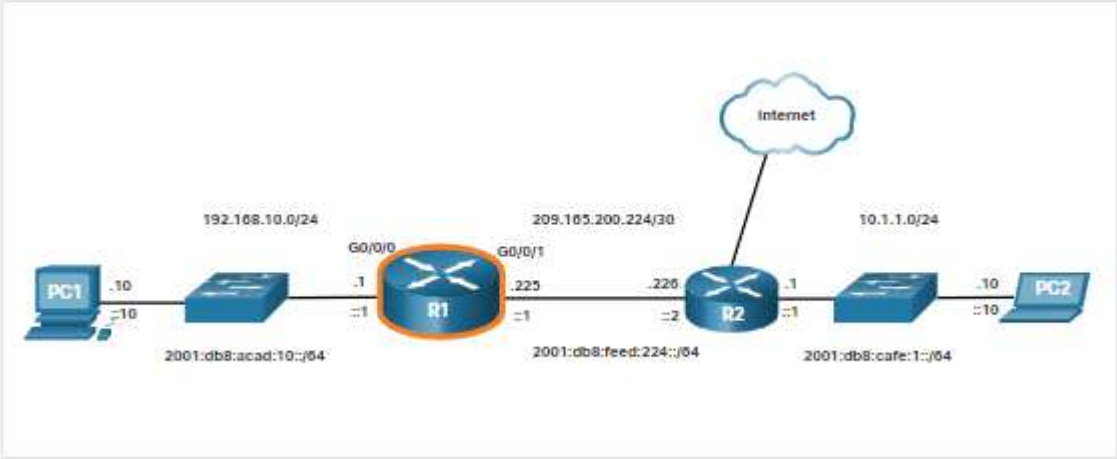
Al usar el comando **no shutdown** se activa la interfaz y es similar a darle energía. La interfaz también debe estar conectada a otro dispositivo, como un switch o un router, para que la capa física se active.

Nota: En las conexiones entre enrutadores donde no hay un conmutador Ethernet, ambas interfaces de interconexión deben estar configuradas y habilitadas.

10.2.2

Ejemplo de Configuración de interfaces de routers

En este ejemplo, se habilitarán las interfaces directamente conectadas de R1 en el diagrama de topología.



El diagrama es una topología de red que muestra el direccionamiento IPv4 e IPv6 de los dispositivos de red. Lo que sigue es una descripción de la topología de izquierda a derecha. PC1 está conectado a un switch conectado al router R1. La dirección IPv4 de red es 192.168.10.0/24 y la dirección IPv6 es 2001:db8:acad:10: :/64. PC1 tiene una dirección de.10 y: :10. Interface G0/0/0 on R1 has an address of .1 and ::1. La interfaz R1 G0/0/1 se conecta

entonces al router R2 en la red IPv4 209.165.200.224/30 y la red IPv6 2001:db8:feed:224: :/64. La interfaz G0/0/1 en R1 tiene una dirección de .225 y: :1. La interfaz en R2 tiene una dirección de.226 y: :2. R2 se conecta a un switch que está conectado a PC2 en la red IPv4 10.1.1.0/24 y la red IPv6 2001:db8:cafe:1: :/64. La interfaz R2 tiene una dirección de .1 y: :1. PC2 tiene una dirección de.10 y: :10. R2 también tiene una conexión a la nube de Internet.

Para configurar las interfaces en R1, utilice los siguientes comandos:

```
R1> enable
R1# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
direcciónR1(config-if)# ipv6 2001:db8:acad:10: :1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug 1 01:43:53 .435: %LINK-3-UPDOWN: Interfaz GigabiteThernet0/0/0, estado cambiado a inactivo
*Aug 1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug 1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state
to up
R1(config)#
R1(config)#
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
direcciónR1(config-if)# ipv6 2001:db8:feed:224: :1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug 1 01:46:29 .170: %LINK-3-UPDOWN: Interfaz GigabiteThernet0/0/1, estado cambiado a inactivo
*Aug 1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, estado cambiado a inactivo
*Aug 1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state
to up
R1(config)#
```

Nota: Observe los mensajes informativos que nos informan de que G0/0/0 y G0/0/1 están activados.

10.2.3

Verificación de configuración de interfaz

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. El más útil de estos es el comando **show ip interface brief** y **show ipv6 interface brief**, como se muestra en el ejemplo.

```
R1#  show ip interface brief
¿Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
GigabiteThernet0/0/1 209.165.200.225 SÍ manual arriba
Vlan1 unassigned YES unset administratively down down
R1#  show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80: :201:C9FF:FE 89:4501
    2001:DB8:ACAD:10: :1
GigabitEthernet0/0/1 [up/up]
    FE80: :201:C9FF:FE 89:4502
    2001:DB8:ALIMENTACIÓN:224: :1
Vlan1 [administratively down/down]
    no asignado
R1#
```

10.2.4

Configuración comandos de Verificación

En la tabla se resumen los comandos **show** más populares utilizados para verificar la configuración de la interfaz.

Comandos	Descripción
show ip interface brief **show ipv6 interface brief**	El resultado muestra todas las interfaces, sus direcciones IP y su estado actual. Las interfaces configuradas y conectadas deben mostrar un Estado de «arriba» y Protocolo de «arriba». Cualquier otra cosa indica que existe un problema con la configuración o con el cableado.
show ip route **show ipv6 route**	Muestra el contenido de la tabla de routing IP que se almacena en la RAM.
show interfaces	Muestra estadísticas de todas las interfaces del dispositivo. Sin embargo, este solo mostrará la información de direccionamiento IPv4.
show ip interfaces	Muestra las estadísticas de IPv4 correspondientes a todas las interfaces de un router.
show ipv6 interface	Muestra las estadísticas de IPv6 correspondientes a todas las interfaces de un router.

Haga clic en cada botón para ver la salida del comando para cada comando de verificación de configuración.

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show ip interface brief
¿Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
GigabiteThernet0/0/1 209.165.200.225 SÍ manual arriba
Vlan1 unassigned YES unset administratively down down
R1#
```

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80: :201:C9FF:FE 89:4501
    2001:DB8:ACAD:10: :1
GigabitEthernet0/0/1 [up/up]
    FE80: :201:C9FF:FE 89:4502
    2001:DB8:ALIMENTACIÓN:224: :1
Vlan1 [administratively down/down]
    no asignado
R1#
```

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 está directamente conectado, GigabitEthernet0/0/0
L 192.168.10.1/32está directamente conectado, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 está directamente conectado, GigabitEthernet0/0/1
L 209.165.200.225/32 está directamente conectado GigabitEthernet0/0/1
R1#
```

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, a - Aplicación
C 2001:DB8:ACAD:10: :/64 [0/0]
     a través de GigabiteThernet0/0/0, conectado directamente
L 2001:DB8:ACAD:10: :1/128 [0/0]
     a través de GigabiteThernet0/0/0, recibir
C 2001:DB8:FEED:224: :/64 [0/0]
     a través de GigabiteThernet0/0/1, conectado directamente
L 2001:DB8:ALIMENTACIÓN:224: :1/128 [0/0]
     a través de GigabiteThernet0/0/1, reciba
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  El hardware es ISR4321-2x1GE, la dirección es a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1096 multicast, 0 pause input
     65 packets output, 22292 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     11 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R1#
```

show ip interface brief | show ipv6 interface brief | show ip route | show ipv6 route | show interfaces | show ip interface | show ipv6 interface

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  Vector turbo IP nulo
  Topologías de enrutamiento de unidifusión asociadas:
        Topología «base», estado de operación es UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Las respuestas de nombre de proxy de sondeo están deshabilitadas
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Características de entrada: MCI Check
  IPv4 WCCP Redirect outbound is disabled
  IPv4 WCCP Redirect inbound is disabled
  IPv4 WCCP Redirect exclude is disabled
R1#
```

```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10: :1, la subred es 2001:DB8:ACAD:10: :/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02: :1:FF 44:49 B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
R1#
```

10.2.5

Comprobador de sintaxis - Configurar interfaces.

Utilice este comprobador de sintaxis para practicar la configuración de la interfaz Gigabitethemet 0/0 en un router.

- Describa el enlace como 'Enlace a LAN'.
- Configure la dirección IPv4 192.168.10.1 con la máscara de subred 255.255.255.0.
- Configure the IPv6 address as 2001:db8:acad:10: :1 con la longitud del prefijo /64.
- Active la interfaz.

Enter global configuration mode.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
```

Configure interface gigabitethernet 0/0/0.

```
R1(config)#interface gigabitethernet 0/0/0
```

Describe the link as “Link to LAN”.

```
R1(config-if)#description Link to LAN
```

Configure the interface with IPv4 address **192.168.10.1** and subnet mask **255.255.255.0**.

```
R1(config-if)#ip address 192.168.1.1 255.255.255.0
You must enter the exact and full command.
R1(config-if)#ip address 192.168.10.1 255.255.255.255
You must enter the exact and full command.
R1(config-if)#ip address 192.168.10.1 255.255.255.0
```

Configure the interface with IPv6 address **2001:db8:acad:10::1** and the prefix length **/64**.

```
R1(config-if)#ipv6 address 2001:db8:acad:10::1/64
```

Enable the interface and return to global configuration mode.

```
R1(config-if)#no shutdown
\*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to down
\*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to up
\*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
R1(config-if)#exit
R1#
```

You have successfully configured the initial settings on router R1.

Configuración del gateway predeterminado

10.3.1

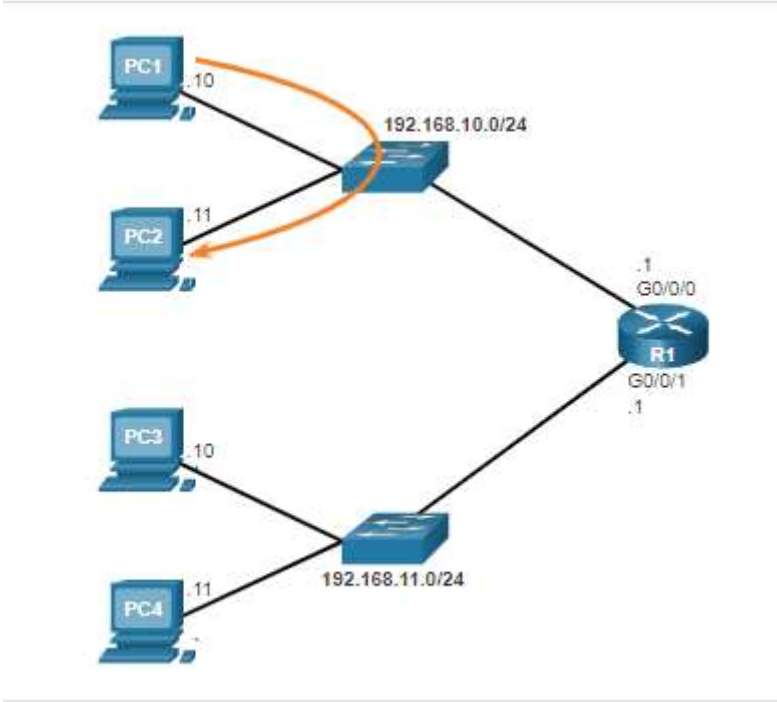
Gateway predeterminado para un host

Si su red local sólo tiene un enrutador, será el enrutador de puerta de enlace y todos los hosts y conmutadores de su red deben estar configurados con esta información. Si la red local tiene varios enrutadores, debe seleccionar uno de ellos para que sea el enrutador de puerta de enlace predeterminado. En este tema se explica cómo configurar la puerta de enlace predeterminada en hosts y conmutadores.

Para que un terminal se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de gateway predeterminado. El gateway predeterminado se usa solamente cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de gateway predeterminado es la dirección de la interfaz de router conectada a la red local del host. La dirección IP del dispositivo host y la dirección de interfaz de router deben estar en la misma red.

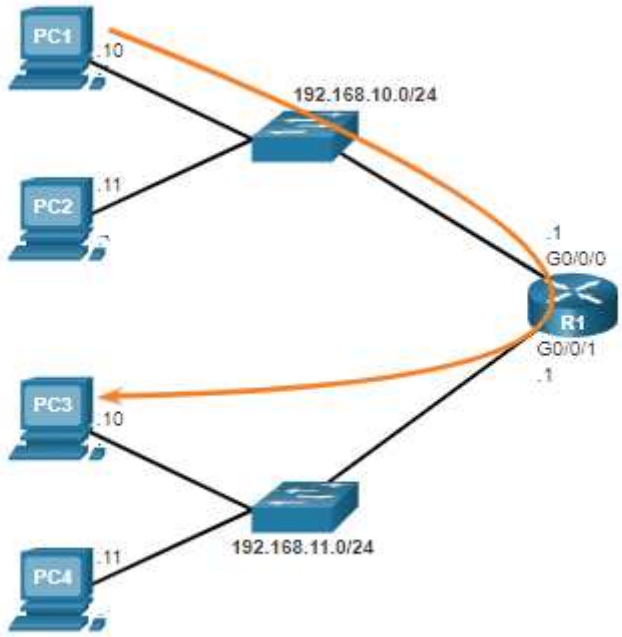
Por ejemplo, supongamos que una topología de red IPv4 consiste en un enrutador que interconecta dos LAN independientes. G0/0 está conecta a la red 192.168.10.0, mientras que G0/1 está conectada a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de gateway predeterminado apropiada.

En este ejemplo, si PC1 envía un paquete a PC2, no se utiliza la puerta de enlace predeterminada. En cambio, PC1 dirige el paquete con la dirección IPv4 de PC2 y lo reenvía directamente a PC2 a través del switch.



El diagrama es una topología de red con un enrutador, dos conmutadores y cuatro PC que muestran el flujo de información entre dispositivos de la misma red. PC1 y PC2 están conectados al switch en la red 192.168.10.0/24 en la interfaz G0/0/0 en el router R1. PC3 y PC4 están conectados a otro conmutador en la red 192.168.11.0/24 en la interfaz G0/0/1 en R1. Una flecha muestra el flujo de información enviada desde PC1 pasando a través del conmutador conectado en su camino a PC2.

¿Qué pasa si PC1 envió un paquete a PC3? PC1 dirigiría el paquete con la dirección IPv4 de PC3, pero reenviaría el paquete a su puerta de enlace predeterminada, que es la interfaz G0/0/0 de R1. El router acepta el paquete, accede a su tabla de routing para determinar la interfaz de salida apropiada según la dirección de destino. R1 reenvía el paquete fuera de la interfaz apropiada para llegar a PC3.



El diagrama es una topología de red con un enrutador, dos conmutadores y cuatro PC que muestran el flujo de información entre dispositivos en diferentes redes. PC1 y PC2 están conectados al switch en la red 192.168.10.0/24 en la interfaz G0/0/0 en el router R1. PC3 y PC4 están conectados a otro conmutador en la red 192.168.11.0/24 en la interfaz G0/0/1 en R1. Una flecha muestra el flujo de información enviada desde PC1 pasando por R1 y hacia PC3.

El mismo proceso ocurriría en una red IPv6, aunque esto no se muestra en la topología. Los dispositivos usarían la dirección IPv6 del enrutador local como puerta de enlace predeterminada.

10.3.2

Gateway predeterminado para un switch

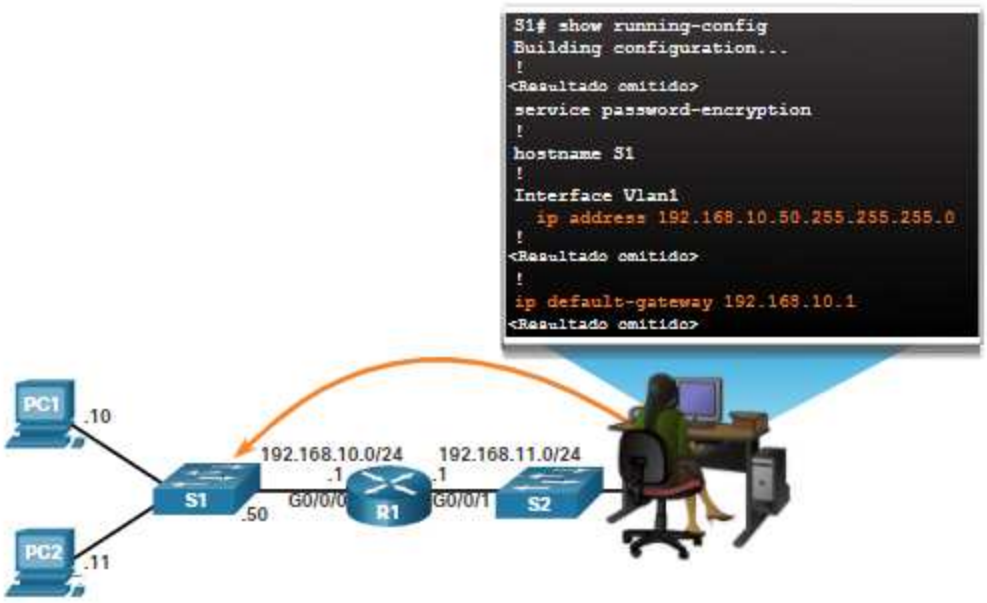
Por lo general, un switch de grupo de trabajo que interconecta equipos cliente es un dispositivo de capa 2. Como tal, un switch de capa 2 no necesita una dirección IP para funcionar adecuadamente. Sin embargo, se puede configurar una configuración IP en un conmutador para dar a un administrador acceso remoto al conmutador.

Para conectarse y administrar un switch a través de una red IP local, debe tener configurada una interfaz virtual de switch (SVI). El SVI se configura con una dirección IPv4 y una máscara de subred en la LAN local. El conmutador también debe tener una dirección de puerta de enlace predeterminada configurada para administrar el conmutador de forma remota desde otra red.

Por lo general, la dirección del gateway predeterminado se configura en todos los dispositivos que desean comunicarse más allá de la red local.

Para configurar un gateway predeterminado en un switch, use el comando de configuración global **ip default-gateway** ip default-gateway. La dirección IP que se configura es la dirección IPv4 de la interfaz del enrutador local conectada al switch.

En la Figura 1 se muestra un administrador que establece una conexión remota al switch S1 en otra red.



El diagrama es una topología de red que muestra un router R1 conectado a dos switches, S1 en la red 192.168.10.0/24 y S2 en la red 192.168.11.0/24. Un usuario está conectado a S2 y una flecha muestra que el usuario está accediendo a S1 de forma remota. Encima del usuario hay un cuadro que muestra que el usuario tiene acceso CLI a S1 y está mostrando la configuración en ejecución.

En este ejemplo, el host administrador usaría su puerta de enlace predeterminada para enviar el paquete a la interfaz G0/0/1 de R1. R1 reenviaría el paquete a S1 desde su interfaz G0/0/0. Dado que la dirección IPv4 de origen del paquete provenía de otra red, S1 requeriría una puerta de enlace predeterminada para reenviar el paquete a la interfaz G0/0/0 de R1. Por lo tanto, el switch S1 se debe configurar con un gateway predeterminado, para que pueda responder y establecer una conexión SSH con el host administrativo.

Nota: Los paquetes que se originan en servidores conectados al switch ya deben crearse con la dirección de gateway predeterminado configurada en el sistema operativo de su servidor.

Un conmutador de grupo de trabajo también se puede configurar con una dirección IPv6 en un SVI. Sin embargo, el conmutador no requiere que la dirección IPv6 de la puerta de enlace predeterminada se configure manualmente. El conmutador recibirá automáticamente su puerta de enlace predeterminada del mensaje ICMPv6 Router Advertisement del router.

10.3.3

Comprobador de sintaxis - Configurar la puerta de enlace predeterminada

Utilice el verificador de sintaxis de la figura 2 para practicar la configuración de un gateway predeterminado en un switch.

Enter global configuration mode.

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Configure 192.168.10.1 as the default gateway for S1.

```
S1(config)#ip default-gateway 192.168.10.1
S1(config)#
You have successfully set the default gateway on switch S1.
```

10.3.4

Packet Tracer: Conexión de un router a una LAN

En esta actividad, utilizará diversos comandos **show** para visualizar el estado actual del router. A continuación, utilizará la tabla de direccionamiento para configurar las interfaces Ethernet del router. Por último, utilizará comandos para verificar y probar las configuraciones.

Conexión de un router a una LAN

Conexión de un router a una LAN

10.3.5

Packet Tracer: Solución de problemas del gateway predeterminado

Para que un dispositivo se comunique en varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se usa

cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de gateway predeterminado es la dirección de la interfaz de router conectada a la red local a la que se conecta el host. En esta actividad, terminará de registrar la red. Luego, verificará el registro de la red mediante la prueba de la conectividad completa y la solución de problemas. Los métodos de solución de problemas que usted usará constan de los siguientes pasos:

1. Verificar el registro de la red y usar pruebas para aislar problemas.
2. Determinar una solución apropiada para un problema determinado.
3. Implementar la solución.
4. Realizar pruebas para verificar que se haya solucionado el problema.
5. Registrar la solución

Solución de problemas del gateway predeterminado
Solución de problemas del gateway predeterminado

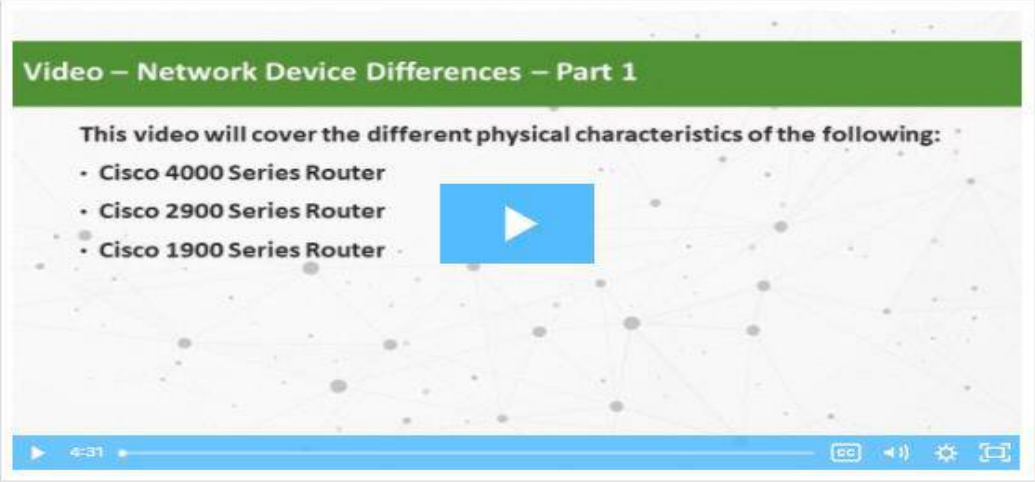
Configuración básica de un router / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

10.4.1

Video - Diferencias de dispositivos de red: Parte 1

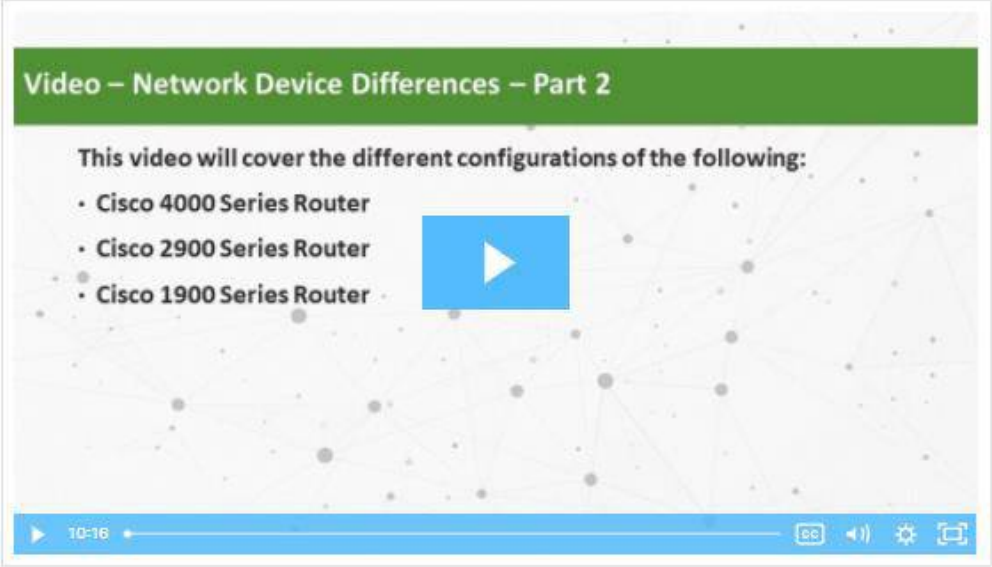
Haga clic en Reproducir en la figura para ver la Parte 1 de un vídeo que explica los diferentes dispositivos de router y switch que puede experimentar durante las prácticas de Packet Tracer y Lab.



10.4.2

Video - Diferencias de dispositivos de red: Parte 2

Haga clic en Reproducir en la figura para ver la Parte 2 de un vídeo que explica los diferentes dispositivos de router y switch que puede experimentar durante las prácticas de Packet Tracer y Lab.



10.4.3

Packet Tracer - Configuración básica del dispositivo

La administradora de red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración de parámetros básicos de un router y un switch con Cisco IOS. Luego, probará la conectividad completa para verificar la configuración realizada por usted, así como la configuración de los dispositivos existentes.

Configuración básica del dispositivo

Configuración básica del dispositivo

10.4.4

Laboratorio: Armar una red con un switch y un router

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Establecer la topología e inicializar los dispositivos
- Parte 2: Configurar los dispositivos y verificar la conectividad
- Parte 3: Mostrar información del dispositivo

Armar una red con un switch y un router

10.4.5

¿Qué aprendí en este módulo?

Configurar propiedades iniciales del router

Las siguientes tareas deben completarse al configurar la configuración inicial en un enrutador.

1. Configure el nombre del dispositivo.
2. Proteja el modo EXEC con privilegios.
3. Proteger el modo EXEC de usuario
4. Proteger el acceso remoto por Telnet y SSH
5. Proteja todas las contraseñas del archivo de configuración.
6. Proporcione una notificación legal.
7. Guarde la configuración.

Configurar interfaces

Para que se pueda llegar a los routers, se debe configurar la interfaz de router. El router Cisco ISR 4321 está equipado con dos interfaces Gigabit Ethernet: GigabitEthernet 0/0/0 (G0 / 0/0) y GigabitEthernet 0/0/1 (G0 / 0/1). Las tareas para configurar una interfaz de router son muy similares a un SVI de administración en un switch. Mediante el comando **no shutdown** se activa la interfaz. La interfaz también debe estar conectada a otro dispositivo, como un switch o un router, para que la capa física se active. Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. ***show ip interface brief***, ***show ipv6 interface brief***, ***show ip route,*** *y* ***show ipv6 route***, ***show interfaces***, ***show ip interface*** *y* ***show ipv6 interface.***

Configurar el Gateway Predeterminado

Para que un terminal se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de gateway predeterminado. En general, la dirección de gateway predeterminado es la dirección de la interfaz de router conectada a la red local del host. La dirección IP del dispositivo host y la dirección de interfaz de router deben estar en la misma red. Para conectarse y administrar un switch a través de una red IP local, debe tener configurada una interfaz virtual de switch (SVI). El SVI se configura con una dirección IPv4 y una máscara de subred en la LAN local. El switch también debe tener una dirección de puerta de enlace predeterminada configurada para administrar el switch de forma remota desde otra red. Para configurar un gateway predeterminado en un switch, use el comando **ip default-gateway ip-address** de configuración global Use la dirección IPv4 de la interfaz del enrutador local que está conectada al conmutador.

10.4.6

Prueba del módulo: configuración básica de un router.

Correcto

Identificó bien las respuestas correctas.

Has tenido 13 respuestas correctas de 13.

1. Un enrutador arranca e ingresa al modo de configuración. ¿Por qué razón?

Tema 10.1.0 - Si un router no puede localizar el archivo startup-config en NVRAM, entrará en modo de configuración para permitir que la configuración se introduzca desde el dispositivo de consola.

- La imagen del IOS está dañada.
- Cisco IOS no está en la memoria flash.
- (•) Falta el archivo de configuración en NVRAM.
- El proceso POST ha detectado un error de hardware.

2. ¿Qué comando se puede utilizar para cifrar todas las contraseñas presentes en el archivo de configuración?

Tema 10.1.0 - El comando **service password-encryption** se utiliza para cifrar y proteger las contraseñas de texto sin formato configuradas en un router.

- Router_A (config) # **enable secret** <password>
- (•) Router_A (configuración) # **service password-encryption**
- Router_A (config) # **enable password** *<password>*
- Router_A (configuración) # **encrypt password**

3. La política de la empresa requiere el uso del método más seguro para salvaguardar el acceso al modo ejecutivo y configuración privilegiado en los routers. La contraseña ejecutiva privilegiada es *trustknow1*. ¿Cuál de los siguientes comandos del router logra el objetivo de proporcionar el más alto nivel de seguridad?

3. La política de la empresa requiere el uso del método más seguro para salvaguardar el acceso al modo ejecutivo y configuración privilegiado en los routers. La contraseña ejecutiva privilegiada es *trustknow1*. ¿Cuál de los siguientes comandos del router logra el objetivo de proporcionar el más alto nivel de seguridad?

Tema 10.1.0 - El comando **service password-encryption** se utiliza para cifrar y proteger las contraseñas de texto sin formato configuradas en un router

- contraseña**secreta trustknow1**
- **habilitar contraseña trustknow1**
- **cifrado de contraseña de servicio**
- **habilitar confianza secretaconocimiento1**

4. ¿Cuál será la respuesta del enrutador después de ingresar el comando**router(config)# hostname portsmouth**""?

Tema 10.1.0 - El comando **hostname portsmouth** se utiliza para cambiar el nombre del router actual a portsmouth.

- Portsmouth#
- portsmouth (configuración)#
- entrada no válida detectada
- router (config-host)#
- hostname = portsmouth
  Portsmouth#
- ? comando no reconocido
  router(config)#

5. Un administrador está configurando un nuevo router para permitir el acceso a la administración fuera de banda. ¿Qué conjunto de comandos permitirá el inicio de sesión requerido usando una contraseña de **cisco**?

Tema 10.1.0 - Las líneas VTY son las líneas de Terminal Virtual del router, que se utilizan únicamente para controlar las conexiones Telnet entrantes, mientras que la consola 0 es el puerto físico de la consola en el conmutador/enrutador al que se conecta. El comando **line vty** se usa para configurar el acceso remoto al switch/router a través de telnet o ssh.

- Router(config)# **line vty 0 4**
  Router(config-line)# **password manage**
  Router(config-line)# **exit**
  Router(config)# **enable password cisco**
- Router(config)# **line vty 0 4**
  Router(config-line)# **password cisco**
  Router(config-line)# **login**
- Router(config)# **line console 0**
  Router(config-line)# **password cisco**
  Router(config-line)# **login**
- Router(config)# **line console 0**
  Router(config-line)# **password cisco**
  Router(config-line)# **exit**
  Router(config)# **service password-encryption**

6. ¿Qué comando se puede utilizar en un router Cisco para mostrar todas las interfaces, la dirección IPv4 asignada y el estado actual?

Tema 10.2.0 - El comando **show ip interface brief** se puede utilizar en un router Cisco para mostrar todas las interfaces, la dirección IPv4 asignada y el estado actual.

- **show ip interface brief**
- **ping**
- **show ip route**
- **show interface fa0/1**

7. ¿Qué modo CLI permite a los usuarios acceder a todos los comandos del dispositivo, como los utilizados para la configuración, la administración y la solución de problemas?

Tema 10.1.0 – El comando Router#**configure terminal** permite al usuario entrar en el modo privilegiado desde el que se puede acceder a los comandos de configuración, gestión y solución de problemas.

- ( ) Modo EXEC de usuario
- (•) Modo EXEC con privilegios
- ( ) Modo de configuración global
- ( ) Modo de configuración de interfaz

8. ¿Cuál es el propósito del archivo de configuración de inicio en un router Cisco?

Tema 10.1.0 – El archivo de configuración de inicio se almacena en la NVRAM y contiene los comandos que se necesitan para la configuración inicial del router. También crea el archivo de configuración en ejecución que se almacena en la RAM.

- ( ) Facilitar la operación básica de los componentes de hardware de un dispositivo.
- (•) Contener los comandos que se utilizan para la configuración inicial de un router en el inicio.
- ( ) Contener los comandos de configuración que utiliza actualmente el IOS del router.
- ( ) Proporcionar una versión limitada de la copia de respaldo de IOS por si acaso el router no puede cargar IOS con todas las funciones.

9. ¿Cuál de las siguientes características describe el gateway predeterminado de un equipo host?

Tema 10.3.0 – El gateway predeterminado es la dirección IP de una interfaz del router en la misma red que el host emisor.

- (•) La dirección lógica de la interfaz del router en la misma red que el equipo host
- ( ) La dirección física de la interfaz del switch conectado al equipo host
- ( ) La dirección física de la interfaz del router en la misma red que el equipo host
- ( ) La dirección lógica asignada a la interfaz del switch conectado al router

10. ¿Cuál es el objetivo del comando **banner motd**?

Tema 10.1.0 – El comando **banner motd** se utiliza para mostrar un mensaje cuando un usuario intenta iniciar sesión en el router.

- ( ) Configura un mensaje que identificará documentos impresos a los usuarios de LAN.
- ( ) Es una forma en que los routers comunican el estado de sus enlaces entre sí.
- ( ) Proporciona una forma fácil de comunicarse con cualquier usuario conectado a las LAN de un router.
- (•) Proporciona una forma de hacer anuncios a aquellos que inician sesión en un enrutador.

11. Un técnico está configurando un enrutador para permitir todas las formas de acceso de administración. Como parte de cada tipo de acceso diferente, el técnico está intentando escribir el comando ¿ **login**. Qué modo de configuración se debe introducir para realizar esta tarea?

Tema 10.1.0 - El comando **login** se utiliza para permitir el acceso a un router o conmutador a través de líneas auxiliares, líneas de consola y líneas Telnet.

- ○ modo ejecutivo de usuario
- ○ Modo de configuración global
- ◉ modo de configuración de líneas
- ○ Modo EXEC con privilegios

12. ¿Qué se almacena en la NVRAM de un router Cisco?

Tema 10.1.0 - El IOS de Cisco se almacena en flash. La configuración en ejecución se almacena en la RAM. Las instrucciones de inicio se almacenan en ROM. El archivo de configuración de inicio se almacena en NVRAM.

- ○ el Cisco IOS.
- ○ La configuración en ejecución
- ○ Instrucciones de arranque
- ◉ Configuración de inicio

13. ¿Qué afirmación relativa al comando **service password-encryption** es verdadera?

Tema 10.1.0 - El comando **service password-encryption** se utiliza para cifrar todas las contraseñas de texto claro en el archivo de configuración en ejecución.

- ○ Está configurado en modo EXEC privilegiado.
- ○ Cifra solo contraseñas en modo de línea.
- ◉ Tan pronto como se introduce el comando **service password-encryption**, todas las contraseñas establecidas actualmente que se mostraban en texto sin formato se cifran.
- ○ Para ver las contraseñas cifradas por el comando **service password-encryption** en texto sin formato, ejecute el **no service password-encryption** comando.

Correct

You have successfully identified the correct answers.

You got 13 out of 13 questions correct.

1. A router boots and enters setup mode. What is the reason for this?

Topic 10.1.0 - If a router cannot locate the startup-config file in NVRAM it will enter setup mode to allow the configuration to be entered from the console device.

- ○ The IOS image is corrupt.
- ○ Cisco IOS is missing from flash memory.
- ◉ The configuration file is missing from NVRAM.
- ○ The POST process has detected hardware failure.

2. Which command is used to encrypt all passwords in a router configuration file?

Topic 10.1.0 - The command **service password-encryption** is used to encrypt and secure plain-text passwords configured on a router.

- ○ Router_A (config) # **enable secret** <password>
- ◉ Router_A (config) # **service password-encryption**
- ○ Router_A (config) # **enable password** *<password>*
- ○ Router_A (config) # **encrypt password**

3. Company policy requires using the most secure method to safeguard access to the privileged exec and configuration mode on the routers. The privileged exec password is *trustknow1*. Which of the following router commands achieves the goal of providing the highest level of security?

Topic 10.1.0 - The command **service password-encryption** is used to encrypt and secure plain-text passwords configured on a router

- ○ **secret password trustknow1**
- ○ **enable password trustknow1**
- ○ **service password-encryption**
- ◉ **enable secret trustknow1**

4. What will be the response from the router after the command, "router(config)# **hostname portsmouth**" is entered?

Topic 10.1.0 - The command **hostname portsmouth** is used to change the current router name to portsmouth.

- ○ portsmouth#
- ◉ portsmouth(config)#
- ○ invalid input detected
- ○ router(config-host)#
- ○ hostname = portsmouth
  portsmouth#
- ○ ? command not recognized
  router(config)#

5. An administrator is configuring a new router to permit out-of-band management access. Which set of commands will allow the required login using a password of **cisco**?

Topic 10.1.0 - The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections while console 0 is the physical console port on the switch/router you plug into. The **line vty** command is used to remote configure access into the switch/router via telnet or ssh.

- Router(config)# **line vty 0 4**
  Router(config-line)# **password manage**
  Router(config-line)# **exit**
  Router(config)# **enable password cisco**
- Router(config)# **line vty 0 4**
  Router(config-line)# **password cisco**
  Router(config-line)# **login**
- (●) Router(config)# **line console 0**
  Router(config-line)# **password cisco**
  Router(config-line)# **login**
- Router(config)# **line console 0**
  Router(config-line)# **password cisco**
  Router(config-line)# **exit**
  Router(config)# **service password-encryption**

6. Which command can be used on a Cisco router to display all interfaces, the IPv4 address assigned, and the current status?

Topic 10.2.0 - The **show ip interface brief** command can be used on a Cisco router to display all interfaces, the IPv4 address assigned, and the current status.

- (●) **show ip interface brief**
- **ping**
- **show ip route**
- **show interface fa0/1**

7. Which CLI mode allows users to access all device commands, such as those used for configuration, management, and troubleshooting?

Topic 10.1.0 - The command Router#**configure terminal** allows a user to enter the privileged mode from where the configuration,management and troubleshooting commands can be accessed.

- user EXEC mode
- (●) privileged EXEC mode
- global configuration mode
- interface configuration mode

8. What is the purpose of the startup configuration file on a Cisco router?

Topic 10.1.0 - The startup configuration file is stored in NVRAM and contains the commands needed to initially configure a router. It also creates the running configuration file that is stored in in RAM.

- to facilitate the basic operation of the hardware components of a device
- (●) to contain the commands that are used to initially configure a router on startup
- to contain the configuration commands that the router IOS is currently using
- to provide a limited backup version of the IOS, in case the router cannot load the full featured IOS

9. Which characteristic describes the default gateway of a host computer?

Topic 10.3.0 - The default gateway is the IP address of an interface on the router on the same network as the sending host.

- (●) the logical address of the router interface on the same network as the host computer
- the physical address of the switch interface connected to the host computer
- the physical address of the router interface on the same network as the host computer
- the logical address assigned to the switch interface connected to the router

10. What is the purpose of the **banner motd** command?

Topic 10.1.0 - The **banner motd** command is used to display a message when a user attempts to log into the router.

- It configures a message that will identify printed documents to LAN users.
- It is a way that routers communicate the status of their links with one another.
- It provides an easy way of communicating with any user attached to a router's LANs.
- (●) It provides a way to make announcements to those who log in to a router.

11. A technician is configuring a router to allow for all forms of management access. As part of each different type of access, the technician is trying to type the command **login**. Which configuration mode should be entered to do this task?

Topic 10.1.0 - The command **login** is used to allow access to a router or switch through aux lines, console lines, and Telnet lines.

- ○ user executive mode
- ○ global configuration mode
- ◉ any line configuration mode
- ○ privileged EXEC mode

12. What is stored in the NVRAM of a Cisco router?

Topic 10.1.0 - The Cisco IOS is stored in flash.
The running configuration file is stored in RAM.
The bootup instructions are stored in ROM.
The startup configuration file is stored in NVRAM.

- ○ the Cisco IOS
- ○ the running configuration
- ○ the bootup instructions
- ◉ the startup configuration

13. Which statement regarding the **service password-encryption** command is true?

Topic 10.1.0 - The command **service password-encryption** is used to encrypt all the clear text passwords in the running-configuration file.

- ○ It is configured in privileged EXEC mode.
- ○ It encrypts only line mode passwords.
- ◉ As soon as the **service password-encryption** command is entered, all currently set passwords formerly displayed in plain text are encrypted.
- ○ To see the passwords encrypted by the **service password-encryption** command in plain text, issue the **no service password-encryption** command.

Capítulo 11_ Direccionamiento IPv4

Introducción

11.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a direccionamiento IPv4!

Actualmente, todavía hay muchas redes que utilizan direcciones IPv4, incluso cuando las organizaciones que las utilizan están haciendo la transición a IPv6. Por lo tanto, sigue siendo muy importante que los administradores de red sepan todo lo que puedan sobre el direccionamiento IPv4. Este módulo cubre en detalle los aspectos fundamentales del direccionamiento IPv4. Incluye cómo segmentar una red en subredes y cómo crear una máscara de subred de longitud variable (VLSM) como parte de un esquema general de direcciones IPv4. La subred es como cortar un pastel en trozos cada vez más pequeños. La subred puede parecer abrumadora al principio, pero te mostramos algunos trucos para ayudarte en el camino. Este módulo incluye varios videos, actividades para ayudarle a practicar subredes, Packet Tracers y un laboratorio. Una vez que lo consigas, ¡estarás en camino a la administración de la red!

11.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Asignación de direcciones IPv4

Objetivos del módulo: Calcule un esquema de subredes IPv4 para segmentar la red de manera eficiente.

Título del tema	Objetivo del tema
Estructura de la dirección IPv4	Describa la estructura de una dirección IPv4, incluidas la porción de red y de host, y la máscara de subred.
IPv4 Unicast, Broadcast, y Multicast	Compare las características y los usos de las direcciones IPv4 unicast, broadcast y multicast.
Tipos de direcciones IPv4	Explique las direcciones IPv4 públicas, privadas y reservadas.

Título del tema	Objetivo del tema
Segmentación de la red	Explique la forma en que la división en subredes segmenta una red para permitir una mejor comunicación.
División de subredes de una red IPv4	Calcule las subredes IPv4 para un prefijo /24.
Subnet a /16 and a /8 Prefix	Calcule las subredes IPv4 para un prefijo /16 y /8.
División en subredes para cumplir con requisitos	Dado un conjunto de requisitos para subredes, implementar un IPv4 esquema de direccionamiento
Máscara de subred de longitud variable	Explicar cómo crear un esquema de direccionamiento flexible usando variables Máscara de subred de longitud variable (VLSM)
Diseño estructurado	Implemente un esquema de asignación de direcciones VLSM.

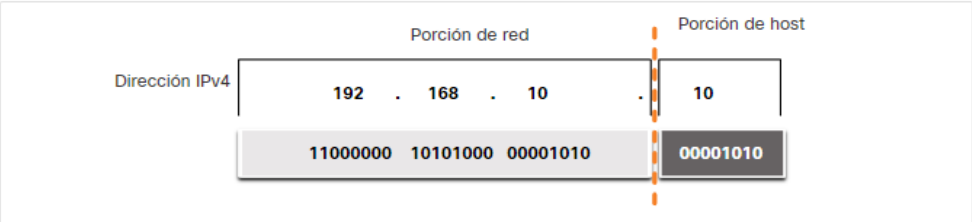
Estructura de la dirección IPv4

11.1.1

Porciones de red y de host

Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una porción de red y una porción de host. Al determinar la porción de red frente a la porción de host, debe mirar la secuencia de 32 bits, como se muestra en la figura.

El diagrama muestra el desglose de una dirección IPv4 en las partes de red y host. La dirección IPv4 es 192.168.10.10. Debajo, la dirección se convierte en 11000000 10101000 00001010 00001010. Una línea discontinua muestra la separación entre las partes de red y host. Esto ocurre después del tercer octeto y el bit 24.



Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits identifica la red y qué porción identifica el host? El rol de la máscara de subred.

11.1.2

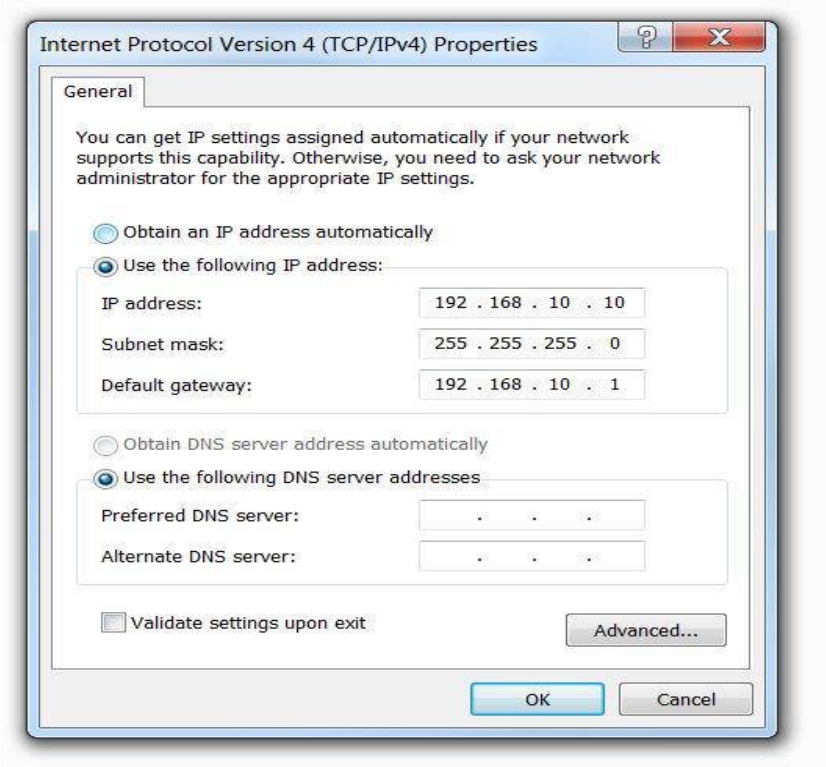
La máscara de subred

Como se muestra en la figura, asignar una dirección IPv4 a un host requiere lo siguiente:

Dirección* **IPv4** - Esta es la dirección IPv4única del host.

- **Máscara de subred**- se usa para identificar la parte de red/host de la dirección IPv4.

Configuración IPv4 en un equipo con Windows

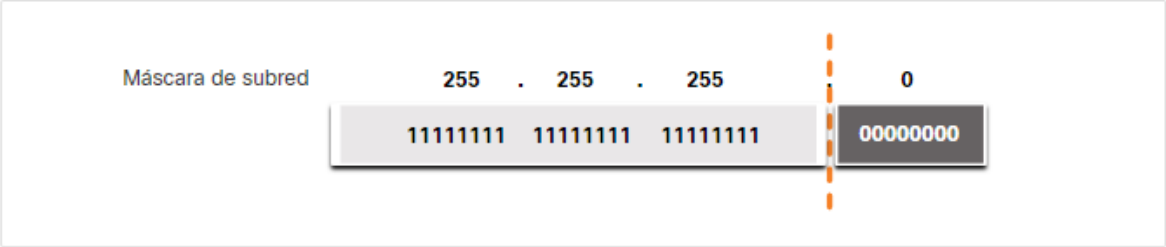


Nota: Se requiere una dirección IPv4 de puerta de enlace predeterminada para llegar a redes remotas y se requieren direcciones IPv4 del servidor DNS para traducir nombres de dominio a direcciones IPv4.

La máscara de subred IPv4 se usa para diferenciar la porción de red de la porción de host de una dirección IPv4. Cuando se asigna una dirección IPv4 a un dispositivo, la máscara de subred se usa para determinar la dirección de red del dispositivo. La dirección de red representa todos los dispositivos de la misma red.

La siguiente figura muestra la máscara de subred de 32 bits en formato decimal y binario punteado.

Máscara de subred



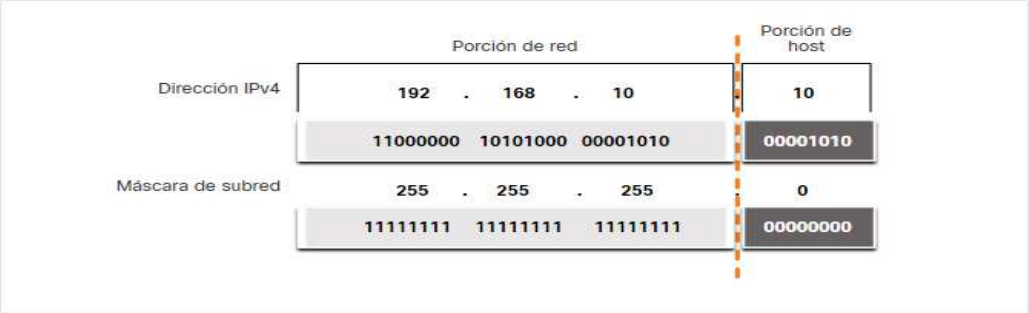
Máscara de subred de 255.255.255.0 en la parte superior con la representación binaria de 11111111 1111111 111111 0000000 debajo; una línea discontinua se dibuja después del tercer octeto y el bit 24.

Observe cómo la máscara de subred es una secuencia consecutiva de 1 bits seguida de una secuencia consecutiva de 0 bits.

Para identificar las porciones de red y host de una dirección IPv4, la máscara de subred se compara con la dirección IPv4 bit por bit, de izquierda a derecha como se muestra en la figura.

La figura muestra una dirección IPv4, escrita en decimal con puntos y binario, con la máscara de subred a continuación, también escrita en decimal con puntos y binario, utilizada para mostrar la división entre la parte de red y la parte de host de la dirección. La dirección IPv4 es 192.168.10.10 que se convierte a 11000000 10101000 00001010 00001010. La máscara de subred es 255.255.255.0 que se convierte en 11111111 111111 111111 00000000. Una línea discontinua muestra la separación entre la red y las porciones de host. Esto ocurre después del tercer octeto y el bit 24.

Asociación de una dirección IPv4 con su máscara de subred



Tenga en cuenta que la máscara de subred en realidad no contiene la porción de red o host de una dirección IPv4, solo le dice a la computadora dónde buscar la parte de la dirección IPv4 que es la porción de red y qué parte es la porción de host.

El proceso real que se usa para identificar la porción de red y la porción de host se denomina AND.

11.1.3

La longitud de prefijo

Puede ser difícil expresar direcciones de red y de host con la dirección de la máscara de subred decimal punteada. Afortunadamente, hay un método alternativo para identificar una máscara de subred, un método llamado longitud del prefijo.

La longitud del prefijo es el número de bits establecido en 1 en la máscara de subred. Está escrito en "notación de barra", que se observa mediante una barra diagonal (/) seguida del número de bits establecido en 1. Por lo tanto, cuente el número de bits en la máscara de subred y anteponga una barra diagonal.

Consulte la tabla para ver ejemplos. En la primera columna, se enumeran varias máscaras de subred que se pueden usar con una dirección de host. En la segunda columna, se muestra la dirección binaria de 32 bits convertida. En la última columna, se muestra la longitud de prefijo resultante.

Comparación de la máscara de subred y la longitud de prefijo

Máscara de subred	Dirección de 32 bits	Longitud de prefijo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Nota: Una dirección de red también se conoce como prefijo o prefijo de red. Por lo tanto, la longitud del prefijo es el número de 1 bits en la máscara de subred.

Al representar una dirección IPv4 utilizando una longitud de prefijo, la dirección IPv4 se escribe seguida de la longitud del prefijo sin espacios. Por ejemplo, 192.168.10.10 255.255.255.0 se escribiría como 192.168.10.10/24. Más adelante se analiza el uso de varios tipos de longitudes de prefijo. Por ahora, el foco estará en el prefijo / 24 (es decir, 255.255.255.0).

11.1.4

Determinación de la red: lógica AND

Un AND lógico es una de las tres operaciones booleanas utilizadas en la lógica booleana o digital. Las otras dos son OR y NOT. La operación AND se usa para determinar la dirección de red.

Y lógico es la comparación de dos bits que producen los resultados que se muestran a continuación. Observe que solo mediante 1 AND 1 se obtiene 1. Cualquier otra combinación da como resultado un 0.

- 1 Y 1 = 1
- 0 Y 1 = 0

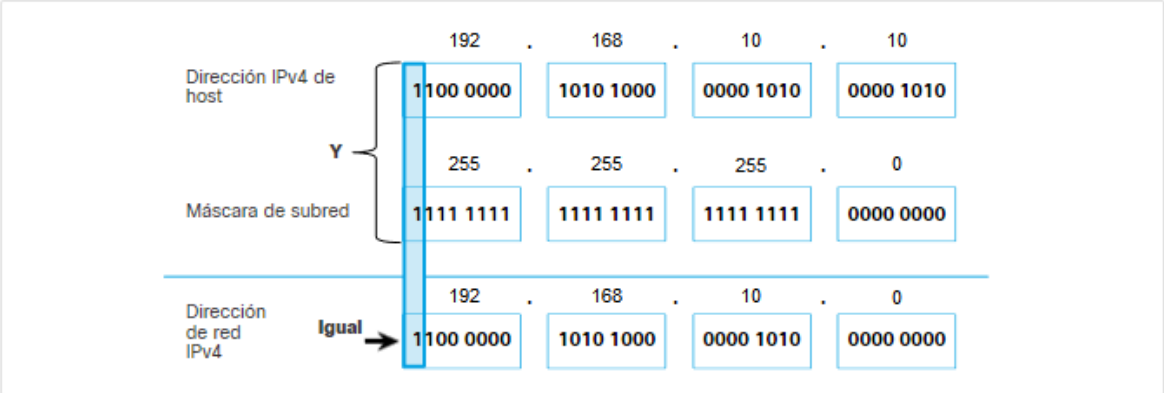
- 1 Y 0 = 0
- 0 Y 0 = 0

Nota: En la lógica digital, 1 representa True y 0 representa False. Cuando se utiliza una operación AND, ambos valores de entrada deben ser True (1) para que el resultado sea True (1).

Para identificar la dirección de red de un host IPv4, se recurre a la operación lógica AND para la dirección IPv4, bit por bit, con la máscara de subred. El uso de la operación AND entre la dirección y la máscara de subred produce la dirección de red.

Para ilustrar cómo se usa AND para descubrir una dirección de red, considere un host con dirección IPv4 192.168.10.10 y una máscara de subred de 255.255.255.0, como se muestra en la figura:

- Dirección de host**IPv4 (192.168.10.10)** - La dirección IPv4 del host en formato decimal y binario con puntos.
- Máscara de**subred (255.255.255.0)** - La máscara de subred del host en formatos decimales y binarios punteados.
- Dirección de**red (192.168.10.0)**: la operación AND lógica entre la dirección IPv4 y la máscara de subred da como resultado una dirección de red IPv4 que se muestra en formato decimal y binario con puntos.



El diagrama muestra el proceso AnDing entre una dirección de host IPv4 y una máscara de subred que da como resultado la dirección de red IPv4 del host. La dirección del host IPv4 es 192.168.10.10. Debajo de eso, la dirección se convierte en 11000000 10101000 00001010 00001010. Debajo de eso, se escribe la máscara de subred de 255.255.255.0. Debajo de eso, la máscara de subred se convierte en 11111111 111111 00000000. Se dibuja una línea debajo del equivalente binario de la máscara de subred. Debajo de la línea se encuentra el decimal con puntos y el equivalente binario de la dirección de red IPv4 determinado por el proceso AnDing. Un cuadro sombreado azul muestra el primer bit de la dirección de host IPv4, un 1, en comparación con el primer bit de la máscara de subred, también un 1, lo que resulta en un 1 como primer valor de bit en la dirección de red IPv4. La dirección de red IPv4 es 192.168.10.0 con un equivalente binario de 11000000 101001000 00001010 00000000.

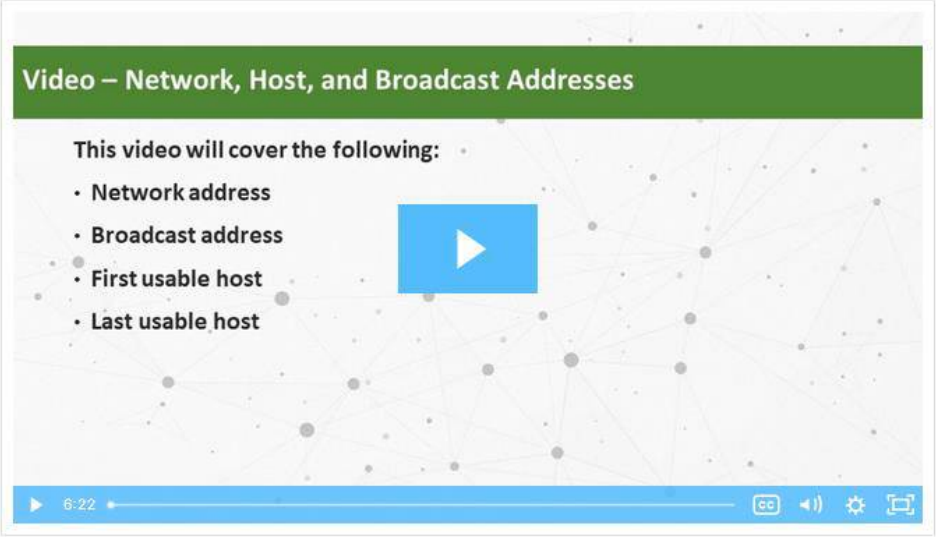
Utilizando la primera secuencia de bits como ejemplo, observe que la operación AND se realiza en el 1 bit de la dirección del host con el 1 bit de la máscara de subred. Esto da como resultado un bit de 1 para la dirección de red. 1 AND 1 = 1.

La operación AND entre una dirección de host IPv4 y una máscara de subred da como resultado la dirección de red IPv4 para este host. En este ejemplo, la operación AND entre la dirección host 192.168.10.10 y la máscara de subred 255.255.255.0 (/24) da como resultado la dirección de red IPv4 192.168.10.0/24. Esta es una operación IPv4 importante, ya que le dice al host a qué red pertenece.

11.1.5

Video - Direcciones de red, host y Broadcast

Haga clic en Reproducir para ver una demostración de cómo se determinan las direcciones de red, de host y de difusión para una dirección IPv4 y una máscara de subred dadas.



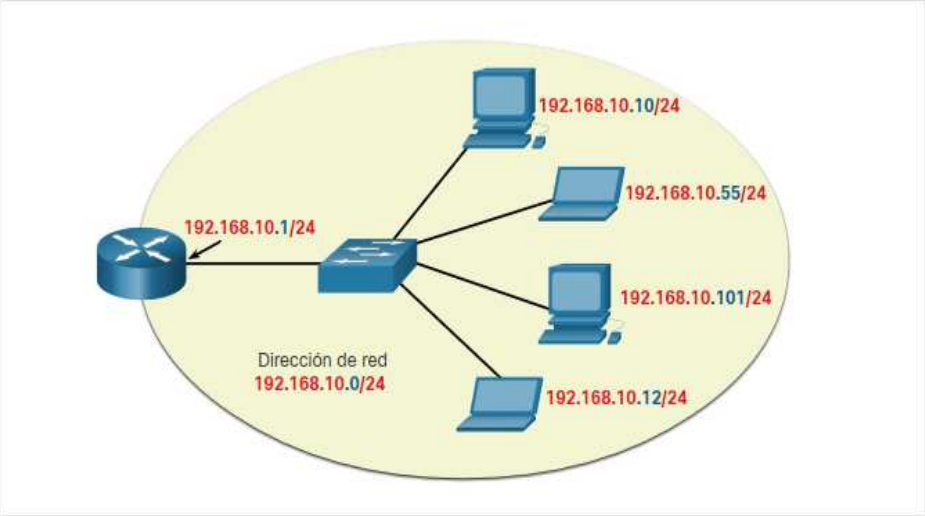
11.1.6

Direcciones de red, de host y de difusión

Dentro de cada red hay tres tipos de direcciones IP:

- Dirección de red
- Direcciones de host
- Dirección de broadcast

Usando la topología de la figura, se examinarán estos tres tipos de direcciones.



El diagrama es topología de red con cuatro hosts conectados a un switch que está conectado a un router. La interfaz del router tiene una dirección IP 192.168.10.1/24 y los hosts tienen las siguientes direcciones IP: 192.168.10.10/24, 192.168.10.55/24, 192.168.10.101/24 y 192.168.10.12/24. El cuarto octeto de la interfaz del router y los hosts se muestra en un color diferente. Un círculo abarca la interfaz del router, el switch y todos los hosts dentro de los cuales se escribe la dirección de red 192.168.10.0/24, también con el cuarto octeto mostrado en un color diferente.

Dirección de red

Una dirección de red es una dirección que representa una red específica. Un dispositivo pertenece a esta red si cumple tres criterios:

- Tiene la misma máscara de subred que la dirección de red.
- Tiene los mismos bits de red que la dirección de red, como indica la máscara de subred.
- Se encuentra en el mismo dominio de difusión que otros hosts con la misma dirección de red.

Un host determina su dirección de red realizando una operación AND entre su dirección IPv4 y su máscara de subred.

Como se muestra en la tabla, la dirección de red tiene todos los 0 bits en la parte del host, según lo determinado por la máscara de subred. En este ejemplo, la dirección de red es 192.168.10.0/24. No se puede asignar una dirección de red a un dispositivo.

Direcciones de red, de host y de difusión

	Porción de red			Porción de host	Bits de host
Máscara de subred **255.255.255**.0 o **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
La dirección de red es **192.168.10**.0 o **/24**	192 11000000	168 10100000	10 00001010	0 00000000	Todos los 0
Primera dirección **192.168.10**.1 ó **/24**	192 11000000	168 10100000	10 00001010	1 00000001	Todos los 0s y un 1
Última dirección **192.168.10**.254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	Todos los 1s y un 0
Dirección de difusión **192.168.10**.255 ó **/24**	192 11000000	168 10100000	10 00001010	255 11111111	Todos los 1s

Direcciones de host

Las direcciones de host son direcciones que se pueden asignar a un dispositivo, como un equipo host, un portátil, un teléfono inteligente, una cámara web, una impresora, un router, etc. La parte de host de la dirección son los bits indicados por 0 bits en la máscara de subred. Las direcciones de host pueden tener cualquier combinación de bits en la parte del host excepto los 0 bits (esto sería una dirección de red) o los 1 bits (esto sería una dirección de difusión).

Todos los dispositivos dentro de la misma red deben tener la misma máscara de subred y los mismos bits de red. Solo los bits del host serán diferentes y deben ser únicos.

Observe que, en la tabla, hay una primera y última dirección de host:

- **Primera dirección de host**: este primer host dentro de una red tiene todos los 0 bits con el último bit (más a la derecha) como 1 bit. En este ejemplo es 192.168.10.1/24.
- **Última dirección de host**: este último host dentro de una red tiene los 1 bits con el último bit (más a la derecha) como 0 bit. En este ejemplo es 192.168.10.254/24.

Cualquier dirección entre 192.168.10.1/24 y 192.168.10.254/24 se puede asignar a un dispositivo de la red.

Broadcast address

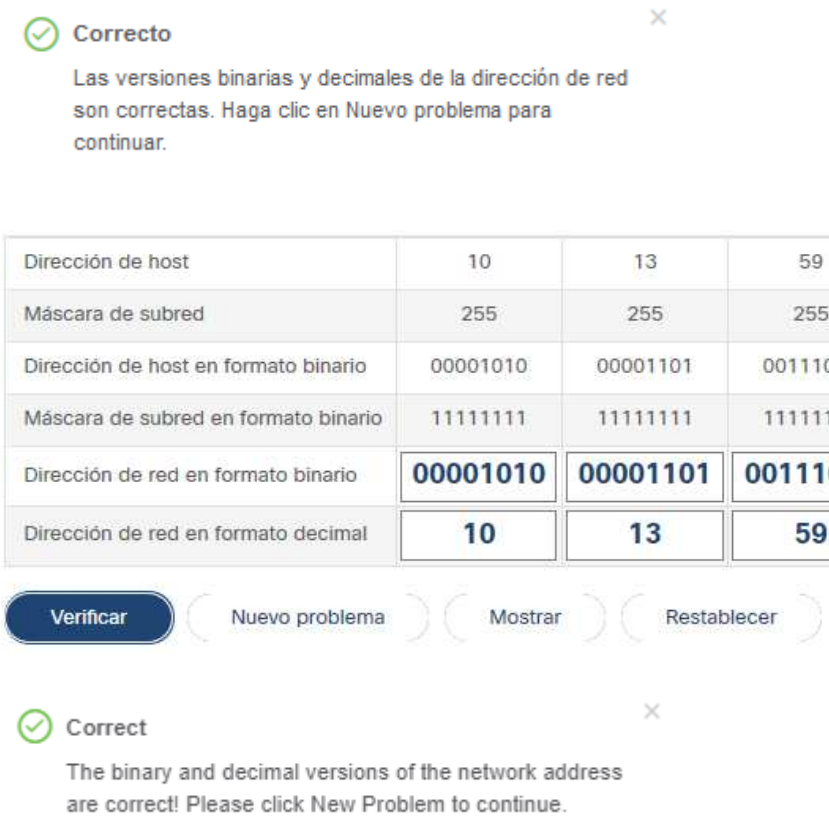
Una dirección de difusión es una dirección que se utiliza cuando se requiere para llegar a todos los dispositivos de la red IPv4. Como se muestra en la tabla, la dirección de difusión de red tiene los 1 bits en la parte del host, según lo determinado por la máscara de subred. En este ejemplo, la dirección de red es 192.168.10.255/24. No se puede asignar una dirección de difusión a un dispositivo.

11.1.7

Actividad: Uso de la operación AND para determinar la dirección de red

Instrucciones:

Utilice la operación AND para determinar la dirección de red (en formatos binario y decimal).



Instructions:

Use the ANDing process to determine the network address (in binary and decimal formats).

Host Address	172	31	104	132
Subnet Mask	255	255	255	240
Host Address in binary	10101100	00011111	01101000	10000100
Subnet Mask in binary	11111111	11111111	11111111	11110000
Network Address in binary	**10101100**	**00011111**	**01101000**	**10000000**
Network Address in decimal	**172**	**31**	**104**	**128**

Check | New Problem | Show Me | Reset

11.1.8

Compruebe su comprensión - Estructura de direcciones IPv4

Verifique su comprensión de la Estructura de direcciones IPv4 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Una dirección IPv4 tiene 32 bits de longitud. Contiene una parte de red y una parte de host.
2. Una máscara de subred tiene 32 bits de longitud. Se diferencia la parte de red de la parte de host de una dirección IPv4. Es una serie consecutiva de 1 bits seguido de 0 bits consecutivos. Los 1 bits indican la parte de red de la dirección IPv4 y los 0 bits indican la parte del host.
3. La operación AND se usa entre la dirección IPv4 y la máscara de subred para determinar la porción de red de la dirección. 1 AND 1 da como resultado un 1, cualquier otra combinación da como resultado un 0.
4. El resultado de una operación lógica AND de 10.128.17.4 255.255.240.0 produce la dirección de red IPv4 10.128.16.0 255.255.240.0.

Has tenido 4 respuestas correctas de 4.

1. ¿Qué dos afirmaciones son correctas sobre una dirección IPv4? (Escoja dos opciones).

¡Lo tienes!

- [x] Contiene una parte de red.
- [x] Contiene una parte de host.
- [ ] Tiene 24 bits de longitud.
- [ ] La información dentro de la dirección IPv4 es suficiente para determinar la parte de red y la parte de host de la dirección.

2. ¿Qué dos instrucciones son correctas acerca de una máscara de subred IPv4? (Escoja dos opciones).

¡Lo tienes!

- [ ] Tiene 24 bits de longitud.
- [x] Se diferencia la parte de red de la parte de host de una dirección IPv4.
- [ ] Es cualquier combinación de 0 y 1 bits.
- [ ] Es una secuencia consecutiva de 0 bits seguida de una secuencia consecutiva de 1 bits.
- [x] Los bits de 1 determinan la parte de red de una dirección IPv4 y los bits de 0 determinan la parte del host.

3. ¿Qué tres afirmaciones son correctas sobre la operación AND? (Escoja tres opciones).

¡Lo tienes!

- [x] La operación AND se realiza entre una dirección IPv4 y una máscara de subred.
- [ ] La operación AND se realiza entre dos direcciones IPv4.
- [ ] 1 AND 1 resultados en un 0
- [x] 1 AND 0 resultados en un 0
- [x] Se utiliza para determinar las porciones de red y host de una dirección IPv4.

4. ¿Cuál es el resultado de una operación lógica AND de: 10.128.17.4 255.255.240.0?

¡Lo tienes!

- ( ) La dirección de red IPv4 de 10.128.0.0 255.255.240.0
- (•) La dirección de red IPv4 de 10.128.16.0 255.255.240.0
- ( ) La dirección de red IPv4 de 10.128.17.0 255.255.240.0
- ( ) La dirección de red IPv4 de 10.128.17.4 255.255.240.0

Good job!

You have successfully identified the best answers.

1. The network address for 10.5.4.100 with a subnet mask of 255.255.255.0 is 10.5.4.0.
2. The network address for 172.16.4.100 with a subnet mask of 255.255.0.0 is 172.16.0.0.
3. Host A is on network 10.5.4.0. Therefore, devices with the IPv4 addresses 10.5.4.1 and 10.5.4.99 are on the same network.
4. Host A is on network 172.16.0.0. Therefore, devices with the IPv4 addresses 172.16.4.99 and 172.16.0.1 are on the same network.
5. Host A is on network 192.168.1.0. Therefore, devices with the IPv4 addresses 192.168.1.1 and 192.168.1.100 are on the same network.

You got 5 out of 5 questions correct.

1. Host-A has the IPv4 address and subnet mask: 10.5.4.100 255.255.255.0. What is the network address of Host-A?

Correct.

- ○ 10.0.0.0
- ○ 10.5.0.0
- ◉ 10.5.4.0
- ○ 10.5.4.100

2. Host-A has the IPv4 address and subnet mask: 172.16.4.100 255.255.0.0. What is the network address of Host-A?

Correct.

- ○ 172.0.0.0
- ◉ 172.16.0.0
- ○ 172.16.4.0
- ○ 172.16.4.100

3. Host-A has the IPv4 address and subnet mask: 10.5.4.100 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

Correct.

- ☑ 10.5.4.1
- ☐ 10.5.0.1
- ☑ 10.5.4.99
- ☐ 10.0.0.98
- ☐ 10.5.100.4

4. Host-A has the IPv4 address and subnet mask: 172.16.4.100 255.255.0.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

Correct.

- [x] 172.16.4.99
- [x] 172.16.0.1
- [ ] 172.17.4.99
- [ ] 172.17.4.1
- [ ] 172.18.4.1

5. Host-A has the IPv4 address and subnet mask: 192.168.1.50 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

Correct.

- [ ] 192.168.0.1
- [ ] 192.168.0.100
- [x] 192.168.1.1
- [x] 192.168.1.100
- [ ] 192.168.2.1

Asignación de direcciones IPv4 / IPv4 Unicast, Broadcast, y Multicast

IPv4 Unicast, Broadcast, y Multicast

11.2.1

Unidifusión

En el tema anterior, aprendió acerca de la estructura de una dirección IPv4; cada una tiene una parte de red y una parte de host. Existen diferentes formas de enviar un paquete desde un dispositivo de origen, y estas diferentes transmisiones afectan a las direcciones IPv4 de destino.

La transmisión unidifusión se refiere a un dispositivo que envía un mensaje a otro dispositivo en comunicaciones uno a uno.

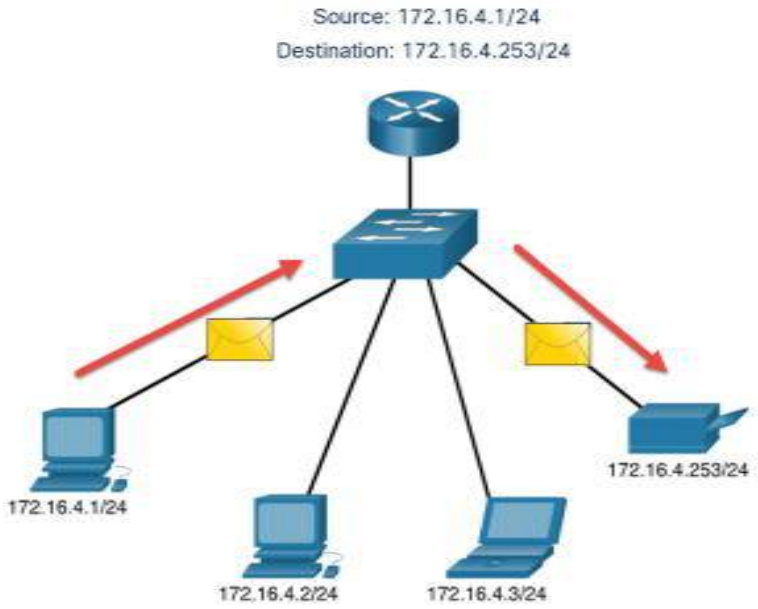
Un paquete de unidifusión tiene una dirección IP de destino que es una dirección de unidifusión que va a un único destinatario. Una dirección IP de origen sólo puede ser una dirección de

unidifusión, ya que el paquete sólo puede originarse de un único origen. Esto es independientemente de si la dirección IP de destino es una unidifusión, difusión o multidifusión.

Reproduzca la animación para ver un ejemplo de transmisión de unidifusión.

Esta animación consta de tres hosts y una impresora conectada a un switch y router. La animación ilustra el host con la dirección IP 172.16.4.1 que envía un paquete de unidifusión a la dirección IP 172.16.4.253. Cuando el conmutador recibe el marco, lo reenvía a la impresora con la dirección IP 172.16.4.253.

Transmisión de unicast



Nota: En este curso, toda la comunicación entre dispositivos es unidifusión a menos que se indique lo contrario.

Las direcciones de host de unidifusión IPv4 están en el rango de direcciones de 1.1.1.1 a 223.255.255.255. Sin embargo, dentro de este intervalo existen muchas direcciones reservadas para fines específicos. Estas direcciones de propósito especial se discutirán más adelante en este módulo.

11.2.2

Dirección

Transmisión de transmisión hace referencia a un dispositivo que envía un mensaje a todos los dispositivos de una red en comunicaciones unipersonales.

Los paquetes de difusión tienen una dirección IPv4 de destino que contiene solo números uno (1) en la porción de host.

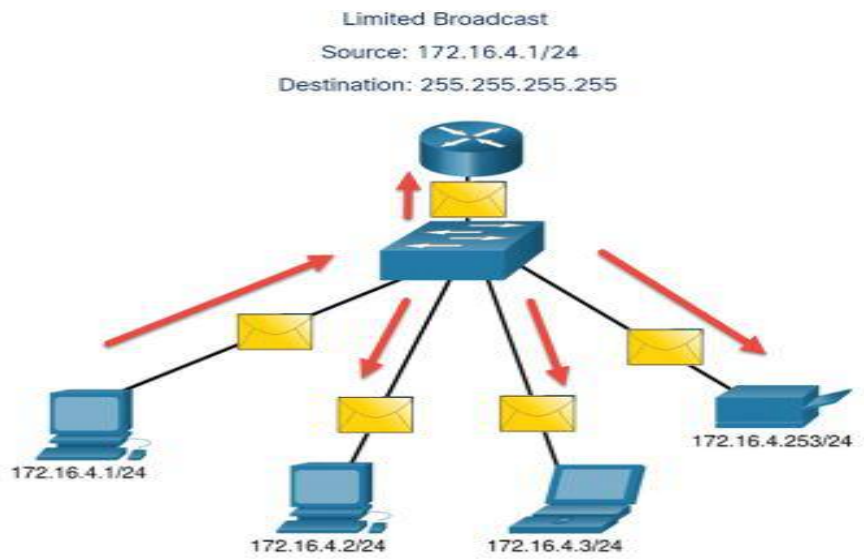
Nota: IPv4 usa paquetes de difusión. Sin embargo, no hay paquetes de difusión con IPv6.

Todos los dispositivos del mismo dominio de difusión deben procesar un paquete de difusión. Un dominio de difusión identifica todos los hosts del mismo segmento de red. Una transmisión puede ser dirigida o limitada. Una difusión dirigida se envía a todos los hosts de una red específica. Por ejemplo, un host de la red 172.16.4.0/24 envía un paquete a la dirección 172.16.4.255. Se envía una difusión limitada a 255.255.255.255. De manera predeterminada, los routers no reenvían transmisiones por difusión.

Reproduzca la animación para ver un ejemplo de transmisión de difusión limitada.

Esta animación consta de tres hosts y una impresora conectada a un switch y router. La animación ilustra el host con la dirección IP 172.16.4.1 que envía un paquete de difusión. Cuando el conmutador recibe el paquete de difusión, lo reenvía todos los puertos a los demás hosts, impresora y router.

Transmisión de difusión limitada



Los paquetes de difusión usan recursos en la red y hacen que cada host receptor en la red procese el paquete. Por lo tanto, se debe limitar el tráfico de difusión para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan los dominios de difusión, la subdivisión de redes puede mejorar el rendimiento de la red al eliminar el exceso de tráfico de difusión.

Difusiones dirigidas por IP

Además de la dirección de difusión 255.255.255.255, hay una dirección IPv4 de difusión para cada red, llamada difusión dirigida. Esta dirección utiliza la dirección más alta de la red, que es

la dirección donde todos los bits de host son 1s. Por ejemplo, la dirección de difusión dirigida para 192.168.1.0/24 es 192.168.1.255. Esta dirección permite la comunicación con todos los hosts de esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de difusión de la red.

Un dispositivo que no está conectado directamente a la red de destino reenvía una difusión dirigida IP de la misma manera que reenvía paquetes IP de unidifusión destinados a un host de esa red. Cuando un paquete de difusión dirigida llega a un router que está conectado directamente a la red de destino, ese paquete se transmite en la red de destino.

Nota: Debido a problemas de seguridad y abuso previo de usuarios malintencionados, las transmisiones dirigidas se desactivan de forma predeterminada a partir de Cisco IOS Release 12.0 con el comando de configuración global **no ip directed-broadcasts**.

11.2.3

Multidifusión

La transmisión de multidifusión reduce el tráfico al permitir que un host envíe un único paquete a un grupo seleccionado de hosts que estén suscritos a un grupo de multidifusión.

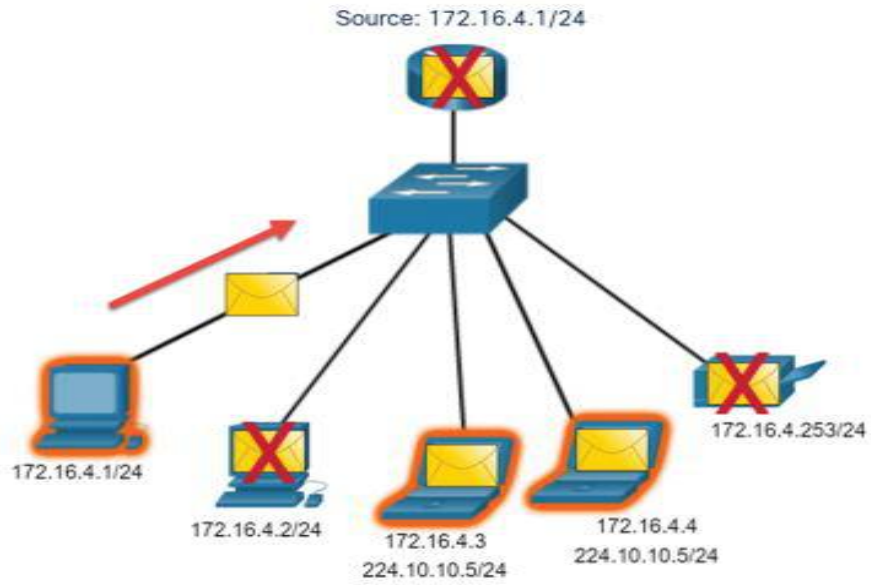
Un paquete de multidifusión es un paquete con una dirección IP de destino que es una dirección de multidifusión. IPv4 reservó las direcciones de 224.0.0.0 a 239.255.255.255 como rango de multidifusión.

Los hosts que reciben paquetes de multidifusión particulares se denominan clientes de multidifusión. Los clientes de multidifusión utilizan servicios solicitados por un programa cliente para subscribirse al grupo de multidifusión.

Cada grupo de multidifusión está representado por una sola dirección IPv4 de destino de multidifusión. Cuando un host IPv4 se suscribe a un grupo de multidifusión, el host procesa los paquetes dirigidos a esta dirección de multidifusión y los paquetes dirigidos a la dirección de unidifusión asignada exclusivamente.

Los protocolos de enrutamiento como OSPF utilizan transmisiones de multidifusión. Por ejemplo, los routers habilitados con OSPF se comunican entre sí mediante la dirección de multidifusión OSPF reservada 224.0.0.5. Sólo los dispositivos habilitados con OSPF procesarán estos paquetes con 224.0.0.5 como dirección IPv4 de destino. Todos los demás dispositivos ignorarán estos paquetes.

En la animación, se muestran clientes que aceptan paquetes de multidifusión.



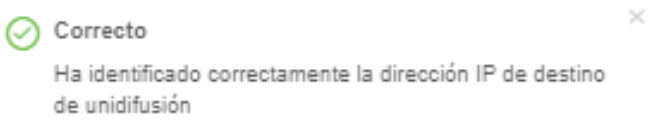
Esta animación consta de tres hosts y una impresora conectada a un switch y router. La animación ilustra el host con la dirección IP 172.16.4.1 que envía un paquete de multidifusión a la dirección IP del grupo de multidifusión 224.10.10.5. Cuando el conmutador recibe el paquete de multidifusión, lo reenvía todos los puertos a los demás hosts, impresoras y routers. Sin embargo, sólo dos hosts que son miembros de la dirección del grupo de multidifusión procesarán los paquetes. Todos los demás hosts descartan el paquete.

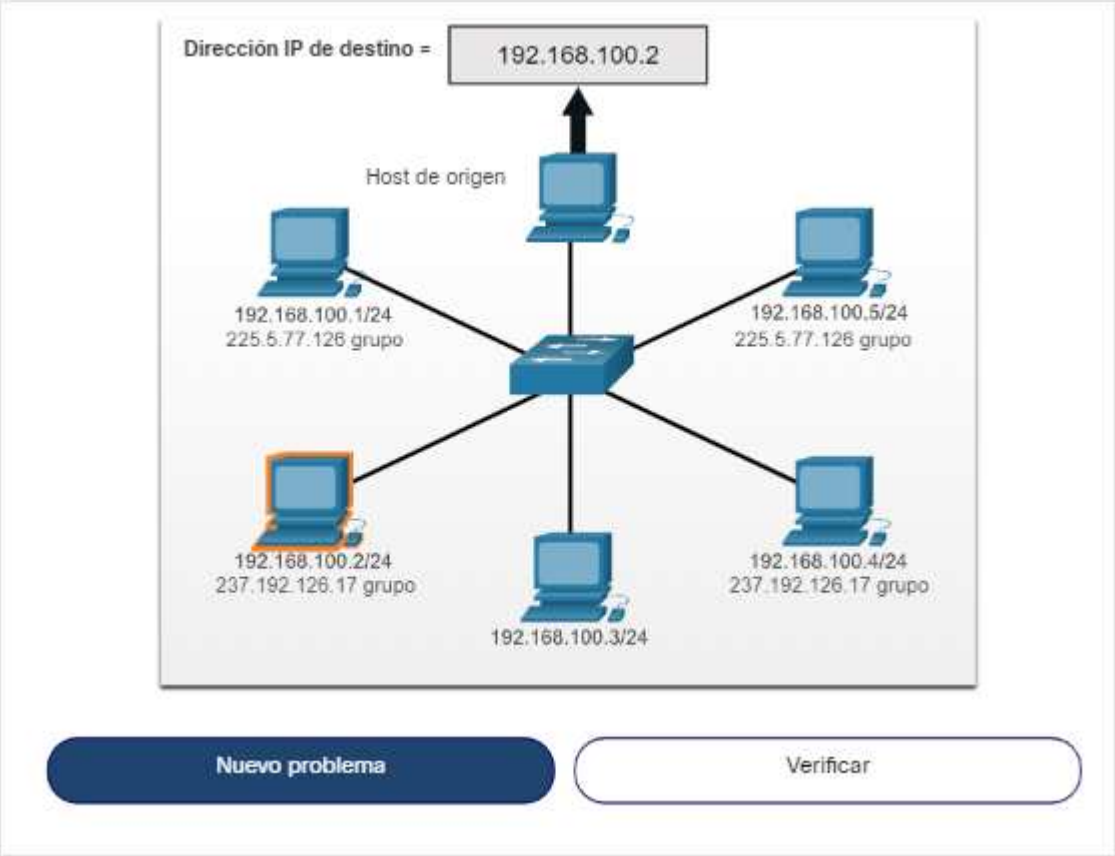
11.2.4

Actividad: Unidifusión, difusión y multidifusión?

Instrucciones:

Haga clic en **Inicio** para ver la dirección IP de destino. A continuación, haga clic en los hosts que recibirá un paquete según el tipo de dirección (unicast, broadcast o multicast). Esta actividad se controla por tiempo. Haga clic en **Verificar** para revisar sus respuestas. Haga clic **Nuevo problema** para obtener un nuevo problema.





Asignación de direcciones IPv4 / Tipos de direcciones IPv4

Tipos de direcciones IPv4

11.3.1

Direcciones IPv4 públicas y privadas

Del mismo modo que hay diferentes formas de transmitir un paquete IPv4, también hay diferentes tipos de direcciones IPv4. Algunas direcciones IPv4 no se pueden usar para salir a Internet, y otras se asignan específicamente para enrutar a Internet. Algunos se utilizan para verificar una conexión y otros se autoasignan. Como administrador de red, eventualmente se familiarizará con los tipos de direcciones IPv4, pero por ahora, al menos debe saber qué son y cuándo usarlas.

Las direcciones IPv4 públicas son direcciones que se enrutan globalmente entre routers de proveedores de servicios de Internet (ISP). Sin embargo, no todas las direcciones IPv4

disponibles pueden usarse en Internet. Existen bloques de direcciones denominadas direcciones privadas que la mayoría de las organizaciones usan para asignar direcciones IPv4 a los hosts internos.

A mediados de la década de 1990, con la introducción de la World Wide Web (WWW), se introdujeron direcciones IPv4 privadas debido al agotamiento del espacio de direcciones IPv4. Las direcciones IPv4 privadas no son exclusivas y cualquier red interna puede usarlas.

Nota: La solución a largo plazo para el agotamiento de direcciones IPv4 fue IPv6.

Estos son los bloques de direcciones privadas

Dirección de red y prefijo	Rango de direcciones privadas de RFC 1918
10.0.0.0/8	10.0.0.0 a 10.255.255.255
172.16.0.0/12	172.16.0.0 a 172.31.255.255
192.168.0.0/16	192.168.0.0 a 192.168.255.255

Nota: Las direcciones privadas se definen en RFC 1918 y a veces se denomina espacio de direcciones RFC 1918.

11.3.2

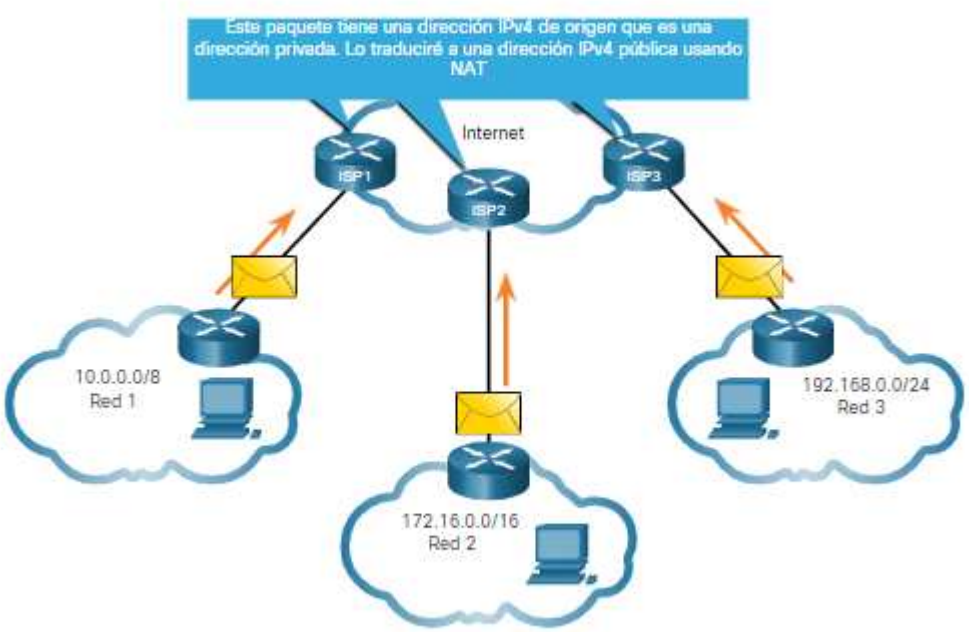
Enrutamiento en Internet

La mayoría de las redes internas, desde grandes empresas hasta redes domésticas, utilizan direcciones IPv4 privadas para dirigirse a todos los dispositivos internos (intranet), incluidos los hosts y routers. Sin embargo, las direcciones privadas no son enrutables globalmente.

En la figura, las redes de clientes 1, 2 y 3 están enviando paquetes fuera de sus redes internas. Estos paquetes tienen una dirección IPv4 de origen que es una dirección privada y una dirección IPv4 de destino que es pública (enrutable globalmente). Los paquetes con una dirección privada deben filtrarse (descartarse) o traducirse a una dirección pública antes de reenviar el paquete a un ISP.

El diagrama es una topología de red con tres redes, cada una conectada a un router ISP diferente. Los routers ISP realizan NAT entre cada red e Internet.

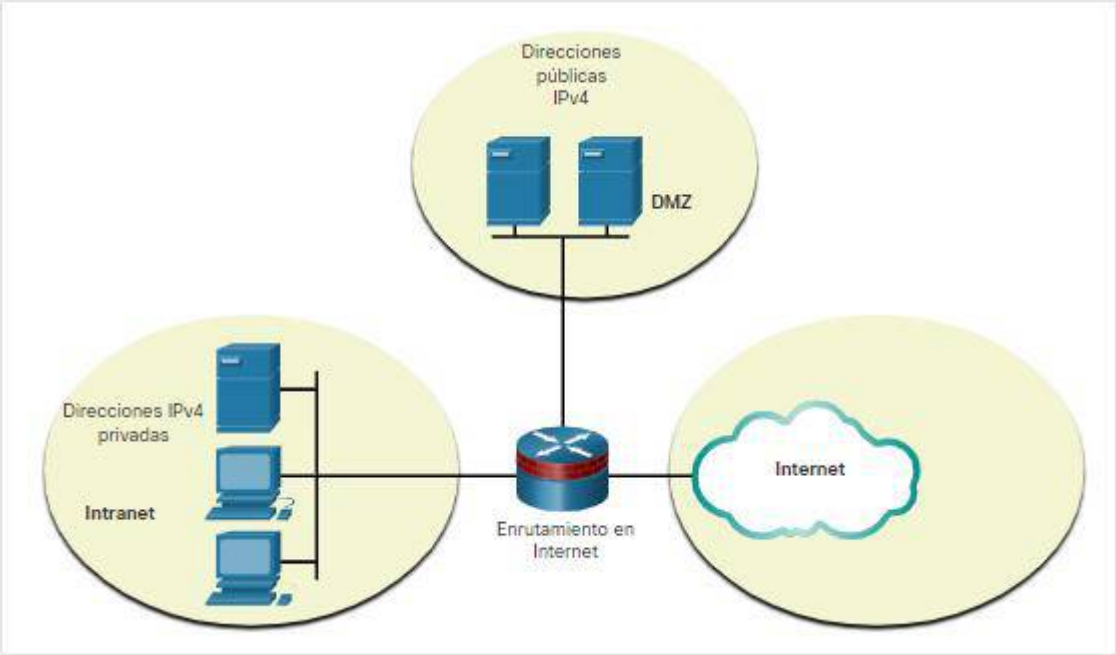
Traducción de direcciones de red (NAT), para utilizar direcciones IP privadas



Antes de que el ISP pueda reenviar este paquete, debe traducir la dirección IPv4 de origen, que es una dirección privada, a una dirección IPv4 pública mediante la traducción de direcciones de red (NAT). Se usa la traducción de direcciones de red (NAT) para traducir entre direcciones IPv4 privadas y públicas. Esto generalmente se realiza en el router que conecta la red interna a la red ISP. Las direcciones IPv4 privadas de la intranet de la organización se traducirán a direcciones IPv4 públicas antes de enrutar a Internet.

Nota: Aunque no se puede acceder directamente a un dispositivo con una dirección IPv4 privada desde otro dispositivo a través de Internet, el IETF no considera las direcciones IPv4 privadas o NAT como medidas de seguridad efectivas.

Las organizaciones que tienen recursos disponibles para Internet, como un servidor web, también tendrán dispositivos que tengan direcciones IPv4 públicas. Como se muestra en la figura, esta parte de la red se conoce como DMZ (zona desmilitarizada). El router en la figura no solo realiza enrutamiento, sino que también realiza NAT y actúa como un firewall para la seguridad.



El diagrama es una topología de red que muestra un router en el centro con tres conexiones; una a la Intranet de la empresa, otra a una DMZ y otra a Internet. A la izquierda está la Intranet con dispositivos que usan direcciones IPv4 privadas. En la parte superior, se encuentra la DMZ con dos servidores que utilizan direcciones IPv4 públicas. A la derecha está la nube de Internet. El router está actuando como un firewall y realizando NAT.

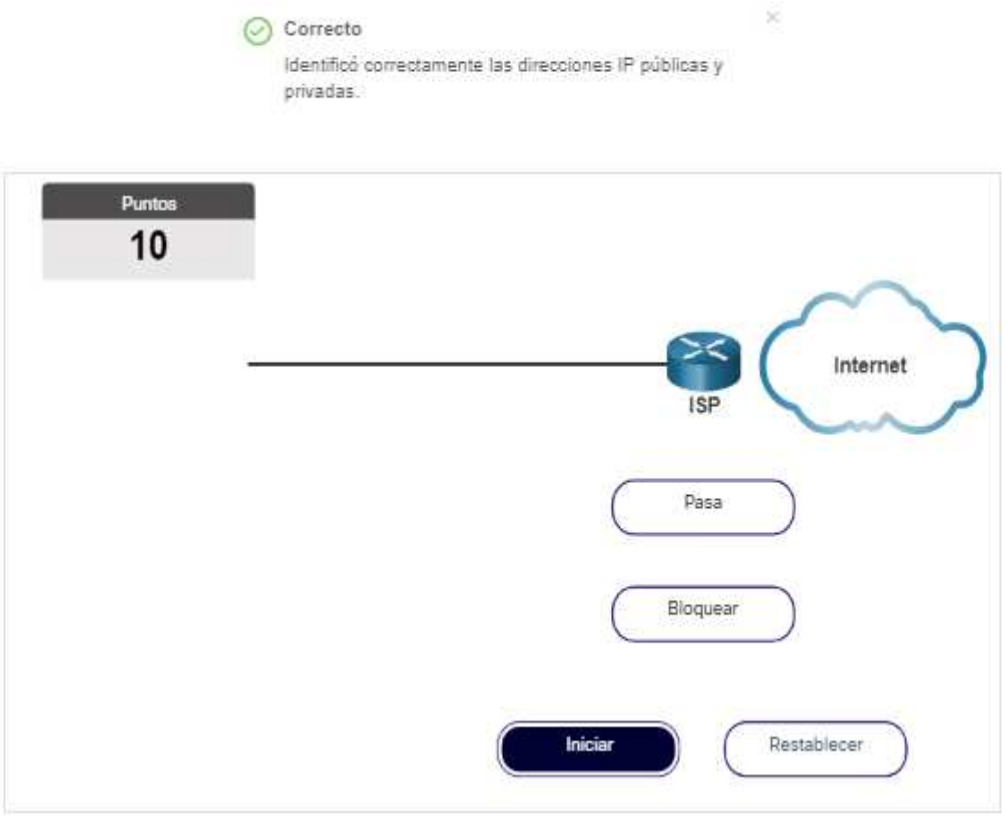
Nota: Las direcciones IPv4 privadas se utilizan comúnmente con fines educativos en lugar de utilizar una dirección IPv4 pública que probablemente pertenezca a una organización.

11.3.3

Actividad: Admitir o bloquear direcciones IPv4

Instrucciones:

Decida admitir o bloquear cada dirección IP según si es pública (Internet) o privada (red local pequeña). Haga clic en Inicio para comenzar y haga clic en Pase o Bloquear.



11.3.4

Direcciones IPv4 de uso especial

Existen ciertas direcciones, como la dirección de red y la dirección de difusión, que no se pueden asignar a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar dentro de la red.

Direcciones de Loopback

Direcciones de Loopback (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) generalmente identificadas solo como 127.0.0.1, son direcciones especiales que usa un host para dirigir el tráfico hacia sí mismo. Por ejemplo, se puede usar en un host para probar si la configuración TCP/IP funciona, como se muestra en la ilustración. Observe cómo la dirección de loopback 127.0.0.1 responde al comando ping **ping** También observe cómo todas las direcciones de este bloque realizan un bucle invertido hacia el host local, como se muestra con el segundo **ping** ping de la ilustración.

Ping a la interfaz de bucle invertido

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Estadísticas de ping para 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad > ping 127.1.1.1
Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad >
```

Direcciones link-local

Direcciones link-local o direcciones IP privadas automáticas (APIPA) 169.254.0.0/16o 169.254.0.1 a 169.254.255.254 Los utiliza un cliente DHCP de Windows para autoconfigurarse en caso de que no haya servidores DHCP disponibles. Las direcciones locales de vínculo se pueden utilizar en una conexión de punto a punto, pero no se utilizan comúnmente para este propósito.

11.3.5

Direccionamiento con clase antigua

En 1981, las direcciones IPv4 de Internet se asignaban mediante el direccionamiento con clase, según se define en RFC 790 (https://tools.ietf.org/html/rfc790), Números asignados. A los clientes se les asignaba una dirección de red basada en una de tres clases: A, B o C. RFC dividía los rangos de unidifusión en las siguientes clases específicas:

- **Clase A (0.0.0.0/8 a 127.0.0.0/8)**: diseñada para admitir redes extremadamente grandes, con más de 16 millones de direcciones de host. La clase A utilizó un prefijo fijo / 8 con el primer octeto para indicar la dirección de red y los tres octetos restantes para las direcciones de host (más de 16 millones de direcciones de host por red).
- **Clase B (128.0.0.0 /16 - 191.255.0.0 /16)**: diseñada para satisfacer las necesidades de redes de tamaño moderado a grande, con hasta 65000 direcciones de host. La clase B utilizó un prefijo fijo / 16 con los dos octetos de alto orden para indicar la dirección de red y los dos octetos restantes para las direcciones de host (más de 65,000 direcciones de host por red).

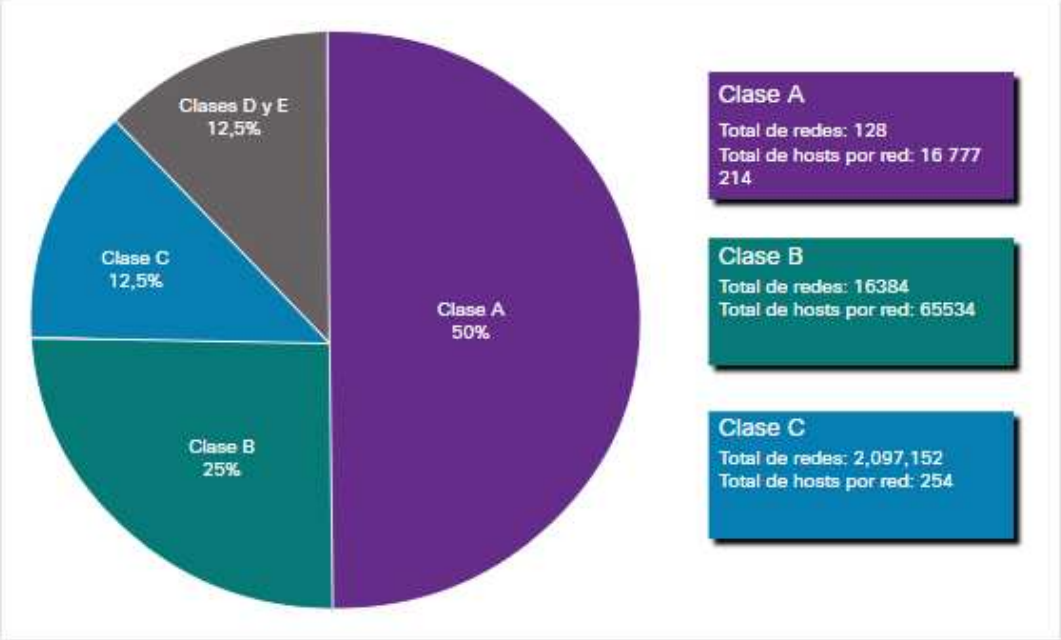
- **Clase C (192.0.0.0 /24 - 223.255.255.0 /24)** - diseñada para admitir redes pequeñas con un máximo de 254 hosts. La clase C utilizó un prefijo fijo / 24 con los primeros tres octetos para indicar la red y el octeto restante para las direcciones de host (solo 254 direcciones de host por red).

Nota: También existe un bloque de multidifusión de clase D que va de 224.0.0.0 a 239.0.0.0, y un bloque de direcciones experimentales de clase E que va de 240.0.0.0 a 255.0.0.0.

En ese momento, con un número limitado de computadoras que utilizan Internet, el direccionamiento con clase era un medio eficaz para asignar direcciones. Como se muestra en la figura, las redes de clase A y B tienen un número muy grande de direcciones de host y la clase C tiene muy pocas. Las redes de clase A representaron el 50% de las redes IPv4. Esto hizo que la mayoría de las direcciones IPv4 disponibles no se utilizaran.

El diagrama es un gráfico circular que muestra el porcentaje de direcciones IPv4 de clase A, B, C, D y E con el número total de redes y hosts por redes de clase A, B y C. Los porcentajes son: clase A = 50%, clase B = 25%, clase C = 12,5%, y clase D y E = 12,5%. Para el número total de redes y número total de hosts por red: clase A = 128 redes con 16.777.214 hosts totales por red; clase B = 16.384 redes con 65.534 hosts totales por red; y clase C = 2.097.152 redes con 254 hosts totales por red.

Resumen de asignación de direcciones con distinción de clases



A mediados de la década de 1990, con la introducción de la World Wide Web (WWW), el direccionamiento de clase fue obsoleto para asignar de manera más eficiente el limitado

espacio de direcciones IPv4. La asignación de direcciones con clase se reemplazó con direcciones sin clase, que se usa hoy en día. El direccionamiento sin clases ignora las reglas de las clases (A, B, C). Las direcciones de red IPv4 públicas (direcciones de red y máscaras de subred) se asignan en función del número de direcciones que se pueden justificar.

11.3.6

Asignación de direcciones IP

Las direcciones IPv4 públicas son direcciones en las que se realiza routing globalmente entre los routers ISP. Las direcciones IPv4 públicas deben ser únicas.

Tanto las direcciones IPv4 como las IPv6 son administradas por la Autoridad de Números Asignados a Internet (Internet Assigned Numbers Authority, IANA) (La IANA administra y asigna bloques de direcciones IP a los Registros Regionales de Internet (RIR). Los cinco RIR se muestran en la figura.

Los RIR se encargan de asignar direcciones IP a los ISP, quienes a su vez proporcionan bloques de direcciones IPv4 a las organizaciones y a los ISP más pequeños. Las organizaciones pueden obtener sus direcciones directamente de un RIR, según las políticas de ese RIR.

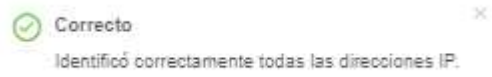
Registros regionales de Internet

11.3.7

Actividad: Direcciones IPv4 públicas o privadas

Instrucciones:

Haga clic en la flecha desplegable de cada dirección para elegir el tipo de red correcto «Público» o «Privado» para cada dirección.



Elija el tipo de red correcto «Público» o «Privado» para cada dirección

172.16.35.2	Pública	**Privada**
192.168.3.5	Pública	**Privada**
192.0.3.15	**Pública**	Privada
64.104.0.22	**Pública**	Privada
209.165.201.30	**Pública**	Privada
192.168.11.5	Pública	**Privada**
172.16.30.30	Pública	**Privada**
10.55.3.168	Pública	**Privada**

11.3.8

Verifique su comprensión - Tipos de direcciones IPv4

Verifique su comprensión de la Estructura de direcciones IPv4 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Las direcciones IPv4 privadas se asignan a dispositivos dentro de la intranet de una organización (red interna) y cualquier organización (hogar, escuela, oficina, empresa) puede usar la dirección 10.0.0.0/8.
2. Para acceder a un dispositivo a través de Internet, la dirección IPv4 de destino debe ser una dirección pública. El agotamiento de direcciones IPv4 públicas es una razón por la que hay direcciones IPv4 privadas y por qué las organizaciones están en transición a IPv6.
3. Los RIR reciben direcciones IP de IANA y son responsables de asignar estas direcciones a los ISP y a algunas otras organizaciones.

Has tenido 3 respuestas correctas de 3.

Correct

You have successfully identified the correct answers.

1. Private IPv4 addresses are assigned to devices within an organization's intranet (internal network) and any organization (home, school, office, company) can use the 10.0.0.0/8 address.
2. To access a device over the internet, the destination IPv4 address must be a public address. Public IPv4 address exhaustion is a reason why there are private IPv4 address and why organizations are transitioning to IPv6.
3. RIRs receive IP addresses from IANA and are responsible for allocating these addresses to ISPs and some other organizations.

You got 3 out of 3 questions correct.

1. ¿Cuáles dos declaraciones son correctas acerca de las direcciones IPv4 privadas? (Escoja dos opciones).

¡Lo tienes!

- [x] Las direcciones IPv4 privadas se asignan a dispositivos dentro de la intranet de una organización (red interna).
- [ ] Los routeres de Internet normalmente reenvían cualquier paquete con una dirección de destino que sea una dirección IPv4 privada.
- [ ] 172.99.1.1 es una dirección IPv4 privada.
- [x] Cualquier organización (hogar, escuela, oficina, empresa) puede usar la dirección 10.0.0.0/8.

2. ¿Cuáles dos instrucciones son correctas acerca de las direcciones IPv4 públicas? (Escoja dos opciones).

¡Lo tienes!

- [ ] Se permite asignar direcciones IPv4 públicas a dispositivos dentro de la intranet de una organización (red interna).
- [x] Para acceder a un dispositivo a través de Internet, la dirección IPv4 de destino debe ser una dirección pública.
- [ ] 192.168.1.10 es una dirección IPv4 pública.
- [x] El agotamiento de direcciones IPv4 públicas es una razón por la que hay direcciones IPv4 privadas y por qué las organizaciones están en transición a IPv6.

3. ¿Qué organización o grupo de organizaciones recibe direcciones IP de IANA y es responsable de asignar estas direcciones a los ISP y a algunas organizaciones?

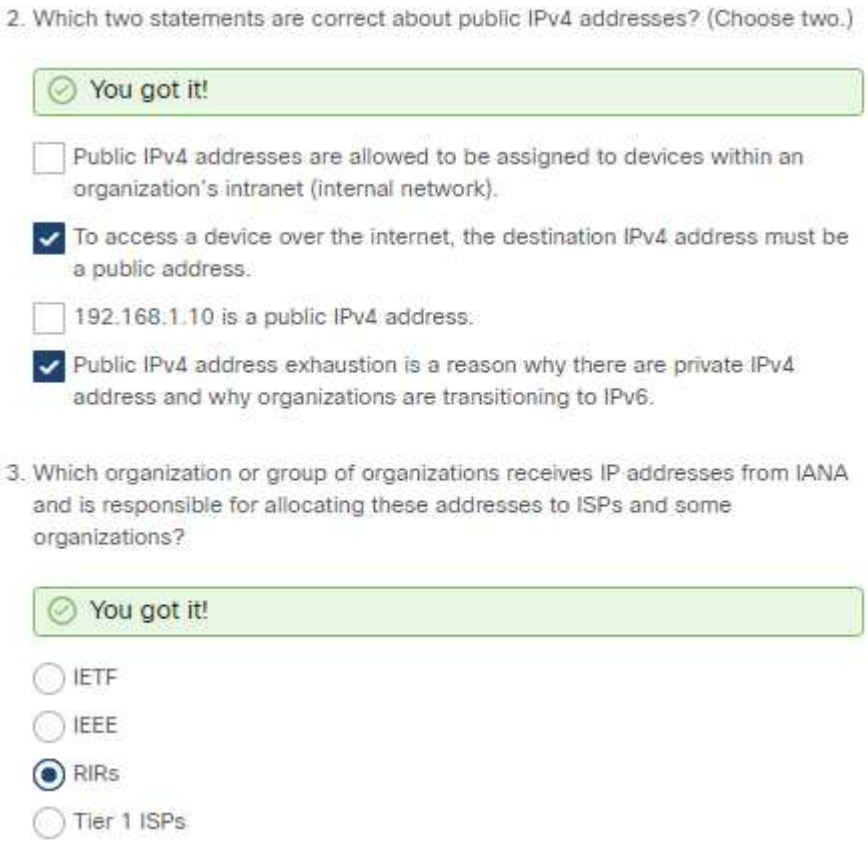
¡Lo tienes!

- ( ) IETF
- ( ) IEEE
- (•) RIR
- ( ) ISP de nivel 1

1. Which two statements are correct about private IPv4 addresses? (Choose two.)

You got it!

- [x] Private IPv4 addresses are assigned to devices within an organization's intranet (internal network).
- [ ] Internet routers will typically forward any packet with a destination address that is a private IPv4 address.
- [ ] 172.99.1.1 is a private IPv4 address.
- [x] Any organization (home, school, office, company) can use the 10.0.0.0/8 address.



Segmentación de la red

11.4.1

Dominios de difusión y segmentación

¿Ha recibido alguna vez un correo electrónico dirigido a todas las personas de su trabajo o escuela? Este era un email de transmisión. Con suerte, contenía información que cada uno de ustedes necesitaba saber. Pero a menudo una transmisión no es realmente pertinente para todos en la lista de correo. A veces, sólo un segmento de la población necesita leer esa información.

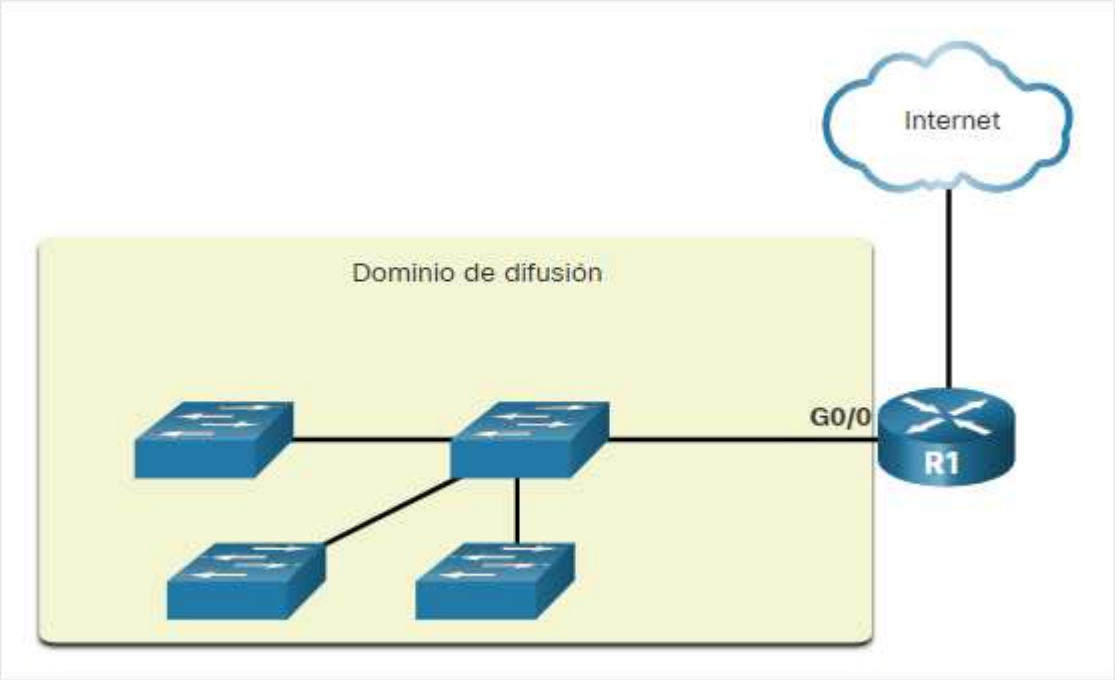
En una LAN Ethernet, los dispositivos utilizan difusiones y el Protocolo de resolución de direcciones (ARP) para localizar otros dispositivos. ARP envía transmisiones de capa 2 a una dirección IPv4 conocida en la red local para descubrir la dirección MAC asociada. Los dispositivos de LAN Ethernet también localizan otros dispositivos que utilizan servicios. Un

host normalmente adquiere su configuración de dirección IPv4 utilizando el Protocolo de configuración dinámica de host (DHCP) que envía transmisiones en la red local para localizar un servidor DHCP.

Los switches propagan las difusiones por todas las interfaces, salvo por aquella en la cual se recibieron. Por ejemplo, si un switch de la ilustración recibiera una difusión, la reenviaría a los demás switches y a otros usuarios conectados en la red.

Un router, R1, está conectado a un switch a través de la interfaz G0/0. El switch está conectado a tres otros switches. El dominio de difusión consiste en los cuatro conmutadores y la interfaz del router a la que están conectados. Una conexión desde el router a Internet no está dentro del dominio de difusión.

Dominios de difusión de segmentos de router



Los routers no propagan difusiones. Cuando un router recibe una difusión, no la reenvía por otras interfaces. Por ejemplo, cuando el R1 recibe una difusión en la interfaz Gigabit Ethernet 0/0, no la reenvía por otra interfaz.

Por lo tanto, cada interfaz de router se conecta a un dominio de transmisión y las transmisiones solo se propagan dentro de ese dominio de transmisión específico.

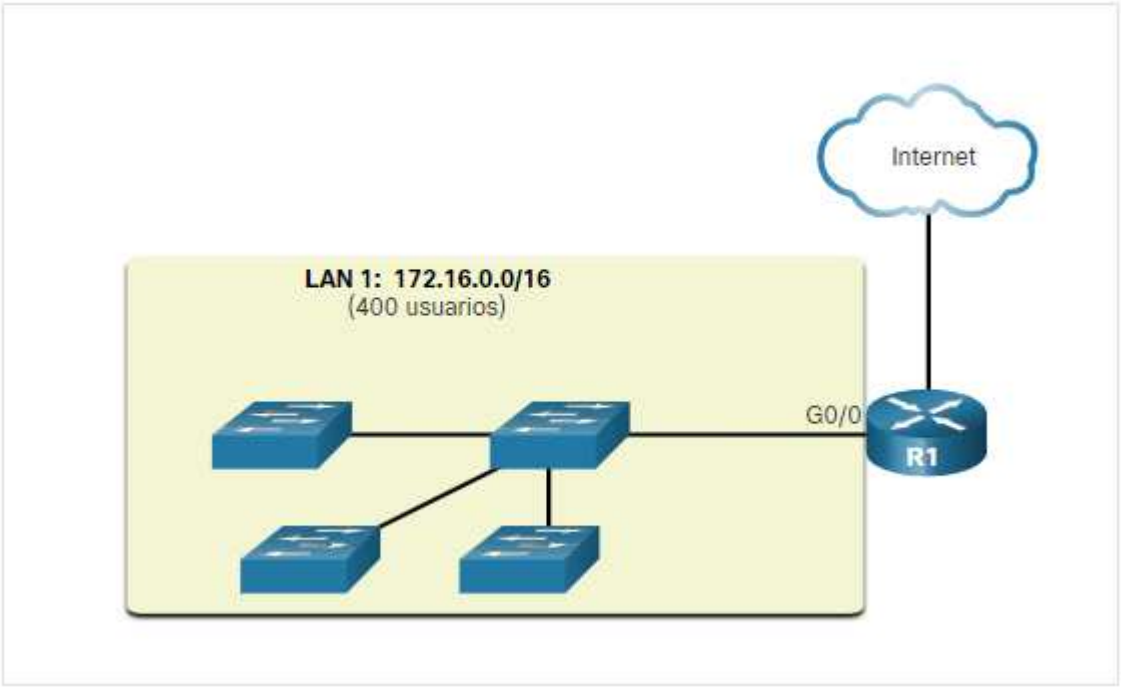
11.4.2

Problemas con los dominios de difusión grandes

Un dominio de difusión grande es una red que conecta muchos hosts. Un problema con un dominio de difusión grande es que estos hosts pueden generar difusiones excesivas y afectar la red de manera negativa. En la figura, LAN 1 conecta a 400 usuarios que podrían generar una cantidad excesiva de tráfico de difusión. Esto da como resultado operaciones de red lentas debido a la cantidad significativa de tráfico que puede causar, y operaciones de dispositivo lentas porque un dispositivo debe aceptar y procesar cada paquete de difusión.

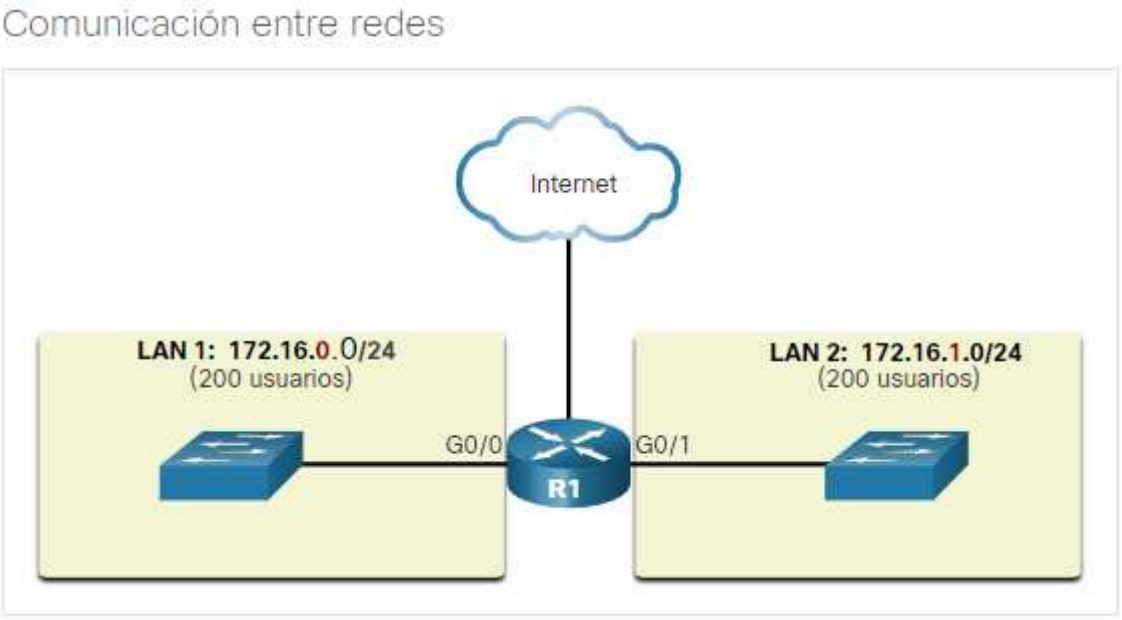
Un router, R1, está conectado a un switch a través de la interfaz G0/0. El switch está conectado a tres otros switches. El dominio de difusión consiste en los cuatro conmutadores y la interfaz del router a la que están conectados. Esto se identifica como LAN1 con una dirección de 172.16.0.0/16. Una conexión desde el enrutador a Internet no está dentro del dominio de difusión.

Un dominio de difusión amplio



La solución es reducir el tamaño de la red para crear dominios de difusión más pequeños mediante un proceso que se denomina división en subredes. Estos espacios de red más pequeños se denominan subredes.

En la figura, los 400 usuarios en LAN 1 con la dirección de red 172.16.0.0 / 16 se han dividido en dos subredes de 200 usuarios cada una: 172.16.0.0 / 24 y 172.16.1.0 / 24. Las difusiones solo se propagan dentro de los dominios de difusión más pequeños. Por lo tanto, una transmisión en LAN 1 no se propagaría a LAN 2.



Un router, R1, está conectado a dos LAN que representan dos dominios de difusión diferentes. Conectado a la izquierda a través de G0/0 hay un conmutador que admite 200 usuarios en LAN 1 con una dirección de red 172.16.0.0/24. Conectado a la derecha a través de G0/1 hay un conmutador que admite 200 usuarios en LAN 2 con una dirección de red 172.16.1.0/24.

Observe cómo la longitud del prefijo ha cambiado de una sola red /16 a dos /24 redes. Esta es la base de la división en subredes: el uso de bits de host para crear subredes adicionales.

Nota: Los términos subred y red a menudo se usan indistintamente. La mayoría de las redes son una subred de un bloque de direcciones más grande.

11.4.3

Razones para segmentar redes

La división en subredes disminuye el tráfico de red general y mejora su rendimiento. A su vez, le permite a un administrador implementar políticas de seguridad, por ejemplo, qué subredes están habilitadas para comunicarse entre sí y cuáles no lo están. Otra razón es que reduce el número de dispositivos afectados por el tráfico de difusión anormal debido a

configuraciones incorrectas, problemas de hardware o software o intenciones malintencionadas.

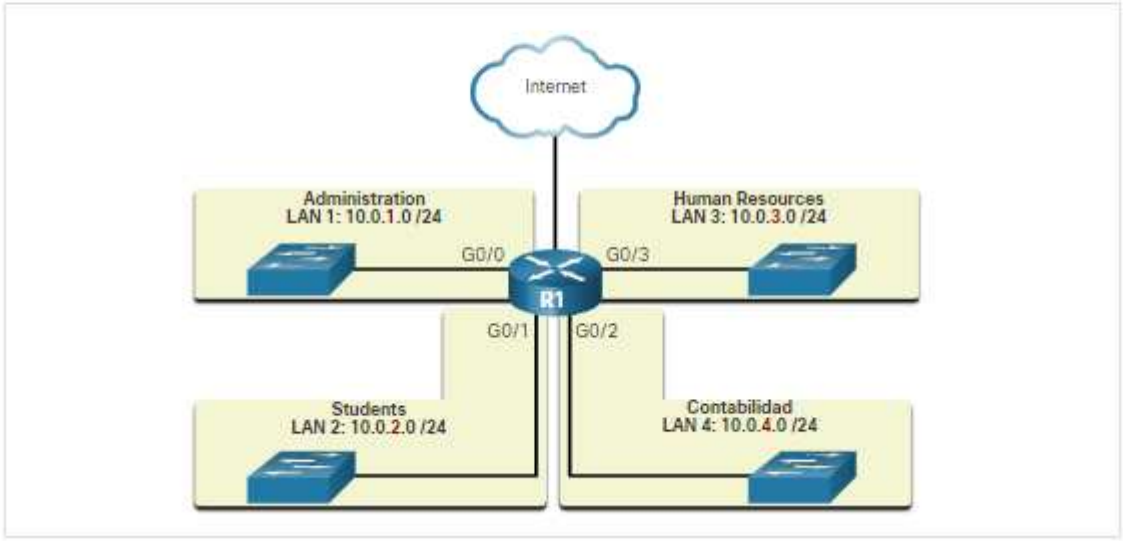
Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.

División en subredes por ubicación

El diagrama muestra un edificio de cinco plantas con un interruptor en cada planta. Cada switch está en una LAN/subred diferente con una dirección de red diferente, todos conectados al mismo router, R1, a través de una interfaz Gigabit Ethernet diferente. Las siguientes subredes se muestran desde el primer hasta el quinto piso: LAN 1 tiene una dirección de red de 10.0.1.0/24 y está conectada a G0/0; LAN 2 tiene una dirección de red de 10.0.2.0/24 y está conectada a G0/1; LAN 3 tiene una dirección de red de 10.0.3.0/24 y está conectada a G0/2; LAN 4 tiene una dirección de red de 10.0.4.0/ 24 y está conectado a G0/3; y LAN 5 tiene una dirección de red de 10.0.5.0/24 y está conectado a G0/4. R1 también tiene una conexión a Internet.

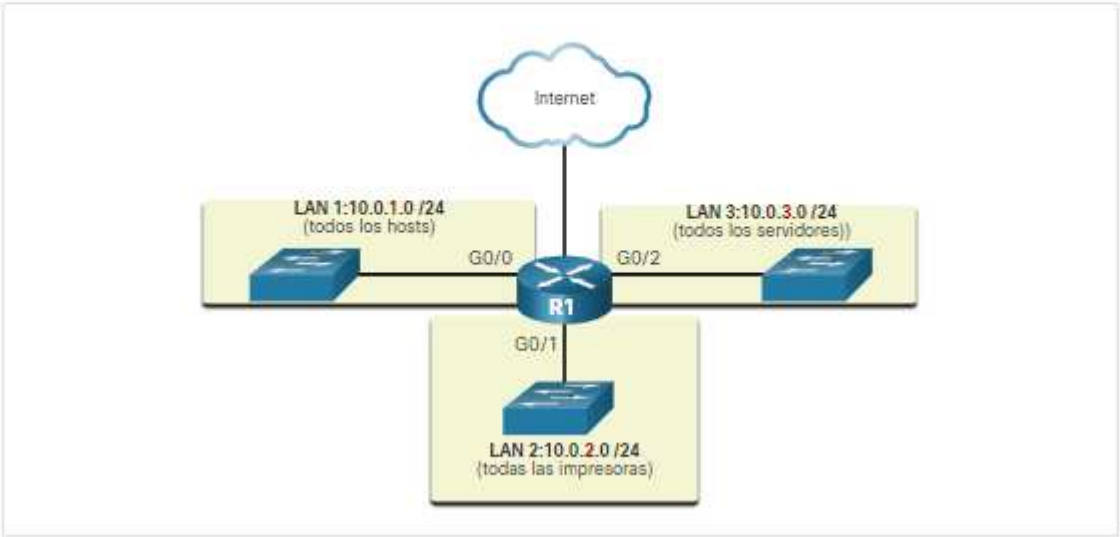
Ubicación | Grupo o función | Tipo de dispositivo

Subredes por grupo o función



Ubicación | Grupo o función | Tipo de dispositivo

Tipo de dispositivo para Subnetting



Los administradores de red pueden crear subredes utilizando cualquier otra división que tenga sentido para la red. Observe que, en cada ilustración, las subredes usan longitudes de prefijo más largas para identificar las redes.

Entender cómo dividir redes en subredes es una aptitud fundamental que deben tener todos los administradores de redes. Se desarrollaron diversos métodos que contribuyen a la comprensión de este proceso. Aunque un poco abrumador al principio, preste mucha atención a los detalles y, con práctica, la división en subredes será más fácil.

11.4.4

Verifique su comprensión - Segmentación de red

Verifique su comprensión de la segmentación de la red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Los routeres no reenviarán un paquete de difusión IPv4 de forma predeterminada.
2. Las operaciones de red lentas y las operaciones lentas del dispositivo son el resultado del tráfico de difusión excesivo.

Has tenido 2 respuestas correctas de 2.

1. ¿Cuál dispositivo no reenviará un paquete de difusión IPv4 de forma predeterminada?

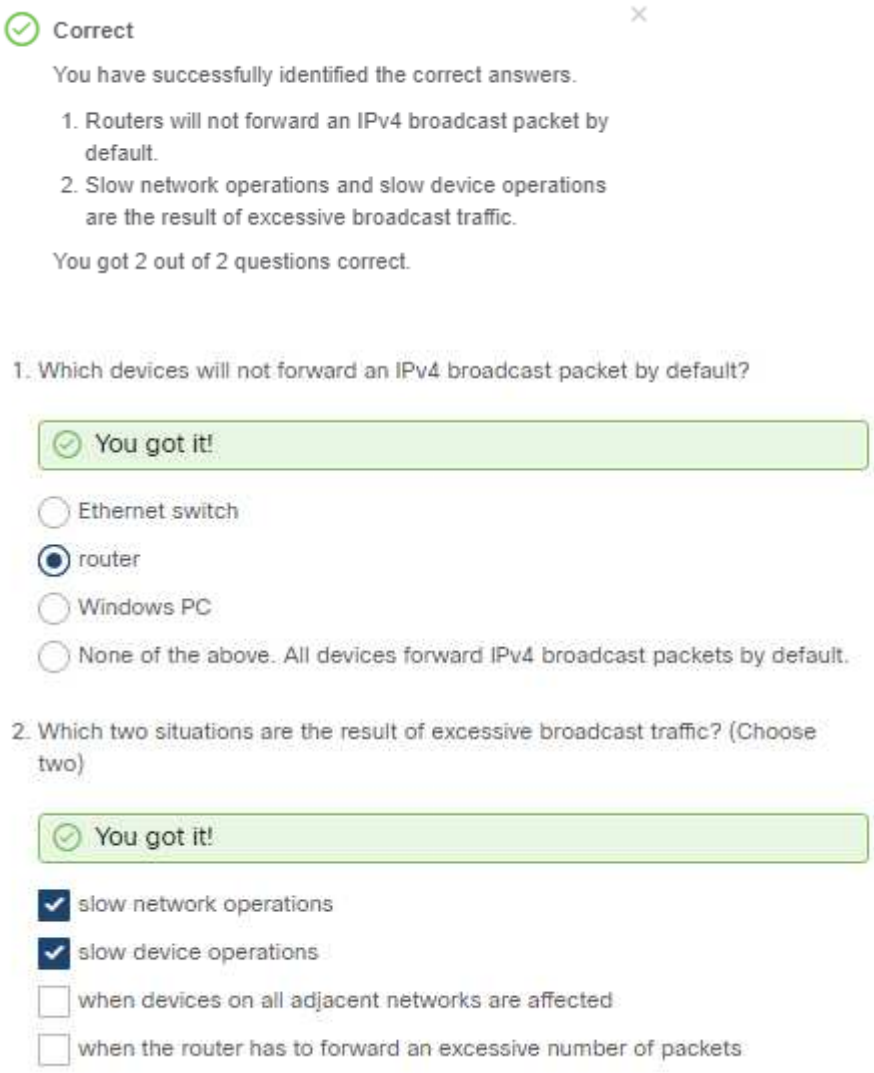
¡Lo tienes!

- ○ Switch Ethernet
- ◉ Router
- ○ PC con Windows
- ○ Ninguna de las opciones anteriores. Todos los dispositivos reenvían paquetes de difusión IPv4 de forma predeterminada.

2. ¿Cuáles dos situaciones son el resultado del tráfico de difusión excesivo? Elija dos opciones.

¡Lo tienes!

- ☑ operaciones de red lentas
- ☑ operaciones lentas del dispositivo
- ☐ cuando los dispositivos de todas las redes adyacentes se ven afectados
- ☐ cuando el router tiene que reenviar un número excesivo de paquetes



Asignación de direcciones IPv4 / División de subredes de una red IPv4

División de subredes de una red IPv4

11.5.1

División en subredes en el límite del octeto

En el tema anterior aprendiste varias buenas razones para segmentar una red. También ha aprendido que la segmentación de una red se denomina subred. La subred es una habilidad

crítica a tener al administrar una red IPv4. Es un poco desalentador al principio, pero se hace mucho más fácil con la práctica.

Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red. Esto se realiza por medio de la ampliación de la máscara de subred para que tome prestados algunos de los bits de la porción de host de la dirección a fin de crear bits de red adicionales. Cuantos más bits de host se tomen prestados, mayor será la cantidad de subredes que puedan definirse. Cuantos más bits se prestan para aumentar el número de subredes reduce el número de hosts por subred.

Las redes se subdividen con más facilidad en el límite del octeto de /8 /16 y /24. La tabla identifica estas longitudes de prefijo. Observe que el uso de longitudes de prefijo más extensas disminuye la cantidad de hosts por subred.

Máscaras de subred en límites de octeto

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n=red, h=host)	# de hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16777214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Comprender cómo ocurre la división en subredes en el límite del octeto puede ser de utilidad. En el siguiente ejemplo, se muestra este proceso. Suponga que una empresa eligió como su dirección de red interna la dirección privada 10.0.0.0/8. Dicha dirección de red puede conectar 16777214 hosts en un dominio de difusión. Obviamente, tener más de 16 millones de hosts en una sola subred no es ideal.

La empresa podría subdividir aún más la dirección 10.0.0.0/8 en el límite de octeto de / 16 como se muestra en la tabla. Esto proporcionaría a la empresa la capacidad de definir hasta 256 subredes (es decir, 10.0.0.0/16 - 10.255.0.0/16) con cada subred capaz de conectar 65.534 hosts Observe cómo los primeros dos octetos identifican la porción de red de la dirección, mientras que los dos últimos octetos son para direcciones IP de host.

Red de subredes 10.0.0.0/8 usando un /16

Dirección de subred (256 subredes posibles)	Rango de host (65.534 posibles hosts por subred)	Dirección
10.0.0.0/16	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/16	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/16	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10,3,0.0/16	**10,3**0,1 - **10,3**.255.254	**10.3**.255.255
10,4,0.0/16	**10,4**,0,1 - **10,4**,255,254	**10.4**.255.255
10,5,0.0/16	**10,5**,0,1 - **10,5**,255,254	**10.5**.255.255
10,6,0.0/16	**10,6**,0,1 - **10,6**.255.254	**10.6**.255.255
10,7,0.0/16	**10,7**,0,1 - **10,7**,255,254	**10.7**.255.255
...	...	...
10.255.0.0/16	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Alternativamente, la empresa podría elegir subred la red 10.0.0.0/8 en el límite de / 24 octetos, como se muestra en la tabla. Esto le permitiría a la empresa definir 65536 subredes, cada una capaz de conectar 254 hosts. El uso del límite /24 está muy difundido en la división en subredes debido a que admite una cantidad razonable de hosts y permite dividir en subredes en el límite del octeto de manera conveniente.

Red de subredes 10.0.0.0/8 mediante un prefijo /24

Dirección de subred (65,536 subredes posibles)	Rango de host (254 posibles hosts por subred)	Dirección
10.0.0.0/24	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/24	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/24	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
...	...	...
10.0.255.0/24	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/24	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/24	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/24	**10.1.2**.1 - **10.1.2**254	**10.1.2**.255
...	...	...
10.100,0.0/24	**10,100,0**,1 - 10,100,0 ,254	**10.100,0**.255
...	...	...
10.255.255.0/24	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

11.5.2

Subred dentro de un límite de octeto

Los ejemplos mostrados hasta ahora tomaron prestados bits de host de los prefijos de red comunes /8, /16 y /24. Sin embargo, las subredes pueden tomar prestados bits de cualquier posición de bit de host para crear otras máscaras.

Por ejemplo, una dirección de red /24 se suele dividir en subredes con longitudes de prefijo más extensas al tomar prestados bits del cuarto octeto. Esto le proporciona al administrador mayor flexibilidad al asignar direcciones de red a un número menor de terminales.

Consulte la tabla para ver seis formas de subred una red /24.

Subred a / 24 Red

Longitud de prefijo	Máscara de subred	Máscara de subred en binario (n = network, h = host)	# de subredes	# de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Por cada bit que se toma prestado en el cuarto octeto, la cantidad de subredes disponible se duplica, al tiempo que se reduce la cantidad de direcciones de host por subred.

- **/25 filas:** - Tomar prestado 1 bit del cuarto octeto crea 2 subredes que admiten 126 hosts cada una.
- **/26 fila** - Tomar prestados 2 bits crea 4 subredes que admiten 62 hosts cada una.
- **/27 fila** - Tomar prestados 3 bits crea 8 subredes que admiten 30 hosts cada una.
- **/28 fila** - Tomar prestados 4 bits crea 16 subredes que admiten 14 hosts cada una.
- **/29 fila** - Tomar prestados 5 bits crea 32 subredes que admiten 6 hosts cada una.
- **/30 fila** - Tomar prestados 6 bits crea 64 subredes que admiten 2 hosts cada una.

11.5.3

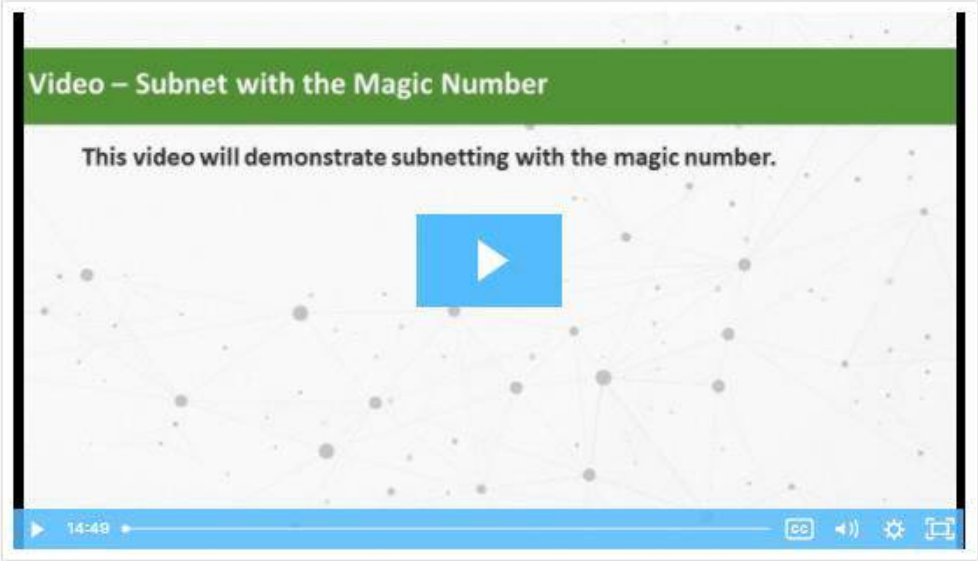
Vídeo: La máscara de subred

Haga clic en Reproducir para ver una explicación de la máscara de subred.

11.5.4

Video - Subred con el número mágico

Haga clic en Reproducir para ver una explicación del número mágico.



11.5.5

Packet Tracer - Subred una red IPv4

En esta actividad, a partir de una única dirección de red y máscara de red, se dividirá la red del Cliente en varias subredes. El esquema de la subred se debe basar en la cantidad de computadoras host requeridas en cada subred y en otras consideraciones de red, como la expansión de hosts de red en el futuro.

Una vez que haya creado un esquema de subred y completado el diagrama de red con las direcciones IP de los hosts y de las interfaces, configurará los equipos host y las interfaces de router, incluidas las interfaces de bucle invertido.

Después de configurar los dispositivos de red y las PC host, utilizará el comando **ping** para probar la conectividad de red.

Subred una red IPv4

Subred una red IPv4

Asignación de direcciones IPv4 / Subred una barra diagonal 16 y un prefijo de barra diagonal 8

Subred una barra diagonal 16 y un prefijo de barra diagonal 8

11.6.1

Crear subredes con un prefijo Slash 16

Algunas subredes son más fáciles que otras subredes. En este tema se explica cómo crear subredes que tengan el mismo número de hosts.

En una situación en la que se necesita una mayor cantidad de subredes, se requiere una red IPv4 con más bits de host para tomar prestados. Por ejemplo, la dirección de red 172.16.0.0 tiene una máscara predeterminada de 255.255.0.0 o /16. Esta dirección tiene 16 bits en la porción de red y 16 bits en la porción de host. Estos 16 bits en la porción de host se pueden tomar prestados para crear subredes. La tabla resalta todos los escenarios posibles para dividir en subredes un prefijo /16.

Subred a / 16 Red

Longitud de prefijo	Máscara de subred	Dirección de red (n = network, h = host)	# de subredes	# de hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	**2**	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	**4**	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	**8**	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	**16**	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	**32**	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	**64**	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	**128**	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	**256**	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	**512**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	**1024**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	**2048**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	**4096**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	**8192**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	**16384**	2

Aunque no es necesario memorizar esta tabla, todavía necesita una buena comprensión de cómo se genera cada valor de la tabla. No se deje intimidar por el tamaño de la tabla. La razón por la que es grande es que tiene 8 bits adicionales que se pueden pedir prestados y, por lo tanto, el número de subredes y hosts es simplemente mayor.

11.6.2

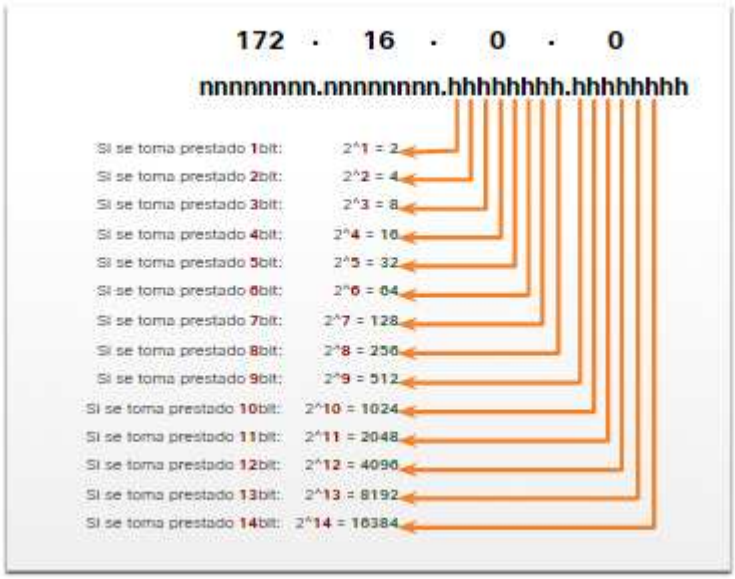
Cree 100 subredes con un prefijo Slash 16

Imagine una gran empresa que requiere, como mínimo, 100 subredes y eligió la dirección privada 172.16.0.0/16 como su dirección de red interna.

Al tomar prestados bits de una dirección /16, comience a tomarlos del tercer octeto, de izquierda a derecha. Tome prestado un solo bit por vez hasta que se alcance la cantidad de bits necesarios para crear 100 subredes.

La figura muestra el número de subredes que se pueden crear al tomar prestados bits del tercer octeto y el cuarto octeto. Observe que ahora hay hasta 14 bits de host que pueden ser prestados.

Cantidad de subredes creadas

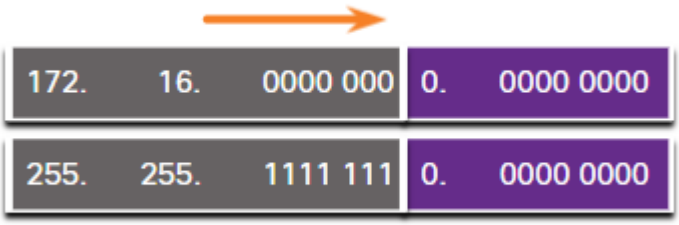


El gráfico muestra cómo calcular el número de subredes creadas al tomar prestados bits del tercer y cuarto octetos de una dirección de red IPv4. La fórmula para determinar el número de subredes creadas es 2 a la potencia del número de bits prestados. El gráfico muestra una dirección de 172.16.0.0. Debajo, están las letras nnnnnnnnnnnnnn.hhhhhhhhhhhhh. Comienza tomando prestado el primer bit h en el tercer octeto que resulta en 2 a la potencia de 1 = 2 subredes. Cuando se toman prestados los primeros dos bits h en el tercer octeto, la fórmula es 2 a la potencia de 2 = 4. Esto continúa hasta que los primeros 14 bits h se toman prestados del tercer y cuarto octetos resultando en 2 a la potencia de 14 = 16384. Los últimos dos bits h en el cuarto octeto siguen siendo los mismos.

Para satisfacer el requisito de 100 subredes para la empresa, se necesitarían prestar 7 bits (es decir, 27 = 128 subredes) (para un total de 128 subredes), como se muestra en la figura.

El gráfico muestra la representación decimal y de bits de una dirección de red, y debajo de ella una máscara de subred, cuando se toman prestados siete bits en el tercer octeto para crear subredes. Los dos primeros octetos se muestran en decimal y los dos últimos se muestran en binario. La dirección de red es 172.16.0000 0000.0000 0000. La máscara de subred es 255.255.1111 1110.0000 0000.

Red 172.16.0.0/23

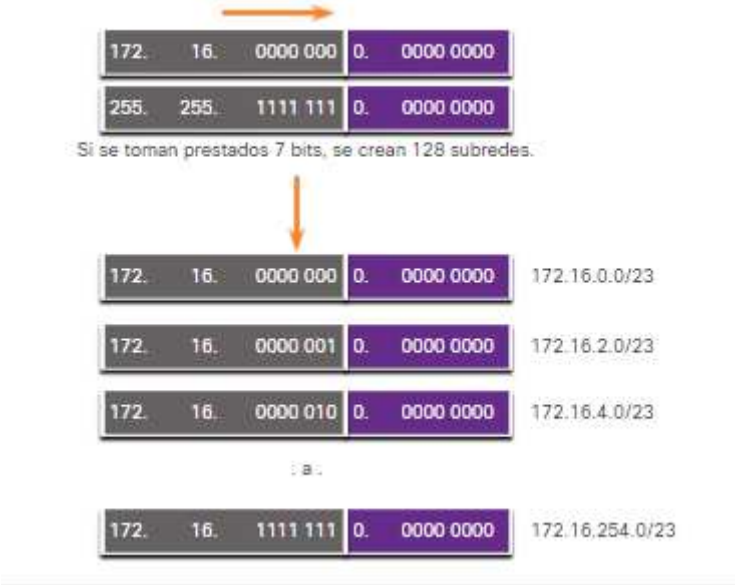


Recuerde que la máscara de subred debe modificarse para que se muestren los bits que se tomaron prestados. En este ejemplo, cuando se toman prestados 7 bits, la máscara se extiende 7 bits en el tercer octeto. En formato decimal, la máscara se representa como 255.255.254.0, o como el prefijo /23, debido a que, en formato binario, el tercer octeto es 11111110 y el cuarto octeto es 00000000.

En la figura 3, se muestran las subredes resultantes desde 172.16.0.0 /23 hasta 172.16.254.0 /23.

El gráfico muestra las subredes creadas cuando se utiliza una máscara de subred /23 con la dirección 172.16.0.0. Primero, muestra la representación decimal y bit de la dirección de red, y debajo de ella la máscara de subred. Los dos primeros octetos se muestran en decimal y los dos últimos se muestran en binario. La dirección de red es 172.16.0000 0000.0000 0000. La máscara de subred es 255.255.1111 1110.0000 0000. Los primeros dos octetos y los primeros siete bits en el tercer octeto están sombreados en gris y el último bit en el tercer octeto y todo el cuarto octeto están sombreados en púrpura. Si se toman prestados 7 bits, se crean 128 subredes. Debajo de eso, muestra las tres primeras subredes y la última subred creada. Nuevamente, los dos primeros octetos se muestran en decimal y los dos últimos se muestran en binario. La primera subred es 172.16.0000 0000.0000 0000 o 172.16.0.0/23. La segunda subred es 172.16.0000 0010.0000 0000 o 172.16.2.0/23. La tercera subred es 172.16.0000 0100.0000 0000 o 172.16.4.0/23. El texto to. se utiliza para mostrar que este proceso continúa hasta llegar a la última subred creada que es 172.16.1111 1110.0000 0000 o 172.16.254.0/23.

Resultado: subredes de /23



Después de tomar prestados 7 bits para la subred, queda un bit de host en el tercer octeto y 8 bits de host en el cuarto octeto, para un total de 9 bits que no fueron prestados. 29 resultados en 512 direcciones de host totales. La primera dirección está reservada para la dirección de red y la última para la dirección de difusión, por lo que restar para estas dos direcciones (29 - 2) equivale a 510 direcciones de host disponibles para cada /23 subred.

Como se muestra en la figura, la primera dirección de host para la primera subred es 172.16.0.1, y la última dirección de host es 172.16.1.254.

El gráfico muestra el rango de direcciones de la subred 172.16.0.0/23. Los dos primeros octetos se muestran en decimal y los dos últimos se muestran en binario, luego la dirección se muestra en su formato decimal punteado. La dirección de red es 172.16.0000 0000.0000 0000 = 172.16.0.0/23. La primera dirección de host es 172.16.0000 0000.0000 0001 = 172.16.0.1/23. La última dirección de host es 172.16.0000 0001.1111 1110 = 172.16.255.254/23 (cambie a 172.16.1.254 cuando esté fijo). La dirección de difusión es 172.16.0000 0001.1111 1111 = 172.16.255.255/23 (cambie a 172.16.1.255 cuando esté fijo).

Intervalo de direcciones para la subred 172.16.0.0/23

11.6.3

Cree 1000 subredes con un prefijo Slash 8

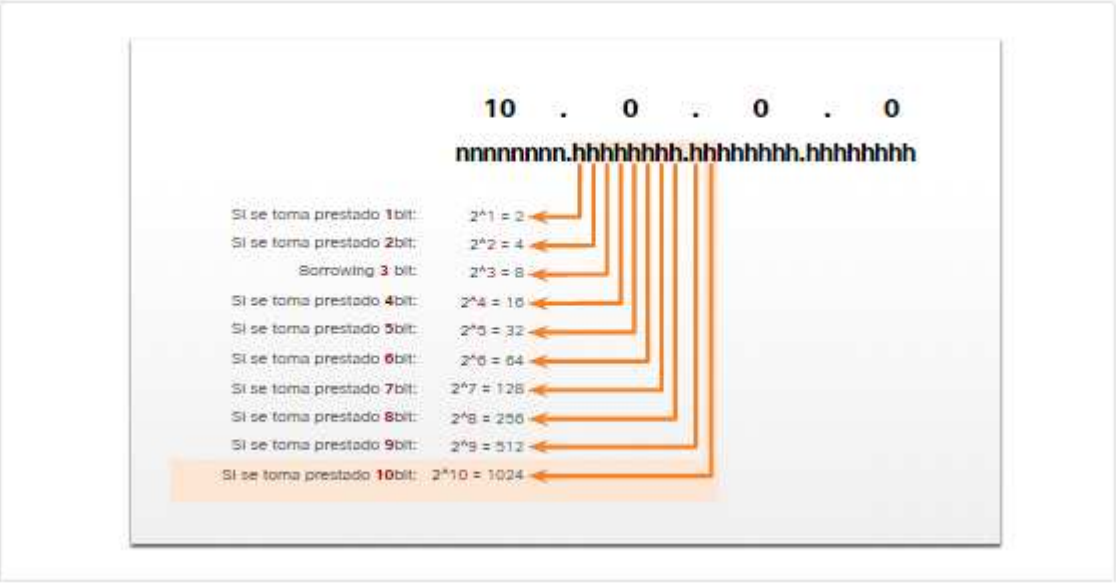
Es posible que algunas organizaciones, como pequeños proveedores de servicios o grandes empresas, puedan necesitar aún más subredes. Por ejemplo, tome un ISP pequeño que requiera 1000 subredes para sus clientes. Cada cliente necesitará mucho espacio en la parte del host para crear sus propias subredes.

El ISP tiene una dirección de red 10.0.0.0 255.0.0.0 o 10.0.0.0/8. Esto significa que hay 8 bits en la porción de red y 24 bits de host disponibles para tomar prestados a fin de realizar la división en subredes. Por lo tanto, el ISP pequeño dividirá la red 10.0.0.0/8 en subredes.

Para crear subredes, debe tomar prestados bits de la parte del host de la dirección IPv4 de la red existente. Comenzando de izquierda a derecha con el primer bit de host disponible, pida prestado un solo bit a la vez hasta alcanzar el número de bits necesarios para crear 1000 subredes. Como se muestra en la figura, debe tomar prestados 10 bits para crear 1024 subredes $(210 = 1024)$. Esto incluye 8 bits en el segundo octeto y 2 bits adicionales del tercer octeto.

El gráfico muestra cómo calcular el número de subredes creadas al tomar prestados bits del segundo y tercer octeto de una dirección de red IPv4. La fórmula para determinar el número de subredes creadas es 2 a la potencia del número de bits prestados. El gráfico muestra una dirección de 10.0.0.0. Debajo, están las letras nnnnnnnn.hhhhhhhhhhhhhhhhhh. Comienza tomando prestado el primer bit h en el segundo octeto que resulta en 2 a la potencia de 1 = 2 subredes. Cuando se toman prestados los primeros dos bits h en el segundo octeto, la fórmula es 2 a la potencia de 2 = 4. Esto continúa hasta que los primeros bits de 10 h se toman prestados del segundo y tercer octeto, resultando en 2 a la potencia de 10 = 1024.

Cantidad de subredes creadas

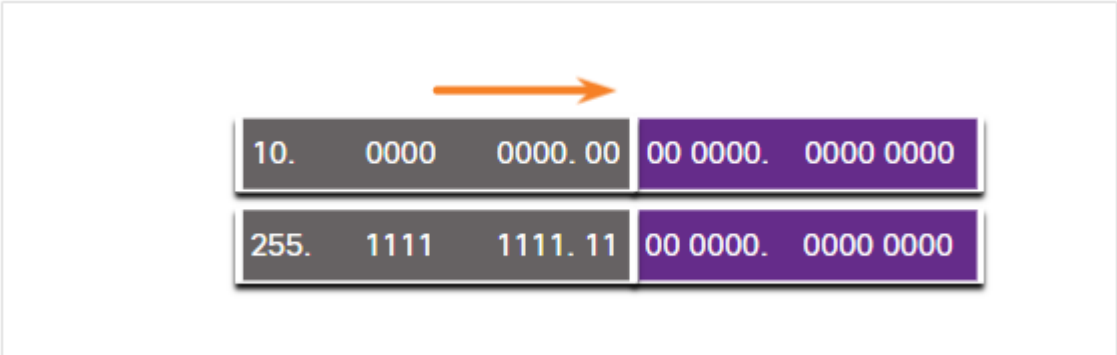


En la figura 2, se muestra la dirección de red y la máscara de subred resultante, la cual se convierte en 255.255.192.0 o un prefijo /18.

El gráfico muestra la representación decimal y de bits de una dirección de red, y debajo de ella una máscara de subred, cuando se toman prestados 10 bits en el segundo y tercer octetos para crear subredes. El primer octeto se muestra en decimal y los últimos tres octetos se muestran en binario. La dirección de red es 10.1111 1111.1100 0000.0000 0000 (debe ser 10.0000 0000.0000 0000 0000 cuando está fijo). La máscara de subred es 255.255.1111 1110.0000 0000.

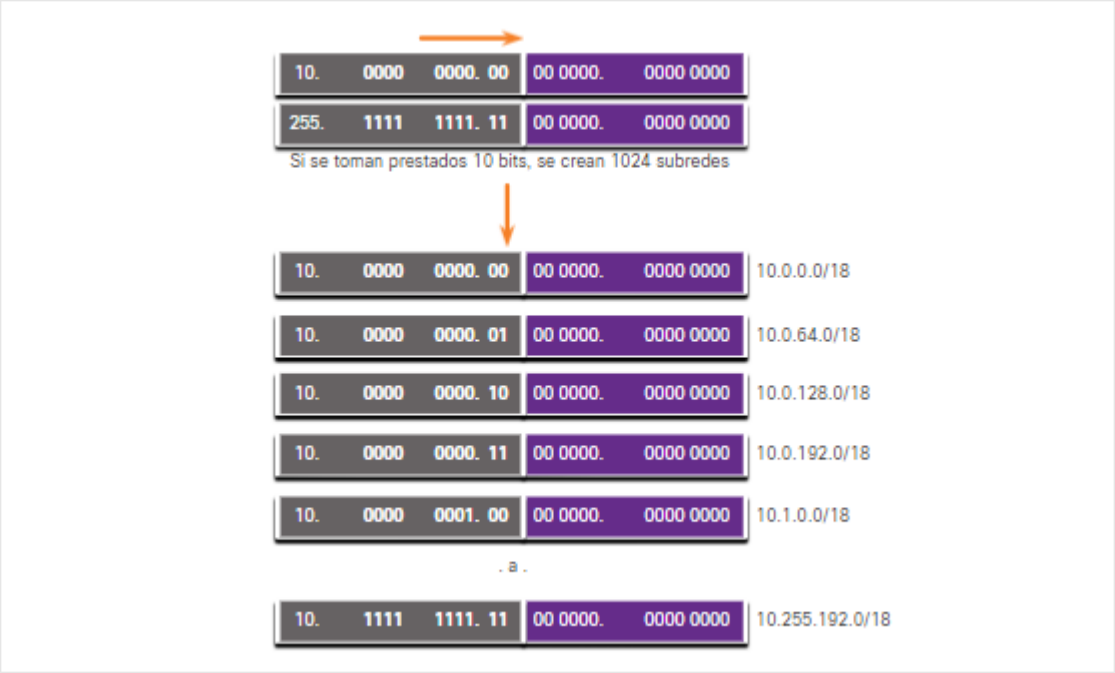
Red 10.0.0.0/18

Esta figura muestra las subredes resultantes de tomar prestados 10 bits, creando subredes de 10.0.0.0/18 a 10.255.128.0/18.



El gráfico muestra las subredes creadas cuando se utiliza una máscara de subred /18 con la dirección 10.0.0.0. Primero, muestra la representación decimal y bit de la dirección de red, y debajo de ella la máscara de subred. El primer octeto se muestra en decimal y los últimos tres octetos se muestran en binario. La dirección de red es 10.0000 0000.0000 0000.0000 0000. La máscara de subred es 255.1111 1111.1100 0000.0000 0000. El primer octeto y los siguientes 10 bits están sombreados en gris y los bits restantes están sombreados en púrpura. A continuación, el texto dice: pedir prestados 10 bits crea 1024 subredes. Debajo de eso, muestra las primeras cinco subredes y la última subred creada. Nuevamente, el primer octeto se muestra en decimal y los últimos tres octetos se muestran en binario. La primera subred es 10.0000 0000.0000 0000 0000 o 10.0.0.0/18. La segunda subred es 10.0000 0000.0100 0000.0000 0000 o 10.0.64.0/18. La tercera subred es 10.0000 0000.1000 0000.0000 0000 o 10.0.128.0/18. La cuarta subred es 10.0000 0000.1100 0000.0000 0000 o 10.0.192.0/18. La quinta subred es 10.0000 0001.0000 0000.0000 o 10.1.0.0/18. El texto to, se utiliza para mostrar que este proceso continúa hasta llegar a la última subred creada que es 10.1111 1111.1100 0000.0000 0000 o 10.255.192.0/18.

Subredes /18 resultantes



Prestar 10 bits para crear las subredes, deja 14 bits host para cada subred. Restar dos hosts por subred (uno para la dirección de red y otro para la dirección de difusión) equivale a 214 - 2 = 16382 hosts por subred. Esto indica que cada una de las 1000subredes puede admitir hasta 16382 hosts.

Esta figura muestra los detalles de la primera subred.

El gráfico muestra el rango de direcciones de la subred 10.0.0.0/18. El primer octeto se muestra en decimal y los últimos tres octetos se muestran en binario, luego la dirección se muestra en su formato decimal punteado. La dirección de red es 10.0000 0000.0000 0000.0000 0000 = 10.0.0.0/18. La primera dirección de host es 10.0000 0000.0000 0000.0000

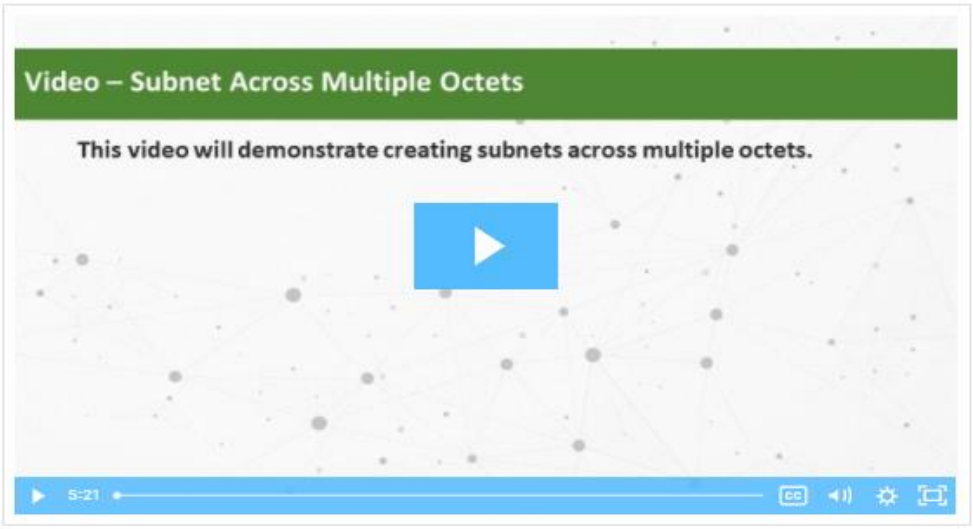
0001 = 10.0.0.1/18. La última dirección de host es 10.0000 0000.0011 1111.1111 1110 = 10.0.63.254/18. La dirección de difusión es 10.0000 0000.0011 1111. 1111 1111 = 10,0,63.255/18.

Intervalo de direcciones para la subred 10.0.0.0/18

11.6.4

Video: subred en varios octetos

Haga clic en Reproducir para ver una explicación de cómo usar el número mágico a través de los límites de los octetos.



11.6.5

Actividad: Cálculo de máscara de subred

Instrucciones:

En esta actividad, se le da una máscara de subred en formato decimal. Introduzca la representación binaria de la máscara de subred en los campos de octetos proporcionados. Además, convierta la máscara al formato de notación de prefijo en el campo Notación de prefijo.

Correcto

Convirtió correctamente la máscara de subred a los formatos binario y de notación de prefijo. Haga clic en Nuevo problema para continuar.

Máscara de subred	255	255	255	248
Máscara de subred en formato binario	11111111	11111111	11111111	11111000
Notación de prefijo	/	29		

Verificar | Nuevo problema | Mostrar | Restablecer

Correcto

Convirtió correctamente la máscara de subred a los formatos binario y de notación de prefijo. Haga clic en Nuevo problema para continuar.

Máscara de subred	255	255	255	192
Máscara de subred en formato binario	11111111	11111111	11111111	11000000
Notación de prefijo	/	26		

Verificar | Nuevo problema | Mostrar | Restablecer

11.6.6

Práctica de laboratorio: Cálculo de subredes IPv4

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Determinar la división en subredes de la dirección IPv4
- Parte 2: Calcular la división en subredes de la dirección IPv4

Cálculo de subredes IPv4

1. Asignación de direcciones IPv4
2. División en subredes para cumplir con requisitos

División en subredes para cumplir con requisitos

11.7.1

Espacio de direcciones IPv4 privado de subred frente al espacio público

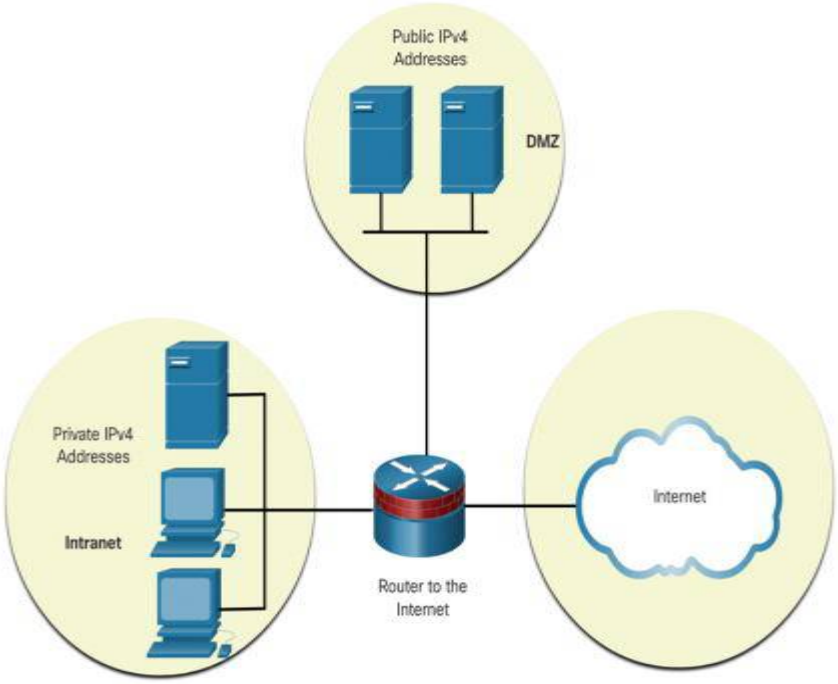
Aunque es bueno segmentar rápidamente una red en subredes, la red de su organización puede usar direcciones IPv4 públicas y privadas. Esto afecta a la forma en que va a subred la red.

La figura muestra una red empresarial típica:

- **Intranet -** Esta es la parte interna de la red de una empresa, accesible sólo dentro de la organización. Los dispositivos de la intranet utilizan direcciones IPv4 privadas.
- **DMZ -** Esto es parte de la red de la compañía que contiene recursos disponibles para Internet, como un servidor web. Los dispositivos de la DMZ utilizan direcciones IPv4 públicas.

El diagrama es una topología de red que muestra un enrutador en el centro con tres conexiones; una a la Intranet de la empresa, otra a una DMZ y otra a Internet. A la izquierda está la Intranet con dispositivos que usan direcciones IPv4 privadas. En la parte superior, se encuentra la DMZ con dos servidores que utilizan direcciones IPv4 públicas. El router está etiquetado como router a Internet y tiene una conexión a la nube de Internet.

Espacio de direcciones IPv4 público y privado



Tanto la intranet como la DMZ tienen sus propios requisitos y desafíos de subredes.

La intranet utiliza espacio de direcciones IPv4 privado. Esto permite a una organización utilizar cualquiera de las direcciones de red IPv4 privadas, incluido el prefijo 10.0.0.0/8 con 24 bits de host y más de 16 millones de hosts. El uso de una dirección de red con 24 bits de host hace que la subred sea más fácil y flexible. Esto incluye la subred en un límite de octetos utilizando un /16 o /24.

Por ejemplo, la dirección de red IPv4 privada 10.0.0.0/8 se puede subred utilizando una máscara /16. Como se muestra en la tabla, esto da como resultado 256 subredes, con 65.534 hosts por subred. Si una organización necesita menos de 200 subredes, lo que permite cierto crecimiento, esto da a cada subred más que suficientes direcciones de host.

Red de subredes 10.0.0.0/8 usando un /16

Dirección de subred (256 subredes posibles)	**Rango de host (65,534 posibles hosts por subred)**	**Dirección**
10.0.0.0**/16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0**/16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255

Dirección de subred (256 subredes posibles)	Rango de host (65,534 posibles hosts por subred)	Dirección
10.2.0.0/16	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10,3,0.0**/16**	**10,3**0,1 - **10,3**.255.254	**10.3**.255.255
10,4,0.0**/16**	**10,4**,0,1 - **10,4**,255,254	**10.4**.255.255
10,5,0.0**/16**	**10,5**,0,1 - **10,5**,255,254	**10.5**.255.255
10,6,0.0**/16**	**10,6**0,1 - **10,6.**255.254	**10.6**.255.255
10,7,0.0**/16**	**10,7**,0,1 - **10,7**,255,254	**10.7**.255.255
…	…	…
10.255.0.0**/16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Otra opción que utiliza la dirección de red privada IPv4 10.0.0.0/8 es subred usando una máscara /24. Como se muestra en la tabla, esto da como resultado 65.536 subredes, con 254 hosts por subred. Si una organización necesita más de 256 subredes, se puede utilizar un /24 con 254 hosts por subred.

Red de subredes 10.0.0.0/8 usando un /24

Dirección de subred (65,536 subredes posibles)	Rango de host (254 posibles hosts por subred)	Dirección
10.0.0.0**/24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0**/24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0**/24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0**/24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0**/24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255

Dirección de subred (65,536 subredes posibles)	Rango de host (254 posibles hosts por subred)	Dirección
10.1.1.0**/24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0**/24**	**10.1.2**.1 - **10.1.2**254	**10.1.2**.255
…	…	…
10.100,0.0**/24**	**10,100,0**,1 - 10,100,0 ,254	**10.100,0**.255
…	…	…
10.255.255.0**/24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

El 10.0.0.0/8 también se puede subred usando cualquier otro número de longitudes de prefijo, como /12, /18, /20, etc. Esto daría al administrador de red una amplia variedad de opciones. El uso de una dirección de red IPv4 privada 10.0.0.0/8 facilita la planificación e implementación de subredes.

What about the DMZ?

Debido a que estos dispositivos deben ser accesibles públicamente desde Internet, los dispositivos de la DMZ requieren direcciones IPv4 públicas. El agotamiento del espacio público de direcciones IPv4 se convirtió en un problema a partir de mediados de la década de 1990. Desde 2011, IANA y cuatro de cada cinco RIR se han quedado sin espacio de direcciones IPv4. Aunque las organizaciones están realizando la transición a IPv6, el espacio de direcciones IPv4 restante sigue siendo muy limitado. Esto significa que una organización debe maximizar su propio número limitado de direcciones IPv4 públicas. Esto requiere que el administrador de red subred su espacio de direcciones públicas en subredes con diferentes máscaras de subred, a fin de minimizar el número de direcciones de host no utilizadas por subred. Esto se conoce como máscara de longitud de subred variable (VLSM).

11.7.2

Minimizar las direcciones IPv4 de host no utilizadas y maximizar las subredes

Para minimizar el número de direcciones IPv4 de host no utilizadas y maximizar el número de subredes disponibles, hay dos consideraciones al planificar subredes: el número de direcciones de host necesarias para cada red y el número de subredes individuales necesarias.

La tabla muestra los detalles para subredes a una red / 24. Observe que existe una relación inversa entre la cantidad de subredes y la cantidad de hosts. Cuantos más bits se toman prestados para crear subredes, menor es la cantidad de bits de host disponibles. Si se necesitan más direcciones de host, se requieren más bits de host, lo que tiene como resultado menos subredes.

La cantidad de direcciones de host que se requieren en la subred más grande determina cuántos bits se deben dejar en la porción de host. Recuerde que no se pueden usar dos de las direcciones, por lo que el número de direcciones utilizables se puede calcular como 2n \ -2.

División de una red /24 en subredes

Longitud de prefijo	Máscara de subred	Máscara de subred en binario (n = network, h = host)	# de subredes	# hosts por subred.
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Los administradores de redes deben diseñar un esquema de direccionamiento de red que admita la cantidad máxima de hosts para cada red y la cantidad de subredes. El esquema de direccionamiento debe permitir el crecimiento tanto de la cantidad de direcciones de host por subred como de la cantidad total de subredes.

11.7.3

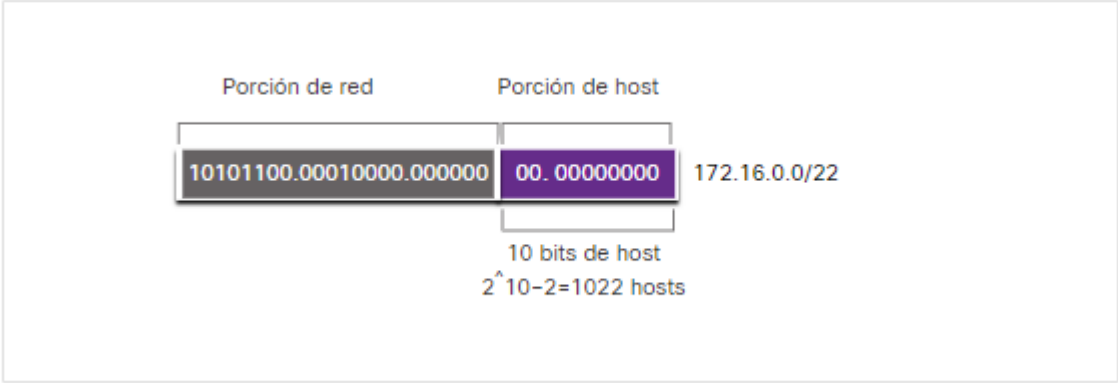
Ejemplo: Subredes IPv4 eficientes

En este ejemplo, su ISP ha asignado una dirección de red pública de 172.16.0.0/22 (10 bits de host) a su sede central. Como se muestra en la figura, esto proporciona 1022 direcciones de host.

Nota: 172.16.0.0/22 forma parte del espacio de direcciones privadas IPv4. Estamos utilizando esta dirección en lugar de una dirección IPv4 pública real.

El gráfico muestra el número de hosts proporcionados cuando se utiliza una red 172.16.0.0/22. La parte de red de la dirección en binario es: 10101100.00010100.000000. La parte del host en binario es: 00.00000000. La porción de host consta de 10 bits de host, por lo tanto, 2 a la potencia de 10 - 2 = 1.022 hosts.

Dirección de red

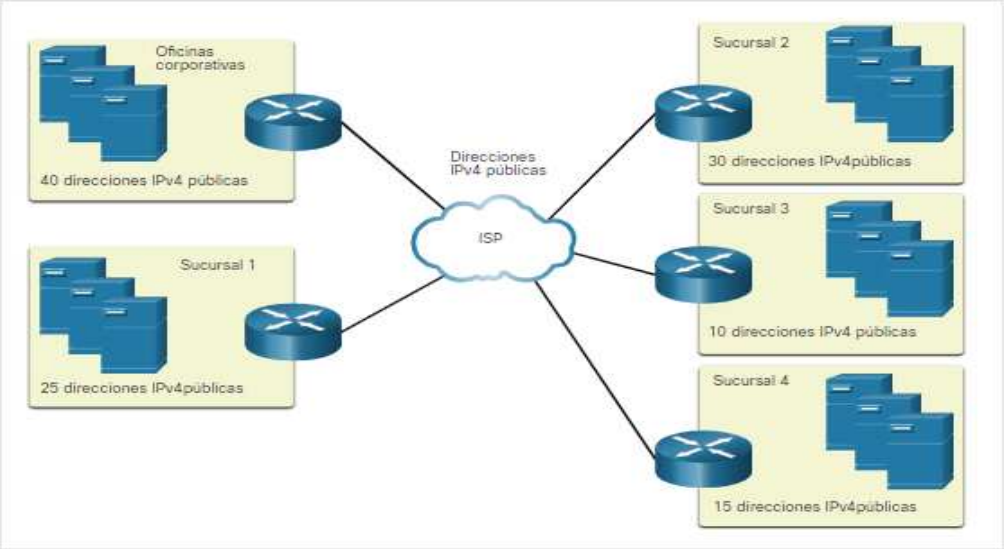


La sede corporativa cuenta con una DMZ y cuatro sucursales, cada una de las cuales necesita su propio espacio de direcciones IPv4 públicas. Las oficinas centrales corporativas deben aprovechar al máximo su limitado espacio de direcciones IPv4.

La topología mostrada en la figura consta de cinco sitios; una oficina corporativa y cuatro sucursales. Cada sitio requiere conectividad a Internet y, por lo tanto, cinco conexiones a Internet. Esto significa que la organización requiere 10 subredes de la dirección pública 172.16.0.0/22 de la compañía. La subred más grande requiere 40 hosts.

El diagrama es una topología de red corporativa con cinco sitios. En el medio está la nube de ISP. Conectados a la nube hay cinco sitios, cada uno de los cuales se muestra con un router, varios servidores y los requisitos públicos de direccionamiento IPv4. Los sitios son: sede corporativa con 40 direcciones; sucursal 1 con 25 direcciones; sucursal 2 con 30 direcciones; sucursal 3 con 10 direcciones; y sucursal 4 con 15 direcciones.

Topología corporativa con cinco sitios



La dirección de red 172.16.0.0/22 tiene 10 bits de host, como se muestra en la figura. Debido a que la subred más grande requiere 40 hosts, se debe tomar prestado un mínimo de 6 bits de host para proporcionar el direccionamiento de los 40 hosts. Esto se determina utilizando esta fórmula:2^6 - 2 = 62 hosts.

El diagrama muestra el esquema de subred para la dirección dada 172.16.0.0/22 con 4 bits tomados de la parte host para crear subredes. Los cuatro octetos se muestran en binario seguido del formato decimal de puntos para la dirección de red dada y para varias subredes creadas. La dirección de red dada en binario es 10101100.00010000.000000 (parte de red resaltada en gris) 00.00000000 (parte del host resaltada en púrpura) = 172.16.0.0/22. Para las subredes que se enumeran a continuación, los primeros 22 bits se resaltan en gris (parte de red), los siguientes 4 bits se sombrean en azul y los últimos 6 bits son la parte restante del host sombreada en púrpura. La subred 0 es 10101100.00010000.00000000.00000000 = 172.16.0.0/26. La subred 1 es 10101100.00010000.0000000.01000000 = 172.16.0.64/26. La subred 2 es 10101100.00010000.00000000.10000000 = 172.16.0.128/26. La subred 3 es 10101100.00010000.00000000.11000000 = 172.16.0.192/26. La subred 4 es 10101100.00010000.00000001.00000000 = 172.16.1.0/26. La subred 5 es 10101100.00010000.00000001.01000000 = 172.16.1.64/26. La subred 6 es 10101100.00010000.00000001.10000000 = 172.16.1.128/26. La subred 7 - 13 no se muestran. La subred 14 es 10101100.00010000.00000011.10000000 = 172.16.3.128/26. La subred 15 es 10101100.00010000.00000011.11000000 = 172.16.3.192/26.

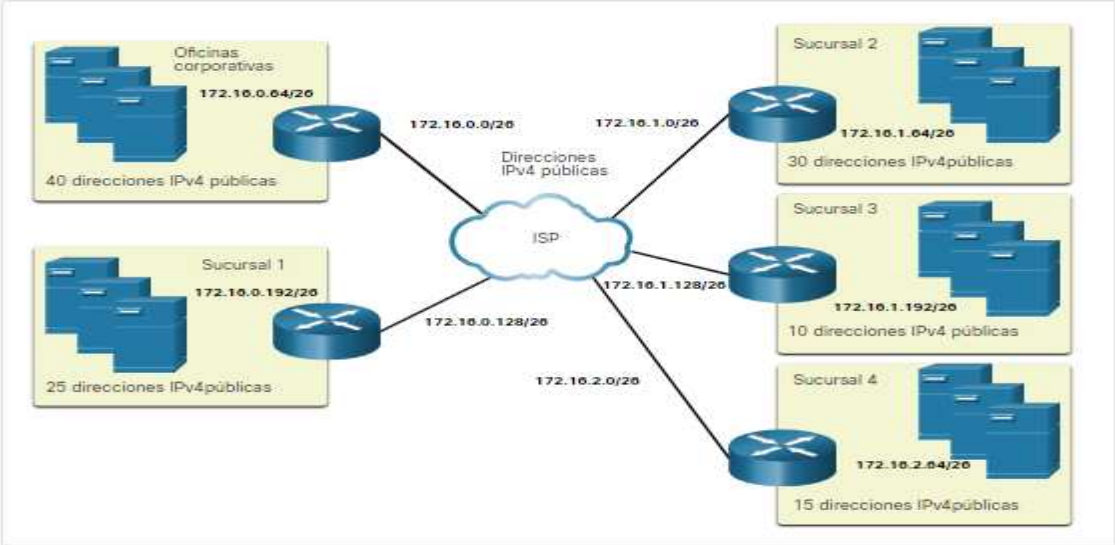
Esquema de subredes

La fórmula para determinar subredes da un resultado de 16 subredes: 2^4= 16. Debido a que la interconexión de redes de ejemplo requiere 10 subredes, esto cumplirá con el requisito y permitirá un crecimiento adicional.

Por lo tanto, los primeros 4 bits de host se pueden usar para asignar subredes. Esto significa que se prestarán dos bits del 3er octeto y dos bits del 4to octeto. Cuando se piden prestados 4 bits, la nueva longitud de prefijo es /26, con la máscara de subred 255.255.255.192.

Como se muestra en esta figura, las subredes se pueden asignar a cada ubicación y conexiones de router a ISP.

Asignaciones de subred a cada sitio e ISP



El diagrama muestra las asignaciones de subred para una topología corporativa con cinco sitios conectados a una nube de ISP. Cada sitio muestra un router conectado al ISP, varios servidores, los requisitos públicos de direccionamiento IPv4 y la dirección de subred asignada. A cada conexión de router a ISP también se le ha asignado una dirección de subred. A la conexión de la sede corporativa se le asigna la subred 172.16.0.0/26 y al sitio con 40 direcciones se le asigna la subred 172.16.0.64/26. A la conexión de la rama 1 se le asigna la subred 172.16.0.128/26 y al sitio con 25 direcciones se le asigna 172.16.0.192/26. A la conexión Branch 2 se le asigna la subred 172.16.1.0/26 y al sitio con 30 direcciones se le asigna la subred 172.16.1.64/26. A la conexión Branch 3 se le asigna la subred 172.16.1.128/26 y al sitio con 10 direcciones se le asigna la subred 172.16.1.192/26. A la conexión Branch 4 se le asigna la subred 172.16.2.0/26 y al sitio con 15 direcciones se le asigna la subred 172.16.2.64/26.

11.7.4

Actividad: Determinar la cantidad de bits que se deben tomar prestados

Instrucciones:

En esta actividad, se le da el número de hosts que se necesitan. Determine la máscara de subred que admitiría el número de hosts especificado. Introduzca sus respuestas en formato binario, decimal y de notación de prefijo en los campos proporcionados.

Hosts necesarios	Máscara de subred (formato binario)	Máscara de subred (formato decimal)	Notación de prefijo (/x)
250	11111111.11111111.11111111.00000000	255.255.255.0	/24
25	11111111 . 11111111 . 11111111 . 11100000	255.255.255.224	/ 27
1000	11111111 . 11111111 . 11111100 . 00000000	255.255.252.0	/ 22
75	11111111 . 11111111 . 11111111 . 10000000	255.255.255.128	/ 25
10	11111111 . 11111111 . 11111111 . 11110000	255.255.255.240	/ 28
500	11111111 . 11111111 . 11111110 . 00000000	255.255.254.0	/ 23

Verificar Mostrar Restablecer

11.7.5

Packet Tracer: División en subredes, situación

En esta actividad, se le asigna la dirección de red 192.168.100.0/24 para que cree una subred y proporcione la asignación de direcciones IP para la red que se muestra en la topología. Cada LAN de la red requiere espacio suficiente para al menos 25 direcciones, lo que incluye dispositivos finales, así como el conmutador y el router. La conexión entre el R1 y el R2 requiere una dirección IP para cada extremo del enlace.

División en subredes situación

División en subredes situación

1. Asignación de direcciones IPv4
2. VLSM

VLSM

11.8.1

Vídeo - Aspectos básicos de VLSM

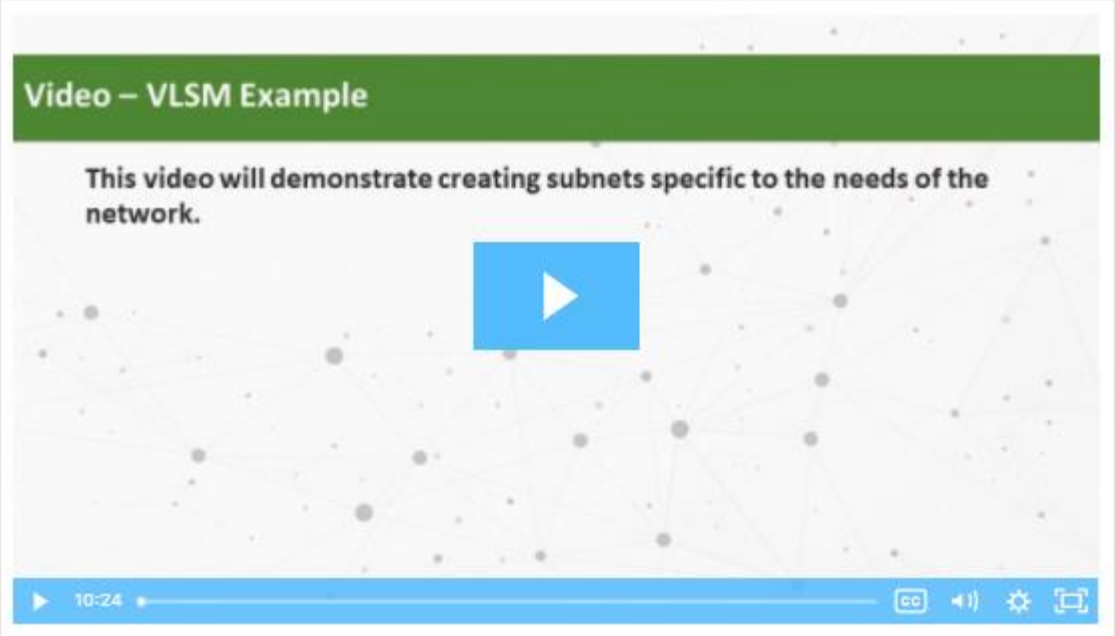
Como se mencionó en el tema anterior, las direcciones públicas y privadas afectan a la forma en que se subnetea la red. También hay otros problemas que afectan a los esquemas de subcompensación. Un esquema de subredes estándar /16 crea subredes que cada una tiene el mismo número de hosts. No todas las subredes que cree necesitarán tantos hosts, dejando muchas direcciones IPv4 sin utilizar. Tal vez necesite una subred que contenga muchos más hosts. Esta es la razón por la que se desarrolló la máscara de subred de longitud variable (VLSM).

Haga clic en Reproducir para ver una demostración de las técnicas de VLSM básicas.

11.8.2

Video: Ejemplo de VLSM

Haga clic en Reproducir para ver una demostración de la división en subredes VLSM.



11.8.3

Conservación de direcciones IPv4

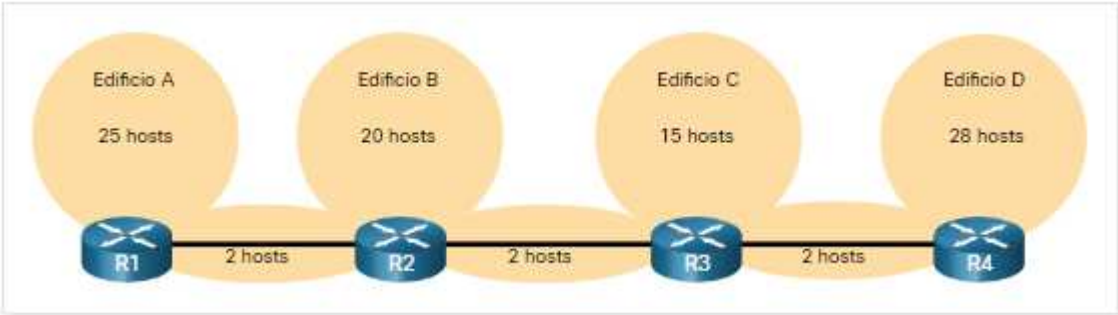
Debido al agotamiento del espacio de direcciones IPv4 público, sacar el máximo partido a las direcciones de host disponibles es una preocupación primordial cuando se subredes de redes IPv4.

Nota: La dirección IPv6 más grande permite una planificación y asignación de direcciones mucho más fáciles de lo que permite IPv4. Conservar direcciones IPv6 no es un problema. Esta es una de las fuerzas impulsoras para la transición a IPv6.

Mediante la división en subredes tradicional, se asigna la misma cantidad de direcciones a cada subred. Si todas las subredes tienen los mismos requisitos para la cantidad de hosts, o si la conservación del espacio de direcciones IPv4 no es un problema, estos bloques de direcciones de tamaño fijo serían eficientes. Normalmente, con direcciones IPv4 públicas, ese no es el caso.

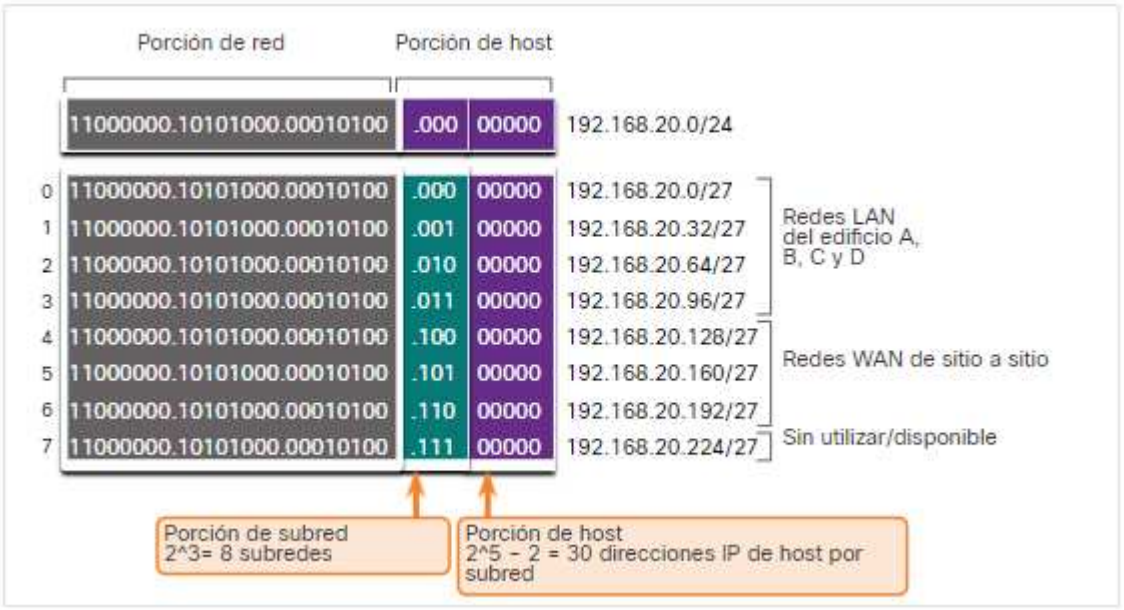
Por ejemplo, la topología que se muestra en la figura requiere siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres conexiones WAN entre los routers.

El diagrama muestra una topología de red que consta de siete subredes. Hay cuatro routers, cada uno con una LAN conectada y requisitos de direccionamiento de host, y tres conexiones de router a router que requieren 2 hosts cada uno. La LAN del router R1 es el edificio A con 25 hosts; la LAN del router R2 es el edificio B con 20 hosts; la LAN del router R3 es el edificio C con 15 hosts; y la LAN del router R4 es el edificio D con 28 hosts.



Utilizando la división en subredes tradicional con la dirección dada de 192.168.20.0/24, se pueden tomar prestados tres bits de la parte del host en el último octeto para cumplir con el requisito de subred de siete subredes. Como se muestra en la figura, tomar prestados 3 bits crea 8 subredes y deja 5 bits de host con 30 hosts utilizables por subred. Mediante este esquema, se crean las subredes necesarias y se cumplen los requisitos de host de la LAN más grande.

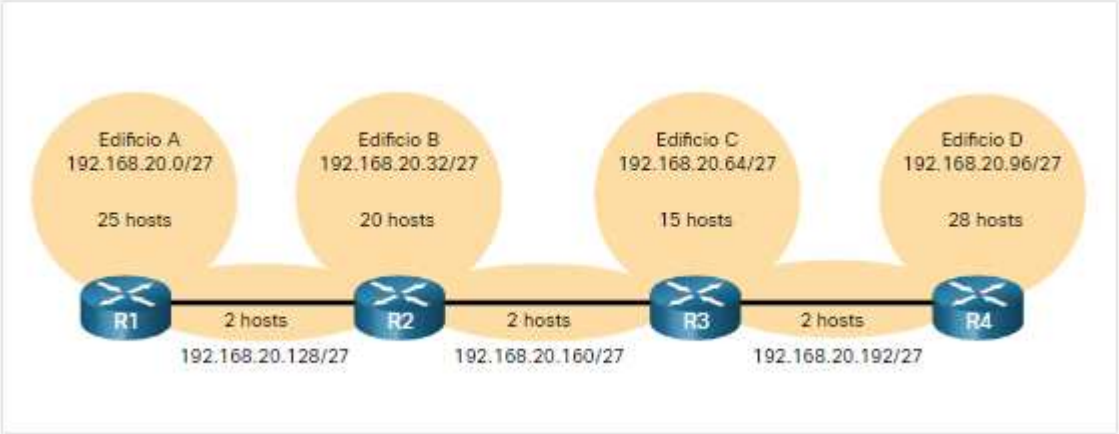
Esquema de subredes básico



El diagrama muestra el esquema básico de subred para una dirección determinada de 192.168.20.0/24 con tres bits prestados para subredes. Tener 3 bits para subredes da como resultado 2 a la potencia de 3 = 8 subredes. Tener 5 bits para hosts da como resultado 2 a la potencia de 5 - 2 = 30 direcciones IP de host por subred. Los cuatro octetos se muestran en binario seguido del formato decimal punteado para la dirección dada y para todas las subredes creadas. La dirección de red dada en binario es 11000000.10101000.00010100 (parte de red resaltada en gris) .00000000 (parte de host resaltada en púrpura) = 192.168.20.0/24. Para las subredes que se enumeran a continuación, los primeros 24 bits se resaltan en gris (parte de red), los siguientes tres bits se resaltan en azul (parte de subred) y los últimos cinco bits son los bits host restantes resaltados en púrpura.

La subred 0 es 11000000.10101000.00010100.00000000 = 192.168.20.0/27.
La subred 1 es 11000000.10101000.00010100.00100000 = 192.168.20.32/27.
La subred 2 es 11000000.10101000.00010100.01000000 = 192.168.20.64/27.
La subred 3 es 11000000.10101000.00010100.01100000 = 192.168.20.96/27.
Las subredes 0 - 3 se asignan a la construcción de LAN A, B, C y D.
La subred 4 es 11000000.10101000.00010100.10000000 = 192.168.20.128/27.
La subred 5 es 11000000.10101000.00010100.10100000 = 192.168.20.160/27.
La subred 6 es 11000000.10101000.00010100.11000000 = 192.168.20.192/27.
Las subredes 4, 5 y 6 se asignan al sitio WAN del sitio.
La subred 7 es 11000000.10101000.00010100.11100000 = 192.168.20.224/27.
La subred 7 no está utilizada/disponible.

Estas siete subredes podrían asignarse a las redes LAN y WAN, como se muestra en la figura.



El diagrama muestra las asignaciones de subred para una topología de red que consta de siete subredes. Hay cuatro enrutadores, cada uno con una LAN conectada y requisitos de direccionamiento de host, y tres conexiones de enrutador a enrutador que requieren 2 hosts cada uno.

El router R1 Building A LAN tiene 25 hosts y se le asigna la subred 192.168.20.0/27.
El router R2 Building B LAN tiene 20 hosts y se le asigna la subred 192.168.20.32/27.
El router R3 Building C LAN tiene 15 hosts y se le asigna la subred 192.168.20.64/27.
El router R4 Building D LAN tiene 28 hosts y se le asigna la subred 192.168.20.96/27.
A la conexión R1 a R2 se le asigna la subred 192.168.20.128/27.
A la conexión R2 a R3 se le asigna la subred 192.168.20.160/27.
A la conexión R3 a R4 se le asigna la subred 192.168.20.192/27.

Si bien la división en subredes tradicional satisface las necesidades de la LAN más grande y divide el espacio de direcciones en una cantidad adecuada de subredes, da como resultado un desperdicio significativo de direcciones sin utilizar.

Por ejemplo, solo se necesitan dos direcciones en cada subred para los tres enlaces WAN. Dado que cada subred tiene 30 direcciones utilizables, hay 28 direcciones sin utilizar en cada una de estas subredes. Como se muestra en la figura, esto da como resultado 84 direcciones no utilizadas (28x3).

Direcciones sin utilizar en subredes WAN

El gráfico muestra las direcciones no utilizadas de cuatro subredes WAN utilizando una máscara de subred /27. Los cuatro octetos se muestran en binario seguido del formato decimal punteado para la subred. Los primeros 24 bits se resaltan en gris (porción de red), los siguientes tres bits se resaltan en azul y los últimos cinco bits son los bits de host restantes resaltados en morado.

La subred 4 es 11000000.10101000.00010100.10000000 = 192.168.20.128/27.
La subred 5 es 11000000.10101000.00010100.10100000 = 192.168.20.160/27.
La subred 6 es 11000000.10101000.00010100.11000000 = 192.168.20.192/27.
Tener 5 bits para hosts da como resultado 2 a la potencia de 5 - 2 = 30 direcciones IP de host por subred. 30 - 2 = 28; cada subred WAN desperdicia 28 direcciones. 28 x 3 = 84; 84 direcciones no se utilizan.

Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de las direcciones es característico de la división en subredes tradicional. La aplicación de un esquema de división en subredes tradicional a esta situación no resulta muy eficiente y genera desperdicio.

La máscara de subred de longitud variable (VLSM) se desarrolló para evitar el desperdicio de direcciones al permitirnos subred una subred.

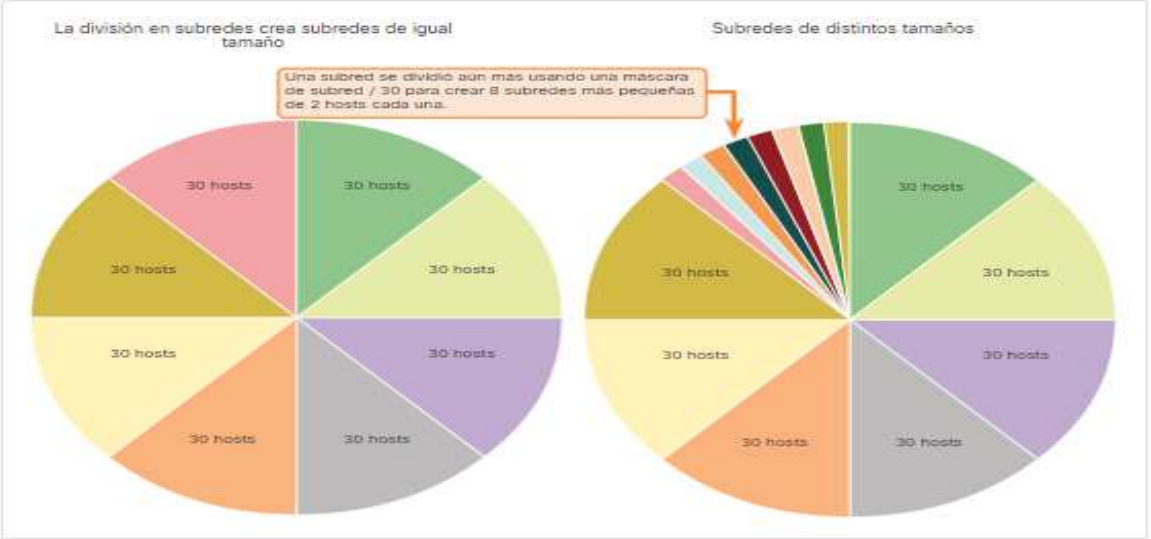
11.8.4

VLSM

En todos los ejemplos de división en subredes anteriores, se aplicó la misma máscara de subred en todas las subredes. Esto significa que cada subred tiene la misma cantidad de direcciones de host disponibles. Como se ilustra en la figura, mediante la división en subredes tradicional se crean subredes de igual tamaño. Cada subred en un esquema tradicional utiliza la misma máscara de subred. Como se muestra en la figura, VLSM permite dividir un espacio de red en partes desiguales. Con VLSM, la máscara de subred varía según la cantidad de bits

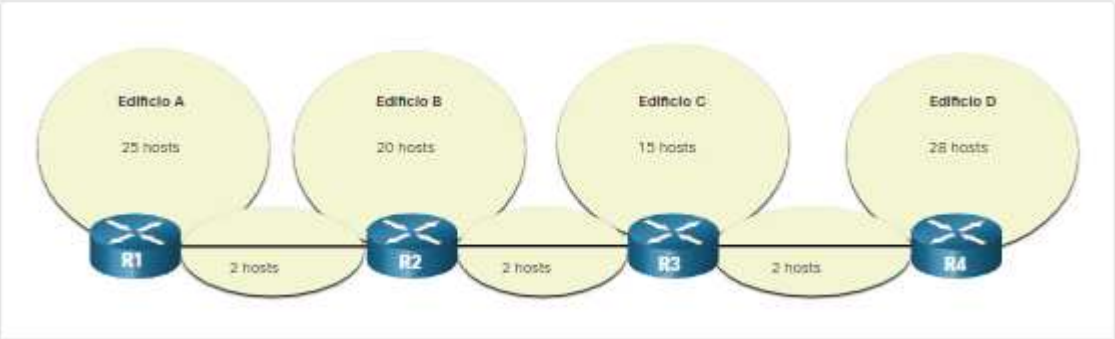
que se toman prestados para una subred específica, de lo cual deriva la parte “variable” de la VLSM.

El gráfico muestra dos gráficos circulares que comparan las subredes tradicionales con VLSM. A la derecha hay un gráfico circular titulado: las subredes tradicionales crean subredes de igual tamaño. El pastel se divide en 8 rebanadas de igual tamaño, cada una con 30 hosts. A la izquierda hay un gráfico circular titulado: subredes de diferentes tamaños. Este pastel tiene 7 rebanadas idénticas a la primera tarta. La octava rebanada se ha dividido en 8 rebanadas más pequeñas. Texto que apunta a la octava división lee: una subred se dividió aún más usando una máscara de subred /30 para crear 8 subredes más pequeñas de 2 hosts cada una.



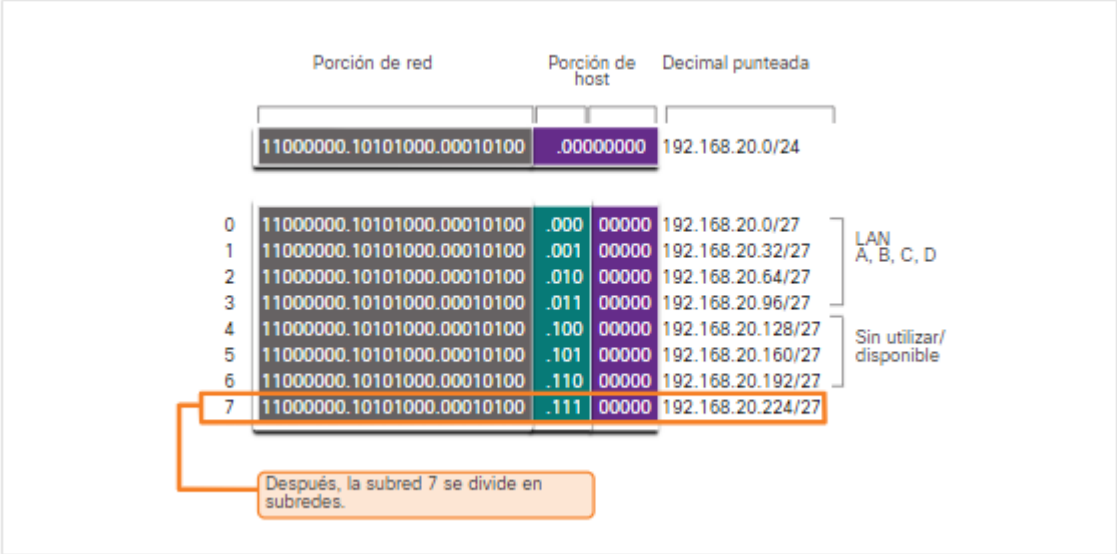
VLSM simplemente subdivide una subred. La misma topología utilizada anteriormente se muestra en la figura. Nuevamente, usaremos la red 192.168.20.0/24 y la subred para siete subredes, una para cada una de las cuatro LAN, y una para cada una de las tres conexiones entre los routers.

El diagrama muestra una topología de red que consta de siete subredes. Hay cuatro enrutadores, cada uno con una LAN conectada y requisitos de direccionamiento de host, y tres conexiones de enrutador a enrutador que requieren 2 hosts cada uno. La LAN del enrutador R1 es el edificio A con 25 hosts; la LAN del enrutador R2 es el edificio B con 20 hosts; la LAN del enrutador R3 es el edificio C con 15 hosts; y la LAN del enrutador R4 es el edificio D con 28 hosts.



La figura muestra cómo la red 192.168.20.0/24 se subredes en ocho subredes de igual tamaño con 30 direcciones de host utilizables por subred. Se usan cuatro subredes para las LAN y tres subredes para las conexiones entre los routers.

Esquema Básico de Subredes



El diagrama muestra el esquema básico de subred para una dirección determinada de 192.168.20.0/24 con tres bits prestados para subredes. Los cuatro octetos se muestran en binario seguido del formato decimal punteado para la dirección dada y para todas las subredes creadas. La dirección de red dada en binario es 11000000.10101000.00010100 (parte de red resaltada en gris) .00000000 (parte de host resaltada en púrpura) = 192.168.20.0/24. Para las subredes que se enumeran a continuación, los primeros 24 bits se resaltan en gris (parte de red), los siguientes tres bits se resaltan en azul (parte de subred) y los últimos cinco bits son los bits host restantes resaltados en púrpura.

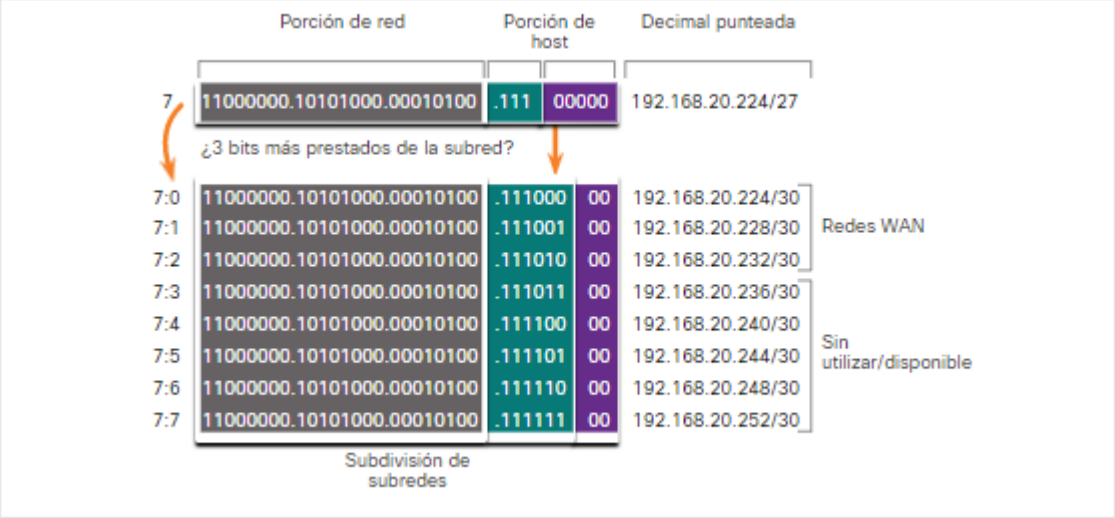
La subred 0 es 11000000.10101000.00010100.00000000 = 192.168.20.0/27.
La subred 1 es 11000000.10101000.00010100.00100000 = 192.168.20.32/27.
La subred 2 es 11000000.10101000.00010100.01000000 = 192.168.20.64/27.

La subred 3 es 11000000.10101000.00010100.01100000 = 192.168.20.96/27.
Las subredes 0 - 3 se asignan a la construcción de LAN A, B, C y D.
La subred 4 es 11000000.10101000.00010100.10000000 = 192.168.20.128/27.
La subred 5 es 11000000.10101000.00010100.10100000 = 192.168.20.160/27.
La subred 6 es 11000000.10101000.00010100.11000000 = 192.168.20.192/27.
Las subredes 4, 5 y 6 no están utilizadas/disponibles.
La subred 7 es 11000000.10101000.00010100.11100000 = 192.168.20.224/27. Después, la subred 7 se divide en subredes.

Sin embargo, las conexiones entre los routers requieren sólo dos direcciones de host por subred (una dirección de host para cada interfaz del router). Actualmente todas las subredes tienen 30 direcciones de host utilizables por subred. Para evitar desperdiciar 28 direcciones por subred, VLSM puede usarse para crear subredes más pequeñas para las conexiones entre routers.

Para crear subredes más pequeñas para los enlaces WAN, se dividirá una de las subredes. En este ejemplo, la última subred, 192.168.20.224/27, puede subdividirse aún más. La figura muestra que la última subred se ha subred utilizando la máscara de subred 255.255.255.252 o /30.

Esquema de división en subredes de VLSM



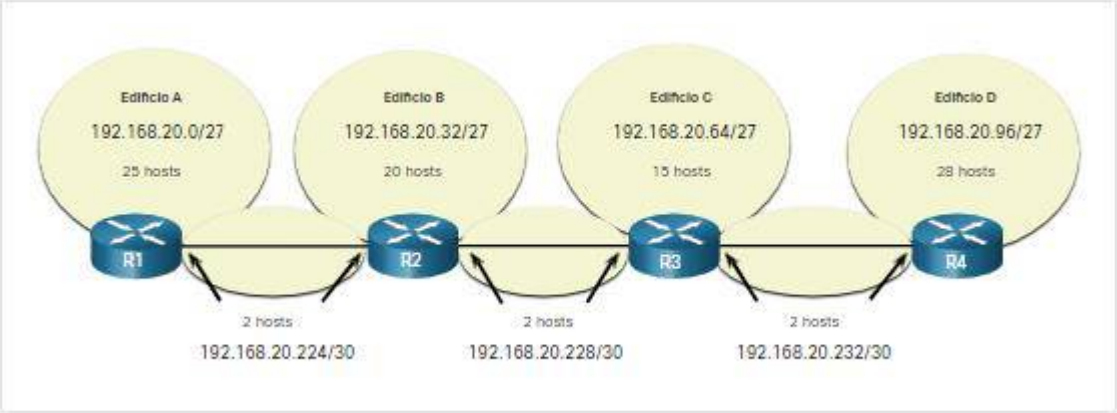
El diagrama muestra el esquema de subred VLSM cuando la subred 192.168.20.224/27 se subred adicionalmente tomando prestados 3 bits más. Para la subred original, los primeros 24 bits representan la parte de red y son 11000000.10101000.00010100. Los tres bits siguientes representan la parte de la subred y son 111. Los últimos cinco bits representan la parte del host y son 00000. La dirección en decimal con puntos es 192.168.20.224/27. Prestar 3 bits adicionales, subred una subred, da como resultado dividir la subred original en 8 subredes más pequeñas. Para las subredes más pequeñas, los primeros 24 bits son la parte de

red, los siguientes seis bits son la parte de subred y los dos últimos bits son la parte restante del host.

La subred 7:0 es 11000000.10101000.00010100.11100000 = 192.168.20.224/30.
La subred 7:1 es 11000000.10101000.00010100.11100100 = 192.168.20.228/30.
La subred 7:2 es 11000000.10101000.00010100.11101000 = 192.168.20.232/30.
La subred 7:3 es 11000000.10101000.00010100.11101100 = 192.168.20.236/30.
La subred 7:4 es 11000000.10101000.00010100.11110000 = 192.168.20.240/30.
La subred 7:5 es 11000000.10101000.00010100.11110100 = 192.168.20.244/30.
La subred 7:6 es 11000000.10101000.00010100.11111000 = 192.168.20.248/30.
La subred 7:7 es 11000000.10101000.00010100.11111100 = 192.168.20.252/30.
Las subredes 7:0, 7:1 y 7:2 se asignan a las WAN y las subredes restantes no están utilizadas/disponibles.

¿Por qué /30? Recuerde que cuando se conoce el número de direcciones de host necesarias, se puede usar la fórmula 2n \ -2 (donde n es igual al número de bits de host restantes). Para proporcionar dos direcciones utilizables, se deben dejar dos bits de host en la parte del host.

Debido a que hay cinco bits de host en el espacio de direcciones subred 192.168.20.224/27, se pueden pedir prestados tres bits más, dejando dos bits en la porción de host. Los cálculos que se realizan llegado este punto son exactamente los mismos que se utilizan para la división en subredes tradicional: Se toman prestados los bits, y se determinan los rangos de subred. La figura muestra cómo las cuatro subredes /27 se han asignado a las LAN y tres de las subredes /30 se han asignado a los enlaces entre routers.



El diagrama muestra las asignaciones de subred VLSM para una topología de red que consta de cuatro LAN y tres WAN. Hay cuatro enrutadores, cada uno con una LAN conectada y requisitos de direccionamiento de host, y tres conexiones de enrutador a enrutador que requieren 2 hosts cada uno.

El router R1 Building A LAN tiene 25 hosts y se le asigna la subred 192.168.20.0/27.
El router R2 Building B LAN tiene 20 hosts y se le asigna la subred 192.168.20.32/27.
El router R3 Building C LAN tiene 15 hosts y se le asigna la subred 192.168.20.64/27.

El router R4 Building D LAN tiene 28 hosts y se le asigna la subred 192.168.20.96/27.
A la conexión R1 a R2 se le asigna la subred 192.168.20.224/30.
A la conexión R2 a R3 se le asigna la subred 192.168.20.228/30.
A la conexión R3 a R4 se le asigna la subred 192.168.20.232/30.

Este esquema de subredes VLSM reduce el número de direcciones por subred a un tamaño apropiado para las redes que requieren menos subredes. La subred 7 para enlaces entre routers permite que las subredes 4, 5 y 6 estén disponibles para redes futuras, así como cinco subredes adicionales disponibles para conexiones entre routers.

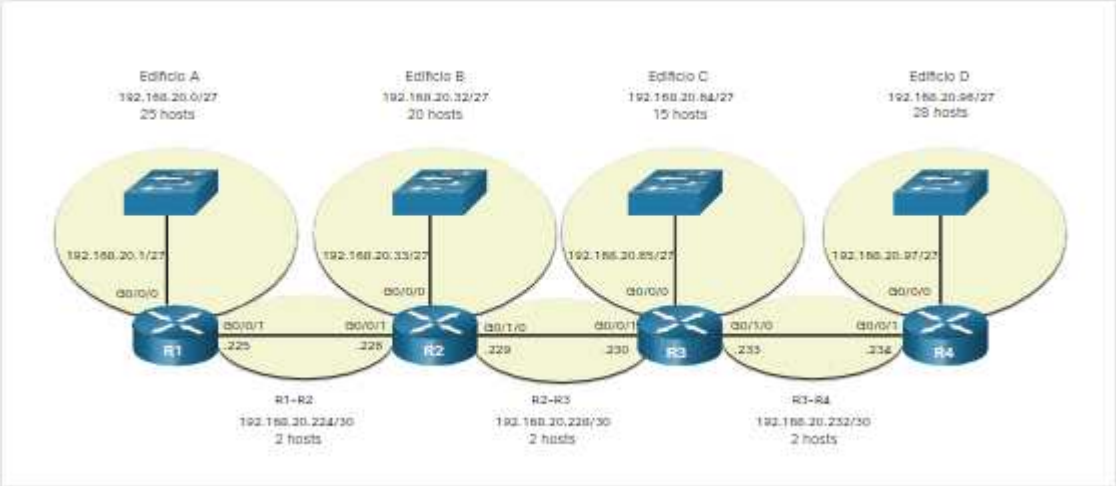
Nota: Cuando use VLSM, siempre comience por satisfacer los requisitos de host de la subred más grande. Siga con la división en subredes hasta que se cumplan los requisitos de host de la subred más pequeña.

11.8.5

Asignación de direcciones de topología VLSM

Usando las subredes VLSM, las redes LAN y entre routers se pueden abordar sin desperdicio innecesario.

La figura muestra las asignaciones de direcciones de red y las direcciones IPv4 asignadas a cada interfaz de router.



El diagrama muestra las asignaciones de subred VLSM y el direccionamiento IP de interfaz para una topología de red que consta de cuatro LAN y tres WAN. Hay cuatro enrutadores, cada uno con una LAN conectada y requisitos de direccionamiento de host, y tres conexiones de enrutador a enrutador que requieren 2 hosts cada uno.

El router R1 Building A LAN está conectado a la interfaz G0/0/0 de R1 en 192.168.20.1/27, tiene 25 hosts y se le asigna la subred 192.168.20.0/27.
El router R2 Building B LAN está conectado a la interfaz G0/0/0 de R2 en 192.168.20.33/27, tiene 20 hosts y se le asigna la subred 192.168.20.32/27.
El router R3 Building C LAN está conectado a la interfaz G0/0/0 de R3 en 192.168.20.65/27, tiene 15 hosts y se le asigna la subred 192.168.20.64/27.
El router R4 Building D LAN está conectado a la interfaz G0/0/0 de R4 en 192.168.20.97/27, tiene 28 hosts y se le asigna la subred 192.168.20.96/27.
La conexión R1 a R2, subred asignada 192.168.20.224/30, conecta la interfaz G0/0/1 de R1 con la dirección .225 a la interfaz G0/0/1 de R2 con la dirección .226.
La conexión R2 a R3, subred asignada 192.168.20.228/30, conecta la interfaz G0/1/0 de R2 con la dirección .229 a la interfaz G0/0/1 de R3 con la dirección .230.
La conexión R3 a R4, subred asignada 192.168.20.232/30, conecta la interfaz G0/1/0 de R2 con la dirección .233 a la interfaz G0/0/1 de R4 con la dirección .234.

Mediante un esquema de direccionamiento común, la primera dirección IPv4 de host para cada subred se asigna a la interfaz de la red LAN del router. Los hosts en cada subred tendrán una dirección IPv4 de host del intervalo de direcciones de host para esa subred y una máscara adecuada. Los hosts utilizarán la dirección de la interfaz de la red LAN del router conectada como dirección de gateway predeterminado.

La tabla muestra las direcciones de red y el intervalo de direcciones de host para cada red. Se muestra la dirección de puerta de enlace predeterminada para las cuatro LAN.

	Dirección de red	Intervalo de direcciones de host	Dirección de puerta de enlace predeterminada
Edificio A	192.168.20.0/27	192.168.20.1/27 to 192.168.20.30/27	192.168.20.1/27
Edificio B	192.168.20.32/27	192.168.20.33/27 to 192.168.20.62/27	192.168.20.33/27
Edificio C	192.168.20.64/27	192.168.20.65/27 to 192.168.20.94/27	192.168.20.65/27
Edificio D	192.168.20.96/27	192.168.20.97/27 to 192.168.20.126/27	192.168.20.97/27
R1-R2	192.168.20.224/30	192.168.20.225/30 to 192.168.20.226/30	
R2-R3	192.168.20.228/30	192.168.20.229/30 to 192.168.20.230/30	
R3-R4	192.168.20.232/30	192.168.20.233/30 to 192.168.20.234/30	

11.8.6

Actividad - VLSM Practice

192.168.5.0/24 | Tabla 1 - Primer cálculo de subredes

En la tabla 1, se utiliza la división en redes común para trabajar con la red que se muestra. La tabla 2 utiliza **VLSM** para subred más la red. Calcule 50 usuarios por subred

Haga clic en la nueva máscara de subred (decimal)

Correcto

Calculó la subred correctamente.

Haga clic en la nueva máscara de subred (decimal)

192.168.5.0- 192.168.5.63	/26	255.255.255.192	192.168.5.192- 192.168.5.255	192.168.5.64- 192.168.5.127

Haga clic en la primera notación de prefijo

192.168.5.0- 192.168.5.63	/26	255.255.255.192	192.168.5.192- 192.168.5.255	192.168.5.64- 192.168.5.127

Haga clic en el primer rango completo de subred

192.168.5.0- 192.168.5.63	/26	255.255.255.192	192.168.5.192- 192.168.5.255	192.168.5.64- 192.168.5.127

Haga clic en la primera notación de prefijo

192.168.5.0- 192.168.5.63	/26	255.255.255.192	192.168.5.192- 192.168.5.255	192.168.5.64- 192.168.5.127

Haga clic en el primer rango completo de subred

192.168.5.0- 192.168.5.63	/26	255.255.255.192	192.168.5.192- 192.168.5.255	192.168.5.64- 192.168.5.127

Verificar | Mostrar | Restablecer

192.168.5.0/24 | Tabla 2 - Cálculo de VLSM

Use el segundo rango completo de subred de la Tabla 1 y VLSM para calcular 20 usuarios por subred.

Segundo rango de subred **completo** (/26) de la tabla 1

Correcto

Calculó correctamente la subred mediante VLSM.

Segundo rango de subred **completo**(/26) de la tabla 1

192.168.5.96-192.168.5.127	/27	192.168.5.64-192.168.5.127	255.255.255.224	192.168.5.64-192.168.5.95

Haga clic en la nueva máscara de subred VLSM (decimal)

192.168.5.96-192.168.5.127	/27	192.168.5.64-192.168.5.127	255.255.255.224	192.168.5.64-192.168.5.95

Haga clic en la notación de prefijo **VLSM**

192.168.5.96-192.168.5.127	/27	192.168.5.64-192.168.5.127	255.255.255.224	192.168.5.64-192.168.5.95

Haga clic en el primer rango completo de subred **VLSM**

192.168.5.96-192.168.5.127	/27	192.168.5.64-192.168.5.127	255.255.255.224	192.168.5.64-192.168.5.95

Haga clic en el último rango completo de subred **VLSM**

192.168.5.96-192.168.5.127	/27	192.168.5.64-192.168.5.127	255.255.255.224	192.168.5.64-192.168.5.95

Verificar | Mostrar | Restablecer

Diseño estructurado

11.9.1

Planificación de direcciones de red IPv4

Antes de iniciar la subred, debe desarrollar un esquema de direccionamiento IPv4 para toda la red. Necesitará saber cuántas subredes necesita, cuántos hosts requiere una subred concreta, qué dispositivos forman parte de la subred, qué partes de la red utilizan direcciones privadas y cuáles utilizan público, y muchos otros factores determinantes. Un buen esquema de direccionamiento permite el crecimiento. Un buen esquema de direccionamiento es también el signo de un buen administrador de red.

La planificación de las subredes de la red requiere un análisis tanto de las necesidades de uso de red de la organización como de la forma en que se estructurarán las subredes. El punto de partida consiste en llevar a cabo un estudio de los requisitos de la red. Esto significa mirar toda la red, tanto la intranet como la DMZ, y determinar cómo se segmentará cada área. El plan de direcciones incluye determinar dónde se necesita la conservación de direcciones (generalmente dentro de la DMZ) y dónde hay más flexibilidad (generalmente dentro de la intranet).

Cuando se requiera la conservación de direcciones, el plan debe determinar cuántas subredes se necesitan y cuántos hosts por subred. Como se mencionó anteriormente, esto suele ser necesario para el espacio de direcciones IPv4 público dentro de la DMZ. Esto probablemente incluirá el uso de VLSM.

Dentro de la intranet corporativa, la conservación de direcciones suele ser menos problemática. Esto se debe en gran medida al uso de direcciones IPv4 privadas, incluyendo 10.0.0.0/8, con más de 16 millones de direcciones IPv4 de host.

Para la mayoría de las organizaciones, las direcciones IPv4 privadas permiten más que suficientes direcciones internas (intranet). Para muchas organizaciones e ISP más grandes, incluso el espacio de direcciones IPv4 privado no es lo suficientemente grande como para satisfacer sus necesidades internas. Esta es otra razón por la que las organizaciones están haciendo la transición a IPv6.

Para las intranets que utilizan direcciones IPv4 privadas y DMZs que utilizan direcciones IPv4 públicas, la planificación y asignación de direcciones es importante.

Cuando sea necesario, el plan de direcciones incluye determinar las necesidades de cada subred en términos de tamaño. ¿Cuántos hosts habrá en cada subred? El plan de direcciones también debe incluir cómo se asignarán las direcciones de host, qué hosts requerirán direcciones IPv4 estáticas y qué hosts pueden usar DHCP para obtener su información de direccionamiento. Esto también ayudará a evitar la duplicación de direcciones, al tiempo que permitirá supervisar y administrar direcciones por razones de rendimiento y seguridad.

Conocer los requisitos de direcciones IPv4 determinará el rango, o intervalos, de direcciones de host que implementa y ayudará a garantizar que haya suficientes direcciones para cubrir sus necesidades de red.

11.9.2

Asignación de direcciones de dispositivo

Dentro de una red, hay diferentes tipos de dispositivos que requieren direcciones:

- **Clientes usuarios finales** la mayoría de las redes asignan direcciones de manera dinámica con el protocolo de configuración dinámica de host (DHCP). Esto reduce la carga sobre el personal de soporte de red y elimina de manera virtual los errores de entrada. Con DHCP, las direcciones sólo se alquilan durante un período de tiempo y se pueden reutilizar cuando caduque la concesión. Esta es una característica importante para las redes que admiten usuarios transitorios y dispositivos inalámbricos. Cambiar el esquema de subredes significa que el servidor DHCP necesita ser reconfigurado y los clientes deben renovar sus direcciones IPv4. Los clientes IPv6 pueden obtener información de dirección mediante DHCPv6 o SLAAC.
- **Servidores y periféricos:** -deben tener una dirección IP estática predecible. Utilice un sistema de numeración coherente para estos dispositivos.
- **Servidores a los que se puede acceder desde Internet**: los servidores que deben estar disponibles públicamente en Internet deben tener una dirección IPv4 pública, a la que se accede con mayor frecuencia mediante NAT. En algunas organizaciones, los servidores internos (no disponibles públicamente) deben ponerse a disposición de los usuarios remotos. En la mayoría de los casos, a estos servidores se les asignan direcciones privadas internamente y se requiere que el usuario cree una conexión de red privada virtual (VPN) para acceder al servidor. Esto tiene el mismo efecto que si el usuario accede al servidor desde un host dentro de la intranet.
- **Dispositivos intermediarios:** -estos dispositivos tienen direcciones asignadas para la administración, monitoreo y seguridad de la red. Debido a que es necesario saber cómo comunicarse con dispositivos intermediarios, estos deben tener asignadas direcciones predecibles y estáticas.
- **Puerta de enlace:** -los routers y los dispositivos de firewall tienen una dirección IP asignada a cada interfaz que sirve como puerta de enlace para los hosts en esa red. Normalmente, la interfaz de router utiliza la dirección más baja o más alta de la red.

Al desarrollar un esquema de direccionamiento IP, generalmente se recomienda que tenga un patrón establecido de cómo se asignan las direcciones a cada tipo de dispositivo. Esto beneficia a los administradores a la hora de agregar y quitar dispositivos, ya que filtra el tráfico basado en IP, y también simplifica el registro.

11.9.3

Packet Tracer - Práctica de Diseño e Implementación de VLSM

En esta actividad, se le proporciona una dirección de red /24 que debe utilizar para diseñar un esquema de direccionamiento VLSM. Según un conjunto de requisitos, asignará subredes y direccionamiento, configurará dispositivos y verificará la conectividad.

Práctica de Diseño e Implementación de VLSM

Práctica de Diseño e Implementación de VLSM

Asignación de direcciones IPv4 / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

11.10.1

"Packet Tracer: Diseño e implementación de un esquema de direccionamiento VLSM"

En este laboratorio diseñará un esquema de direccionamiento VLSM dado una dirección de red y requisitos de host. Configurará el direccionamiento en routeres, conmutadores y hosts de red.

- Diseñe un esquema de direccionamiento IP VLSM según los requisitos.
- Configure el direccionamiento en dispositivos y hosts de red.
- Verifique la conectividad IP.
- Solucione problemas de conectividad según sea necesario.

Diseño e implementación de un esquema de direccionamiento VLSM

Diseño e implementación de un esquema de direccionamiento VLSM

11.10.2

Práctica de laboratorio: Diseño e implementación de un esquema de direccionamiento VLSM

En esta práctica de laboratorio, use la dirección de red 192.168.33.128/25 para desarrollar un esquema de direccionamiento para la red que se muestra en el diagrama de topología. VLSM se utiliza para cumplir con los requisitos de direccionamiento IPv4. Después de diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información

de dirección IP adecuada. Las futuras LAN en BR2 necesitan tener direcciones asignadas, pero no se configurará ninguna interfaz en este momento.

Diseño e implementación de un esquema de direccionamiento VLSM

11.10.3

¿Qué aprendí en este módulo?

IPv4 Addressing Structure

Una dirección IPv4 es una dirección jerárquica de 32 bits que se compone de una porción de red y una porción de host. Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Un host requiere una dirección IPv4 única y una máscara de subred para mostrar las partes de red o host de la dirección. La longitud del prefijo es el número de bits establecido en 1 en la máscara de subred. Se escribe mediante la "notación de barra diagonal", es decir, una "/" seguida por el número de bits fijados en 1. La operación lógica AND es la comparación de dos bits. Sólo un 1 AND 1 produce un 1 y todas las demás combinaciones resultan en un 0. Cualquier otra combinación da como resultado un 0. Dentro de cada red hay direcciones de red, direcciones de host y una dirección de difusión.

IPv4 Unicast, Broadcast, and Multicast

La transmisión unidifusión se refiere a un dispositivo que envía un mensaje a otro dispositivo en comunicaciones uno a uno. Un paquete de unidifusión es un paquete con una dirección IP de destino que es una dirección de unidifusión que es la dirección de un único destinatario. Transmisión de transmisión hace referencia a un dispositivo que envía un mensaje a todos los dispositivos de una red en comunicaciones unipersonales. Los paquetes de difusión tienen una dirección IPv4 de destino que contiene solo números uno (1) en la porción de host. La transmisión de multidifusión reduce el tráfico al permitir que un host envíe un único paquete a un grupo seleccionado de hosts que estén suscritos a un grupo de multidifusión. Un paquete de multidifusión es un paquete con una dirección IP de destino que es una dirección de multidifusión. IPv4 reservó las direcciones de 224.0.0.0 a 239.255.255.255 como rango de multidifusión.

Types of IPv4 Addresses

Las direcciones IPv4 públicas se enrutan globalmente entre routers ISP. No todas las direcciones IPv4 disponibles se pueden usar en Internet. Existen bloques de direcciones denominadas direcciones privadas que la mayoría de las organizaciones usan para asignar direcciones IPv4 a los hosts internos. La mayoría de las redes internas utilizan direcciones IPv4 privadas para dirigirse a todos los dispositivos internos (intranet); sin embargo, estas

direcciones privadas no son enrutables globalmente. Direcciones de bucle invertido utilizadas por un host para dirigir el tráfico hacia sí mismo. Las direcciones locales de vínculo se conocen con más frecuencia como direcciones APIPA o direcciones autoasignadas. En 1981, las direcciones IPv4 se asignaron utilizando direcciones de clase: A, B o C. Las direcciones IPv4 públicas deben ser únicas y se enrutan globalmente a través de Internet. Las direcciones IPv4 e IPv6 son administradas por la IANA, que asigna bloques de direcciones IP a los RIR.

Network Segmentation

En una LAN Ethernet, los dispositivos transmiten para localizar otros dispositivos usando ARP. Los switches propagan las difusiones por todas las interfaces, salvo por aquella en la cual se recibieron. Los routers propagan transmisiones, en cambio, cada interfaz de router conecta un dominio de transmisión y las transmisiones solo se propagan dentro de ese dominio específico. Un dominio de difusión grande es una red que conecta muchos hosts. Un problema con un dominio de difusión grande es que estos hosts pueden generar difusiones excesivas y afectar la red de manera negativa. La solución es reducir el tamaño de la red para crear dominios de difusión más pequeños mediante un proceso que se denomina división en subredes. Estos espacios de red más pequeños se denominan subredes. La división en subredes disminuye el tráfico de red general y mejora su rendimiento. Un administrador puede subred por ubicación, entre redes o por tipo de dispositivo.

Subnet an IPv4 Network

Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red. Esto se realiza por medio de la ampliación de la máscara de subred para que tome prestados algunos de los bits de la porción de host de la dirección a fin de crear bits de red adicionales. Cuantos más bits de host se tomen prestados, mayor será la cantidad de subredes que puedan definirse. Cuantos más bits se prestan para aumentar el número de subredes también reduce el número de hosts por subred. Las redes se subdividen con más facilidad en el límite del octeto de /8 /16 y /24. Las subredes pueden tomar prestados bits de cualquier posición de bit del host para crear otras máscaras.

Subnet a /16 and a /8 Prefix

En una situación en la que se necesita una mayor cantidad de subredes, se requiere una red IPv4 con más bits de host para tomar prestados. Para crear subredes, debe tomar prestados bits de la parte del host de la dirección IPv4 de la red existente. Comenzando de izquierda a derecha con el primer bit de host disponible, pida prestado un bit a la vez hasta que alcance el número de bits necesarios para crear el número de subredes requeridas. Al tomar prestados bits de una dirección /16, comience a tomarlos del tercer octeto, de izquierda a derecha. La primera dirección está reservada para la dirección de red y la última para la dirección de difusión.

Subnet to Meet Requirements

Una red empresarial típica contiene una intranet y una DMZ. Ambos tienen requisitos y desafíos de subcompensación. La intranet utiliza espacio de direcciones IPv4 privado. El 10.0.0.0/8 también se puede subred usando cualquier otro número de longitudes de prefijo, como /12, /18, /20, etc., dando al administrador de red muchas opciones. Debido a que estos dispositivos deben ser accesibles públicamente desde Internet, los dispositivos de la DMZ requieren direcciones IPv4 públicas. Las organizaciones deben maximizar su propio número limitado de direcciones IPv4 públicas. Para reducir el número de direcciones de host no utilizadas por subred, el administrador de red debe subred su espacio de direcciones públicas en subredes con máscaras de subred diferentes. Esto se conoce como máscara de longitud de subred variable (VLSM). Los administradores deben tener en cuenta cuántas direcciones de host se requieren para cada red y cuántas subredes se necesitan.

Variable Length Subnet Masking

La subred tradicional puede satisfacer las necesidades de una organización de su LAN más grande y dividir el espacio de direcciones en un número adecuado de subredes. Pero es probable que también resulte en un desperdicio significativo de direcciones no utilizadas. VLSM permite que un espacio de red se divida en partes desiguales. Con VLSM, la máscara de subred variará dependiendo de cuántos bits se hayan prestado para una subred particular (esta es la parte "variable" del VLSM). VLSM simplemente subdivide una subred. Cuando use VLSM, siempre comience por satisfacer los requisitos de host de la subred más grande. Siga con la división en subredes hasta que se cumplan los requisitos de host de la subred más pequeña. Las subredes siempre deben iniciarse en un límite de bits apropiado.

Structured Design

Un administrador de red debe estudiar los requisitos de red para planificar mejor cómo se estructurarán las subredes de red IPv4. Esto significa mirar toda la red, tanto la intranet como la DMZ, y determinar cómo se segmentará cada área. El plan de direcciones incluye determinar dónde se necesita la conservación de direcciones (generalmente dentro de la DMZ) y dónde hay más flexibilidad (generalmente dentro de la intranet). Cuando se requiera la conservación de direcciones, el plan debe determinar cuántas subredes se necesitan y cuántos hosts por subred. Esto suele ser necesario para el espacio de direcciones IPv4 público dentro de la DMZ. Esto probablemente incluirá el uso de VLSM. El plan de direcciones también debe incluir cómo se asignarán las direcciones de host, qué hosts requerirán direcciones IPv4 estáticas y qué hosts pueden usar DHCP para obtener su información de direccionamiento. Dentro de una red, hay diferentes tipos de dispositivos que requieren direcciones: clientes de usuarios finales, servidores y periféricos, servidores a los que se puede acceder desde Internet, dispositivos intermediarios y puertas de enlace. Al desarrollar un esquema de asignación de direcciones IP, por lo general se recomienda tener un patrón establecido de la forma en que se asignan las direcciones a cada tipo de dispositivo. Esto ayuda al agregar y quitar dispositivos, al filtrar el tráfico basado en IP, así como a simplificar la documentación.

11.10.4

Módulo Quiz - Direccionamiento IPv4

Correcto

Identificó bien las respuestas correctas.

Has tenido 15 respuestas correctas de 15.

1. ¿Cuál es la notación de longitud de prefijo para la máscara de subred 255.255.255.224?

Tema 11.1.0 - El formato binario para 255.255.255.224 es 11111111.11111111.111111.11100000. La longitud del prefijo es el número de 1s consecutivos en la máscara de subred. Por lo tanto, la longitud del prefijo es /27.

- /25
- /26
- (•) /27
- /28

2. ¿Cuántas direcciones de host válidas están disponibles en una subred IPv4 configurada con la máscara /26?

Tema 11.5.0: cuando se usa una máscara / 26, se usan 6 bits como bits de host. Con 6 bits de host, hay disponibles 64 direcciones, pero una de ellas corresponde al número de subred, y otra corresponde a la dirección de difusión. Por lo tanto, se pueden utilizar 62 direcciones para asignar a los dispositivos de red.

- 254
- 190
- 192
- (•) 62
- 64

3. ¿Cuál de las siguientes máscaras de subred se utilizaría si hubiera 5 bits de host disponibles?

Tema 11.1.0: la máscara de subred de 255.255.255.0 tiene 8 bits de host. La máscara 255.255.255.128 da como resultado 7 bits de host. La máscara 255.255.255.224 tiene 5 bits de host. Por último, 255.255.255.240 representa 4 bits de host.

- ○ 255.255.255.0
- ○ 255.255.255.128
- ◉ 255.255.255.224
- ○ 255.255.255.240

4. Un administrador de redes divide la red 192.168.10.0/24 en subredes con máscaras /26. ¿Cuántas subredes de igual tamaño se crean?

Tema 11.5.0: la máscara normal para 192.168.10.0 es / 24. Una máscara /26 indica que se tomaron prestados 2 bits para la división en subredes. Con 2 bits, se pueden crear cuatro subredes de igual tamaño.

- ○ 1
- ○ 2
- ◉ 4
- ○ 8
- ○ 16
- ○ 64

5. ¿Cuál de las siguientes máscaras de subred se representa con la notación de barra diagonal /20?

Tema 11.1.0: la notación de barra diagonal / 20 representa una máscara de subred con 20 1s. Esto se traduciría a 11111111.11111111.11110000.0000, lo que se podría convertir, a su vez, en 255.255.240.0.

- ○ 255.255.255.248
- ○ 255.255.224.0
- ◉ 255.255.240.0
- ○ 255.255.255.0
- ○ 255.255.255.192

6. ¿Cuál de las siguientes afirmaciones es verdadera acerca de las máscaras de subred de longitud variable?

Tema 11.8.0: en el enmascaramiento de subred de longitud variable, los bits se toman prestados para crear subredes. Se pueden tomar prestados bits adicionales para crear más subredes a partir de las subredes originales. Este proceso se puede repetir hasta que no haya bits disponibles para tomar prestados.

- ○ Todas las subredes son del mismo tamaño.
- ◉ El tamaño de cada subred puede ser diferente, según los requisitos.
- ○ Las subredes se pueden dividir en más subredes solamente una vez.
- ○ Se devuelven bits, en lugar de tomárselos prestados, para crear subredes adicionales.

7. ¿Por qué un dispositivo de capa 3 realiza el proceso AND en una dirección IP y en una máscara de subred de destino?

Tema 11.1.0: ANDing nos permite identificar la dirección de red a partir de la dirección IP y la máscara de red.

- ○ Para identificar la dirección de difusión de la red de destino
- ○ Para identificar la dirección del host de destino
- ○ Para identificar las tramas defectuosas
- ◉ Para identificar la dirección de red de la red de destino

8. ¿Cuántas direcciones IP se encuentran disponibles en la red 192.168.1.0/27?

Tema 11.1.0 - La máscara A /27 es la misma que 255.255.255.224. Esto deja libres 5 bits de host. Con 5 bits de host, hay disponibles 32 direcciones IP, pero una de ellas representa el número de subred, y otra representa la dirección de difusión. Por lo tanto, se pueden utilizar 30 direcciones para asignar a los dispositivos de red.

- ○ 256
- ○ 254
- ○ 62
- ◉ 30
- ○ 16
- ○ 32

9. ¿Cuál de las siguientes máscaras de subred se utilizaría si hubiera 4 bits de host disponibles?

Tema 11.1.0: la máscara de subred de 255.255.255.224 tiene 5 bits de host. La máscara 255.255.255.128 da como resultado 7 bits de host. La máscara de 255.255.255.240 tiene 4 bits de host. Finalmente, 255.255.255.248 representa 3 bits de host.

- ○ 255.255.255.224
- ○ 255.255.255.128
- ◉ 255.255.255.240
- ○ 255.255.255.248

10. ¿Qué dos partes son componentes de una dirección IPv4? (Escoja dos opciones).

Tema 11.1.0 - Una dirección IPv4 se divide en dos partes: una parte de red (para identificar la red específica en la que reside un host) y una parte de host (para identificar hosts específicos de una red). Una máscara de subred se utiliza para identificar la longitud de cada porción.

- ☐ porción de de subred
- ☑ porción de red
- ☐ porción lógica
- ☑ porción de host
- ☐ porción física
- ☐ porción de difusión

11. Si un dispositivo de red tiene la máscara /26, ¿cuántas direcciones IP están disponibles para los hosts en esta red?

Tema 11.1.0 - La máscara A / 26 es la misma que 255.255.255.192. Esto deja libres 6 bits de host. Con 6 bits de host, son posibles 64 direcciones IP, pero una dirección representa el número de subred y una dirección representa la dirección de difusión. Por lo tanto, 62 direcciones se pueden asignar a hosts de red.

- ○ 64
- ○ 30
- ◉ 62
- ○ 32
- ○ 16
- ○ 14

12. ¿Qué representa la dirección IP 172.17.4.250/24?

Tema 11.1.0: el /24 muestra que la dirección de red es 172.17.4.0. La dirección de difusión para esta red sería 172.17.4.255. Las direcciones de host disponibles para esta red van de 172.17.4.1 a 172.17.4.254.

- ○ Dirección de red
- ○ Dirección de multidifusión
- ◉ Dirección de host
- ○ Dirección de difusión

13. Si un dispositivo de red tiene la máscara /28, ¿cuántas direcciones IP están disponibles para los hosts en esta red?

Tema 11.1.0: la máscara A / 28 es la misma que 255.255.255.240. Esto deja libres 4 bits de host. Con 4 bits de host, hay disponibles 16 direcciones IP, pero una de ellas representa el número de subred, y otra representa la dirección de difusión. Se pueden utilizar 14 direcciones para asignar a los dispositivos de red.

- ○ 256
- ○ 254
- ○ 62
- ○ 32
- ○ 16
- ◉ 14

14. ¿Cuál es el propósito de la máscara de subred en conjunto con una dirección IP?

Tema 11.1.0 - Con la dirección IPv4, también es necesaria una máscara de subred. Una máscara de subred es un tipo especial de dirección IPv4 que, combinada con la dirección IP, determina de qué subred forma parte el dispositivo.

- ○ Identificar un host en una red de manera única.
- ○ Identificar si la dirección es pública o privada.
- ◉ Determinar la subred a la que pertenece el host.
- ○ Ocultar la dirección IP para las personas ajenas.

15. Un administrador de redes divide una red en subredes de forma variable. La subred más pequeña tiene la máscara 255.255.255.224. ¿Cuántas direcciones de host utilizables proporcionará esta subred?

Tema 11.8.0: la máscara de subred 255.255.255.224 es equivalente al prefijo /27. Esto deja 5 bits para los hosts, proporcionando un total de 30 direcciones IP utilizables (2^{25} = 32 – 2 = 30).

- ○ 2
- ○ 6
- ○ 14
- ◉ 30
- ○ 62

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. What is the prefix length notation for the subnet mask 255.255.255.224?

Topic 11.1.0 – The binary format for 255.255.255.224 is 11111111.11111111.11111111.11100000. The prefix length is the number of consecutive 1s in the subnet mask. Therefore, the prefix length is /27.

- ○ /25
- ○ /26
- ◉ /27
- ○ /28

2. How many valid host addresses are available on an IPv4 subnet that is configured with a /26 mask?

Topic 11.5.0 – When a /26 mask is used, 6 bits are used as host bits. With 6 bits, 64 addresses are possible, but one address is for the subnet number and one address is for a broadcast. This leaves 62 addresses that can be assigned to network devices.

- ○ 254
- ○ 190
- ○ 192
- ◉ 62
- ○ 64

3. Which subnet mask would be used if 5 host bits are available?

Topic 11.1.0 – The subnet mask of 255.255.255.0 has 8 host bits. The mask of 255.255.255.128 results in 7 host bits. The mask of 255.255.255.224 has 5 host bits. Finally, 255.255.255.240 represents 4 host bits.

- ○ 255.255.255.0
- ○ 255.255.255.128
- ◉ 255.255.255.224
- ○ 255.255.255.240

4. A network administrator subnets the 192.168.10.0/24 network into subnets with /26 masks. How many equal-sized subnets are created?

Topic 11.5.0 - The normal mask for 192.168.10.0 is /24. A /26 mask indicates 2 bits have been borrowed for subnetting. With 2 bits, four subnets of equal size could be created.

- ○ 1
- ○ 2
- ◉ 4
- ○ 8
- ○ 16
- ○ 64

5. What subnet mask is represented by the slash notation /20?

Topic 11.1.0 - The slash notation /20 represents a subnet mask with 20 1s. This would translate to: 11111111.11111111.11110000.0000, which in turn would convert into 255.255.240.0.

- ○ 255.255.255.248
- ○ 255.255.224.0
- ◉ 255.255.240.0
- ○ 255.255.255.0
- ○ 255.255.255.192

6. Which statement is true about variable-length subnet masking?

Topic 11.8.0 - In variable-length subnet masking, bits are borrowed to create subnets. Additional bits may be borrowed to create additional subnets within the original subnets. This may continue until there are no bits available to borrow.

- ○ Each subnet is the same size.
- ◉ The size of each subnet may be different, depending on requirements.
- ○ Subnets may only be subnetted one additional time.
- ○ Bits are returned, rather than borrowed, to create additional subnets.

7. Why does a Layer 3 device perform the ANDing process on a destination IP address and subnet mask?

Topic 11.1.0 - ANDing allows us to identify the network address from the IP address and the network mask.

- ○ to identify the broadcast address of the destination network
- ○ to identify the host address of the destination host
- ○ to identify faulty frames
- ◉ to identify the network address of the destination network

8. How many usable IP addresses are available on the 192.168.1.0/27 network?

Topic 11.1.0 - A /27 mask is the same as 255.255.255.224. This leaves 5 host bits. With 5 host bits, 32 IP addresses are possible, but one address represents the subnet number and one address represents the broadcast address. Thus, 30 addresses can then be used to assign to network devices.

- ○ 256
- ○ 254
- ○ 62
- ◉ 30
- ○ 16
- ○ 32

9. Which subnet mask would be used if exactly 4 host bits are available?

Topic 11.1.0 - The subnet mask of 255.255.255.224 has 5 host bits. The mask of 255.255.255.128 results in 7 host bits. The mask of 255.255.255.240 has 4 host bits. Finally, 255.255.255.248 represents 3 host bits.

- ○ 255.255.255.224
- ○ 255.255.255.128
- ◉ 255.255.255.240
- ○ 255.255.255.248

10. Which two parts are components of an IPv4 address? (Choose two.)

Topic 11.1.0 - An IPv4 address is divided into two parts: a network portion - to identify the specific network on which a host resides, and a host portion - to identify specific hosts on a network. A subnet mask is used to identify the length of each portion.

- [ ] subnet portion
- [x] network portion
- [ ] logical portion
- [x] host portion
- [ ] physical portion
- [ ] broadcast portion

11. If a network device has a mask of /26, how many IP addresses are available for hosts on this network?

Topic 11.1.0 - A /26 mask is the same as 255.255.255.192. This leaves 6 host bits. With 6 host bits, 64 IP addresses are possible, but one address represents the subnet number and one address represents the broadcast address. Thus 62 addresses can then be assigned to network hosts.

- ( ) 64
- ( ) 30
- (•) 62
- ( ) 32
- ( ) 16
- ( ) 14

12. What does the IP address 172.17.4.250/24 represent?

Topic 11.1.0 - The /24 shows that the network address is 172.17.4.0. The broadcast address for this network would be 172.17.4.255. Useable host addresses for this network are 172.17.4.1 through 172.17.4.254.

- ( ) network address
- ( ) multicast address
- (•) host address
- ( ) broadcast address

13. If a network device has a mask of /28, how many IP addresses are available for hosts on this network?

Topic 11.1.0 - A /28 mask is the same as 255.255.255.240. This leaves 4 host bits. With 4 host bits, 16 IP addresses are possible, but one address represents the subnet number and one address represents the broadcast address. 14 addresses can then be used to assign to network devices.

- ○ 256
- ○ 254
- ○ 62
- ○ 32
- ○ 16
- ◉ 14

14. What is the purpose of the subnet mask in conjunction with an IP address?

Topic 11.1.0 - With the IPv4 address, a subnet mask is also necessary. A subnet mask is a special type of IPv4 address that coupled with the IP address determines the subnet of which the device is a member.

- ○ to uniquely identify a host on a network
- ○ to identify whether the address is public or private
- ◉ to determine the subnet to which the host belongs
- ○ to mask the IP address to outsiders

15. A network administrator is variably subnetting a network. The smallest subnet has a mask of 255.255.255.224. How many usable host addresses will this subnet provide?

Topic 11.8.0 - The subnet mask 255.255.255.224 is equivalent to the /27 prefix. This leaves 5 bits for hosts, providing a total of 30 usable IP addresses (2^5 = 32 - 2 = 30).

- ○ 2
- ○ 6
- ○ 14
- ◉ 30
- ○ 62

Capítulo 12_Asignación de direcciones IPv6

Introducción

12.0.1

¿Por qué debería tomar este módulo?

Bienvenido a IPv6 Addressing!

¡Es un buen momento para ser (o convertirse) administrador de red! ¿Por qué? Porque en muchas redes, encontrará tanto IPv4 como IPv6 trabajando juntos. Después del duro trabajo de aprender a subred una red IPv4, puede encontrar que la subred de una red IPv6 es mucho más fácil. Probablemente no esperabas eso, ¿verdad? Un Packet Tracer al final de este módulo le dará la oportunidad de subred una red IPv6. ¡Adelante, súbete!

12.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Asignación de direcciones IPv6

Objetivos del módulo: Implemente un esquema de asignación de direcciones IPv6.

Título del tema	Objetivo del tema
Problemas con IPv4	Explique la necesidad de la asignación de direcciones IPv6.
Direccionamiento Dinámico para las GUAs de IPv6	Explique cómo se representan las direcciones IPv6.
Tipos de direcciones IPv6	Compare los tipos de direcciones de red IPv6.
Configuración estática de GUA y LLA	Explicar cómo configurar la unidifusión global estática y IPv6 local de vínculo Direcciones de red.
Direccionamiento dinámico para GUA IPv6	Explique cómo configurar las direcciones global unicast de forma dinámica.
Direccionamiento dinámico para LLA de IPv6	Configure dinámicamente direcciones locales de vínculo.
Direcciones IPv6 de multidifusión	Identificar direcciones IPv6.

Título del tema	Objetivo del tema
División de subredes de una red IPv6	Implementación de un esquema de direccionamiento IPv6 dividido en subredes

Asignación de direcciones IPv6 / Problemas con IPv4

Problemas con IPv4

12.1.1

Necesidad de utilizar IPv6

Ya sabe que IPv4 se está quedando sin direcciones. Es por eso que necesita aprender acerca de IPv6.

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un espacio de direcciones más grande de 128 bits, que proporciona 340 undecillones (es decir, 340 seguidos de 36 ceros) posibles direcciones. Sin embargo, IPv6 es más que solo direcciones más extensas.

Cuando el IETF comenzó a desarrollar un sucesor de IPv4, aprovechó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras. Un ejemplo es el Protocolo de mensajes de control de Internet versión 6 (ICMPv6), que incluye la resolución de direcciones y la configuración automática de direcciones que no se encuentran en ICMP para IPv4 (ICMPv4).

El agotamiento del espacio de direcciones IPv4 fue el factor que motivó la migración a IPv6. A medida que África, Asia y otras áreas del mundo están más conectadas a Internet, no hay suficientes direcciones IPv4 para acomodar este crecimiento. Como se muestra en la ilustración, a cuatro de cinco RIR se les agotaron las direcciones IPv4.

El gráfico muestra un mapa global de los cinco registros regionales de Internet y las fechas de agotamiento IPv4. La fecha de agotamiento de ARINs IPv4 es julio de 2015, los datos de agotamiento de los NCCs RIPE son septiembre de 2012, la fecha de agotamiento de APNIC es junio de 2014, la fecha de agotamiento de LACNIC es abril de 2011 y la fecha de agotamiento proyectada de AfrINICS es 2020.

Fechas de agotamiento de las direcciones IPv4 de RIR

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas en combinación con la traducción de direcciones de red (NAT) fueron esenciales para demorar la reducción del espacio de direcciones IPv4. Sin embargo, NAT es problemático para muchas aplicaciones, crea latencia y tiene limitaciones que impiden severamente las comunicaciones entre pares.

Con el número cada vez mayor de dispositivos móviles, los proveedores de telefonía móvil han estado liderando el camino con la transición a IPv6. Los dos principales proveedores de telefonía móvil en los Estados Unidos informan que más del 90% de su tráfico es sobre IPv6.

La mayoría de los principales proveedores de Internet y proveedores de contenido, como YouTube, Facebook y Netflix, también han hecho la transición. Muchas empresas como Microsoft, Facebook y LinkedIn están haciendo la transición a IPv6 solo internamente. En 2018, el ISP de banda ancha Comcast reportó un despliegue de más del 65% y British Sky Broadcasting más del 86%.

Internet of Things

En la actualidad, Internet es significativamente distinta de cómo era en las últimas décadas. Actualmente, Internet es mucho más que el correo electrónico, las páginas web y la transferencia de archivos entre equipos. Internet evoluciona y se está convirtiendo en una Internet de las cosas (IoT). Ya no serán solo los equipos, las tabletas y los teléfonos inteligentes los únicos dispositivos que accedan a Internet. Los dispositivos del futuro

preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales.

Con una población de Internet cada vez mayor, un espacio limitado de direcciones IPv4, problemas con NAT y el IoT, ha llegado el momento de comenzar la transición a IPv6.

12.1.2

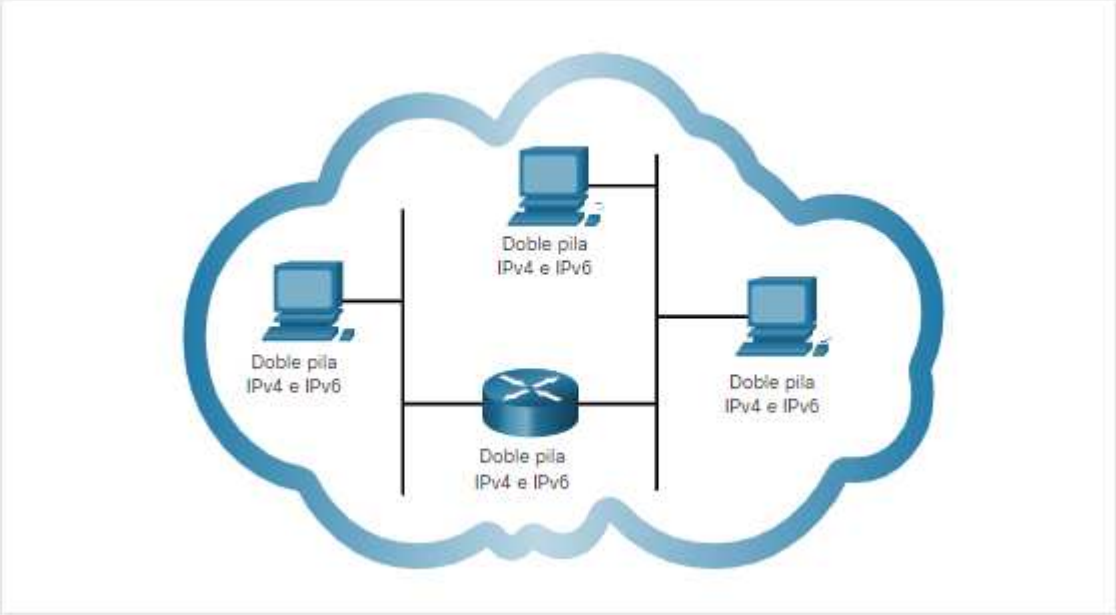
Coexistencia de IPv4 e IPv6

No hay una fecha específica para pasar a IPv6. Tanto IPv4 como IPv6 coexistirán en un futuro próximo y la transición llevará varios años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

Haga clic en cada botón para obtener más información.

Dual-stack | Tunelización | Traducción

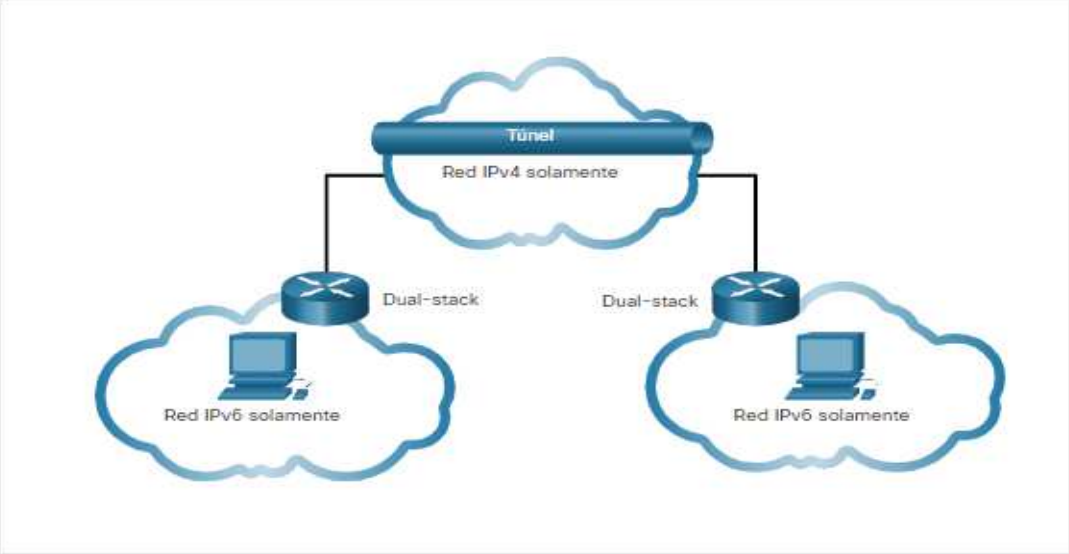
Dual-stack permite que IPv4 e IPv6 coexistan en el mismo segmento de red. Los dispositivos dual-stack ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea. Conocido como IPv6 nativo, esto significa que la red del cliente tiene una conexión IPv6 a su ISP y puede acceder al contenido que se encuentra en Internet a través de IPv6.



Topología física que muestra tres PC de doble pila y un enrutador de doble pila.

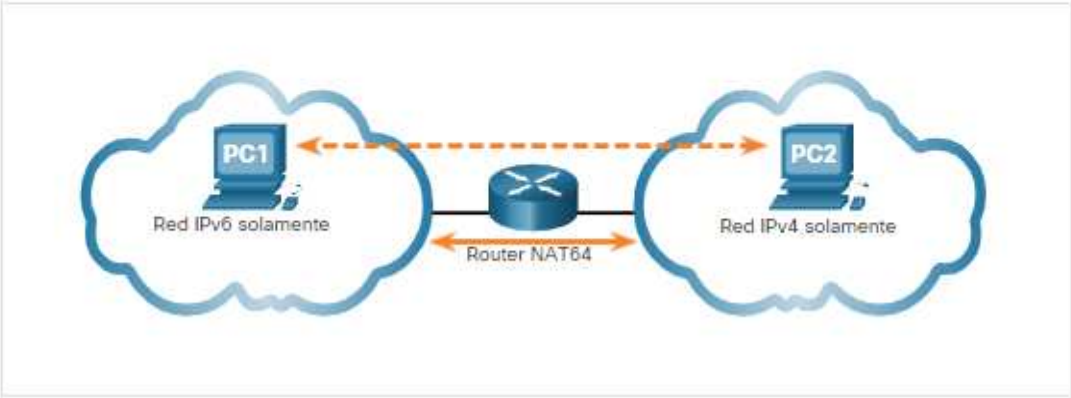
Dual-stack | Tunelización | Traducción

La tunelización es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPv4, de manera similar a lo que sucede con otros tipos de datos.



Dual-stack | Tunelización | Traducción

La traducción de direcciones de redes 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce a un paquete IPv4 y un paquete IPv4 se traduce a un paquete IPv6.



Nota: La tunelización y la traducción son para la transición a IPv6 nativo y solo deben usarse cuando sea necesario. El objetivo debe ser las comunicaciones IPv6 nativas de origen a destino.

12.1.3

Verifique su comprensión - Problemas de IPv4

Verifique su comprensión de los problemas de IPv4 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El controlador principal o el factor más importante para IPv6 es el agotamiento del espacio de direcciones IPv4.
2. La respuesta correcta es verdadero. Cuatro de los cinco RIR, ARIN, APNIC, LACNIC y RIPENCC han agotado sus grupos de direcciones IPv4. Sólo Afrinic tiene espacio de direcciones IPv4 restante para asignar a los clientes.
3. Solo la pila doble usa conectividad IPv6 nativa.

Has tenido 3 respuestas correctas de 3.

1. ¿Cuál es el factor motivador más importante para pasar a IPv6?

¡Lo tienes!

- ○ mejor rendimiento con IPv6
- ○ Direcciones IPv6 que son más fáciles de trabajar con
- ○ mejor seguridad con IPv6
- ◉ agotamiento de direcciones IPv4

2. Verdadero o Falso: 4 de cada 5 RIR ya no tienen suficientes direcciones IPv4 para asignarlas a los clientes de forma regular.

¡Lo tienes!

- ◉ Verdadero
- ○ Falso

3. ¿Cuál de las siguientes técnicas utiliza conectividad IPv6 nativa?

¡Lo tienes!

- ◉ Dual-stack
- ○ Tunelización
- ○ Traducción
- ○ todas las opciones anteriores

Correct

You have successfully identified the correct answers.

1. The main driver or most important factor for IPv6 is the depletion of the IPv4 address space.
2. The correct answer is True. Four of the five RIRs, ARIN, APNIC, LACNIC, and RIPENCC have exhausted their IPv4 address pools. Only AfriNIC has remaining IPv4 address space to allocate to customers.
3. Only dual stack uses native IPv6 connectivity.

You got 3 out of 3 questions correct.

1. What is the most important motivating factor for moving to IPv6?

You got it!

- ○ better performance with IPv6
- ○ IPv6 addresses that are easier to work with
- ○ better security with IPv6
- ◉ depletion of IPv4 addresses

2. True or False: 4 out of 5 RIRs no longer have enough IPv4 addresses to allocate to customers on a regular basis.

You got it!

- ◉ True
- ○ False

3. Which of the following techniques use native IPv6 connectivity?

You got it!

- ◉ dual stack
- ○ tunneling
- ○ translation
- ○ all of the above

Direccionamiento Dinámico para las GUAs de IPv6

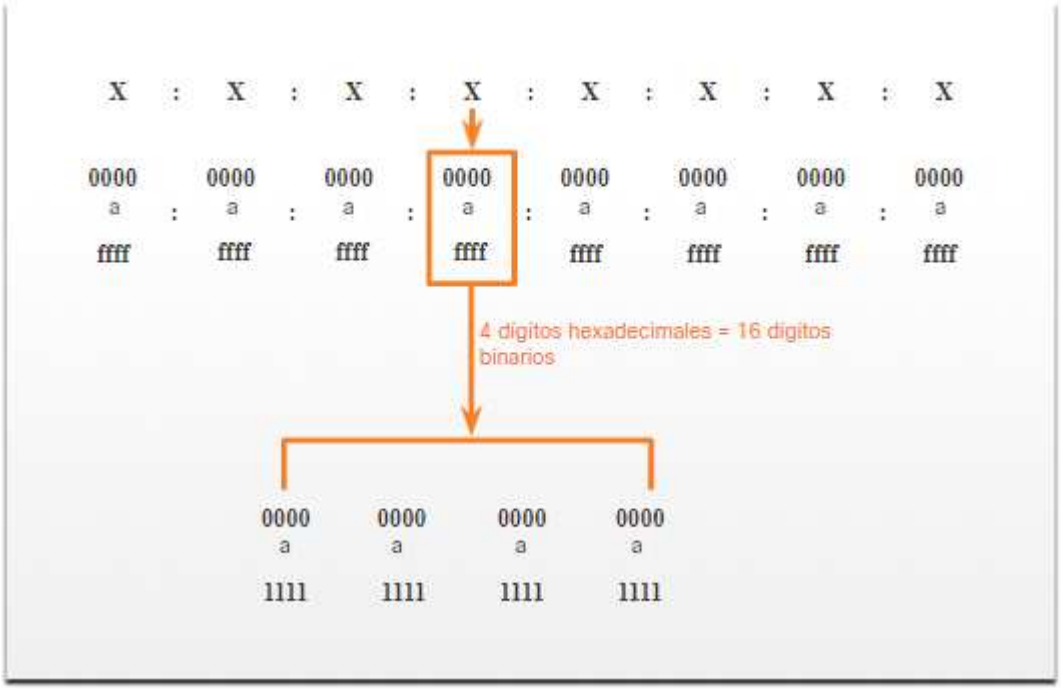
12.2.1

Formatos de direccionamiento IPv6

El primer paso para aprender acerca de IPv6 en las redes es comprender la forma en que se escribe y se formatea una dirección IPv6. Las direcciones IPv6 son mucho más grandes que las direcciones IPv4, por lo que es poco probable que se nos quede sin ellas.

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales, como se muestra en la figura. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.

Segmentos o hexetos de 16 bits



Preferred Format

La figura anterior también muestra que el formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales. El término octeto hace referencia a los ocho bits de una dirección IPv4. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada "x" es un único hexteto que tiene 16 bits o cuatro dígitos hexadecimales.

El formato preferido significa que escribe la dirección IPv6 utilizando los 32 dígitos hexadecimales. No significa necesariamente que sea el método ideal para representar la dirección IPv6. En este módulo, verá dos reglas que ayudan a reducir la cantidad de dígitos necesarios para representar una dirección IPv6.

Estos son ejemplos de direcciones IPv6 en el formato preferido:

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000
```

12.2.2

Regla 1: Omitir los ceros iniciales

La primera regla para ayudar a reducir la notación de las direcciones IPv6 es omitir los ceros (ceros) iniciales en cualquier hexteto. Aquí hay cuatro ejemplos de formas de omitir ceros a la izquierda:

- 01ab se puede representar como 1ab
- 09f0 se puede representar como 9f0
- 0a00 se puede representar como a00
- 00ab se puede representar como ab

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto "abc" podría ser "0abc" o "abc0", pero no representan el mismo valor.

Omisión de ceros iniciales

Tipo	Formato
Recomendado	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Sin ceros iniciales	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200
Recomendado	2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234
Sin ceros iniciales	2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234
Recomendado	2001 : 0db8 : 000a : 0001 : c012 : 90ff : fe90 : 0001
Sin ceros iniciales	2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1
Recomendado	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Sin ceros iniciales	2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0
Recomendado	fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
Sin ceros iniciales	fe80 : 0 : 0 : 0 : 123 : 4567 : 89ab : cdef
Recomendado	fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Sin ceros iniciales	fe80 : 0 : 0 : 0 : 0 : 0 : 0 : 1
Recomendado	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Sin ceros iniciales	0 : 0 : 0 : 0 : 0 : 0 : 0 : 1
Recomendado	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
Sin ceros iniciales	0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

12.2.3

Regla 2 - Doble Colon

La segunda regla para ayudar a reducir la notación de las direcciones IPv6 es que un doble punto (: :) puede reemplazar cualquier cadena única y contigua de uno o más hextetos de 16 bits que consisten en todos los ceros. Por ejemplo, 2001:db8:cafe: 1:0:0:0:1 (0 iniciales omitidos) podría representarse como 2001:db8:cafe:1: :1. El doble colon (::) se utiliza en lugar de los tres hexetos all-0 (0:0:0).

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la

técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como “formato comprimido”.

Aquí hay un ejemplo del uso incorrecto del doble coma: 2001:db8::abcd: :1234.

Los dos puntos dobles se utilizan dos veces en el ejemplo anterior. Aquí están las posibles expansiones de esta dirección de formato comprimido incorrecto:

- 2001:db8::abcd:0000:0000:1234
- 2001:db8::abcd:0000:0000:0000:1234
- 2001:db8:0000:abcd::1234
- 2001:db 8:0000:0000:abcd: :1234

Si una dirección tiene más de una cadena contigua de hextets todo-0, la práctica recomendada es usar los dos puntos dobles (::) en la cadena más larga. Si las cadenas son iguales, la primera cadena debe usar los dos puntos dobles (::).

Omitir 0 a la izquierda y todos los 0 segmentos

Tipo	Formato
Recomendado	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Comprimido/espacios	2001 : db8 : 0 : 1111 : : 200
Comprimido	2001:db8:0:1111::200
Recomendado	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Comprimido / espacios	2001 : db8 : 0 : 0 : ab00 ::
Comprimido	2001:db8:0:0:ab00::
Recomendado	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Comprimido / espacios	2001 : db8 : aaaa : 1 ::
Comprimido	2001:db8:aaaa:1::
Recomendado	fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
Comprimido / espacios	fe80 : : 123 : 4567 : 89ab : cdef
Comprimido	fe80::123:4567:89ab:cdef
Recomendado	fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Comprimido / espacios	fe80 : : 1
Comprimido	fe80::1
Recomendado	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Comprimido / espacios	: : 1
Comprimido	::1
Recomendado	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
Comprimido / espacios	: :
Comprimido	::

12.2.4

Actividad: representación de dirección IPv6

Instrucciones:

Convierta las direcciones IPv6 en formatos cortos (omita los ceros iniciales) y comprimidos. Escriba letras en minúsculas. Haga clic en Siguiente para avanzar la actividad a la siguiente dirección.

1. Asignación de direcciones IPv6
2. Tipos de direcciones IPv6

Tipos de direcciones IPv6

12.3.1

Unidifusión, Multidifusión, difusión ilimitada

Al igual que con IPv4, existen diferentes tipos de direcciones IPv6. De hecho, existen tres categorías amplias de direcciones IPv6:

- **Unicast** - una dirección de unidifusión IPv6 identifica de forma exclusiva una interfaz en un dispositivo habilitado para IPv6.
- **Multicast** - una dirección de multidifusión IPv6 se usa para enviar un único paquete IPv6 a múltiples destinos.
- **Anycast** - una dirección de difusión ilimitada de IPv6 es cualquier dirección de unidifusión de IPv6 que se puede asignar a varios dispositivos. Los paquetes enviados a una dirección de difusión por proximidad se enrutan al dispositivo más cercano que tenga esa dirección. Las direcciones de difusión por proximidad exceden el ámbito de este curso.

A diferencia de IPv4, IPv6 no tiene una dirección de difusión. Sin embargo, existe una dirección IPv6 de multidifusión de todos los nodos que brinda básicamente el mismo resultado.

12.3.2

Longitud de prefijo IPv6

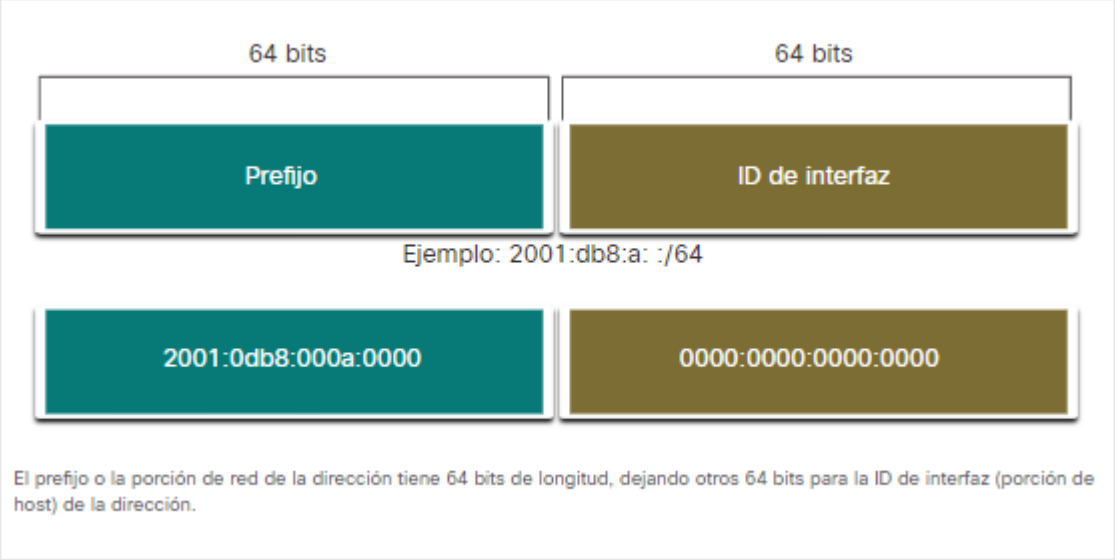
El prefijo, o porción de red, de una dirección IPv4 se puede identificar mediante una máscara de subred decimal o longitud de prefijo (notación de barra). Por ejemplo, la dirección IPv4 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

En IPv4 el /24 se llama prefijo. En IPv6 se llama longitud de prefijo. IPv6 no utiliza la notación decimal punteada de máscara de subred. Al igual que IPv4, la longitud del prefijo se representa en notación de barra inclinada y se usa para indicar la porción de red de una dirección IPv6.

La longitud de prefijo puede ir de 0 a 128. La longitud recomendada del prefijo IPv6 para las LAN y la mayoría de los otros tipos de redes es / 64, como se muestra en la figura.

El gráfico muestra una dirección IPv6 dividida en un prefijo de 64 bits y un ID de interfaz de 64 bits. El prefijo de 64 bits es 2001:0 db 8:000 a:0000. El ID de interfaz de 64 bits es 0000:0000:0000:0000.

Longitud de prefijo IPv6



Se recomienda encarecidamente utilizar un ID de interfaz de 64 bits para la mayoría de las redes. Esto se debe a que la autoconfiguración de direcciones sin estado (SLAAC) utiliza 64 bits para el Id. de interfaz. También facilita la creación y gestión de subredes.

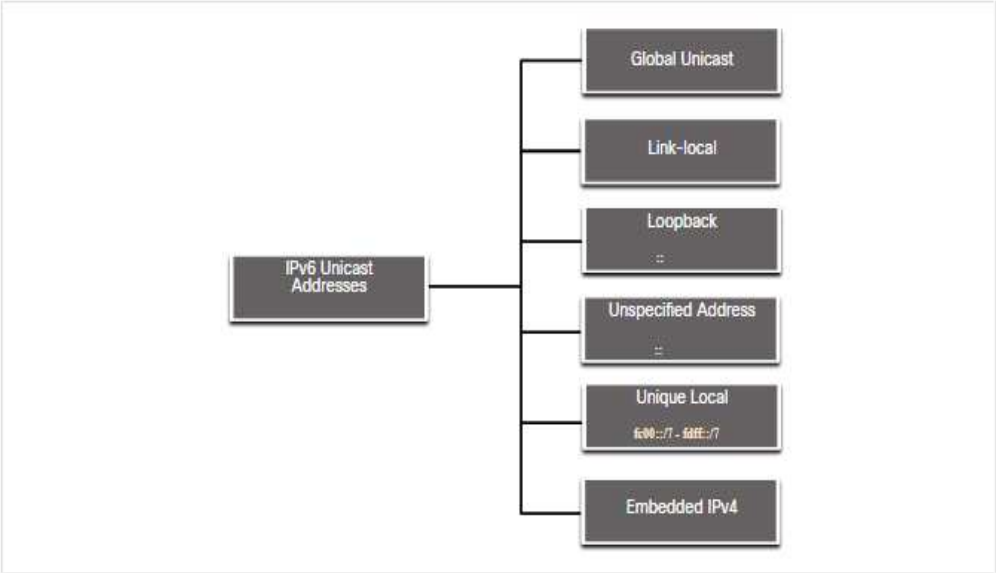
12.3.3

Tipos de direcciones de unidifusión IPv6

Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. La interfaz a la que se le asigna esa dirección recibe un paquete enviado a una dirección de unidifusión. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones de unidifusión. Las direcciones IPv6 de destino pueden ser direcciones de unidifusión o de multidifusión. La figura muestra los diferentes tipos de direcciones de unidifusión IPv6.

El gráfico muestra un gráfico de seis tipos de direcciones de unidifusión IPv6. De arriba a abajo, los tipos de direcciones IPv6 en el gráfico son: Unidifusión global, Link-Local, Loopback: :1/128, Unspecified: :/128, Unique local fc00: :/7 - fdff: :/7 e IPv4 incrustado.

IPv6 Unicast Addresses



A diferencia de los dispositivos IPv4 que tienen una sola dirección, las direcciones IPv6 suelen tener dos direcciones de unidifusión:

- **Dirección de unidifusión global (GUA):** - es similar a una dirección IPv4 pública. Estas son direcciones enrutables de Internet globalmente exclusivas. Las GUA pueden configurarse estáticamente o asignarse dinámicamente.
- **Dirección local de enlace (LLA):** - se requiere para cada dispositivo habilitado para IPv6. Los LLA se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término "enlace" hace referencia a una subred. Las LLA se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.

12.3.4

Una nota sobre la dirección local única

Las direcciones locales únicas (rango fc00: :/7 a fdff: :/7) aún no se implementan comúnmente. Por lo tanto, este módulo sólo cubre la configuración GUA y LLA. Sin embargo, se pueden usar direcciones locales únicas para dirigir dispositivos a los que no se debe acceder desde el exterior, como servidores internos e impresoras.

Se pueden utilizar direcciones locales únicas para dispositivos que nunca necesitarán acceder a otra red.

- Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios.

- Se pueden utilizar direcciones locales únicas para dispositivos que nunca necesitarán acceder a otra red. Las direcciones locales* únicas no se enrutan o traducen globalmente a una dirección IPv6 global.

Nota: Muchos sitios también usan la naturaleza privada de las direcciones RFC 1918 para intentar proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso previsto de estas tecnologías, y el IETF siempre ha recomendado que los sitios tomen las precauciones de seguridad adecuadas en sus enrutadores con conexión a Internet.

12.3.5

IPv6 GUA

Las direcciones IPv6 unicast globales (GUA) son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Corporación de Internet para la Asignación de Nombres y Números (ICANN), operador de la IANA, asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se están asignando GUAs con los primeros tres bits de 001 o 2000:: / 3, como se muestra en la figura.

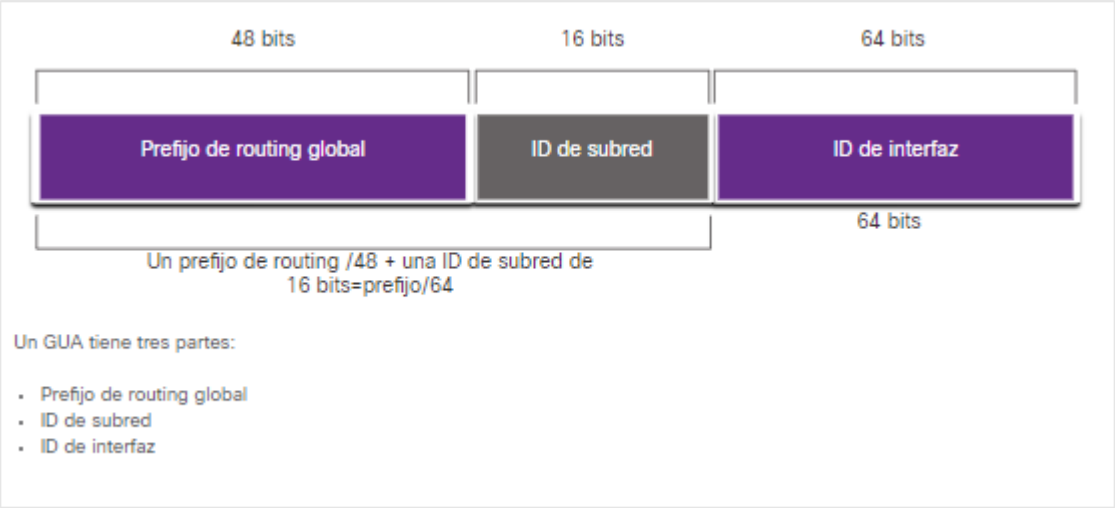
La figura muestra el rango de valores para el primer hexteto donde el primer dígito hexadecimal para las GUA disponibles actualmente comienza con un 2 o un 3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones de unidifusión y multidifusión.

Nota: La dirección 2001: db8:: / 32 se ha reservado para fines de documentación, incluido el uso en ejemplos.

El gráfico muestra las tres partes de un GUA: Primero es el prefijo de enrutamiento global, luego el ID de subred y, finalmente, el ID de interfaz. Los tres primeros bits del prefijo de enrutamiento global son 001. El rango del primer hextexto se muestra entre 0010 0000 0000 0000 0000 (2000) y 0011 1111 1111 1111 (3fff).

La siguiente figura muestra la estructura y el rango de una GUA.

Dirección IPv6 con un prefijo de enrutamiento global /48 y un prefijo /64



El gráfico muestra las tres partes de un GUA: Primero es el prefijo de enrutamiento global que tiene 48 bits de longitud, luego el ID de subred que tiene 16 bits de longitud, luego finalmente el ID de interfaz que tiene 64 bits de longitud. El texto debajo del gráfico indica el prefijo de enrutamiento A / 48 + ID de subred de 16 bits = / 64 prefijo.

12.3.6

Estructura IPv6 GUA

Prefijo Global de Enrutamiento

El prefijo de routing global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. Por ejemplo, es común que los ISP asignen un prefijo de enrutamiento global /48 a sus clientes. El prefijo de enrutamiento global suele variar dependiendo de las políticas del ISP.

La figura anterior muestra un GUA que utiliza un prefijo de enrutamiento global /48. Los prefijos / 48 son un prefijo de enrutamiento global común que se asigna y se utilizará en la mayoría de los ejemplos a lo largo de este curso.

Por ejemplo, la dirección IPv6 2001: db8: acad:: / 48 tiene un prefijo de enrutamiento global que indica que los primeros 48 bits (3 hextetos) (2001: db8: acad) es cómo el ISP conoce este prefijo (red). Los dos puntos dobles (: :) que siguen a la longitud del prefijo / 48 significa que el resto de la dirección contiene todos los 0. El tamaño del prefijo de routing global determina el tamaño de la ID de subred.

ID de subred

El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz. A diferencia de IPv4, donde debe tomar prestados bits de la parte del host para crear subredes, IPv6 se diseñó teniendo en cuenta la subred. Las organizaciones utilizan la ID de subred para identificar subredes dentro de su ubicación. Cuanto mayor es la ID de subred, más subredes habrá disponibles.

Nota: Muchas organizaciones reciben un prefijo de enrutamiento global /32. El uso del prefijo /64 recomendado para crear un ID de interfaz de 64 bits deja un ID de subred de 32 bits. Esto significa que una organización con un prefijo de enrutamiento global /32 y un Id. de subred de 32 bits tendrá 4.300 millones de subredes, cada una con 18 quintillion de dispositivos por subred. ¡Son tantas subredes como direcciones IPv4 públicas!

La dirección IPv6 de la figura anterior tiene un prefijo de enrutamiento global /48, que es común entre muchas redes empresariales. Esto hace que sea especialmente fácil examinar las diferentes partes de la dirección. Usando una longitud de prefijo / 64 típica, los primeros cuatro hextetos son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hextetos restantes son para la ID de interfaz.

ID de Interface

La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término “ID de interfaz” debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6. La figura muestra un ejemplo de la estructura de un GUA IPv6. Se recomienda encarecidamente que en la mayoría de los casos se utilicen subredes / 64, lo que crea una ID de interfaz de 64 bits. Un ID de interfaz de 64 bits permite 18 quintillion de dispositivos o hosts por subred.

Una subred o prefijo /64 (prefijo de enrutamiento global + ID de subred) deja 64 bits para el ID de interfaz. Esto se recomienda para permitir que los dispositivos habilitados para SLAAC creen su propio ID de interfaz de 64 bits. También hace que el desarrollo de un plan de direccionamiento IPv6 sea sencillo y eficaz.

Nota: A diferencia de IPv4, en IPv6, las direcciones de host todo-0 y todo-1 se pueden asignar a un dispositivo. La dirección all-1s se puede utilizar porque las direcciones de difusión no se utilizan en IPv6. Las direcciones compuestas solo por ceros también pueden usarse, pero se reservan como dirección de difusión por proximidad subred-router, y solo deben asignarse a los routers.

12.3.7

IPv6 LLA

Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunique con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred). Los paquetes con un LLA de origen o destino no se pueden enrutar más allá del enlace desde el que se originó el paquete.

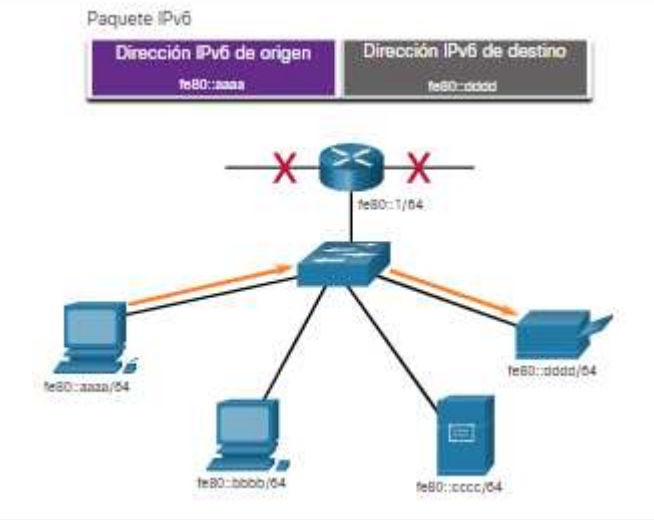
La GUA no es un requisito. Sin embargo, cada interfaz de red habilitada para IPv6 debe tener una LLA.

Si un LLA no se configura manualmente en una interfaz, el dispositivo creará automáticamente el suyo sin comunicarse con un servidor DHCP. Los hosts con IPv6 habilitado crean un LLA de IPv6 incluso si el dispositivo no tiene asignada una dirección IPv6 de unidifusión global. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

Las LLAS IPv6 están en el rango fe80: :/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hextet tiene un rango de 1111 1110 10**00 0000** (fe80) to 1111 1110 10**11 1111** (febf).

La figura muestra un ejemplo de comunicación utilizando LLA de IPv6. El PC es capaz de comunicarse directamente con la impresora utilizando las LLA.

Comunicaciones de enlace local de IPv6



Topología física que muestra dos PC, un servidor, una impresora, un conmutador y un enrutador. Representa que las comunicaciones locales de enlace no se enrutan fuera de la red.

La siguiente figura muestra algunos de los usos de las LLA IPv6.

El gráfico muestra dos enrutadores conectados por un vínculo con sus direcciones LLA. El número 1 con una flecha bidireccional que apunta a cada router está sobre el enlace junto con el texto Mensajes de protocolo de enrutamiento. Una PC está conectada al enrutador de la izquierda con un número 2 una flecha que apunta desde la PC al enrutador. El texto debajo del gráfico dice 1. Los enrutadores utilizan la LLA de los enrutadores vecinos para enviar actualizaciones de enrutamiento. 2. Los hosts utilizan la LLA de un enrutador local como la puerta de enlace predeterminada.

Nota: Por lo general, es el LLA del enrutador, y no la GUA, que se usa como la puerta de enlace predeterminada para otros dispositivos en el enlace.

Hay dos maneras en que un dispositivo puede obtener una LLA:

- **Estáticamente** \ - Esto significa que el dispositivo se ha configurado manualmente.
- **Dinámicamente** \ - Esto significa que el dispositivo crea su propio ID de interfaz utilizando valores generados aleatoriamente o utilizando el método Identificador único extendido (EUI), que utiliza la dirección MAC del cliente junto con bits adicionales.

12.3.8

Verifique su comprensión - Tipos de dirección IPv6

Verifique su comprensión de los tipos de dirección IPv6 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La mayoría de las subredes IPv6 tendrán una longitud de prefijo de /64.
2. El prefijo de enrutamiento global es la parte de una GUA asignada por un ISP.
3. Las direcciones IPv6 locales de vínculo son para la comunicación de sólo vínculos y no se pueden enrutar.
4. La respuesta correcta es falso. Las GUA no utilizan un bit del ID de interfaz para crear subredes.
5. Las direcciones IPv6 locales de vínculo comienzan con el prefijo fe80.

Has tenido 5 respuestas correctas de 5.

1. ¿Cuál es la longitud de prefijo recomendada para la mayoría de las subredes IPv6?

¡Lo tienes!

- ○ /32
- ○ /48
- ◉ /64
- ○ /128

2. ¿Qué parte de un GUA es asignada por el ISP?

¡Lo tienes!

- ◉ Prefijo de routing global
- ○ Prefijo de enrutamiento global e ID de subred
- ○ Prefijo
- ○ Prefijo RIR

3. ¿Qué tipo de dirección de unidifusión IPv6 no se puede enrutar entre redes?

¡Lo tienes!

- ○ dirección local única
- ○ GUA
- ○ dirección IPv4 incrustada
- ◉ • Sí

4. True o False: el campo ID de subred de un GUA debe tomar prestados bits del ID de interfaz.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

5. ¿Qué tipo de dirección IPv6 comienza con fe80?

¡Lo tienes!

- ○ GUA
- ◉ • Sí
- ○ dirección de multidifusión
- ○ Ninguno. Una dirección IPv6 debe comenzar con 2001

Correct

You have successfully identified the correct answers.

1. Most IPv6 subnets will have a prefix length of /64.
2. The global routing prefix is the part of a GUA that is assigned by an ISP.
3. Link-local IPv6 addresses are for link only communication and are not routable.
4. The correct answer is False. GUAs do not use a bit from the interface ID to create subnets.
5. Link-local IPv6 addresses start with the prefix fe80.

You got 5 out of 5 questions correct.

1. What is the recommended prefix length for most IPv6 subnets?

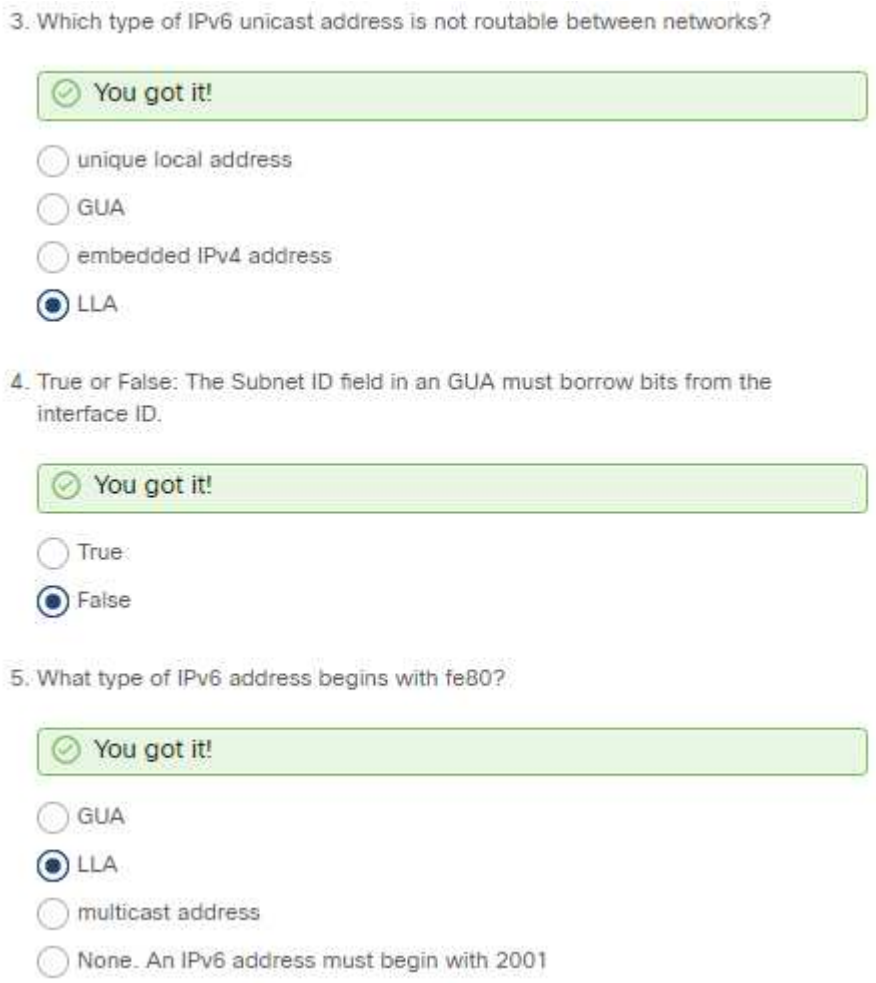
You got it!

- ○ /32
- ○ /48
- ◉ /64
- ○ /128

2. Which part of a GUA is assigned by the ISP?

You got it!

- ◉ Global Routing Prefix
- ○ Global Routing Prefix and Subnet ID
- ○ Prefix
- ○ RIR Prefix



Asignación de direcciones IPv6 / Configuración estática de GUA y LLA

Configuración estática de GUA y LLA

12.4.1

Configuración de GUA estática en un router

Como aprendió en el tema anterior, las GUA IPv6 son las mismas que las direcciones IPv4 públicas. Ellas son globalmente únicas y enrutables en Internet IPv6. Una URL IPv6 permite que dos dispositivos habilitados para IPv6 se comuniquen entre sí en el mismo vínculo (subred). Es fácil configurar estáticamente las GUA y las LAs IPv6 en los enrutadores para ayudarle a crear una red IPv6. ¡Este tema te enseña cómo hacer exactamente eso!

La mayoría de los comandos de configuración y verificación IPv6 de Cisco IOS son similares a sus equivalentes de IPv4. En muchos casos, la única diferencia es el uso de **ipv6** en lugar de **ip** dentro de los comandos.

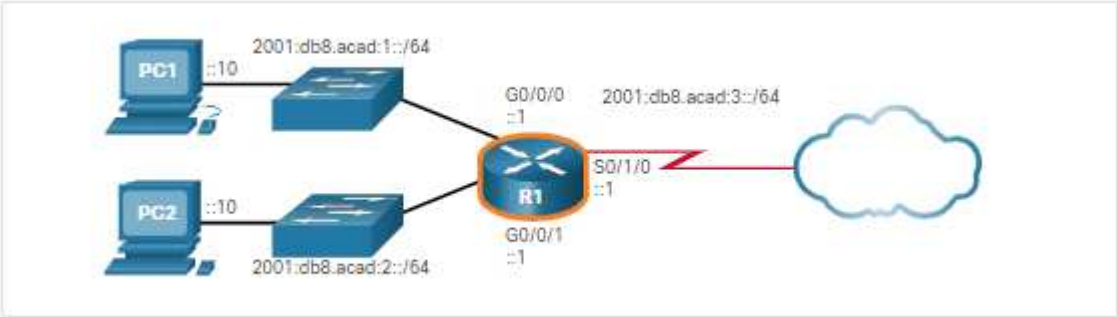
Por ejemplo, el comando de Cisco IOS para configurar una dirección IPv4 en una interfaz es **ip address** *ip-address subnet-mask*. Por el contrario, el comando para configurar un GUA IPv6 en una interfaz es **ipv6 address** *ipv6-address/prefix-length*.

Observe que no hay espacio entre *ipv6-address* y *prefix-length*.

La configuración de ejemplo utiliza la topología que se muestra en la figura y estas subredes IPv6:

- 2001:db8:acad:1: /64
- 2001:db8:acad:2: /64
- 2001:db8:acad:3:/64

Topología de ejemplo



El gráfico muestra dos PC, PC1 y PC2. PC1 está conectado a un switch y tiene la dirección IPv6 2001:db8:acad:1: :10/64. PC2 está conectado a un switch y tiene la dirección IPv6 2001:db8:acad:2: :10/64. Los dos switches están conectados a un router, R1. PC1 se conecta a través del conmutador a la interfaz R1s G0/0/0 que tiene dirección IPv6 2001:db8:acad:1: :1/64. PC2 se conecta a través del conmutador a la interfaz R1s G0/0/1 que tiene dirección IPv6 2001:db8:acad:2: :1/64. R1 se conecta a la nube a través de su interfaz S0/1/0 que tiene dirección IPv6 2001:db8:acad:3: :1/64.

El ejemplo muestra los comandos necesarios para configurar la GUA IPv6 en GigabitEthernet 0/0/0, GigabitEthernet 0/0/1 y la interfaz Serial 0/1/0 de R1.

Configuración de IPv6 GUA en el router R1

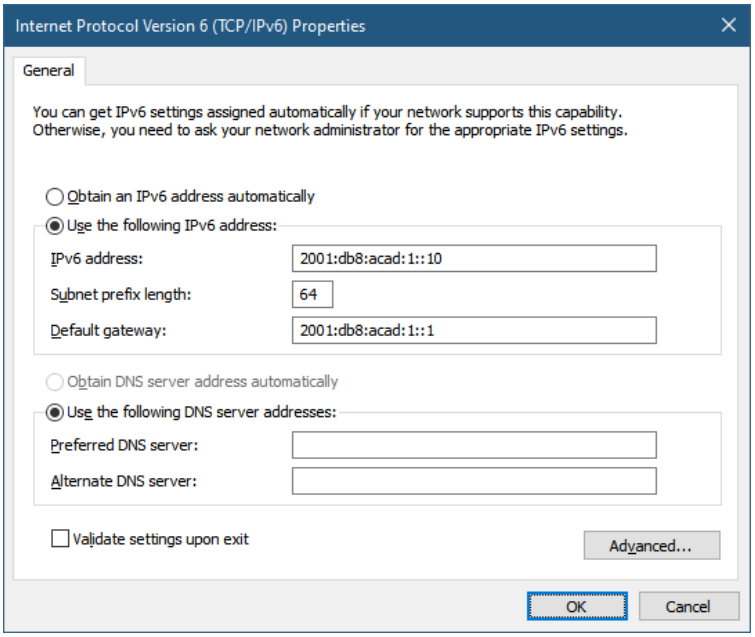
```
R1(config)# interfaz gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interfaz gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

12.4.2

Configuración de GUA estática en un host de Windows

Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.

Como se muestra en la figura, la dirección de puerta de enlace predeterminada configurada para PC1 es 2001: db8: acad: 1:: 1. Esta es la GUA de la interfaz R1 GigabitEthernet en la misma red. Alternativamente, la dirección de puerta de enlace predeterminada se puede configurar para que coincida con el LLA de la interfaz GigabitEthernet. El uso de la LLA del enrutador como dirección de puerta de enlace predeterminada se considera una práctica recomendada. Cualquiera de las dos configuraciones funciona.



El gráfico muestra la ventana Propiedades del Protocolo de Internet de Windows Versión 6 (TCP / IPv6). El botón Usar la siguiente dirección IPv6 está seleccionado. La dirección IPv6 es 2001:db8:acad:1: :1. La longitud del prefijo de subred es 64. La puerta de enlace predeterminada es 2001:db8:acad:1: :1. El botón Usar la siguiente dirección de servidor DNS está seleccionado.

Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de redes en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Hay dos formas en que un dispositivo puede obtener una GUA IPv6 automáticamente:

- Configuración automática de direcciones independiente del estado (SLAAC)
- DHCPv6 con información de estado

SLAAC y DHCPv6 se tratan en el siguiente tema.

Nota: Cuando se utiliza DHCPv6 o SLAAC, el LLA del enrutador se especificará automáticamente como la dirección de puerta de enlace predeterminada.

12.4.3

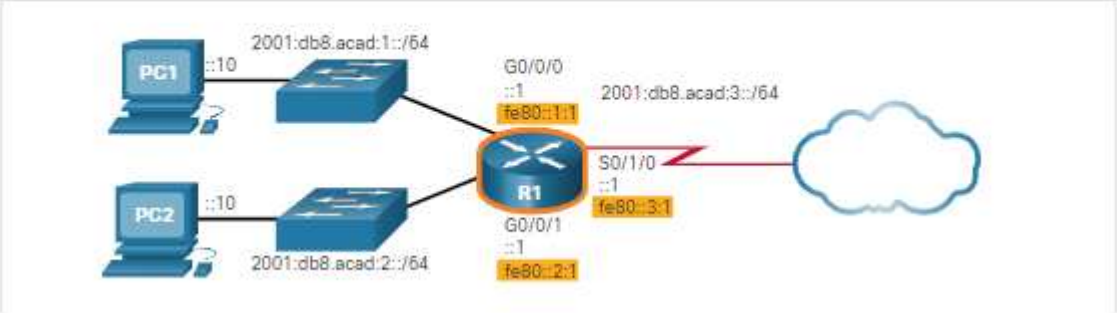
Configuración estática de una dirección de unidifusión local de enlace

Configurar la LLA manualmente permite crear una dirección reconocible y más fácil de recordar. Por lo general, solo es necesario crear LLA reconocibles en los enrutadores. Esto es beneficioso porque los LLA de enrutador se usan como direcciones de puerta de enlace predeterminadas y en el enrutamiento de mensajes publicitarios.

Las LLAS se pueden configurar manualmente mediante el comando **ipv6 address***ipv6-link-local-address*.**link-local**. Cuando una dirección comienza con este hexteto dentro del rango de fe80 a febf, el parámetro **link-local** debe seguir a la dirección.

La figura muestra un ejemplo de topología con LLA en cada interfaz.

Ejemplo de topología con LLAS



El gráfico muestra dos PC, PC1 y PC2.
PC1 está conectado a un conmutador y tiene la dirección IPv6 2001: db8: acad:1:: 10/64.
PC2 está conectado a un conmutador y tiene la dirección IPv6 2001: db8: acad:2:: 10/64.
Los dos interruptores están conectados a un enrutador, R1.
PC1 se conecta a través del conmutador a la interfaz R1s G0/0/0 que tiene la dirección IPv6 2001:db8:acad:1: :1/64 y la dirección LLA fe80:: 1:1.
PC2 se conecta a través del conmutador a la interfaz R1s G0/0/1 que tiene la dirección IPv6 2001:db8:acad:2: :1/64 y la dirección LLA fe80:: 2:1.
R1 se conecta a la nube a través de su interfaz S0/1/0 que tiene dirección IPv6 2001:db8:acad:3: :1/64 y la dirección LLA de fe80:: 3:1.

El ejemplo muestra la configuración de un LLA en el router R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address fe80::2:1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address fe80::3:1 link-local
R1(config-if)# exit
```

Las LAs configuradas estáticamente se utilizan para hacerlas más fácilmente reconocibles como pertenecientes al router R1. En este ejemplo, todas las interfaces del router R1 se han configurado con un LLA que comienza con **fe80::1:**n y un dígito único «n» a la derecha. El «**1**» representa el router R1.

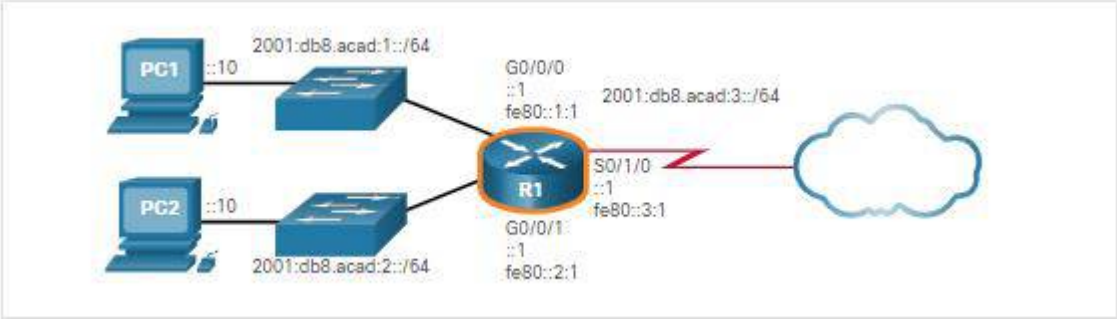
Siguiendo la misma sintaxis que el router R1, si la topología incluía el router R2, tendría sus tres interfaces configuradas con las LAs fe80:: 2:1, fe80:2:2 y fe80:: 2:3.

Nota: Se podría configurar exactamente la misma LLA en cada enlace siempre que sea único en ese enlace. Esto se debe a que los LLA solo tienen que ser únicos en ese enlace. Sin embargo, la práctica común es crear un LLA diferente en cada interfaz del router para facilitar la identificación del router y la interfaz específica.

12.4.4

Comprobador de sintaxis: configuración estática GUA y LLA

Asigne GUA y LAs IPv6 a las interfaces especificadas en el router R1.



El gráfico muestra dos PC, PC1 y PC2. PC1 está conectado a un conmutador y tiene la dirección IPv6 2001: db8: acad: 1 :: 10/64. PC2 está conectado a un switch y tiene la dirección IPv6 2001:db8:acad:2: :10/64. Los dos interruptores están conectados a un enrutador, R1. La PC1 se conecta a través del conmutador a la interfaz R1s G0 / 0/0 que tiene la dirección IPv6 2001: db8: acad: 1 :: 1/64 y la dirección LLA de fe80 :: 1: 1. PC2 se conecta a través del conmutador a la interfaz R1s G0 / 0/1 que tiene la dirección IPv6 2001: db8: acad: 2 :: 1/64 y la dirección LLA de fe80 :: 2: 1. R1 se conecta a la nube a través de su interfaz S0/1/0 que tiene dirección IPv6 2001:db8:acad:3: :1/64 y la dirección LLA de fe80:: 3:1.

R1::10::10S0/1/0::1fe80::3:1PC12001:db8.acad:2::/642001:db8.acad:1::/642001:db8.acad:3::/64G0/0/0::1fe80::1:1G0/0/1::1fe80::2:1PC2R1

Configure and activate IPv6 on the Gigabit Ethernet 0/0/0 interface with the following addresses:

- Use **g0/0/0** as the interface name
- LLA - fe80::1:1
- GUA - 2001:db8:acad:1::1/64
- Activate the interface
- Exit interface configuration mode

```
R1(config)#interface g0/0/0
R1(config-if)#ipv6 address fe80::1:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:1::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
R1(config-if)#exit
```

Configure and activate IPv6 on the Gigabit Ethernet 0/0/1 interface with the following addresses:

- Use **g0/0/1** as the interface name
- LLA - fe80::2:1
- GUA - 2001:db8:acad:2::1/64
- Activate the interface
- Exit interface configuration mode

```
R1(config)#interface g0/0/1
R1(config-if)#ipv6 address fe80::2:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:2::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
R1(config-if)#exit
```

Configure and activate IPv6 on the serial 0/1/0 interface with the following addresses:

- Use **s0/1/0** as the interface name
- LLA - fe80::3:1
- GUA - 2001:db8:acad:3::1/64
- Activate the interface
- Exit interface configuration mode

```
R1(config)#interface s0/1/0
R1(config-if)#ipv6 address fe80::3:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:3::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial0/1/0, changed state to up
R1(config-if)#exit

R1(config)#
You successfully configured IPv6 GUAs on the interfaces of router R1.
```

Direccionamiento dinámico para GUA IPv6

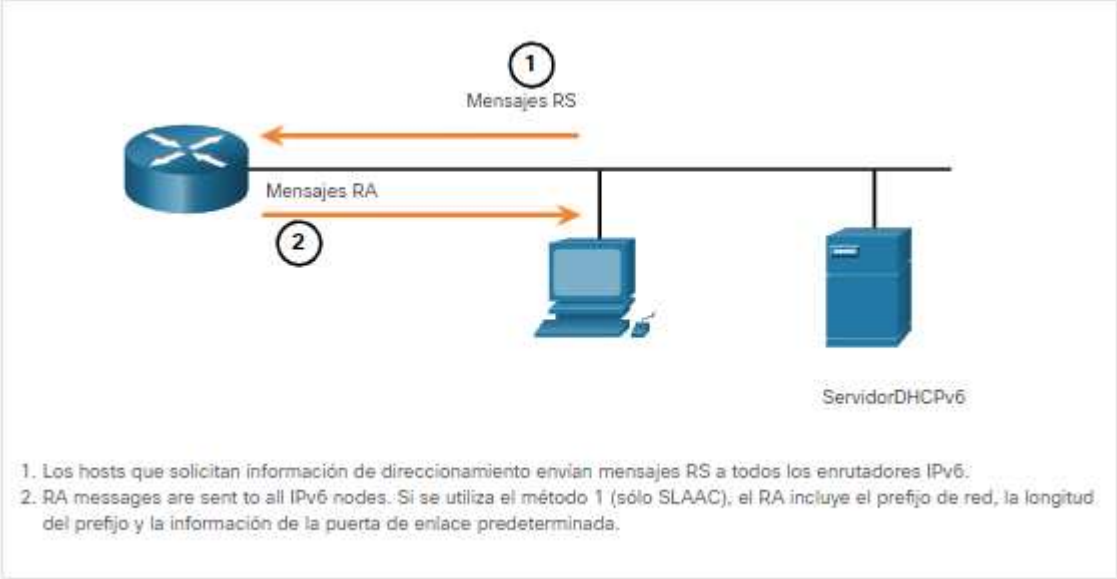
12.5.1

Mensajes RS y RA

Si no desea configurar estáticamente las GUA IPv6, no hay necesidad de preocuparse. La mayoría de los dispositivos obtienen sus GUA IPv6 de forma dinámica. En este tema se explica cómo funciona este proceso mediante mensajes de anuncio de enrutador (RA) y solicitud de enrutador (RS). Este tema se vuelve bastante técnico, pero cuando comprenda la diferencia entre los tres métodos que puede usar un anuncio de enrutador, así como cómo el proceso EUI-64 para crear un ID de interfaz difiere de un proceso generado aleatoriamente, ¡habrá dado un gran salto en su experiencia en IPv6!

Para el GUA, un dispositivo obtiene la dirección dinámicamente a través de mensajes del Protocolo de mensajes de control de Internet versión 6 (ICMPv6). Los routers IPv6 envían mensajes RA de ICMPv6 periódicamente, cada 200 segundos, a todos los dispositivos con IPv6 habilitado en la red. También se enviará un mensaje RA en respuesta a un host que envía un mensaje ICMPv6 RS, que es una solicitud de un mensaje RA. Ambos mensajes se muestran en la figura.

Mensajes de RS y RA de ICMPv6



1. Los hosts que solicitan información de direccionamiento envían mensajes RS a todos los enrutadores IPv6.
2. RA messages are sent to all IPv6 nodes. Si se utiliza el método 1 (sólo SLAAC), el RA incluye el prefijo de red, la longitud del prefijo y la información de la puerta de enlace predeterminada.

El gráfico muestra la LAN con un host que envía un mensaje RS hacia el router y el router que envía un mensaje RA a cambio hacia el PC. También en la LAN hay un servidor DHCPv6. El texto debajo del gaphic dice 1. Los hosts que solicitan información de direccionamiento envían mensajes RS a todas las rotues IPv6. 2. Los mensajes RA se envían a todos los nodos IPv6. Si se utiliza el método 1 (sólo SLAAC), el RA incluye el prefijo, la longitud de referencia y la información de la puerta de enlace predeterminada.

Los mensajes RA están en interfaces Ethernet del router IPv6. El enrutador debe estar habilitado para el enrutamiento IPv6, que no está habilitado de forma predeterminada. Para habilitar un enrutador como enrutador IPv6, se debe usar el comando de configuración global **ipv6 unicast-routing** .

El mensaje ICMPv6 RA es una sugerencia para un dispositivo sobre cómo obtener una GUA IPv6. La decisión final depende del sistema operativo del dispositivo. El mensaje ICMPv6 RA incluye lo siguiente:

- **Prefijo de red y longitud del prefijo:** - esto le dice al dispositivo a qué red pertenece.
- **Dirección de puerta de enlace predeterminada:** - es un IPv6 LLA, la dirección IPv6 de origen del mensaje RA.
- **Direcciones DNS y nombre de dominio:** - estas son las direcciones de los servidores DNS y un nombre de dominio.

Existen tres métodos para los mensajes de RA:

- **Method 1: SLAAC** \ - «Tengo todo lo que necesita, incluido el prefijo, la longitud del prefijo y la dirección de la puerta de enlace predeterminada».
- **Method 2: SLAAC con un servidor DHCPv6 sin estado:** - "Aquí está mi información, pero necesita obtener otra información, como direcciones DNS, de un servidor DHCPv6 sin estado".
- **Method 3: DHCPv6 con estado (sin SLAAC)** - «Puedo darle su dirección de puerta de enlace predeterminada. Necesita pedir a un servidor DHCPv6 con estado para toda su otra información».

12.5.2

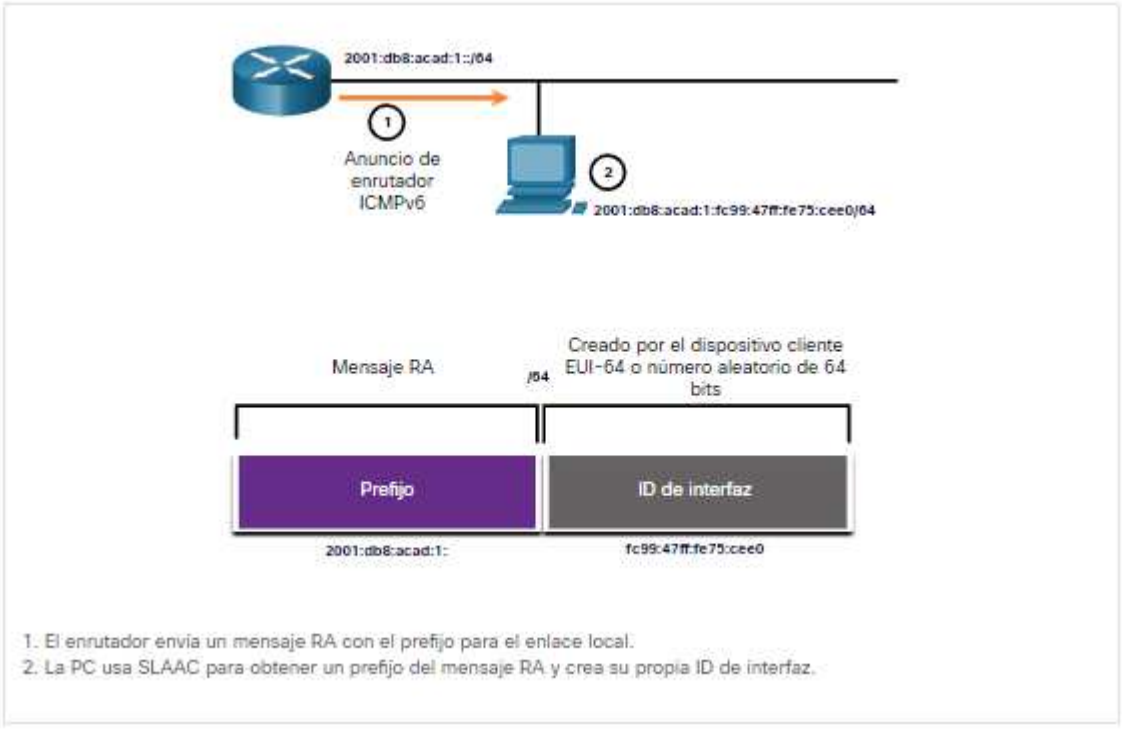
Método 1: SLAAC

SLAAC es un método que permite a un dispositivo crear su propio GUA sin los servicios de DHCPv6. Usando SLAAC, los dispositivos confían en los mensajes ICMPv6 RA del enrutador local para obtener la información necesaria.

Por defecto, el mensaje RA sugiere que el dispositivo receptor use la información en el mensaje RA para crear su propia GUA IPv6 y toda la otra información necesaria. No se requieren los servicios de un servidor DHCPv6.

SLAAC no tiene estado, lo que significa que no hay un servidor central (por ejemplo, un servidor DHCPv6 con estado) que asigne GUA y mantenga una lista de dispositivos y sus direcciones. Con SLAAC, el dispositivo cliente usa la información en el mensaje RA para crear su propia GUA. Como se muestra en la figura, las dos partes de la dirección se crean de la siguiente manera:

- **Prefijo** : se anuncia en el mensaje RA.
- **ID de interfaz:** - utiliza el proceso EUI-64 o genera un número aleatorio de 64 bits, según el sistema operativo del dispositivo.



El gráfico muestra LAN con un router que envía un mensaje de anuncio de router ICMPv6 hacia un PC. El PC tiene la dirección IPv6 de 2001:db8:acad:1:fc 99:47 ff:fe75:cee0/64. El es un gráfico que indica que el prefijo de red recibido en el mensaje RA es 2001:db8:acad:1: y el ID de interfaz creado por el dispositivo cliente EUI-64 o el número aleatorio de 64 bits es fc 99:47 ff:fe75:cee0. El texto debajo del gráfico dice 1. El router envía un mensaje RA con el prefijo para el enlace local. 2. El PC utiliza SLAAC para obtener un prefijo del mensaje RA y crea su propio ID de interfaz.

12.5.3

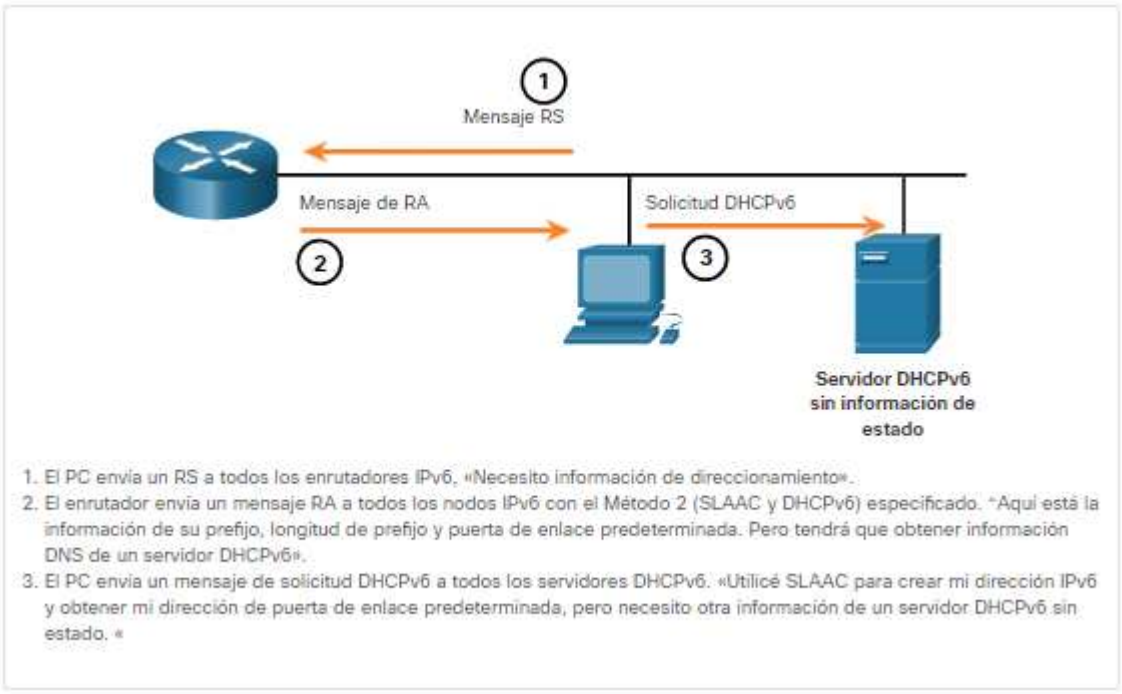
Método 2: SLAAC y DHCPv6 sin estado

Se puede configurar una interfaz de enrutador para enviar un anuncio de enrutador utilizando SLAAC y DHCPv6 sin estado.

Como se muestra en la figura, con este método, el mensaje RA sugiere que los dispositivos utilicen lo siguiente:

- SLAAC para crear su propio IPv6 GUA
- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 stateless, que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio

Nota: Un servidor DHCPv6 sin información de estado distribuye las direcciones del servidor DNS y los nombres de dominio. No asigna GUA.



El gráfico muestra LAN con un PC que está enviando un RS Messages (etiquetado #1) al router. El router está enviando a cambio un mensaje RA (etiquetado #2). El PC también está enviando un mensaje DHCPv6 Solicit (etiquetado #3) a un servidor DHCPv6 sin estado. El texto debajo del gráfico dice 1. La PC envía un RS a todos los enrutadores IPv6, necesito información de direccionamiento. 2. El router envía un mensaje RA a todos los nodos IPv6 con el método 2 (SLAAC y DHCPv6) especificado. Aquí está la longitud del prefijo y la información de la puerta de enlace predeterminada. pero necesitará obtener información de DNS de un servidor DHCPv6. 3. El PC envía un mensaje de solicitud DHCPv6 a todos los servidores DHCPv6. Utilicé SLAAC para crear mi dirección IPv6 y obtener mi dirección de puerta de enlace predeterminada, pero necesito otra información de un servidor DHCPv6 sin estado.

12.5.4

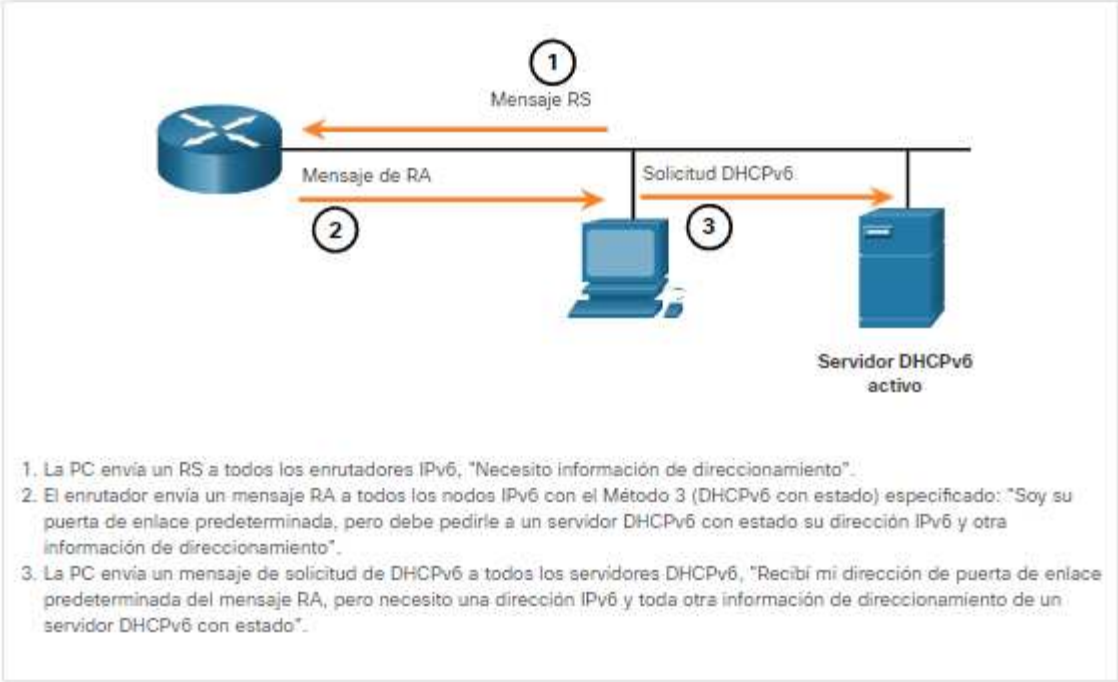
Método 3: DHCPv6 con estado

Una interfaz de router se puede configurar para enviar una RA usando DHCPv6 con estado solamente.

DHCPv6 con información de estado es similar a DHCP para IPv4. Un dispositivo puede recibir automáticamente su información de direccionamiento, incluida una GUA, la longitud del prefijo y las direcciones de los servidores DNS de un servidor DHCPv6 con estado.

Como se muestra en la figura, con este método, el mensaje RA sugiere que los dispositivos usen lo siguiente:

- La dirección LLA del router, que es la dirección IPv6 de origen del RA, para la dirección de gateway predeterminado.
- Un servidor DHCPv6 Stateful, para obtener una GUA, otra información como la dirección del servidor DNS y el nombre de dominio.



El gráfico muestra LAN con un PC que envía (etiquetado #1) a un router. El router está enviando un mensaje (etiquetado #2) a la PC. El PC también está enviando un mensaje (etiquetado #3) al servidor s. El texto debajo del gráfico dice 1. La PC envía un RS a todos los enrutadores IPv6, necesito información de direccionamiento. 2. El router envía un mensaje RA a todos los nodos IPv6 con el Método 3 (DHCPv6 con estado completo) especificado Soy su puerta de enlace predeterminada, pero debe pedir a un servidor DHCPv6 con estado completo para la información de la dirección IPv6. 3. El PC envía un mensaje de

solicitud DHCPv6 a todos los servidores DHCPv6, recibí mi dirección de puerta de enlace predeterminada del mensaje RA, pero necesito una dirección IPv6 y toda la otra información de direccionamiento de un servidor DHCPv6 con estado.

Un servidor DHCPv6 con información de estado asigna y mantiene una lista de qué dispositivo recibe cuál dirección IPv6. DHCP para IPv4 tiene información de estado.

Nota: La dirección de puerta de enlace predeterminada solo se puede obtener dinámicamente a partir del mensaje RA. El servidor DHCPv6 con información de estado o sin ella no brinda la dirección de gateway predeterminado.

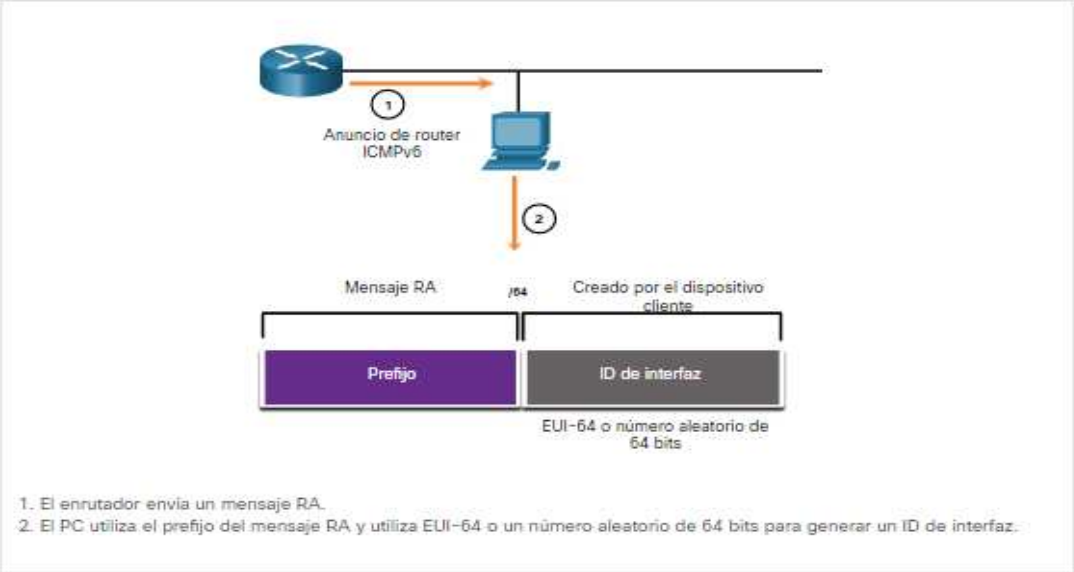
12.5.5

Proceso EUI-64 versus generado aleatoriamente

Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 sin estado, el cliente debe generar su propia ID de interfaz. El cliente conoce la parte del prefijo de la dirección del mensaje RA, pero debe crear su propia ID de interfaz. El ID de la interfaz se puede crear utilizando el proceso EUI-64 o un número de 64 bits generado aleatoriamente, como se muestra en la figura.

El gráfico muestra un router que envía un mensaje de anuncio de router ICMPv6 (etiquetado #1) a un PC. El PC se muestra en un paso etiquetado #2 creando su prefijo /64 a partir del mensaje RA y creando su ID de interfaz usando EUI-64 o número aleatorio de 64 bits. El texto debajo del gráfico dice 1. El enrutador envía un mensaje RA. 2. El PC utiliza el prefijo en el mensaje RA y utiliza EUI-64 o un número aleatorio de 64 bits para generar un ID de interfaz

Creación dinámica de un ID de interfaz



12.5.6

Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC Ethernet de 48 bits de un cliente e inserta otros 16 bits en el medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

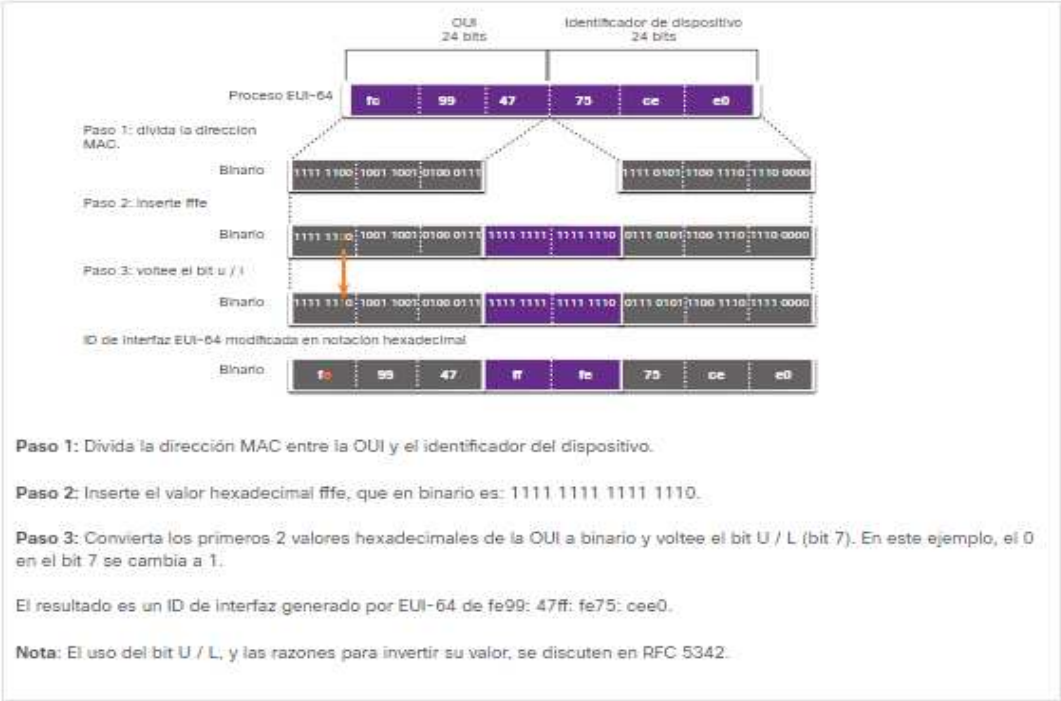
Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

- **Identificador único organizativo (OUI):** - el OUI es un código de proveedor de 24 bits (6 dígitos hexadecimales) asignado por IEEE.
- **Identificador del dispositivo** - el identificador del dispositivo es un valor único de 24 bits (6 dígitos hexadecimales) dentro de una OUI común.

Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

- OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto quiere decir que si el séptimo bit es un 0, se transforma en un 1, y viceversa.
- El valor insertado de 16 bits fffe (en hexadecimal).
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente.

El proceso EUI-64 se ilustra en la figura, utilizando la dirección MAC R1 GigabitEthernet de fc99: 4775: cee0.



Paso 1: Divida la dirección MAC entre la OUI y el identificador del dispositivo.

Paso 2: Inserte el valor hexadecimal fffe, que en binario es: 1111 1111 1111 1110.

Paso 3: Convierta los primeros 2 valores hexadecimales de la OUI a binario y voltee el bit U / L (bit 7). En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es un ID de interfaz generado por EUI-64 de fe99: 47ff: fe75: cee0.

Nota: El uso del bit U / L, y las razones para invertir su valor, se discuten en RFC 5342.

El gráfico muestra los pasos del proceso EUI-64. En la parte superior del gráfico está la dirección MAC fc: 99:47:75:ce:e0. En el paso 1: Dividir la dirección MAC, Los primeros 24-bits del OUI fc: 99:47 en binario es 1111 1100 1001 1001 0100 0111. Los últimos 24 bits del dispositivo identifiere 75:ce:e0 en binario es 1111 0101 1100 1110 0000. Paso 2: Inserte ffee la representación binaria se convierte en 1111 1100 1001 1001 0100 0111 1111 1111 1111 1111 0101 1100 1110 1110 0000. En el paso tres Voltee el bit u/l. El séptimo bit de la izquierda se cambia de 0 a 1. La dirección en binario es ahora 1111 1110 1001 1001 0100 0111 1111 1111 1111 1111 1111 1110 1111 0101 1100 1110 0000. La ID de interfaz EUI-64 modificada en notación hexadecimal es ahora: fe: 99: 47: ff: fe: 75: ce: e0. Pruebe bajo las lecturas gráficas: Paso 1: Divida la dirección MAC entre la OUI y el identificador del dispositivo. Paso 2: inserte el valor hexadecimal fffe, que en binario es: 1111 1111 1111 1110. Paso 3. Convierta los primeros 2 valores hexadecimales de la OUI a binario y voltee el bit U / L (bit 7). En este ejemplo, el 0 en el bit 7 cambia a 1. El resultado es un ID de interfaz generado por EUI-64 de fe99: 47ff: fe75: cee0. Nota: El uso del bit U / L, y las razones para revertir su valor, se discuten en RFC 5342.

El resultado de ejemplo del **ipconfig** comando muestra el GUA IPv6 que se crea dinámicamente mediante SLAAC y el proceso EUI-64. Una manera fácil de identificar que una dirección probablemente se creó usando EUI-64 es **fffe**ubicarse en el medio de la ID de la interfaz.

La ventaja de EUI-64 es que la dirección MAC de Ethernet se puede utilizar para determinar la ID de la interfaz. También permite que los administradores de redes rastreen fácilmente una dirección IPv6 a un terminal mediante la dirección MAC única. Sin embargo, esto ha causado preocupaciones de privacidad entre muchos usuarios que temían que sus paquetes

pudieran rastrearse hasta el equipo físico real. Debido a estas preocupaciones, se puede usar una ID de interfaz generada aleatoriamente.

ID de interfaz generada mediante EUI-64

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
   Sufijo de conexión específica DNS. :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
   Link-local IPv6 Address . . . . .: fe80::fc 99:47ff:fe75:cee0
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

12.5.7

ID de interfaz generadas aleatoriamente

Dependiendo del sistema operativo, un dispositivo puede usar una ID de interfaz generada aleatoriamente en lugar de usar la dirección MAC y el proceso EUI-64. A partir de Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una creada con EUI-64. Windows XP y los sistemas operativos Windows anteriores utilizaban EUI-64.

Una vez establecida la ID de la interfaz, ya sea a través del proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 en el mensaje RA para crear una GUA, como se muestra en la figura.

ID de interfaz de 64 bits generada aleatoriamente

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
   Sufijo de conexión específica DNS. :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . .: fe80: :50a 5:8 a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Nota: Para garantizar la unicidad de cualquier dirección de unidifusión IPv6, el cliente puede usar un proceso conocido como Detección de direcciones duplicadas (DAD). Es similar a una solicitud de ARP para su propia dirección. Si no se obtiene una respuesta, la dirección es única.

12.5.8

Compruebe su comprensión - Direccionamiento dinámico para GUA IPv6

Verifique su comprensión del direccionamiento dinámico de las GUA IPv6 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es falso. Los mensajes de anuncio de enrutador (RA) se envían a todos los nodos IPv6. Si se utiliza el Método 1 (solo SLAAC), la RA incluye información sobre el prefijo de red, la longitud del prefijo y la puerta de enlace predeterminada.
2. SLAAC es un método donde los dispositivos crean su propia GUA sin los servicios de DHCPv6. Con SLAAC, los dispositivos se basan en los mensajes RA del ICMPv6 del enrutador local para obtener la información necesaria.
3. El DHCPv6 con estado es un método en el que los dispositivos reciben automáticamente su información de direccionamiento, incluida una GUA, la longitud del prefijo y las direcciones de los servidores DNS de un servidor DHCPv6 con estado.
4. SLAAC y DHCPv6 sin estado es un método en el que los dispositivos utilizan SLAAC para el GUA y la dirección de puerta de enlace predeterminada. A continuación, los dispositivos utilizan un servidor DHCPv6 sin estado para servidores DNS y otra información de direccionamiento.
5. Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 sin estado, el cliente debe generar su propia ID de interfaz utilizando el proceso EUI-64 o un número de 64 bits generado aleatoriamente.

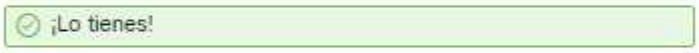
Has tenido 5 respuestas correctas de 5.

1. Verdadero o falso. Los hosts que solicitan información de direccionamiento envían mensajes RA a todos los enrutadores IPv6.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

2. ¿Qué método de direccionamiento dinámico para GUA es aquel en el que los dispositivos se basan únicamente en el contenido del mensaje RA para su información de direccionamiento?


¡Lo tienes!

- ◉ Método 1: SLAAC
- ○ Método 2: SLAAC y DHCPv6 sin estado
- ○ Método 3: DHCPv6 con estado

3. ¿Qué método de direccionamiento dinámico para GUA es aquel en el que los dispositivos dependen únicamente de un servidor DHCPv6 para su información de direccionamiento?

¡Lo tienes!

- ○ Método 1: SLAAC
- ○ Método 2: SLAAC y DHCPv6 sin estado
- ◉ Método 3: DHCPv6 con estado

5. ¿Cuáles son los dos métodos que un dispositivo puede usar para generar su propio ID de interfaz IPv6?

¡Lo tienes!

- [ ] SLAAC
- [ ] DHCPv6 sin información de estado
- [ ] DHCPv6 con información de estado
- [x] EUI-64
- [x] generado aleatoriamente

Correct

You have successfully identified the correct answers.

1. The correct answer is False. Router Advertisement (RA) messages are sent to all IPv6 nodes. If Method 1 (SLAAC only) is used, the RA includes network prefix, prefix-length, and default-gateway information.
2. SLAAC is a method where devices create their own GUA without the services of DHCPv6. Using SLAAC, devices rely on the local router ICMPv6 RA messages to obtain the necessary information.
3. Stateful DHCPv6 is a method where devices automatically receive their addressing information including a GUA, prefix length, and the addresses of DNS servers from a stateful DHCPv6 server.
4. SLAAC and stateless DHCPv6 is a method where devices use SLAAC for the GUA and default gateway address. The devices then use a stateless DHCPv6 server for DNS servers and other addressing information.
5. When the RA message is either SLAAC or SLAAC with stateless DHCPv6, the client must generate its own interface ID using the EUI-64 process or a randomly generated 64-bit number.

You got 5 out of 5 questions correct.

1. True or False. RA messages are sent to all IPv6 routers by hosts requesting addressing information.

You got it!

- ○ True
- ◉ False

2. Which dynamic addressing method for GUAs is the one where devices rely solely on the contents of the RA message for their addressing information?

You got it!

- ◉ Method 1: SLAAC
- ○ Method 2: SLAAC and Stateless DHCPv6
- ○ Method 3: Stateful DHCPv6

3. Which dynamic addressing method for GUAs is the one where devices rely solely on a DHCPv6 server for their addressing information?

You got it!

- ○ Method 1: SLAAC
- ○ Method 2: SLAAC and Stateless DHCPv6
- ◉ Method 3: Stateful DHCPv6

4. Which dynamic addressing method for GUAs is the one where devices get their IPv6 configuration in a RA message and request DNS information from a DHCPv6 server?

You got it!

- ○ Method 1: SLAAC
- ◉ Method 2: SLAAC and Stateless DHCPv6
- ○ Method 3: Stateful DHCPv6

5. What are the two methods a device can use to generate its own IPv6 interface ID?

You got it!

- ☐ SLAAC
- ☐ stateless DHCPv6
- ☐ stateful DHCPv6
- ☑ EUI-64
- ☑ randomly generated

Asignación de direcciones IPv6 / Direccionamiento dinámico para las LLAS IPv6

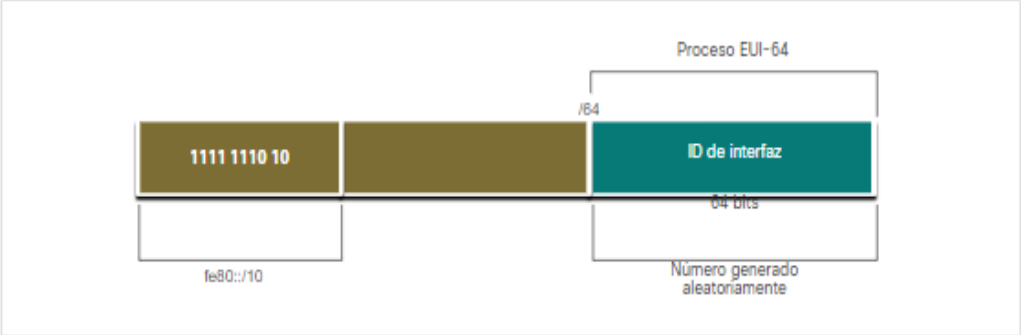
Direccionamiento dinámico para las LLAS IPv6

12.6.1

LLA dinámicos

Todos los dispositivos IPv6 deben tener una LLA IPv6. Al igual que IPv6 GUA, también puede crear LAs dinámicamente. Independientemente de cómo cree las LAs (y las GUA), es importante que verifique toda la configuración de direcciones IPv6. En este tema se explica la verificación de configuración de LLAS y IPv6 generadas dinámicamente.

La figura muestra que el LLA se crea dinámicamente usando el prefijo fe80:: / 10 y la ID de interfaz usando el proceso EUI-64, o un número de 64 bits generado aleatoriamente.



El gráfico muestra el Prefijo de un LLA en binario: 1111 1110 10, y en hexadecimal: fe80: :/10.

12.6.2

LLA dinámicos en Windows

Los sistemas operativos, como Windows, suelen utilizar el mismo método tanto para una GUA creada por SLAAC como para una LLA asignada dinámicamente. Vea las áreas resaltadas en los siguientes ejemplos que se mostraron anteriormente.

ID de interfaz generada mediante EUI-64

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
Sufijo de conexión específica DNS. :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . .: fe80::fc 99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

ID de interfaz de 64 bits generada aleatoriamente

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
   Sufijo de conexión específica DNS. :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

12.6.3

LLA dinámicos en enrutadores Cisco

Los routers Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz. De manera predeterminada, los routers con Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones LLAs en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que un LLA debe ser único solo en ese enlace o red. Sin embargo, una desventaja de usar el LLA asignado dinámicamente es su ID de interfaz larga, lo que dificulta identificar y recordar las direcciones asignadas. El ejemplo muestra la dirección MAC en la interfaz GigabitEthernet 0/0/0 del enrutador R1. Esta dirección se utiliza para crear dinámicamente el LLA en la misma interfaz, y también para la interfaz Serial 0/1/0.

Para que sea más fácil reconocer y recordar estas direcciones en los enrutadores, es común configurar estáticamente los LLA de IPv6 en los enrutadores.

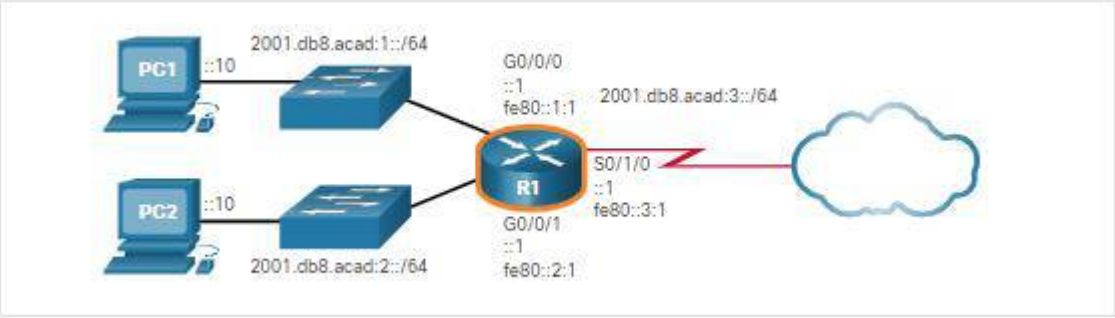
IPv6 LLA con EUI-64 en el router R1

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  El hardware es ISR4221-2x1GE, la dirección es 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1 [up/up]
    FE80::7279:B3FF:FE92:3641
    2001:DB8:ACAD:2::1
Serial0/1/0 [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:3: :1
Serial0/1/1 [abajo/abajo]
    unassigned
R1#
```

12.6.4

Verifique la configuración de la dirección IPv6

La figura muestra el ejemplo de topología:



El gráfico muestra dos PC, PC1 y PC2. PC1 está conectado a un conmutador y tiene la dirección IPv6 2001: db8: acad: 1 :: 10/64. PC2 está conectado a un switch y tiene la dirección IPv6 2001:db8:acad:2: :10/64. Los dos interruptores están conectados a un enrutador, R1. La PC1 se conecta a través del conmutador a la interfaz R1s G0 / 0/0 que tiene la dirección IPv6 2001: db8: acad: 1 :: 1/64 y la dirección LLA de fe80 :: 1: 1. PC2 se conecta a través del conmutador a la interfaz R1s G0 / 0/1 que tiene la dirección IPv6 2001: db8: acad: 2 :: 1/64 y la dirección LLA de fe80 :: 2: 1. R1 se conecta a la nube a través de su interfaz S0 / 1/0 que tiene dirección IPv6 2001: db8: acad: 3 :: 1/64 y la dirección LLA de fe80 :: 3: 1.

R1::10::10S0/1/0::1fe80::3:1PC1PC22001.db8.acad:2::/642001.db8.acad:1::/642001.db8.acad:3::/64G0/0/0::1fe80::1:1G0/0/1::1fe80::2:1R1

Haga clic en cada botón para obtener la salida y una descripción del comando.

show ipv6 interface brief | show ipv6 route | ping

El comando **show ipv6 interface brief** muestra la dirección MAC de las interfaces Ethernet. EUI-64 usa esta dirección MAC para generar la ID de interfaz para el LLA. Además, el comando **show ipv6 interface brief** muestra una salida abreviada para cada una de las interfaces. La salida \ [up / up] en la misma línea que la interfaz indica el estado de la interfaz de Capa 1 / Capa 2. Esto es lo mismo que las columnas Status (Estado) y Protocol (Protocolo) en el comando IPv4 equivalente.

El comando show ipv6 interface brief en R1

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80::1:1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1 [up/up]
    FE80::1:2
    2001:DB8:ACAD:2::1
Serial0/1/0 [up/up]
    FE80::1:3
    2001:DB8:ACAD:3: :1
Serial0/1/1 [down/down]
    unassigned
R1#
```

Observe que cada interfaz tiene dos direcciones IPv6. La segunda dirección de cada interfaz es la GUA que se configuró. La primera dirección, la que comienza con fe80, es la dirección de unidifusión local de enlace para la interfaz. Recuerde que el LLA se agrega automáticamente a la interfaz cuando se asigna una GUA.

Además, observe que el R1 Serial 0/1/0 LLA es el mismo que su interfaz GigabitEthernet 0/0/0. Las interfaces seriales no tienen direcciones MAC de Ethernet, por lo que Cisco IOS usa la dirección MAC de la primera interfaz Ethernet disponible. Esto es posible porque las interfaces link-local solo deben ser únicas en ese enlace.

show ipv6 interface brief | show ipv6 route | ping

Como se muestra en el ejemplo,**show ipv6 route** el comando se puede usar para verificar que las redes IPv6 y las direcciones de interfaz IPv6 específicas se hayan instalado en la tabla de enrutamiento IPv6. El **show ipv6 route** comando solo mostrará redes IPv6, no redes IPv4.

El comando show ipv6 route en R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C 2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3: :/64 [0/0]
     a través de Serial0/1/0, conectado directamente
L 2001:DB8:ACAD:3: :1/128 [0/0]
     a través de Serial0/1/0, recibir
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

Dentro de la tabla de rutas, una **C** al lado de una ruta indica que esta es una red conectada directamente. When the router interface is configured with a GUA and is in the "up/up" state, the IPv6 prefix and prefix length is added to the IPv6 routing table as a connected route.

Nota: **L** Indica una ruta local, la dirección IPv6 específica asignada a la interfaz. Esto no es una LLA. Los LLA no se incluyen en la tabla de enrutamiento del enrutador porque no son direcciones enrutables.

La GUA IPv6 configurada en la interfaz también se instala en la tabla de enrutamiento como una ruta local. La ruta local tiene un prefijo /128. La tabla de enrutamiento utiliza las rutas locales para procesar eficientemente los paquetes con una dirección de destino de la dirección de la interfaz del enrutador.

show ipv6 interface brief | show ipv6 route | ping

El comando **ping** para IPv6 es idéntico al comando usado con IPv4, excepto que se usa una dirección IPv6. Como se muestra en el ejemplo, el comando se usa para verificar la conectividad de Capa 3 entre R1 y PC1. Al hacer ping a un LLA desde un enrutador, Cisco IOS solicitará al usuario la interfaz de salida. Debido a que el LLA de destino puede estar en uno o más de sus enlaces o redes, el enrutador necesita saber a qué interfaz enviar el ping.

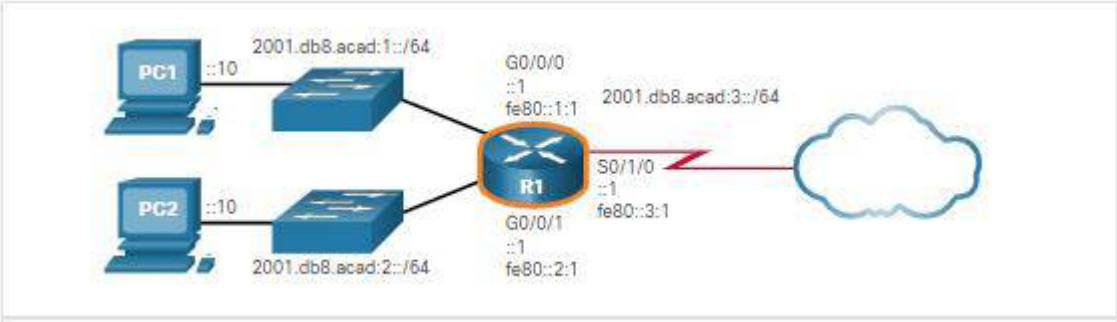
El comando ping en R1

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Envío de 5 ecos de ICMP de 100 bytes al 2001: DB8: ACAD: 1 :: 10, el tiempo de espera es de 2 segundos:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

12.6.5

Comprobador de sintaxis: verificar la configuración de la dirección IPv6

Utilice comandos **show** para verificar la configuración de direcciones IPv6 en las interfaces R1 del router.



El gráfico muestra dos PC, PC1 y PC2. PC1 está conectado a un conmutador y tiene la dirección IPv6 2001: db8: acad: 1 :: 10/64. PC2 está conectado a un switch y tiene la dirección IPv6 2001:db8:acad:2: :10/64. Los dos interruptores están conectados a un enrutador, R1. La PC1 se conecta a través del conmutador a la interfaz R1s G0 / 0/0 que tiene la dirección IPv6 2001: db8: acad: 1 :: 1/64 y la dirección LLA de fe80 :: 1: 1. PC2 se conecta a través del conmutador a la interfaz R1s G0 / 0/1 que tiene la dirección IPv6 2001: db8: acad: 2 :: 1/64 y la dirección LLA de fe80 :: 2: 1. R1 se conecta a la nube a través de su interfaz S0 / 1/0 que tiene dirección IPv6 2001: db8: acad: 3 :: 1/64 y la dirección LLA de fe80 :: 3: 1.

Enter the show command that will display a brief summary of the IPv6 interface status.

```
R1#show ipv6 interface brief
GigabitEthernet0/0/0    \[up/up\]
    FE80::1:1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1    \[up/up\]
    FE80::2:1
    2001:DB8:ACAD:2::1
Serial0/1/0             \[up/up\]
    FE80::3:1
    2001:DB8:ACAD:3::1
Serial0/1/1             \[down/down\]
    unassigned
GigabitEthernet0        \[administratively down/down\]
    unassigned
```

Verify connectivity from R1 to PC2 at 2001:db8:acad:1::10.

```
R1#show ipv6 route
IPv6 Routing Table - default - 7 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr -
Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext
2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
C   2001:DB8:ACAD:1::/64 \[0/0\]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 \[0/0\]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 \[0/0\]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 \[0/0\]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 \[0/0\]
     via Serial0/0/1, directly connected
L   2001:DB8:ACAD:3::1/128 \[0/0\]
     via Serial0/0/1, receive
L   FF00::/8 \[0/0\]
     via Null0, receive
R1#ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
You successfully verified IPv6 address configuration.
```

12.6.6

Packet Tracer: Configuración de direccionamiento IPv6

En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación del direccionamiento IPv6.

Configuración de direccionamiento IPv6

Configuración de direccionamiento IPv6

Asignación de direcciones IPv6 / Direcciones IPv6 de multidifusión

Direcciones IPv6 de multidifusión

12.7.1

Direcciones IPv6 de multidifusión asignadas

Anteriormente, en este módulo, aprendió que hay tres categorías amplias de direcciones IPv6: Unidifusión, Multidifusión, difusión ilimitada Este tema incluye más detalles acerca de las direcciones de multidifusión.

Las direcciones IPv6 de multidifusión son similares a las direcciones IPv4 de multidifusión. Recuerde que las direcciones de multidifusión se utilizan para enviar un único paquete a uno o más destinos (grupo de multidifusión). Las direcciones de multidifusión IPv6 tienen el prefijo ff00:: / 8.

Nota: Las direcciones de multidifusión solo pueden ser direcciones de destino y no direcciones de origen.

Existen dos tipos de direcciones IPv6 de multidifusión:

- Direcciones de multidifusión conocidas
- Direcciones de multidifusión de nodo solicitadas

12.7.2

Direcciones de multidifusión IPv6 bien conocidas

Se asignan direcciones de multidifusión IPv6 conocidas. Las direcciones de multidifusión asignadas son direcciones de multidifusión reservadas para grupos predefinidos de dispositivos. Una dirección de multidifusión asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones de multidifusión asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

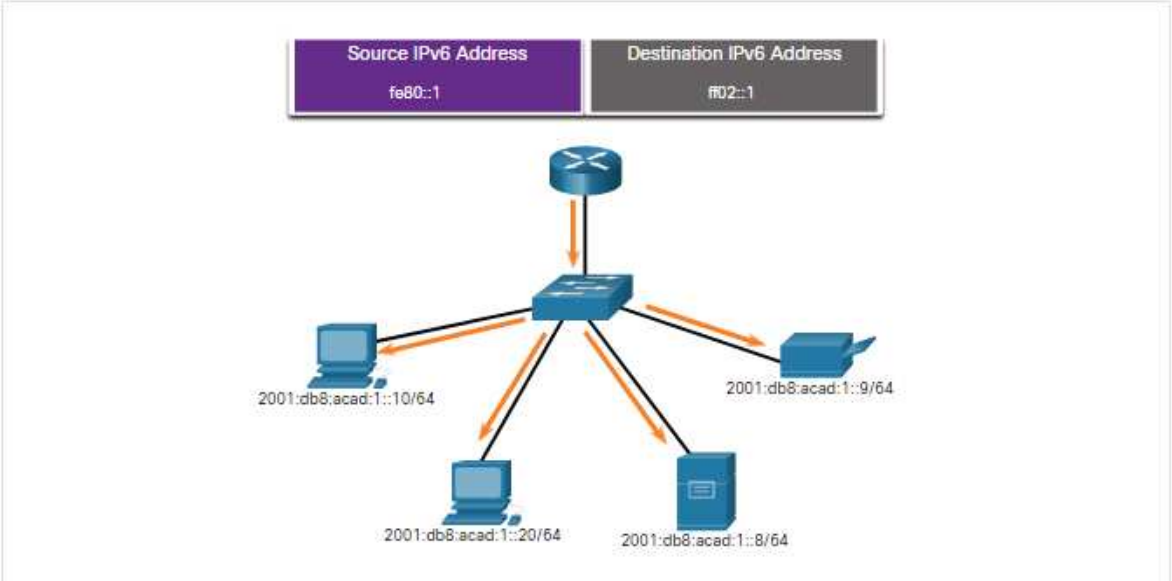
Estos son dos grupos de multidifusión asignados por IPv6 comunes:

- **ff02::1 Grupo de multidifusión de todos los nodos:** - este es un grupo de multidifusión al que se unen todos los dispositivos con IPv6. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de difusión en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante

la dirección de multidifusión de todos los nodos. Un enrutador IPv6 envía mensajes RA ICMPv6 al grupo de multidifusión de todos los nodos.

- **ff02:: 2 Todos los enrutadores multicast group** - This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** comando de configuración global. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

IPv6 All-Nodes Multicast: RA Message



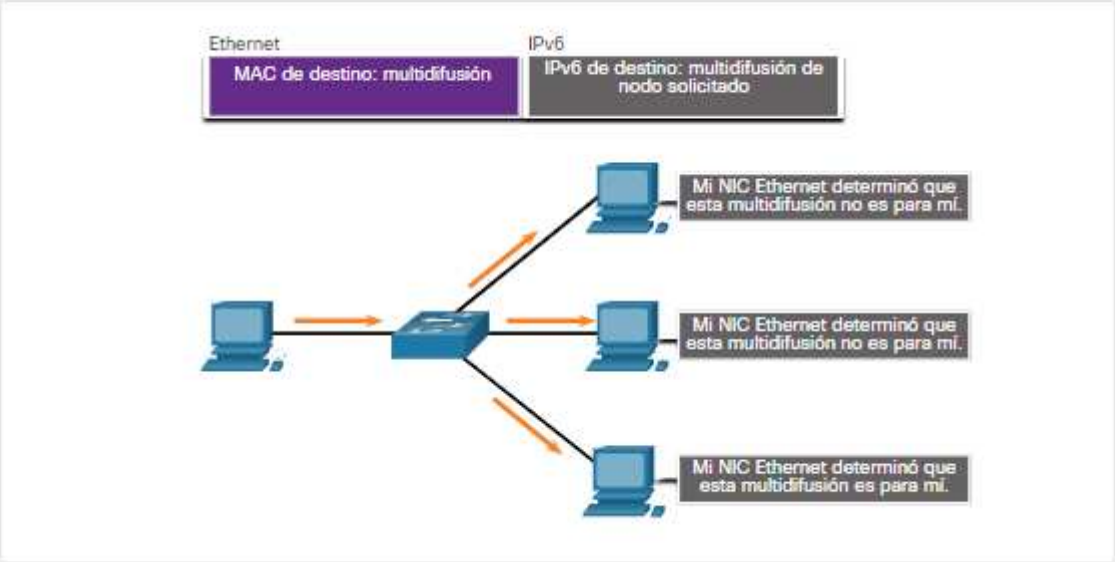
Los dispositivos habilitados para IPv6 envían mensajes ICMPv6 RS a la dirección multicast de todos los routers. El mensaje RS, solicita un mensaje RA IPv6 del router para contribuir a la configuración de direcciones del dispositivo. En router IPv6 responde con un mensaje RA, como se muestra.

El gráfico muestra dos PC con direcciones IPv6 de 2001:db8:acad:1: :10/64 y 2001:db8:acad:1: :20/64, un servidor con dirección IPv6 2001:db8:acad:1: :8/64 y una impresora con dirección IPv6 2001:db8:acad:1: :9/64 conectada a un switch conectado a un router. Encima del gráfico se indica la dirección IPv6 de origen fe80: :1 y la dirección IPv6 de destino ff02: :1. Multidifusión de todos los nodos IPv6: mensaje RA El mensaje RS solicita un mensaje RA desde el enrutador IPv6 para ayudar al dispositivo a configurar su dirección. El enrutador IPv6 responde con un mensaje RA, como se muestra.

12.7.3

Direcciones IPv6 de multidifusión de nodo solicitado

Una dirección de multidifusión de nodo solicitado es similar a una dirección de multidifusión de todos los nodos. La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección especial de multidifusión de Ethernet. Esto permite que la NIC Ethernet filtre el marco al examinar la dirección MAC de destino sin enviarla al proceso de IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.



El gráfico muestra tres PC que reciben un mensaje de un router. Cada PC tiene el siguiente texto informativo: Mi NIC Ethernet determinó que esta multidifusión no es para mí. El enrutador IPv6 responde con un mensaje RA, como se muestra.

12.7.4

Laboratorio: identificación de direcciones IPv6

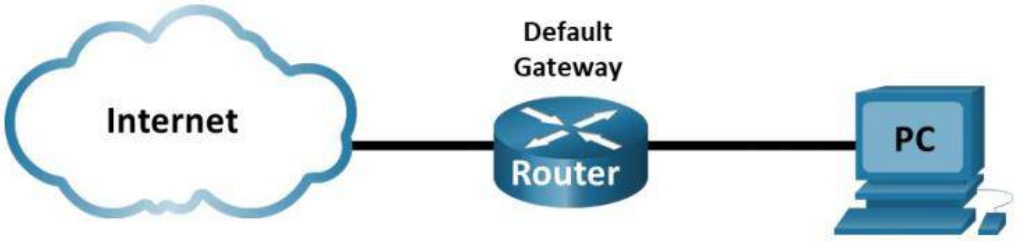
En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Identificar los diferentes tipos de direcciones IPv6
- Parte 2: Examinar una interfaz y una dirección de red de host IPv6
- Parte 3: Practicar la abreviatura de direcciones IPv6

Identifique direcciones IPv6

Networking Academy

Laboratorio – Identifique direcciones IPv6
Topología



Objetivos

Parte 1: Practicar con diferentes tipos de direcciones IPv6

Parte 2: Examinar una interfaz y una dirección IPv6 de red de host

Asignación de direcciones IPv6 / División de subredes de una red IPv6

División de subredes de una red IPv6

12.8.1

Subred con la ID de subred

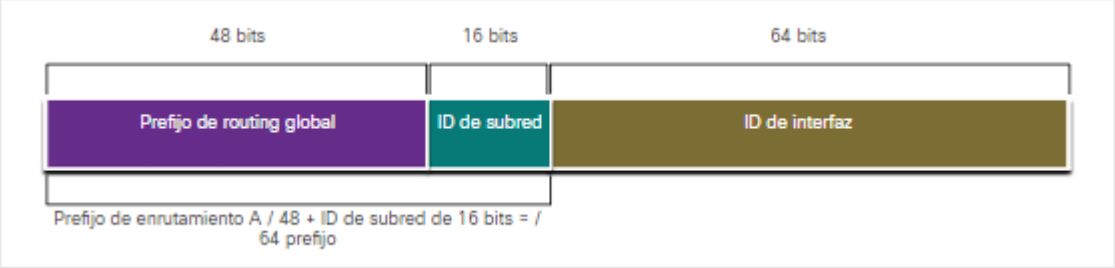
La introducción a este módulo mencionó la subred de una red IPv6. También dijo que podría descubrir que es un poco más fácil que subredes de una red IPv4. ¡Estás a punto de averiguarlo!

Recordemos que con IPv4, debemos tomar prestados bits de la parte del host para crear subredes. Esto se debe a que la subred fue una idea tardía con IPv4. Sin embargo, IPv6 se diseñó teniendo en cuenta las subredes. Se utiliza un campo ID de subred independiente en IPv6 GUA para crear subredes. Como se muestra en la figura, el campo Id. de subred es el área entre el Prefijo de enrutamiento global y el Id. de interfaz.

El gráfico muestra las partes de un GUA. Primero es el prefijo global de enrutamiento de 48 bits seguido por el ID de subred de 16 bits, luego finalmente el ID de interfaz de 64 bits. El

texto debajo del gráfico lee el prefijo de enrutamiento A / 48 + ID de subred de 16 bits = / 64 prefijo.

GUA con un ID de subred de 16 bits



La ventaja de una dirección de 128 bits es que puede admitir más que suficientes subredes y hosts por subred, para cada red. La conservación de direcciones no es un problema. Por ejemplo, si el prefijo de enrutamiento global es /48, y utilizando un típico 64 bits para el ID de interfaz, esto creará un ID de subred de 16 bits:

ID de subred de* **16 bits** : crea hasta 65.536 subredes.

- **ID de interfaz de 64 bits:** - admite hasta 18 quintillones de direcciones IPv6 de host por subred (es decir, 18,000,000,000,000,000,000).

Nota: La división en subredes en la ID de interfaz de 64 bits (o porción de host) también es posible, pero rara vez se requiere.

La división en subredes IPv6 también es más fácil de implementar que la IPv4, ya que no se requiere la conversión al sistema binario. Para determinar la siguiente subred disponible, simplemente se suman los valores en el sistema hexadecimal.

12.8.2

Ejemplo de subred IPv6

Por ejemplo, suponga que a una organización se le ha asignado el prefijo de enrutamiento global 2001: db8: acad :: / 48 con una ID de subred de 16 bits. Esto permitiría a la organización crear 65.536 / 64 subredes, como se muestra en la figura. Observe que el prefijo de routing global es igual para todas las subredes. Solo se incrementa el hexteto de la ID de subred en sistema hexadecimal para cada subred.

Subredización con una ID de subred de 16 bits

El gráfico muestra el prefijo de dirección IPv6 2001:db8:acad: :/48 en subredes /64. Una nota lee Incrementar ID de subred para crear 65.536 subredes. Las subredes son:
2001:db8:acad:0000: :/64,
2001:db8:acad:0001: :/64,
2001:db8:acad:0002: :/64,
2001:db8:acad:0003: :/64,
2001:db8:acad:0004: :/64,
2001:db8:acad:0005: :/64,
2001:db8:acad:0006: :/64,
2001:db8:acad: 0007: :/64,
2001:db8:acad:0008: :/64,
2001:db8:acad:0009: :/64,
2001:db8:acad:000a: :/64,
2001:db8:acad:000b: :/64,
2001:db8:acad:000c: :/64.
Subredes 13-65,534 no se muestran, 2001:db8:acad:ffff: :/64.

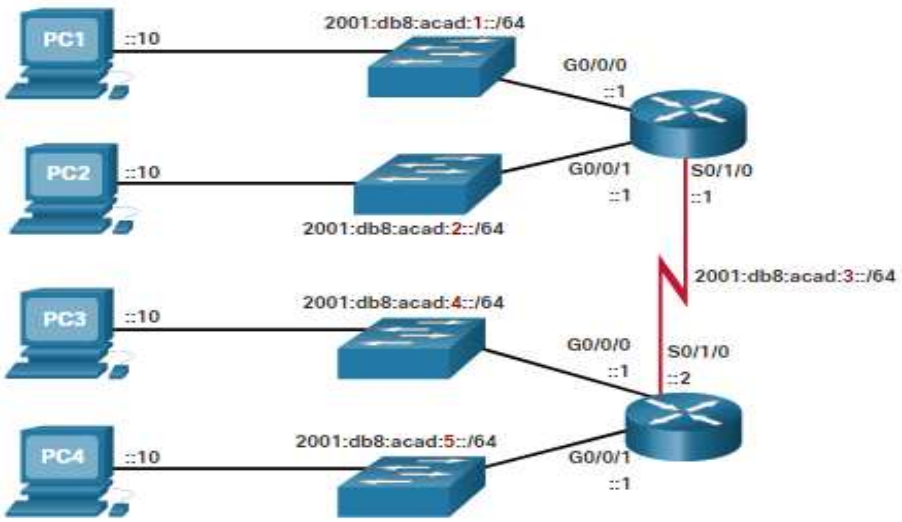
12.8.3

Asignación de subredes IPv6

Con más de 65.536 subredes para elegir, la tarea del administrador de la red es diseñar un esquema lógico para abordar la red.

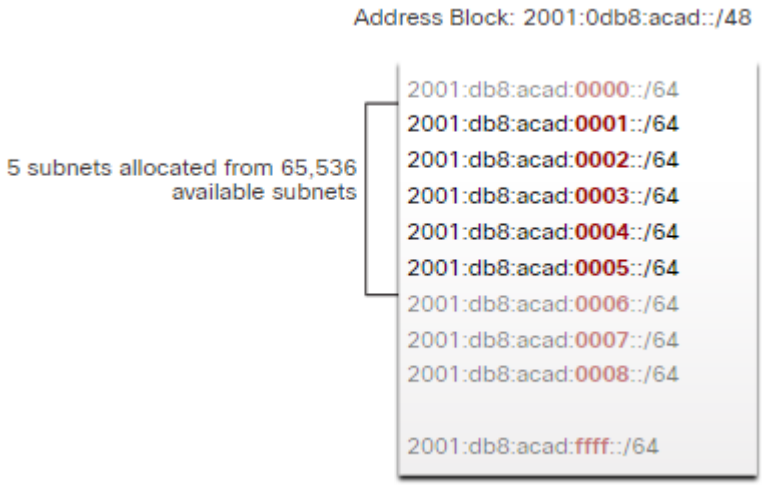
Como se muestra en la figura, la topología de ejemplo requiere cinco subredes, una para cada LAN, así como para el enlace serie entre R1 y R2. A diferencia del ejemplo de IPv4, con IPv6 la subred de enlace serie tendrá la misma longitud de prefijo que las LAN. Aunque esto puede parecer "desperdiciar" direcciones, la conservación de direcciones no es una preocupación cuando se utiliza IPv6.

Topología de ejemplo



El gráfico muestra cuatro PC, PC1, PC2, PC3 y PC4, cada uno con el ID de interfaz de: :10. Cada PC está conectada a un interruptor. PC1 está en la red 2001:db8:acad:1: :/64 y se conecta a través de un switch a la interfaz G0/0/0, con ID de interfaz: :1, del router 1. PC2 está en la red 2001:db8:acad:2: :/64 y se conecta a través de un switch a la interfaz G0/0/1, con ID de interfaz: :1, del router 1. PC3 está en la red 2001:db8:acad:4: :/64 y se conecta a través de un switch a la interfaz G0/0/0, con ID de interfaz: :1, del router 2. PC4 está en la red 2001:db8:acad:5: :/64 y se conecta a través de un switch a la interfaz G0/0/1, con ID de interfaz: :1 del router 2. Los enrutadores 1 y 2 están conectados a través de sus interfaces S0/1/0 con R1 con un ID de interfaz de: :1 y R2 con un ID de interfaz de: :2 en la red 2001:db8:acad:3: :/64.

Como se muestra en la siguiente figura, se asignaron las cinco subredes IPv6, con el campo ID de subred 0001 a 0005 utilizado para este ejemplo. Cada subred /64 proporcionará más direcciones de las que jamás se necesitarán.



El gráfico muestra las subredes del bloque de direcciones: 2001:db8:acad: :/48. Las subredes son: 2001:db8:acad:0000: :/64, 2001:db8:acad:0001: :/64, 2001:db8:acad:0002: :/64, 2001:db8:acad:0003: :/64, 2001:db8:acad:0004: :/64, 2001:db8:acad:0005: :/64, 2001:db8:acad:0006: :/64, 2001:db8:acadacadacad:000acad:0006 7: :/64, 2001:db8:acad:0008: :/64, 2001:db8:acad:ffff: :/64. Una nota lee 5 subredes asignadas de 65.536 disponibles e indica que las cinco subredes asignadas son: 2001:db8:acad:0001: :/64, 2001:db8:acad:0002: :/64, 2001:db8:acad:0003: :/64, 2001:db8:acad:0004: :/64, 2001:db8:acad:0005: :/64.

12.8.4

Enrutador configurado con subredes IPv6

Similar a la configuración de IPv4, el ejemplo muestra que cada una de las interfaces del enrutador se ha configurado para estar en una subred IPv6 diferente.

Configuración de direcciones IPv6 en el enrutador R1

```
R1(config)# interfaz gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interfaz gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

12.8.5

Compruebe su comprensión - Subred una red IPv6

Compruebe su comprensión de la subred de una red IPv6 eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es verdadero. IPv6 tiene un campo Id. de subred independiente en la parte del prefijo de red de la dirección que se puede utilizar para crear subredes.
2. El campo Id. de subred, que se encuentra entre el campo Prefijo de enrutamiento global y el campo Id. de interfaz, se utiliza para subredes.
3. La parte de subred de la dirección es los 16 bits entre los prefijos /48 y /64, que son 2222.
4. La parte de subred de la dirección consta de los 32 bits entre los prefijos /32 y /64.

Has tenido 4 respuestas correctas de 4.

1. ¿Verdadero o falso? IPv6 se diseñó teniendo en cuenta las subredes.

¡Lo tienes!

- (•) Verdadero
- ( ) Falso

2. ¿Qué campo de un GUA IPv6 se utiliza para subredes?

¡Lo tienes!

- ( ) Prefijo
- ( ) Red
- ( ) Prefijo de routing global
- (•) ID de subred
- ( ) ID de interfaz

3. Dado un prefijo de enrutamiento global /48 y un prefijo /64, ¿cuál es la parte de subred de la siguiente dirección: 2001:db8:cafe:1111:2222:3333:4444:5555

¡Lo tienes!

- ( ) cafeteria
- (•) 1111
- ( ) 2222
- ( ) 3333
- ( ) 4444

4. Dado un prefijo de enrutamiento global /32 y un prefijo /64, ¿cuántos bits se asignarían para el ID de subred?

¡Lo tienes!

- 8
- 16
- 32
- 48
- 64

Correct

You have successfully identified the correct answers.

1. The correct answer is True. IPv6 has a separate subnet ID field in the network prefix portion of the address that can be used to create subnets.
2. The Subnet ID field, which is between the Global Routing Prefix field and the Interface ID field, is used for subnetting.
3. The subnet portion of the address is the 16 bits between the /48 and /64 prefixes, which are 2222.
4. The subnet portion of the address consists of the 32 bits between the /32 and /64 prefixes.

You got 4 out of 4 questions correct.

1. True or False? IPv6 was designed with subnetting in mind.

You got it!

- (●) True
- ( ) False

2. Which field in an IPv6 GUA is used for subnetting?

You got it!

- ( ) Prefix
- ( ) Network
- ( ) Global Routing Prefix
- (●) Subnet ID
- ( ) Interface ID

3. Given a /48 Global Routing Prefix and a /64 prefix, what is the subnet portion of the following address: 2001:db8:cafe:1111:2222:3333:4444:5555

You got it!

- ( ) café
- (●) 1111
- ( ) 2222
- ( ) 3333
- ( ) 4444

4. Given a /32 Global Routing Prefix and a /64 prefix, how many bits would be allocated for the Subnet ID?

You got it!

- ( ) 8
- ( ) 16
- (●) 32
- ( ) 48
- ( ) 64

12.8 – Práctica del Módulo y Cuestionario

12.9.1

Packet Tracer: implemente un esquema de direccionamiento IPv6 subred

El administrador de redes desea que asigne cinco subredes IPv6 /64 a la red que se muestra en la topología. Su tarea consiste en determinar las subredes IPv6, asignar direcciones IPv6 a los routers y configurar las PC para que reciban automáticamente el direccionamiento IPv6. El último paso es verificar la conectividad entre los hosts IPv6.

Implemente un esquema de direccionamiento IPv6 subred

Implemente un esquema de direccionamiento IPv6 subred

12.9.2

Lab – Configuración de direcciones IPv6 en dispositivos de red

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Establecer la topología y configurar los parámetros básicos del router y del switch
- Parte 2: Configurar las direcciones IPv6 de forma manual
- Parte 3: Verificar la conectividad completa

configuración de direcciones IPv6 en dispositivos de red

12.9.3

¿Qué aprenderé en este módulo?

Problemas con IPv4

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas en combinación con NAT han ayudado a ralentizar el agotamiento del espacio de direcciones IPv4. Con una población de Internet cada vez mayor, un espacio limitado de direcciones IPv4, problemas con NAT y el IoT, ha llegado el momento de comenzar la transición a IPv6. Tanto IPv4 como IPv6 coexistirán en un futuro próximo y la transición llevará varios años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración se pueden dividir en tres categorías: Dual-stack, tunelización y traducción.

Direccionamiento Dinámico para las GUAs de IPv6

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales. El formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales. Por ejemplo: 2001:0 db 8:0000:1111:0000:0000:0000:0200. Dos reglas que ayudan a reducir la cantidad de dígitos necesarios para representar una dirección IPv6. La primera regla para ayudar a reducir la notación de las direcciones IPv6 es omitir los ceros (ceros) iniciales en cualquier hexteto. Por ejemplo: 2001:db 8:0:1111:0:0:0:200. La segunda regla para ayudar a reducir la notación de las direcciones IPv6 es que un doble punto (: :) puede reemplazar cualquier cadena única y contigua de uno o más hextetos de 16 bits que consisten en todos los ceros. Por ejemplo: 2001:db 8:0:1111: :200.

Tipos de Direcciones IPv6

Existen tres tipos de direcciones IPv6: de **unidifusión (unicast)**, de **multidifusión (multicast)** y de **difusión por proximidad (anycast)**. IPv6 no utiliza la notación decimal punteada de máscara de subred. Al igual que IPv4, la longitud del prefijo se representa en notación de barra inclinada y se usa para indicar la porción de red de una dirección IPv6. Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Las direcciones IPv6 suelen tener dos direcciones de unidifusión: GUA y LLA. Las direcciones locales únicas de IPv6 tienen los siguientes usos: se utilizan para direcciones locales dentro de un sitio o entre un número limitado de sitios, se pueden usar para dispositivos que nunca necesitarán acceder a otra red y no se enrutan o traducen globalmente a una dirección IPv6 global. Las direcciones IPv6 unicast globales (GUA) son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. Un GUA tiene tres partes: un prefijo de enrutamiento global, un Id. de subred y un Id. de interfaz. Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunique con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred). Los dispositivos pueden obtener un LLA de forma estática o dinámica.

Configuración Estática de GUA y LLA

El comando Cisco IOS para configurar una dirección IPv4 en una interfaz es **ip address** *ip-address subnet-mask*. Por el contrario, el comando para configurar un GUA IPv6 en una

interfaz es **ipv6 address** *ipv6-address/prefix-length*. Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de redes en una red IPv6 habilitan la asignación dinámica de direcciones IPv6. Configurar la LLA manualmente permite crear una dirección reconocible y más fácil de recordar. Por lo general, solo es necesario crear LLA reconocibles en los enrutadores. Los LLA se pueden configurar manualmente usando el comando **ipv6 address** *ipv6-link-local-address* **link-local**.

Direccionamiento dinámico para GUA IPv6

Un dispositivo obtiene una GUA dinámicamente a través de mensajes ICMPv6. Los routers IPv6 envían mensajes RA de ICMPv6 periódicamente, cada 200 segundos, a todos los dispositivos con IPv6 habilitado en la red. También se enviará un mensaje RA en respuesta a un host que envía un mensaje ICMPv6 RS, que es una solicitud de un mensaje RA. El mensaje RA ICMPv6 incluye: prefijo de red y longitud de prefijo, dirección de puerta de enlace predeterminada y direcciones DNS y nombre de dominio. Los mensajes RA tienen tres métodos: SLAAC, SLAAC con un servidor DHCPv6 sin estado y DHCPv6 con estado (sin SLAAC). Con SLAAC, el dispositivo cliente utiliza la información del mensaje RA para crear su propio GUA porque el mensaje contiene el prefijo y el ID de interfaz. Con SLAAC con DHCPv6 sin estado, el mensaje RA sugiere que los dispositivos utilicen SLAAC para crear su propia GUA IPv6, utilizar la LLA del router como dirección de puerta de enlace predeterminada y utilizar un servidor DHCPv6 sin estado para obtener otra información necesaria. Con DHCPv6 con estado, RA sugiere que los dispositivos utilicen el enrutador LLA como dirección de puerta de enlace predeterminada, y el servidor DHCPv6 con estado para obtener una GUA, una dirección de servidor DNS, nombre de dominio y toda la información necesaria. La ID de interfaz se puede crear utilizando el proceso EUI-64 o un número de 64 bits generado aleatoriamente. El proceso EUI utiliza la dirección MAC Ethernet de 48 bits del cliente e inserta otros 16 bits en el medio de la dirección MAC para crear una ID de interfaz de 64 bits. Dependiendo del sistema operativo, un dispositivo puede usar una ID de interfaz generada aleatoriamente.

Direccionamiento Dinámico para las LLAs de IPv6

Todos los dispositivos IPv6 deben tener una LLA IPv6. Una LLA se puede configurar manualmente o crear dinámicamente. Los sistemas operativos, como Windows, suelen utilizar el mismo método tanto para una GUA creada por SLAAC como para una LLA asignada dinámicamente. Los routers Cisco crean automáticamente un LLA IPv6 cada vez que se asigna una GUA a la interfaz. De manera predeterminada, los enrutadores Cisco IOS usan EUI-64 para generar la ID de interfaz para todos los LLA en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Para que sea más fácil reconocer y recordar estas direcciones en los enrutadores, es común configurar estáticamente los LLA de IPv6 en los enrutadores. Para verificar la configuración de direcciones IPv6, utilice los tres comandos siguientes: **show ipv6 interface brief**, **show ipv6 route**, y **ping**.

Multidifusión de IPv6

Existen dos tipos de direcciones de multidifusión IPv6: direcciones de multidifusión conocidas y direcciones de multidifusión de nodos solicitados. Las direcciones de multidifusión asignadas son direcciones de multidifusión reservadas para grupos predefinidos de dispositivos. Se asignan direcciones multidifusión conocidas. Dos grupos de multidifusión asignados Communipv6 son: ff02: :1 grupo de multidifusión de todos los nodos y ff02: :2 grupo de multidifusión de todos los enrutadores. Una dirección de multidifusión de nodo solicitado es similar a una dirección de multidifusión de todos los nodos. La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección especial de multidifusión de Ethernet.

Crear Subredes de una Red IPv6

IPv6 se diseñó teniendo en cuenta las subredes. Se utiliza un campo ID de subred independiente en IPv6 GUA para crear subredes. El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz. La ventaja de una dirección de 128 bits es que puede admitir más que suficientes subredes y hosts por subred para cada red. La conservación de la dirección no es un problema. Por ejemplo, si el prefijo de enrutamiento global es un / 48 y utiliza un típico 64 bits para la ID de interfaz, esto creará una ID de subred de 16 bits:

- ID de subred de 16 bits: crea hasta 65.536 subredes.
- ID de interfaz de 64 bits: admite hasta 18 quintillones de direcciones IPv6 de host por subred (es decir, 18,000,000,000,000,000,000).

Con más de 65.536 subredes para elegir, la tarea del administrador de la red es diseñar un esquema lógico para abordar la red. La conservación de direcciones no es una preocupación cuando se utiliza IPv6. Similar a la configuración de IPv4, cada interfaz de enrutador se puede configurar para estar en una subred IPv6 diferente.

12.9.4

Módulo Quiz - Dirección IPv6

1. ¿Qué se indica mediante un ping correcto a la dirección IPv6: :1?

Tema 12.2.0: la dirección IPv6 :: 1 es la dirección de bucle invertido. Un ping correcto a esta dirección significa que la pila TCP/IP está instalada correctamente. Esto no significa que ninguna dirección esté configurada correctamente.

- ( ) El host está correctamente cableado.
- ( ) La dirección de puerta de enlace predeterminada está configurada correctamente.
- ( ) Todos los hosts del enlace local están disponibles.
- ( ) La dirección local del vínculo está configurada correctamente.
- (•) IP está instalada correctamente en el host.

2. ¿Cuál es la representación más comprimida de la dirección IPv6 2001:0000:0000:abcd: 0000:0000:0000:0001?

Tema 12.2.0 - La dirección IPv6 2001:0000:0000:abcd: 0000:0000:0000:0001 en su formato más comprimido sería 2001:0:0:abcd: :1. Los dos primeros hexetos de ceros se comprimirían cada uno a un solo cero. Los tres hexetos consecutivos de ceros se pueden comprimir a dos puntos::. Los tres ceros a la izquierda en el último hextet se pueden eliminar. Los dos puntos dobles :: solo se pueden usar una vez en una dirección.

- ( ) 2001:0:abcd::1
- (•) 2001:0:0:abcd::1
- ( ) 2001: :abcd: :1
- ( ) 2001:0000:abcd::1
- ( ) 2001::abcd:0:1

3. ¿Cuál es el propósito del comando**ping ::1**?

Tema 12.2.0: la dirección :: 1 es una dirección de bucle invertido IPv6. El uso del comando**ping ::1** prueba la pila de IP interna para garantizar que esté configurada y funcione correctamente. No prueba la posibilidad de conexión a ningún dispositivo interno ni confirma que las direcciones IPv6 estén configuradas correctamente en el host.

- (•) Probar la configuración interna de un host IPv6.
- ( ) Probar la funcionalidad de difusión de todos los hosts de la subred.
- ( ) Probar la conectividad de multidifusión a todos los hosts de la subred.
- ( ) Probar la posibilidad de conexión al gateway predeterminado de la red.

4. Como mínimo, ¿cuál es la dirección que se requiere en las interfaces con IPv6 habilitado?

Tema 12.3.0: todas las interfaces habilitadas para IPv6 deben tener, como mínimo, una dirección de enlace local. Las otras direcciones IPv6 se pueden asignar a la interfaz según sea necesario.

- (•) Link-local
- ( ) Local única
- ( ) Local de sitio
- ( ) Unidifusión global

5. ¿Cuál es la ID de interfaz de la dirección IPv6 2001:DB8::1000:A9CD:47FF:FE57:FE94/64?

Tema 12.2.0: la ID de interfaz de una dirección IPv6 son los 64 bits más a la derecha, o los últimos cuatro hextetos, de la dirección si no se han utilizado bits de ID de interfaz para subredes.

- ○ FE94
- ○ FE57:FE94
- ○ 47FF:FE57:FE94
- ◉ A9CD:47FF:FE57:FE94
- ○ 1000:A9CD:47FF:FE57:FE94

6. ¿Cuáles son las tres partes de una dirección de unidifusión global IPv6? (Escoja tres opciones).

Tema 12.3.0 - Hay tres elementos que componen una dirección de unidifusión global IPv6. Prefijo de enrutamiento global proporcionado por un ISP, un Id. de subred determinado por la organización y un Id. de interfaz que identifica de forma exclusiva la interfaz de interfaz de un host.

- ☐ un ID de interfaz que se utiliza para identificar la red local para un host concreto
- ☑ un prefijo de enrutamiento global que se utiliza para identificar la parte de la red de la dirección que ha proporcionado un ISP
- ☑ un Id. de subred que se utiliza para identificar redes dentro del sitio de empresa local
- ☐ un prefijo de enrutamiento global que se utiliza para identificar la parte de la dirección de red proporcionada por un administrador local
- ☑ un ID de interfaz que se utiliza para identificar el host local en la red

7. ¿Cuál es el formato válido más comprimido posible de la dirección IPv6 2001:0DB8:0000:AB00:0000:0000:0000:1234?

Tema 12.2.0: hay dos reglas que definen cómo se puede comprimir una dirección IPv6. La primera regla establece que se pueden eliminar los ceros iniciales de un hexteto. La segunda regla establece que uno o más de un hexteto de todos ceros contiguos puede abreviarse como dos puntos dobles (::). Los dos puntos dobles (::) pueden aparecer solo una vez en una dirección IPv6.

- ◉ 2001:DB8:0:AB00::1234
- ○ 2001:DB8:0:AB::1234
- ○ 2001:DB8::AB00::1234
- ○ 2001:DB8:0:AB:0:1234

8. ¿Cuál es el prefijo asociado a la dirección IPv6 2001:CA48:D15:EA:CC44::1/64?

Tema 12.3.0 - El /64 representa los campos IPv6 de red y subred. El cuarto campo de dígitos hexadecimales se conoce como Id. de subred. El Id. de subred de esta dirección es 2001:CA48:D15:EA::0/64.

- ○ 2001::/64
- ○ 2001:CA48::/64
- ◉ 2001:CA48:D15:EA::/64
- ○ 2001:CA48:D15:EA:CC44::/64

9. ¿Qué tipo de dirección se asigna automáticamente a una interfaz cuando IPv6 está habilitado en esa interfaz?

Tema 12.3.0 - Cuando IPv6 está habilitado en cualquier interfaz, esa interfaz generará automáticamente una dirección local de vínculo IPv6.

- ○ Unidifusión global
- ◉ Link-local
- ○ Bucle invertido
- ○ Local única

10. ¿Qué prefijo de red IPv6 solo está destinado a enlaces locales y no se puede enrutar?

Tema 12.3.0 - FE80: :/10 es un prefijo local de vínculo. Los dispositivos con direcciones locales de enlace sólo pueden comunicarse con otros dispositivos de la misma red, pero no con dispositivos de ninguna otra red.

- ○ 2001: :/3
- ○ FC00::/7
- ◉ FE80::/10
- ○ FEC0::/10

11. Su proveedor de servicios emite el prefijo IPv6 2001:0000:130 F: :/48 a su organización. Con este prefijo, ¿cuántos bits están disponibles para que su organización cree subredes si los bits de ID de interfaz no se toman prestados?

Tema 12.8.0: el prefijo de enrutamiento global asignado a la organización tiene 48 bits. Los siguientes 16 bits se utilizan para el ID de subred. Esto constituye los primeros 64 bits de la dirección, que normalmente es la parte de red de la dirección. Los 64 bits restantes de la dirección IPv6 de 128 bits corresponden a la parte de ID de interfaz (o host) de la dirección.

- ○ 8
- ◉ 16
- ○ 80
- ○ 128

12. ¿Cuál es la dirección de subred para la dirección IPv6 2001:D12:AA04:B5::1/64?

Tema 12.8.0: el / 64 representa los campos IPv6 de red y subred que son los primeros cuatro grupos de dígitos hexadecimales. La primera dirección dentro de ese intervalo es una dirección de subred 2001:D12:AA04:B5::/64.

- ○ 2001::/64
- ○ 2001:D12::/64
- ○ 2001:D12:AA04::/64
- ◉ 2001:D12:AA04:B5::/64

13. ¿Qué tipo de dirección IPv6 no se puede enrutar y se utiliza sólo para la comunicación en una sola subred?

Tema 12.3.0 - Las direcciones locales del vínculo sólo tienen relevancia en el vínculo local. Los enrutadores no reenviarán paquetes que incluyan una dirección local de enlace como dirección de origen o de destino.

- dirección de unidifusión global
- (•) dirección local de enlace
- dirección de loopback
- dirección local única
- dirección no especificada

14. ¿Qué tipo de dirección no se admite en IPv6?

Tema 12.3.0 - IPv6 admite direcciones de unidifusión, privadas y multidifusión, pero no admite difusiones de capa 3.

- Privada
- Multidifusión
- Unidifusión
- (•) Difusión

15. ¿Cuál es la configuración mínima para una interfaz de router que participa en el routing IPv6?

Tema 12.3.0: con IPv6, una interfaz de enrutador generalmente tiene más de una dirección IPv6. El router tendrá, como mínimo, una dirección de enlace local que se podrá generar de forma automática, pero comúnmente el router tiene una dirección de unidifusión global también configurada.

- (•) Tener solo una dirección IPv6 de enlace local.
- Tener una dirección IPv4 y IPv6.
- Tener una dirección de loopback generada.
- Tener una dirección de enlace local y una dirección IPv6 de unidifusión global.
- Tener solo una dirección IPv6 de multidifusión generada automáticamente.

1. What is the valid most compressed format possible of the IPv6 address 2001:0DB8:0000:AB00:0000:0000:0000:1234?

Topic 12.2.0 - There are two rules defining how an IPv6 address can be compressed. The first rule states that leading zeros in a hextet can be eliminated. The second rule states that a single :: can be used to represent one or more contiguous all zero hextets. There can be one and only one :: in an IPv6 address.

- (•) 2001:DB8:0:AB00::1234
- 2001:DB8:0:AB::1234
- 2001:DB8::AB00::1234
- 2001:DB8:0:AB:0:1234

2. What is the prefix associated with the IPv6 address 2001:DB8:D15:EA:CC44::1/64?

Topic 12.3.0 - The /64 represents the network and subnet IPv6 fields. The fourth field of hexadecimal digits is referred to as the subnet ID. The subnet ID for this address is 2001:DB8:D15:EA::0/64.

- ○ 2001::/64
- ○ 2001:DB8::/64
- ◉ 2001:DB8:D15:EA::/64
- ○ 2001:DB8:D15:EA:CC44::/64

3. What type of address is automatically assigned to an interface when IPv6 is enabled on that interface?

Topic 12.3.0 - When IPv6 is enabled on any interface, that interface will automatically generate an IPv6 link-local address.

- ○ global unicast
- ◉ link-local
- ○ loopback
- ○ unique local

4. Which IPv6 network prefix is only intended for local links and can not be routed?

Topic 12.3.0 - FE80::/10 is a link-local prefix. Devices with only link-local addresses can communicate with other devices on the same network but not with devices on any other network.

- ○ 2001::/3
- ○ FC00::/7
- ◉ FE80::/10
- ○ FF00::/12

5. What is the purpose of the command **ping ::1**?

Topic 12.2.0 - The address ::1 is an IPv6 loopback address. Using the command **ping ::1** tests the internal IP stack to ensure that it is configured and functioning correctly. It does not test reachability to any external device, nor does it confirm that IPv6 addresses are properly configured on the host.

- ◉ It tests the internal configuration of an IPv6 host.
- ○ It tests the broadcast capability of all hosts on the subnet.
- ○ It tests the multicast connectivity to all hosts on the subnet.
- ○ It tests the reachability of the default gateway for the network.

6. What is the interface ID of the IPv6 address 2001:DB8::1000:A9CD:47FF:FE57:FE94/64?

Topic 12.2.0 - The interface ID of an IPv6 address is the rightmost 64 bits, or last four hextets, of the address if no interface ID bits have been used for subnets.

- FE94
- FE57:FE94
- 47FF:FE57:FE94
- **A9CD:47FF:FE57:FE94**
- 1000:A9CD:47FF:FE57:FE94

7. What is the network address for the IPv6 address 2001:DB8:AA04:B5::1/64?

Topic 12.8.0 - The /64 represents the network and subnet IPv6 fields which are the first four groups of hexadecimal digits. The first address within that range is the subnetwork address of 2001:DB8:AA04:B5::/64.

- 2001::/64
- 2001:DB8::/64
- 2001:DB8:AA04::/64
- **2001:DB8:AA04:B5::/64**

8. Which address type is not supported in IPv6?

Topic 12.3.0 - IPv6 supports unicast, private, and multicast addresses but does not support Layer 3 broadcasts.

- private
- multicast
- unicast
- **broadcast**

9. What is indicated by a successful ping to the ::1 IPv6 address?

Topic 12.2.0 - The IPv6 address ::1 is the loopback address. A successful ping to this address means that the TCP/IP stack is correctly installed. It does not mean that any addresses are correctly configured.

- The host is cabled properly.
- The default gateway address is correctly configured.
- All hosts on the local link are available.
- The link-local address is correctly configured.
- **IP is properly installed on the host.**

10. What is the most compressed representation of the IPv6 address 2001:0db8:0000:abcd:0000:0000:0000:0001?

Topic 12.2.0 - The IPv6 address 2001:0db8:0000:abcd:0000:0000:0000:0001 in its most compressed format would be 2001:db8:0:abcd::1. The one leading zero in the second hextet can be removed. The first hextet of zeros would be compressed to a single zero. The three consecutive hextets of zeros can be compressed to a double colon ::. The three leading zeros in the last hextet can be removed. The double colon :: can only be used once in an address.

- ○ 2001:0db8:abcd::1
- ◉ 2001:db8:0:abcd::1
- ○ 2001:0db8:abcd::0001
- ○ 2001:0db8:0000:abcd::1
- ○ 2001:db8::abcd:0:1

11. What is the minimum configuration for a router interface that is enabled for IPv6?

Topic 12.3.0 - With IPv6, a router interface typically has more than one IPv6 address. The router will at least have a link-local address that can be automatically generated, but the router commonly has an global unicast address also configured.

- ◉ to have a link-local IPv6 address
- ○ to have both an IPv4 and an IPv6 address
- ○ to have a self-generated loopback address
- ○ to have both a link-local and a global unicast IPv6 address
- ○ to have only an automatically generated multicast IPv6 address

12. At a minimum, which address is required on IPv6-enabled interfaces?

Topic 12.3.0 - All IPv6 enabled interfaces must at minimum have a link-local address. Other IPv6 addresses can be assigned to the interface as required.

- ◉ link-local
- ○ unique local
- ○ site local
- ○ global unicast

13. What are three parts of an IPv6 global unicast address? (Choose three.)

Topic 12.3.0 - There are three elements that make up an IPv6 global unicast address. A global routing prefix which is provided by an ISP, a subnet ID which is determined by the organization, and an interface ID which uniquely identifies the interface interface of a host.

- [ ] an interface ID that is used to identify the local network for a particular host
- [x] a global routing prefix that is used to identify the network portion of the address that has been provided by an ISP
- [x] a subnet ID that is used to identify networks inside of the local enterprise site
- [ ] a global routing prefix that is used to identify the portion of the network address provided by a local administrator
- [x] an interface ID that is used to identify the local host on the network

14. Your organization is issued the IPv6 prefix of 2001:db8:130f::/48 by your service provider. With this prefix, how many bits are available for your organization to create /64 subnetworks if interface ID bits are not borrowed?

Topic 12.8.0 - The global routing prefix that is assigned to the organization has 48 bits. The next 16 bits are used for the subnet ID. This makes up the first 64 bits of the address, which is typically the network portion of the address. The remaining 64 bits of the 128-bit IPv6 address are for the interface ID (or host) portion of the address.

- ( ) 8
- (•) 16
- ( ) 80
- ( ) 128

15. Which type of IPv6 address is not routable and used only for communication on a single subnet?

Topic 12.3.0 - Link-local addresses have relevance only on the local link. Routers will not forward packets that include a link-local address as either the source or destination address.

- ( ) global unicast address
- (•) link-local address
- ( ) loopback address
- ( ) unique local address
- ( ) unspecified address

Capítulo 13_ICMP

Introducción

13.0.1

¿Por qué debería tomar este módulo?

Bienvenido a ICMP!

Imagina que tienes un intrincado juego de tren modelo. Sus vías y trenes están conectados, encendidos y listos para funcionar. Tú lanzas el interruptor. El tren va a la mitad de la pista y se detiene. Usted sabe de inmediato que el problema se encuentra muy probablemente donde el tren se ha detenido, así que mira allí primero. No es tan fácil visualizar esto con una red. Afortunadamente, hay herramientas para ayudarle a localizar áreas problemáticas en su red, ¡Y funcionan con redes IPv4 e IPv6! Usted estará feliz de saber que este módulo tiene un par de actividades Packet Tracer para ayudarle a practicar el uso de estas herramientas, así que vamos a probar!

13.0.2

¿Qué aprenderé en este módulo?

Título del módulo: ICMP

Objetivos del módulo: Utilice varias herramientas para probar la conectividad de red.

Título del tema	Objetivo del tema
Mensajes ICMP	Explique la forma en que se usa ICMP para probar la conectividad de red.
Pruebas de ping y traceroute	Utilice las utilidades de ping y traceroute para probar la conectividad de red.

ICMP / Mensajes ICMP

Mensajes ICMP

13.1.1

Mensajes ICMPv4 e ICMPv6

En este tema, aprenderá acerca de los diferentes tipos de protocolos de mensajes de control de Internet (ICMP) y las herramientas que se utilizan para enviarlos.

Aunque IP es sólo un protocolo de mayor esfuerzo, el conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP en determinadas condiciones, no es hacer que IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

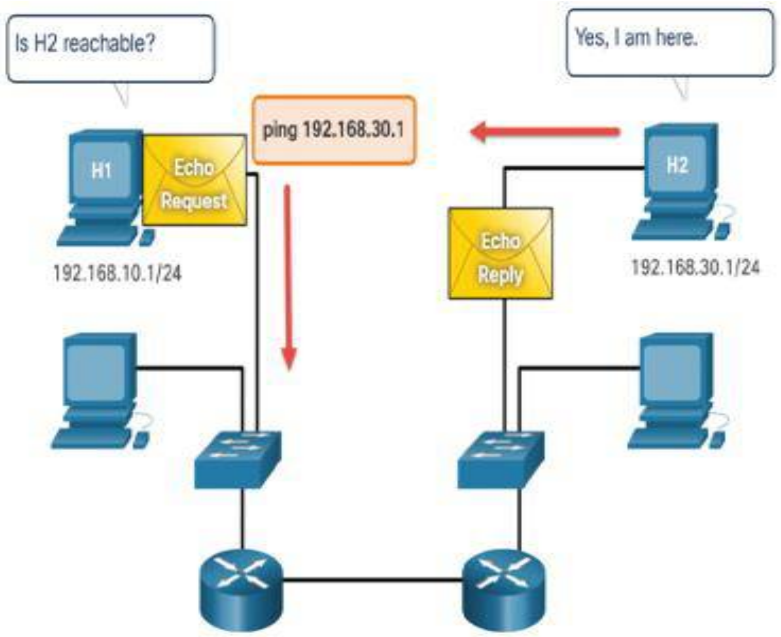
Los tipos de mensajes ICMP y las razones por las que se envían son extensos. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 y discutidos en este módulo incluyen:

- Accesibilidad al host
- Destino o servicio inaccesible
- Tiempo superado

13.1.2

Accesibilidad al host

Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. En la ilustración, haga clic en el botón Reproducir para ver una animación de la solicitud de eco/respuesta de eco ICMP. Este uso de los mensajes ICMP Echo es la base de la utilidad **ping** .



Animación del host 1 enviando una solicitud de eco ICMP ping al host 2 y la respuesta de eco ICMP del host 2 al host 1.

13.1.3

Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

Algunos de los códigos de destino inalcanzable para ICMPv6 son los siguientes:

- 0 - No hay ruta para el destino
- 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
- 2 - Más allá del alcance de la dirección de origen

- 3 - No se puede alcanzar la dirección
- 4 - Puerto inalcanzable

Nota: ICMPv6 tiene códigos similares, pero ligeramente diferentes para los mensajes de destino inalcanzable.

13.1.4

Tiempo excedido

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de tiempo de duración (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. En lugar del campo TTL de IPv4, ICMPv6 usa el campo Límite de salto de IPv6 para determinar si el paquete ha expirado.

La **Nota**: herramienta utiliza los mensajes de **traceroute** tiempo excedido.

13.1.5

Mensajes ICMPv6

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4. Los mensajes ICMPv6 están encapsulados en IPv6.

ICMPv6 incluye cuatro mensajes nuevos como parte del protocolo de detección de vecino (ND o NDP).

Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, son los siguientes:

- Mensaje de solicitud de router (RS)
- Mensaje de anuncio de router (RA)

Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son los siguientes:

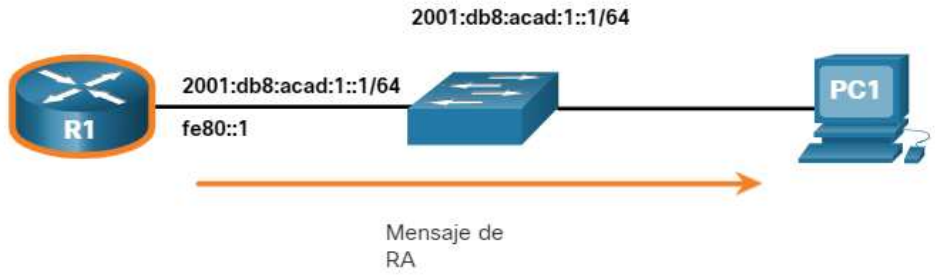
- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

Nota: ICMPv6 ND también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

Haga clic en cada una para obtener una ilustración y una explicación de los mensajes ICMPv6.

Mensaje de RA | Mensaje RS | Mensaje NS | Mensaje de NA

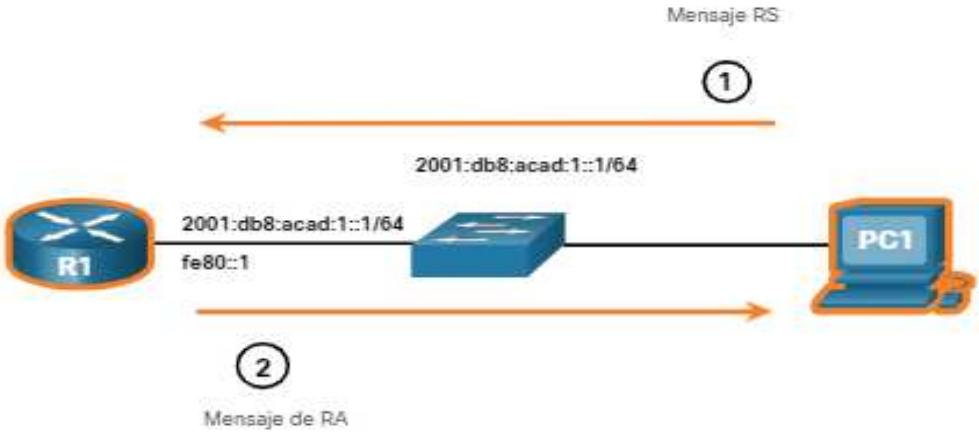
Los enrutadores habilitados para IPv6 envían mensajes de RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6. El mensaje RA puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el nombre de dominio. Un host que utiliza la Configuración automática de direcciones sin estado (SLAAC) establecerá su puerta de enlace predeterminada en la dirección de enlace local del enrutador que envió el RA.



R1 envía un mensaje de RA, «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1: :/64. Por cierto, use mi dirección local de enlace fe80: :1 como su puerta de enlace predeterminada«.

Mensaje de RA | Mensaje RS | Mensaje NS | Mensaje de NA

Un router habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS. En la figura, PC1 envía un mensaje RS para determinar cómo recibir dinámicamente su información de dirección IPv6.



R1 responde a la RS con un mensaje de RA.

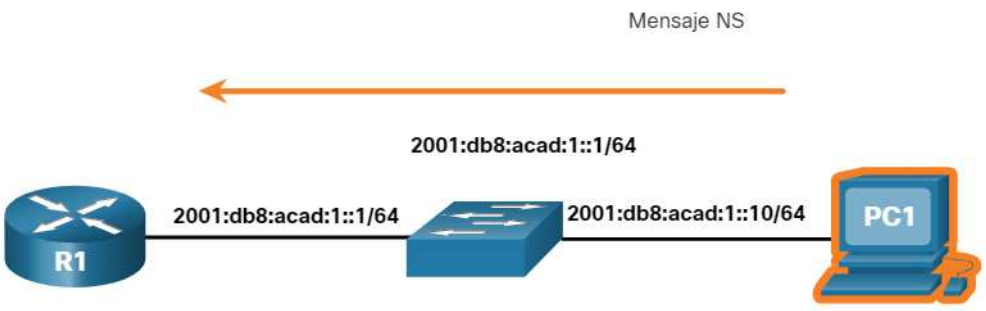
1. PC1 envía un mensaje RS, «Hola, acabo de arrancar. ¿Hay un enrutador IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».
2. R1 responde con un mensaje de RA. «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1::/64. Por cierto, use mi dirección local de enlace fe80::1 como su puerta de enlace predeterminada. »

Mensaje de RA | Mensaje RS | Mensaje NS | Mensaje de NA

Cuando a un dispositivo se le asigna una dirección de unidifusión global IPv6 o unidifusión local de enlace, puede realizar una detección de dirección duplicada (DAD) para garantizar que la dirección IPv6 sea única. Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 objetivo, como se muestra en la figura.

Si otro dispositivo de la red tiene esta dirección, responde con un mensaje NA. Este mensaje NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje NA correspondiente dentro de un cierto período de tiempo, la dirección de unidifusión es única y aceptable para su uso.

Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones unicast.

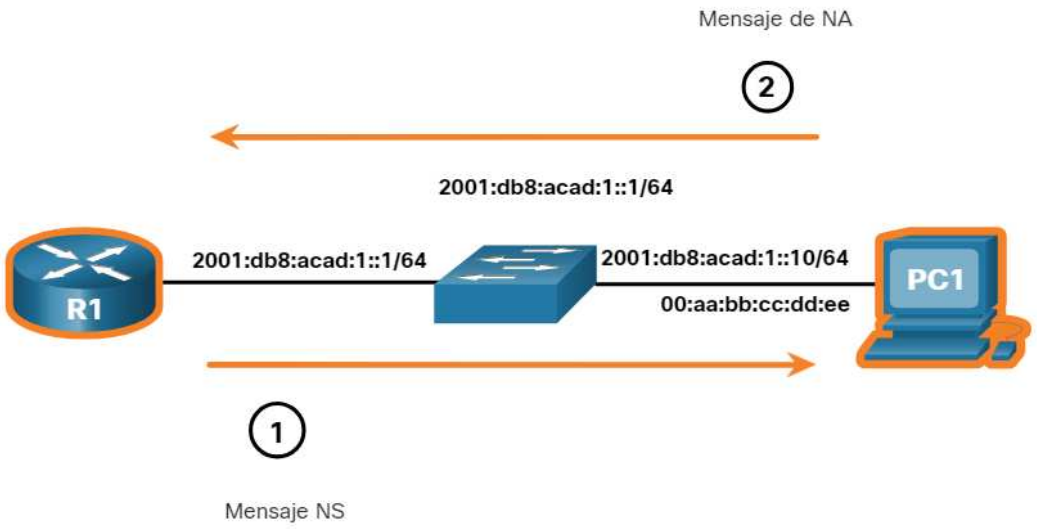


PC1 envía un mensaje NS para comprobar la singularidad de una dirección, “¿Quién tiene la dirección IPv6 2001:db8:acad:1::10, me enviará su dirección MAC?”

Mensaje de RA	Mensaje RS	Mensaje NS	Mensaje de NA

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de unidifusión de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet.

En la figura, R1 envía un mensaje NS a 2001:db8:acad:1: :10 pidiendo su dirección MAC.



1.-R1 envía un mensaje de NS de resolución de dirección, “¿Quién tenga la dirección IPV6 2001:db8:acad:1::10, me enviará su dirección MAC?”

2.-PC1 responde con un mensaje de NA “Soy 2001:db8:acad:1::10 y mi dirección MAC es 00:aa:bb:cc:dd:ee”.

13.1.6

Verifique su comprensión - Mensajes ICMP

Verifique su comprensión de los mensajes ICMP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 incluyen confirmación del host, destino o servicio inalcanzable y tiempo excedido.
2. El arranque de un host habilitado para IPv6 enviaría un mensaje de solicitud de enrutador ICMPv6. Un enrutador habilitado para IPv6 respondería con un mensaje de anuncio de enrutador.

Has tenido 2 respuestas correctas de 2.

1. ¿Qué dos tipos de mensajes ICMP son comunes a ICMPv4 e ICMPv6? (Escoja dos opciones).

¡Lo tienes!

- [x] Destino o servicio inaccesible
- [ ] Resolución de nombre de host
- [ ] Configuración de IP
- [ ] Origen inalcanzable
- [x] Tiempo superado

2. ¿Qué tipo de mensaje ICMPv6 enviaría un host para adquirir una configuración IPv6 al arrancar?

¡Lo tienes!

- ( ) Mensaje de anuncio de vecino (NA)
- ( ) Mensaje de solicitud de vecino (NS)
- ( ) Mensaje de anuncio de router (RA)
- (•) Mensaje de solicitud de router (RS)

Correct

You have successfully identified the correct answers.

1. ICMP messages common to both ICMPv4 and ICMPv6 include host confirmation, destination or service unreachable, and time exceeded.
2. An IPv6-enabled host booting up would send an ICMPv6 router solicitation message. An IPv6-enabled router would respond with a router advertisement message.

You got 2 out of 2 questions correct.

1. Which two types of ICMP messages are common to both ICMPv4 and ICMPv6? (Choose two.)

You got it!

- [x] Destination or Service Unreachable
- [ ] Hostname resolution
- [ ] IP configuration
- [ ] Source Unreachable
- [x] Time exceeded

2. Which type of ICMPv6 message would a host send to acquire an IPv6 configuration when booting up?

You got it!

- ( ) Neighbor Advertisement (NA) message
- ( ) Neighbor Solicitation (NS) message
- ( ) Router Advertisement (RA) message
- (•) Router Solicitation (RS) message

ICMP /Pruebas de ping y traceroute

Pruebas de ping y traceroute

13.2.1

Ping: prueba de conectividad

En el tema anterior, se le presentó a las herramientas **ping** y traceroute (**tracert**). En este tema, aprenderá acerca de las situaciones en las que se usa cada herramienta y cómo usarlas. Ping es una utilidad de prueba de IPv4 e IPv6 que utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts.

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección del host utilizando el comando. **ping** Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, **ping** proporciona comentarios sobre el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta. Esto puede ser una medida del rendimiento de la red.

El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta. Esto puede indicar que hay un problema, pero también podría indicar que las funciones de seguridad que bloquean los mensajes de ping se han habilitado en la red. Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la solicitud de eco ICMP.

Después de enviar todas las solicitudes, la utilidad **ping** proporciona un resumen que incluye la tasa de éxito y el tiempo promedio de ida y vuelta al destino.

Los tipos de pruebas de conectividad que se realizan con **ping** son los siguientes:

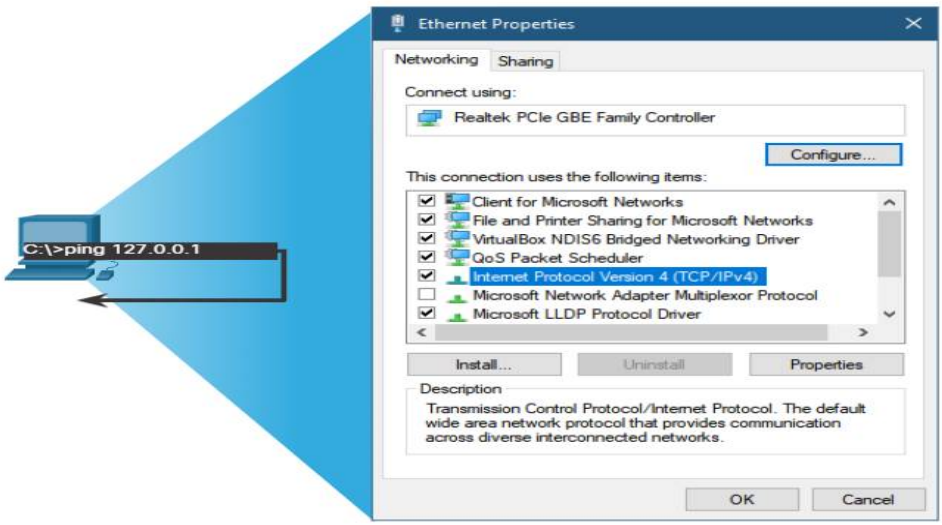
- Hacer ping al loopback local
- Hacer ping a la puerta de enlace predeterminada
- Hacer ping al host remoto

13.2.2

Hacer ping al loopback

Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Para realizar esta prueba, **ping** a dirección de bucle de retorno local de 127.0.0.1 para IPv4 (:: 1 para IPv6).

Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no es una indicación de que las direcciones, máscaras o puertas de enlace estén configuradas correctamente. Tampoco indica nada acerca del estado de la capa inferior de la pila de red. Simplemente, prueba el protocolo IP en la capa de red de dicho protocolo. Un mensaje de error indica que TCP/IP no funciona en el host.



Muestra el cuadro de diálogo Propiedades Ethernet muestra que el Protocolo de Internet versión 4 (TCP/IPv4) está instalado y activo, lo que se demuestra con un ping a 127.0.0.1.

- Hacer ping al host local permite confirmar que el protocolo TCP/IP se encuentra instalado en el host y que funciona.
- Hacer ping a 127.0.0.1 ocasiona que un dispositivo se haga ping a sí mismo.

13.2.3

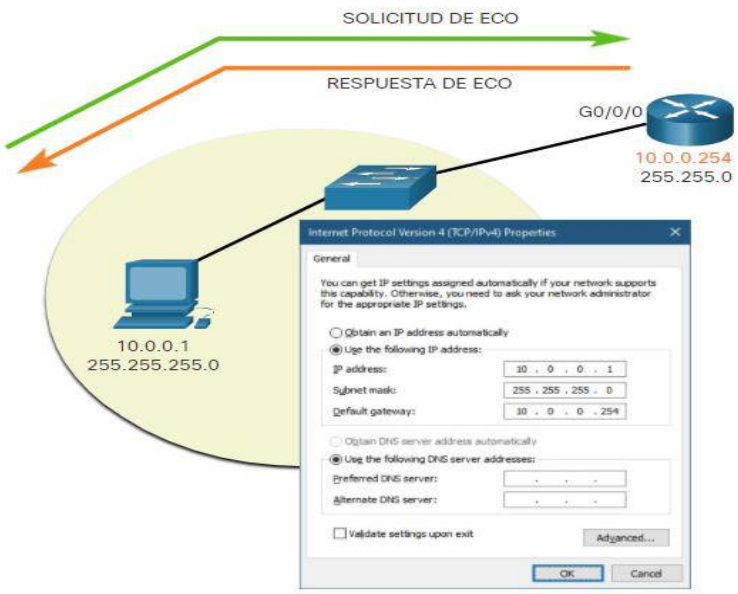
Hacer ping al gateway predeterminado

También puede usar **ping** para probar la capacidad de un host para comunicarse en la red local. Esto generalmente se hace haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un exitoso **ping** en la puerta de enlace predeterminada, indica que el host y la interfaz del enrutador que sirve como puerta de enlace predeterminada están operativos en la red local.

Para esta prueba, la dirección de puerta de enlace predeterminada se usa con mayor frecuencia porque el enrutador normalmente siempre está operativo. Si la dirección de la puerta de enlace predeterminada no responde, **ping** se puede enviar a la dirección IP de otro host en la red local que se sabe que está operativa.

Si la puerta de enlace predeterminada u otro host responde, entonces el host local puede comunicarse con éxito a través de la red local. Si la puerta de enlace predeterminada no responde, pero otro host sí, esto podría indicar un problema con la interfaz del enrutador que funciona como la puerta de enlace predeterminada.

Una posibilidad es que se haya configurado una dirección de puerta de enlace predeterminada incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde solicitudes de ping.



El host hace ping a su puerta de enlace predeterminada, enviando una solicitud de eco ICMP. La puerta de enlace predeterminada envía una respuesta de eco confirmando la conectividad

El gráfico muestra el cuadro de diálogo de propiedades Ethernet configurado con una dirección IP estática, una máscara de subred y una puerta de enlace predeterminada. La topología muestra la PC que envía una solicitud de eco a la puerta de enlace predeterminada del router y la respuesta de respuesta de eco de routers.

.

13.2.4

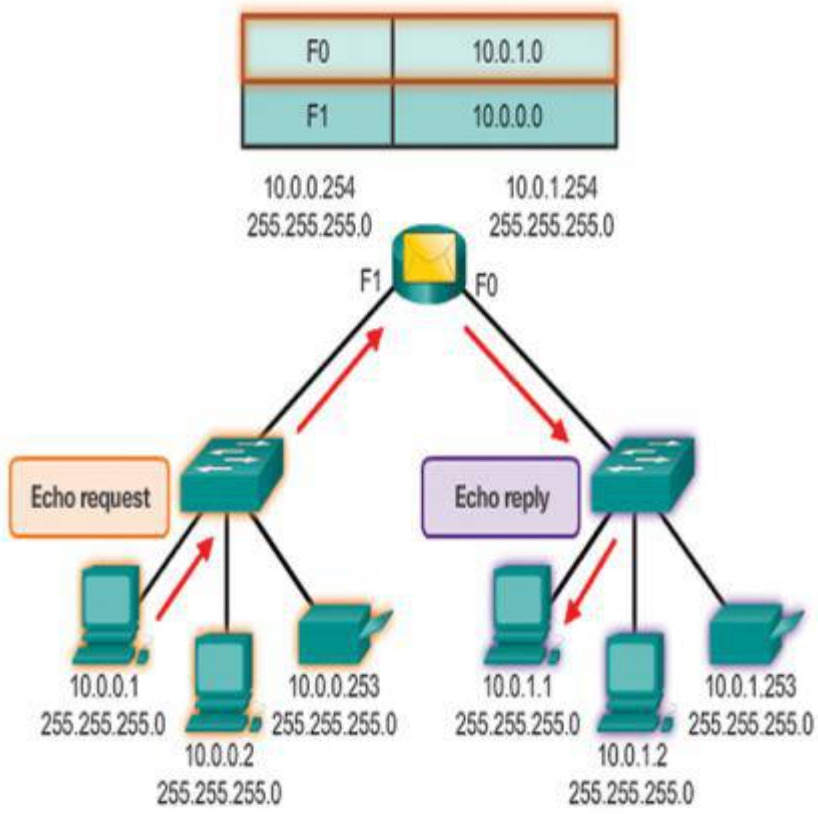
Hacer ping a un host remoto

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración. El router utiliza su tabla de enrutamiento IP para reenviar los paquetes.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un éxito en **ping** toda la red confirma la comunicación en la red local, el funcionamiento del enrutador que sirve como puerta de enlace predeterminada y el funcionamiento de todos los demás enrutadores que podrían estar en la ruta entre la red local y la red del host remoto.

De manera adicional, se puede verificar la funcionalidad del módulo remoto de E/S. Si el módulo remoto de E/S no podía comunicarse fuera de la red local, no hubiera respondido.

Nota: Muchos administradores de red limitan o prohíben la entrada de mensajes ICMP en la red corporativa; **ping** por lo tanto, la falta de respuesta podría deberse a restricciones de seguridad.



La figura muestra una solicitud de eco de ping a una red remota que se enruta a través de un enrutador y la respuesta de eco que se enruta desde la red remota.

13.2.5

Traceroute: prueba el camino

El comando ping se usa para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (**tracert**) es una utilidad que genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la solución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona tiempo de ida y vuelta para cada salto a lo largo del camino e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que tarda un paquete en

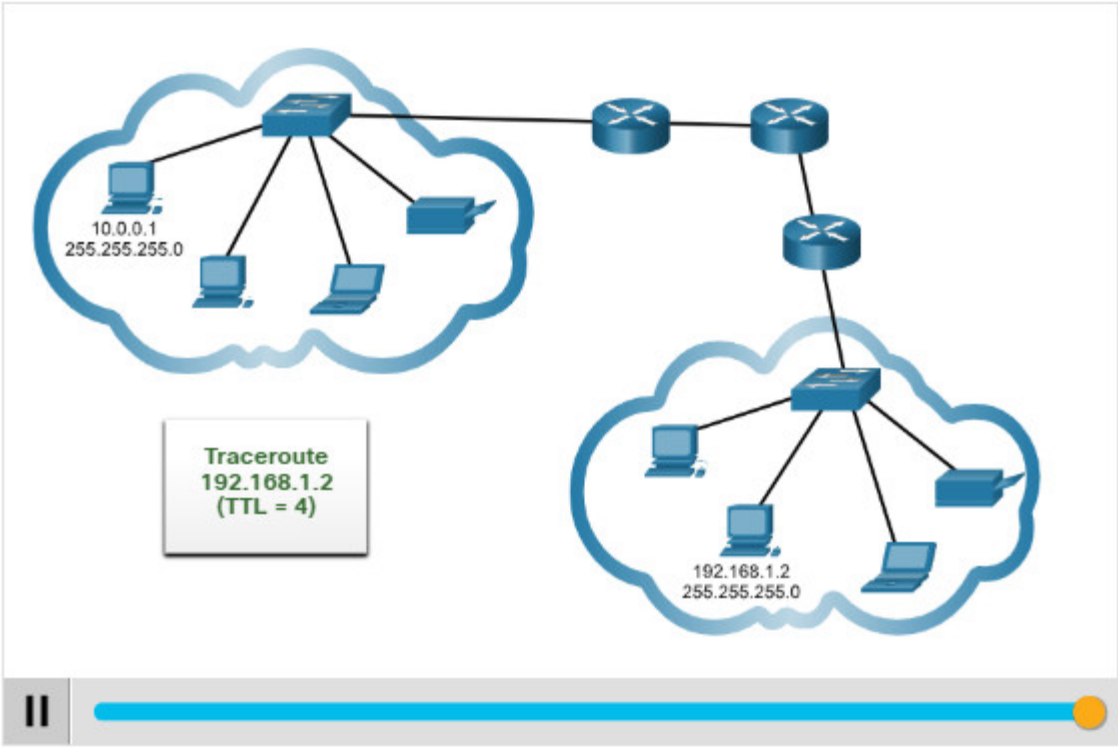
llegar al host remoto y que la respuesta del host regrese. Se utiliza un asterisco (\ *) para indicar un paquete perdido o no respondido.

Esta información se puede usar para localizar un enrutador problemático en la ruta o puede indicar que el enrutador está configurado para no responder. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

IPv4 TTL and IPv6 Hop Limit

Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje ICMP Time Exceeded.

Reproduzca la animación en la figura para ver cómo traceroute aprovecha el TTL.



Muestra un traceroute a una red remota que cruza tres enrutadores. El traceroute tomará 4 solicitudes de eco para llegar a su destino

La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este enrutador responde con un mensaje ICMPv4 Tiempo excedido. Traceroute ahora tiene la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. Esto proporciona el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.

Una vez que se alcanza el destino final, el host responde con un mensaje de puerto inalcanzable ICMP o un mensaje de respuesta de eco ICMP en lugar del mensaje de tiempo excedido ICMP.

13.2.6

Packet Tracer: verificar el direccionamiento IPv4 e IPv6

IPv4 e IPv6 pueden coexistir en la misma red. En el símbolo del sistema de una PC, existen algunas diferencias en el modo en que se emiten comandos y en que se muestra el resultado.

Identificación del direccionamiento IPv4 e IPv6

Identificación del direccionamiento IPv4 e IPv6

13.2.7

Packet Tracer: utilice Ping y Traceroute para probar la conectividad de red

En esta actividad, hay problemas de conectividad. Además de reunir y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad.

Use Ping y Traceroute para probar la conectividad de red

Use Ping y Traceroute para probar la conectividad de red

ICMP / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

13.3.1

Packet Tracer - Utilice ICMP para probar y corregir la conectividad de red

En este laboratorio utilizará ICMP para probar la conectividad de red y localizar problemas de red. También corregirá problemas de configuración simples y restaurará la conectividad a la red.

Use ICMP para localizar problemas de conectividad.

Configure los dispositivos de red para corregir problemas de conectividad.

Utilice ICMP para probar y corregir la conectividad de red

Utilice ICMP para probar y corregir la conectividad de red

13.3.2

Lab - Use Ping y Traceroute para probar la conectividad de red.

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Construcción y configuración de la red
- Parte 2: Utilizar el comando ping para realizar pruebas de red básicas
- Parte 3: Utilizar los comandos tracert y traceroute para realizar pruebas de red básicas
- Parte 4: Solucionar problemas de la topología

Use Ping y Traceroute para probar la conectividad de red

13.3.3

¿Qué aprenderé en este módulo?

Mensajes ICMP

El conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP. Estos mensajes se envían usando ICMP. El propósito de estos mensajes es proporcionar comentarios sobre problemas relacionados con el procesamiento de paquetes IP bajo ciertas condiciones. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 son: Accesibilidad del host, Destino o Servicio inalcanzable y Tiempo excedido. Un mensaje ICMP Echo prueba la accesibilidad de un host en una red IP. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. Esta es la base de la utilidad **ping**. Cuando un host o puerta de enlace recibe un paquete que no puede entregar, puede usar un mensaje ICMP Destination Unreachable para notificar a la fuente. El mensaje incluye un código que

indica el motivo por el cual no se pudo entregar el paquete. Un enrutador utiliza un mensaje ICMPv4 Tiempo excedido para indicar que no se puede reenviar un paquete porque el campo Tiempo de vida (TTL) del paquete se redujo a cero. Si un enrutador recibe un paquete y disminuye el campo TTL a cero, descarta el paquete y envía un mensaje de Tiempo excedido al host de origen. ICMPv6 también envía un Tiempo Excedido en esta situación. ICMPv6 usa el campo de límite de salto de IPv6 para determinar si el paquete ha expirado. La **traceroute** herramienta utiliza los mensajes de tiempo excedido. Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, incluyen RS y RA. Los mensajes entre dispositivos IPv6 incluyen el redireccionamiento (similar a IPv4), NS y NA.

Prueba con Ping y Traceroute

Ping (utilizado por IPv4 e IPv6) utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts. Para probar la conectividad con otro host de una red, se envía una solicitud de eco a la dirección de host mediante el comando ping. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, el comando ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del viaje de ida y vuelta al destino. Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Haga ping a la dirección de bucle de retorno local de 127.0.0.1 para IPv4 (:: 1 para IPv6). Utilícelo **ping** para probar la capacidad de un host para comunicarse en la red local, haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. 1Un ping exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirven como puerta de enlace predeterminada están operativos en la red local. También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede ser un **ping** host IPv4 operativo de una red remota. Traceroute (tracert) genera una lista de saltos que se alcanzaron con éxito a lo largo del camino. Esta lista proporciona información de verificación y solución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad. El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Traceroute utiliza una función del campo TTL en IPv4 y del campo límite de saltos de IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.

13.3.4

Prueba de módulo - ICMP

Correct
You have successfully identified the correct answers.

Has tenido 15 respuestas correctas de 15.

Correct
You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. Un usuario llama para informar de que un equipo no puede acceder a Internet. El técnico de red solicita al usuario que ejecute el comando **ping 127.0.0.1** en una ventana de símbolo del sistema. El usuario informa que el resultado es cuatro respuestas positivas. ¿Qué conclusión se puede extraer sobre la base de esta prueba de conectividad?

Tema 13.2.0 - El **ping 127.0.0.1** comando se utiliza para comprobar que la pila TCP/IP es funcional. Esto verifica que el stack de protocolos funcione correctamente desde la capa de red hasta la capa física, sin enviar una señal en los medios. Es decir, esta prueba no va más allá de la PC en sí. Por ejemplo, no detecta si un cable está conectado a la PC o no.

- (●) La PC puede acceder a la red. El problema existe más allá de la red local.
- ( ) La dirección IP obtenida del servidor DHCP es correcta.
- ( ) La PC puede acceder a la red. Sin embargo, es posible que el navegador web no funcione.
- ( ) La implementación TCP/IP es funcional.

2. ¿Qué comando se puede usar para probar la conectividad entre dos dispositivos mediante mensajes de solicitud de eco y respuesta de eco?

Tema 13.2.0 - **Ping** se usa para probar la conectividad entre dispositivos finales. Se puede utilizar tanto con IPv4 como con IPv6. **Ping** utiliza el protocolo ICMP que emite una solicitud de echo/respuesta de eco. Traceroute es un comando utilizado en un router. **Netstat** se utiliza para mostrar la tabla de enrutamiento local.

- ( ) to obtain a dynamic IP address from the server
- ( ) to request that gateway forward the connection request to the file server
- (●) to test that the host has the capability to reach hosts on other networks
- ( ) to resolve the domain name of the file server to its IP address

3. ¿Qué contenido de campo utiliza ICMPv6 para determinar que un paquete ha caducado?

Topic 13.1.0 - ICMPv6 envía un mensaje de Tiempo excedido si el enrutador no puede reenviar un paquete IPv6 porque el paquete expiró. El router utiliza un campo de límite de salto para determinar si el paquete ha caducado y no tiene un campo TTL.

- ○ Campo TTL
- ◉ Campo CRC
- ○ Campo Límite de salto
- ○ Campo Tiempo excedido

4. Cual protocolo Proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes?

Tema 13.1.0 - El protocolo ICMP funciona en la Capa 3 del modelo OSI, que es la capa de Internet del modelo TCP/IP. ICMP encapsula los **ping** y **traceroute** comandos.

- ○ ARP
- ○ ping
- ◉ time exceeded
- ○ destination unreachable

5. ¿Qué utilidad utiliza el Protocolo de mensajería de control de Internet?

Topic 13.1.0 - Los dispositivos de red utilizan ICMP para enviar mensajes de error.

- ○ RIP
- ○ DNS
- ◉ Ping
- ○ NTP

6. Un administrador de red puede hacer ping con éxito en el servidor en www.cisco.com, pero no puede hacer ping en el servidor Web de la compañía ubicado en un ISP de otra ciudad. ¿Qué herramienta o comando ayudaría a identificar el router específico en donde se perdió o se retrasó el paquete?

Topic 13.2.0 - El **traceroute** comando proporciona información de conectividad sobre la ruta que toma un paquete para llegar al destino y sobre cada enrutador (salto) en el camino. También indica cuánto tarda el paquete en ir del origen a cada salto y volver.

- ◉ ICMP
- ○ NDP
- ○ ARP
- ○ DHCP

7. ¿Qué protocolo utiliza IPv4 e IPv6 para proporcionar mensajes de error?

Tema 13.1.0 - ICMP es utilizado por IPv4 e IPv6 para proporcionar mensajes a ser enviados en caso de ciertos errores y con fines informativos.

- ( ) !
- (•) .
- ( ) U
- ( ) $

8. ¿Qué mensaje envía un host para comprobar la singularidad de una dirección IPv6 antes de usar esa dirección?

Tema 13.1.0 - En IPv6, la detección de direcciones duplicadas (DAD) se utiliza en lugar de ARP. Un host IPv6 realiza DAD enviando un mensaje de solicitud de vecino (NS) a su propia dirección IPv6 para garantizar la exclusividad de la dirección antes de usarla.

- [ ] solicitud de vecinos
- [ ] Solicitud de ARP
- [x] solicitud de eco
- [x] solicitud de enrutador
- [ ] the average time it takes each router in the path between source and destination to respond

9. Un técnico está solucionando problemas de una red en la que se sospecha que un nodo defectuoso en la ruta de red está causando la pérdida de paquetes. El técnico solo tiene la dirección IP del dispositivo de punto final y no tiene ningún detalle de los dispositivos intermedios. ¿Qué comando puede usar el técnico para identificar el nodo defectuoso?

Tema 13.2.0 - El **ping** comando se utiliza para verificar la conectividad a un dispositivo, los comandos **ipconfig /flushdns** harán que el adaptador vacíe la caché DNS, mientras que **ipconfig / displaydns** resultará en la visualización de la información DNS en la caché.

- ( ) The PC can access the network. The problem exists beyond the local network.
- ( ) The IP address obtained from the DHCP server is correct.
- ( ) The PC can access the Internet. However, the web browser may not work.
- (•) The TCP/IP implementation is functional.

10. Un usuario que no puede conectarse al servidor de archivos se comunica con el soporte técnico. El técnico de soporte solicita al usuario que haga ping a la dirección IP del gateway predeterminado que está configurado en la estación de trabajo. ¿Cuál es el propósito de este **ping**comando?

Topic 13.2.0 - El **ping** comando se usa para probar la conectividad entre hosts. Las otras opciones describen tareas no realizadas por **ping**. Hacer ping al gateway predeterminado prueba si el host puede establecer una conexión con otros hosts de su propia red y de otras redes.

- ( ) Obtener una dirección IP dinámica del servidor.
- ( ) Solicitar que el gateway reenvíe la solicitud de conexión al servidor de archivos.
- ( ) Probar que el host pueda establecer una conexión con otros hosts de otras redes.
- (•) Resolver el nombre de dominio del servidor de archivos a su dirección IP.

11. ¿Cuál es una función del **tracert** comando que difiere del **ping** comando cuando se usan en una estación de trabajo?

Tema 13.2.0 - El **tracert** comando envía tres pings a cada salto (router) en la ruta hacia el destino y muestra el nombre de dominio y la dirección IP de los saltos de sus respuestas. Dado que **tracert** utiliza el **ping** comando, el tiempo de viaje es el mismo que un **ping** comando independiente. La función principal de un **ping** comando independiente es probar la conectividad entre dos hosts.

- El **tracert** comando llega al destino más rápido.
- El **tracert** comando muestra la información de los enrutadores en la ruta.
- (•) El **tracert** comando envía un mensaje ICMP a cada salto de la ruta.
- El **tracert** comando se usa para probar la conectividad entre dos dispositivos.

12. ¿Qué mensaje ICMP utiliza la utilidad traceroute durante el proceso de encontrar la ruta entre dos hosts finales?

Tema 13.1.0 - Traceroute incrementa progresivamente el campo TTL (IPv4) o límite de salto (IPv6) (1, 2, 3, 4...) para enviar secuencia de comandos ping. Cuando un router detecta que el TTL o límite de salto es 0, descartará el paquete y enviará un mensaje de tiempo excedido al origen del traceroute. El mensaje devuelto contiene la dirección IP del enrutador que descartó el paquete. Por lo tanto, la utilidad traceroute aprende la dirección del enrutador. Este proceso continúa y proporciona la traza con la dirección de cada salto (enrutador) a medida que los paquetes continúan viajando a través de enrutadores para llegar al destino.

- redireccionamiento
- BOOTP
- Tiempo superado
- (•) destino inalcanzable

13. ¿Qué dos cosas se pueden determinar usando el **ping** comando? Elija dos opciones.

Topic 13.2.0 - Un comando **ping** proporciona comentarios sobre el tiempo transcurrido entre el momento en que se envió una solicitud de eco a un host remoto y el momento en que se recibió la respuesta de eco. Esto puede ser una medida del rendimiento de la red. Un éxito **ping** también indica que se pudo acceder al host de destino a través de la red.

- La cantidad de routers entre el dispositivo de origen y el de destino
- La dirección IP del router más cercano al dispositivo de destino
- El tiempo promedio que tarda un paquete en llegar al destino y que tarda la respuesta en regresar al origen
- (•) Si hay posibilidad de conexión al dispositivo de destino por medio de la red

14. ¿Qué enunciado describe una característica de la utilidad traceroute?

Tema 13.2.0 - Traceroute es una utilidad que genera una lista de saltos (o enrutadores) a lo largo de la ruta desde un host de origen al host de destino.

- (•) Envía cuatro mensajes de solicitud de eco.
- Utiliza los mensajes ICMP Source Quench.
- Se utiliza principalmente para probar la conectividad entre dos hosts.
- Identifica los enrutadores en la ruta de acceso desde un host de origen a un host de destino.

15. What characterizes a traceroute utility?

Topic 13.2.0 - Traceroute is a utility that generates a list of hops (or routers) along the path from a source host to the destination host.

- It sends four Echo Request messages.
- It utilizes the ICMP Route Redirection messages.
- It is primarily used to test connectivity between two hosts.
- (•) It identifies the routers in the path from a source host to a destination host.

1. A technician is troubleshooting a network where it is suspected that a defective node in the network path is causing packets to be dropped. The technician only has the IP address of the end point device and does not have any details of the intermediate devices. What command can the technician use to identify the faulty node?

Topic 13.2.0 - The **ping** command is used to verify connectivity to a device,the commands **ipconfig /flushdns** will cause the adapter to flush the DNS cache, while **ipconfig /****displaydns** will result in the display of the DNS information in the cache.

- (•) **tracert**
- **ping**
- **ipconfig /flushdns**
- **ipconfig /displaydns**

2. A user who is unable to connect to the file server contacts the help desk. The helpdesk technician asks the user to ping the IP address of the default gateway that is configured on the workstation. What is the purpose for this **ping** command?

Topic 13.2.0 - The **ping** command is used to test connectivity between hosts. The other options describe tasks not performed by **ping**. Pinging the default gateway will test whether the host has the capability to reach hosts on its own network and on other networks.

- to obtain a dynamic IP address from the server
- to request that gateway forward the connection request to the file server
- (•) to test that the host has the capability to reach hosts on other networks
- to resolve the domain name of the file server to its IP address

3. What is a function of the **tracert** command that differs from the **ping** command when they are used on a workstation?

Topic 13.2.0 - The **tracert** command sends three pings to each hop (router) in the path toward the destination and displays the domain name and IP address of hops from their responses. Because **tracert** uses the **ping** command, the travel time is the same as a standalone **ping** command. The primary function of a standalone **ping** command is to test the connectivity between two hosts.

- ○ The **tracert** command reaches the destination faster.
- ◉ The **tracert** command shows the information of routers in the path.
- ○ The **tracert** command sends one ICMP message to each hop in the path.
- ○ The **tracert** command is used to test the connectivity between two devices.

4. Which ICMP message is used by the traceroute utility during the process of finding the path between two end hosts?

Topic 13.1.0 - Traceroute progressively increments the TTL (IPv4) or hop limit (IPv6) field (1, 2, 3, 4...) for sending sequence of ping commands. When a router senses that the TTL or hop limit is 0, it will discard the packet and send a time exceeded message to the source of the traceroute. The returned message contains the IP address of the router that discarded the packet. Hence the traceroute utility learns the address of the router. This process continues and provides the trace with the address of each hop (router) as the packets continue traveling through routers to reach the destination.

- ○ redirect
- ○ ping
- ◉ time exceeded
- ○ destination unreachable

5. Which utility uses the Internet Control Messaging Protocol (ICMP)?

Topic 13.1.0 - ICMP is used by network devices to send error messages.

- ○ RIP
- ○ DNS
- ◉ ping
- ○ NTP

6. Which protocol is used by IPv4 and IPv6 to provide error messaging?

Topic 13.1.0 - ICMP is used by IPv4 and IPv6 to provide for messages to be sent in the event of certain errors and for informational purposes.

- (●) ICMP
- ( ) NDP
- ( ) ARP
- ( ) DHCP

7. A network administrator is testing network connectivity by issuing the **ping** command on a router. Which symbol will be displayed to indicate that a time expired during the wait for an ICMP echo reply message?

Topic 13.2.0 - When the **ping** command is issued on a router, the most common indicators are as follows:
- **!** - indicates receipt of an ICMP echo reply message
- **.** - indicates a time expired while waiting for an ICMP echo reply message
- **U** - an ICMP message of unreachability was received

- ( ) !
- (●) .
- ( ) U
- ( ) $

8. Which two things can be determined by using the **ping** command? (Choose two.)

Topic 13.2.0 - A **ping** command provides feedback on the time between when an echo request was sent to a remote host and when the echo reply was received. This can be a measure of network performance. A successful **ping** also indicates that the destination host was reachable through the network.

- [ ] the number of routers between the source and destination device
- [ ] the IP address of the router nearest the destination device
- [x] the average time it takes a packet to reach the destination and for the response to return to the source
- [x] the destination device is reachable through the network
- [ ] the average time it takes each router in the path between source and destination to respond

9. A user calls to report that a PC cannot access the internet. The network technician asks the user to issue the command **ping 127.0.0.1** in a command prompt window. The user reports that the result is four positive replies. What conclusion can be drawn based on this connectivity test?

Topic 13.2.0 - The **ping 127.0.0.1** command is used to verify that the TCP/IP stack is functional. It verifies the proper operation of the protocol stack from the network layer to physical layer, without sending a signal on the media. That is, this test does not go beyond the PC itself. For example, it does not detect whether a cable is connected to the PC or not.

- ○ The PC can access the network. The problem exists beyond the local network.
- ○ The IP address obtained from the DHCP server is correct.
- ○ The PC can access the Internet. However, the web browser may not work.
- ◉ The TCP/IP implementation is functional.

10. Which command can be used to test connectivity between two devices using echo request and echo reply messages?

Topic 13.2.0 - **Ping** is used to test connectivity between end devices. It can be used with both IPv4 and IPv6. **Ping** uses the ICMP protocol which issues an echo request/echo reply. The **ipconfig** command is used at the command line of a Windows computer to display IP addressing information. **Netstat** is used to display the local routing table.

- ○ **netstat**
- ○ **ipconfig**
- ○ **ICMP**
- ◉ **ping**

11. What field content is used by ICMPv6 to determine that a packet has expired?

Topic 13.1.0 - ICMPv6 sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet expired. The router uses a hop limit field to determine if the packet has expired, and does not have a TTL field.

- ○ TTL field
- ○ CRC field
- ◉ Hop Limit field
- ○ Time Exceeded field

12. Which protocol provides feedback from the destination host to the source host about errors in packet delivery?

Topic 13.1.0 - The ICMP protocol operates at Layer 3 of the OSI model, which is the Internet layer of the TCP/IP model. ICMP encapsulates the **ping** and **traceroute** commands.

- ARP
- BOOTP
- DNS
- ICMP

13. A network administrator can successfully ping the server at www.cisco.com, but cannot ping the company web server located at an ISP in another city. Which tool or command would help identify the specific router where the packet was lost or delayed?

Topic 13.2.0 - The **traceroute** command provides connectivity information about the path a packet takes to reach the destination and about every router (hop) along the way. It also indicates how long a packet takes to get from the source to each hop and back.

- **ipconfig**
- **netstat**
- **telnet**
- **traceroute**

14. What message is sent by a host to check the uniqueness of an IPv6 address before using that address?

Topic 13.1.0 - In IPv6, Duplicate Address Detection (DAD) is used in place of ARP. An IPv6 host performs DAD by sending a neighbor solicitation (NS) message to its own IPv6 address to ensure the uniqueness of the address prior to using it.

- neighbor solicitation
- ARP request
- echo request
- router solicitation

15. What characterizes a traceroute utility?

Topic 13.2.0 - Traceroute is a utility that generates a list of hops (or routers) along the path from a source host to the destination host.

- It sends four Echo Request messages.
- It utilizes the ICMP Route Redirection messages.
- It is primarily used to test connectivity between two hosts.
- It identifies the routers in the path from a source host to a destination host.

Capítulo 14_Capa de transporte

Introducción

14.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Capa de transporte!

La capa de transporte es donde, como su nombre indica, los datos se transportan de un host a otro. ¡Aquí es donde su red realmente se mueve! La capa de transporte utiliza dos protocolos: TCP y UDP. Piense en TCP como obtener una carta registrada en el correo. Tienes que firmarlo antes de que el transportista de correo te lo permita. Esto ralentiza un poco el proceso, pero el remitente sabe con certeza que recibió la carta y cuándo la recibió. UDP es más como una carta regular y sellada. Llega a tu buzón de correo y, si lo hace, probablemente esté destinado a ti, pero en realidad podría ser para alguien más que no vive allí. Además, es posible que no llegue a su buzón de correo en absoluto. El remitente no puede estar seguro de que lo recibió. Sin embargo, hay momentos en que UDP, como una carta estampada, es el protocolo que se necesita. En este tema se profundiza en cómo funcionan TCP y UDP en la capa de transporte. Más adelante en este módulo hay varios videos para ayudarle a entender estos procesos.

14.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Capa de transporte

Objetivos del módulo: Compare el funcionamiento de los protocolos de capa de transporte en la admisión de la comunicación de extremo a extremo.

Título del tema	Objetivo del tema
Transporte de datos	Explique el propósito de la capa de transporte en la administración del transporte de datos en comunicación de extremo a extremo.
Descripción general de TCP	Explicar las características de TCP.
Visión general de UDP	Explicar las características de UDP.
Números de puerto	Explique cómo TCP y UDP usan los números de puerto.

Título del tema	Objetivo del tema
Proceso de comunicación TCP	Explicar las características de TCP. facilitar una comunicación fiable.
Confiabilidad y control de flujo	Explicar cómo se transmiten y reconocen las unidades de datos del protocolo TCP a Entrega garantizada.
Comunicación UDP	Compare las operaciones de los protocolos de la capa de transporte en el soporte comunicación de extremo a extremo.

Capa de transporte / Transporte de datos

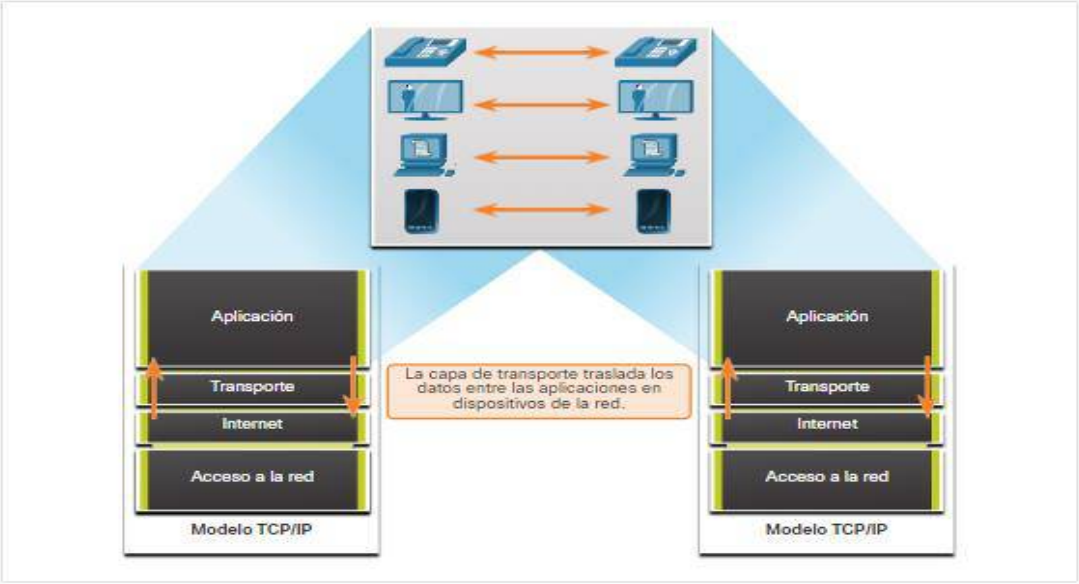
Transporte de datos

14.1.1

Función de la capa de transporte

Los programas de capa de aplicación generan datos que deben intercambiarse entre los hosts de origen y de destino. La capa de transporte es responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts. Esto puede incluir servicios como el establecimiento de una sesión temporal entre dos hosts y la transmisión fiable de información para una aplicación.

Como se muestra en la ilustración, la capa de transporte es el enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión a través de la red.



Muestra un diagrama de cómo los dispositivos utilizan la capa de transporte para mover datos entre aplicaciones en el modelo TCP/IP.

La capa de transporte no tiene conocimiento del tipo de host de destino, el tipo de medio por el que deben viajar los datos, la ruta tomada por los datos, la congestión en un enlace o el tamaño de la red.

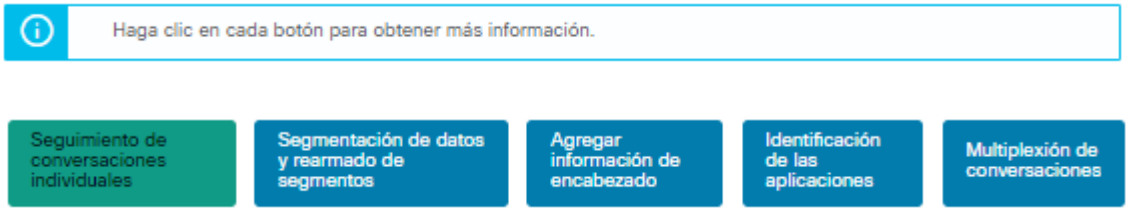
La capa de transporte incluye dos protocolos:

- Protocolo de control de transmisión (TCP)
- Protocolo de datagramas de usuario (UDP)

14.1.2

Tareas de la capa de transporte

La capa de transporte tiene muchas responsabilidades.

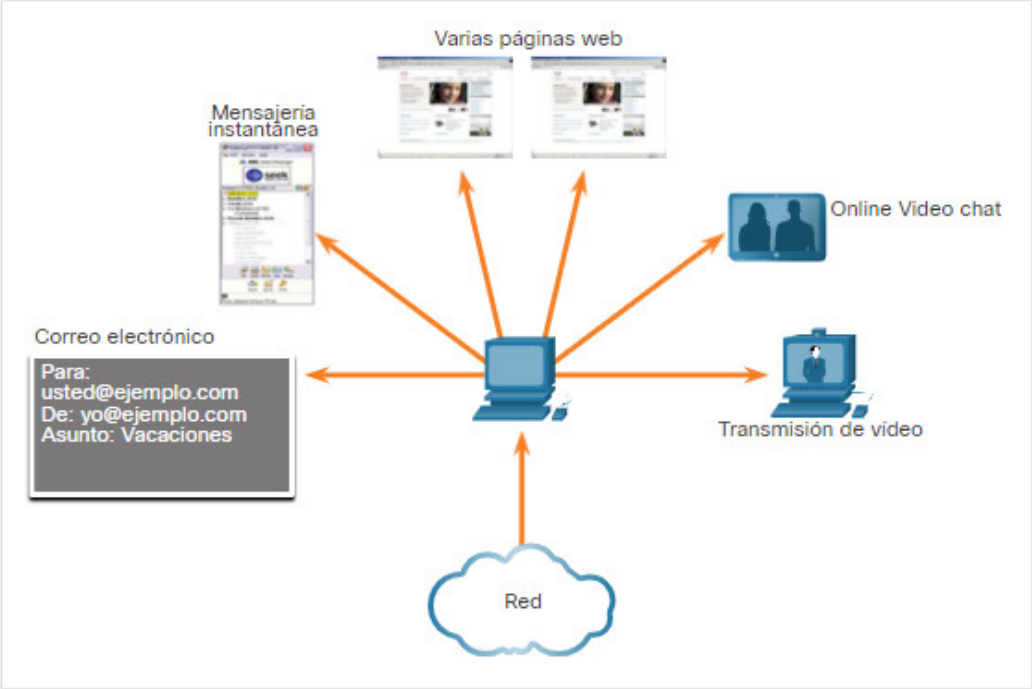


Seguimiento de conversaciones individuales

En la capa de transporte, cada conjunto de datos que fluye entre una aplicación de origen y una aplicación de destino se conoce como una conversación y se rastrea por separado. Es responsabilidad de la capa de transporte mantener y hacer un seguimiento de todas estas conversaciones.

Como se ilustra en la figura, un host puede tener múltiples aplicaciones que se comunican a través de la red simultáneamente.

La mayoría de las redes tienen un límite de la cantidad de datos que se puede incluir en un solo paquete. Por lo tanto, los datos deben dividirse en piezas manejables.

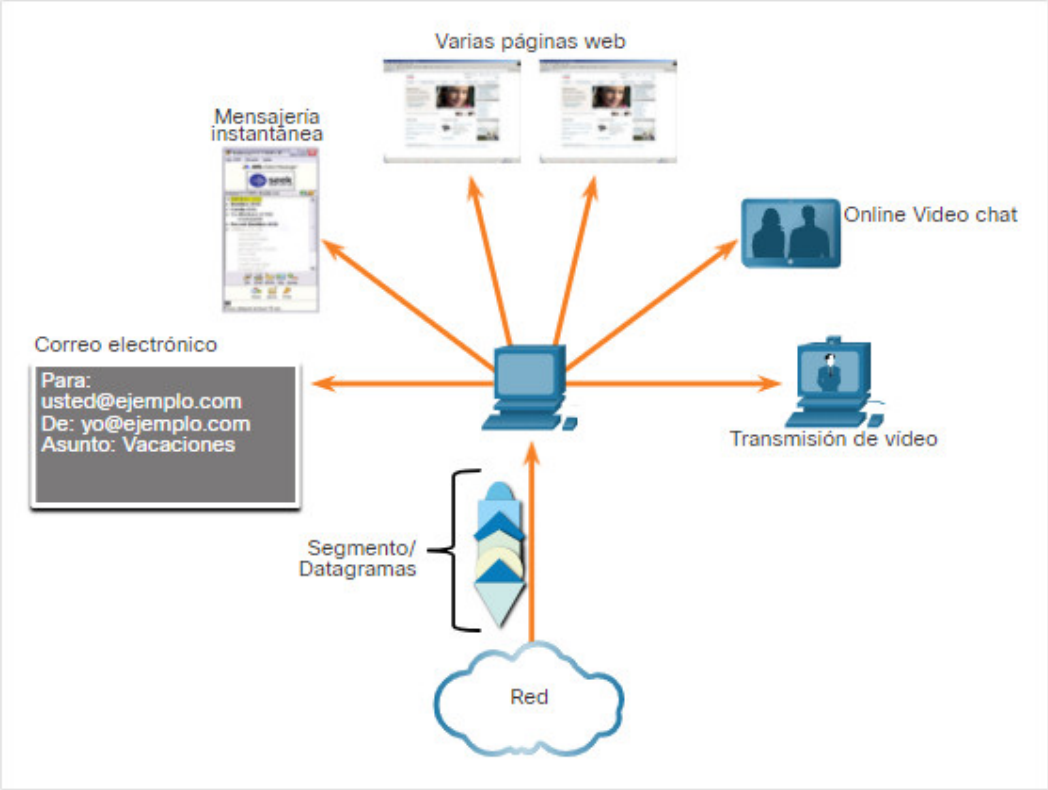


El PC ejecuta simultáneamente varias aplicaciones de red, incluyendo un cliente de correo electrónico, cliente de mensajería instantánea, páginas web del navegador web, streaming de vídeo y un cliente de videoconferencia.

Segmentación de datos y rearmado de segmentos

Es responsabilidad de la capa de transporte dividir los datos de la aplicación en bloques de tamaño adecuado. Dependiendo del protocolo de capa de transporte utilizado, los bloques de capa de transporte se denominan segmentos o datagramas. La figura ilustra la capa de transporte utilizando diferentes bloques para cada conversación.

La capa de transporte divide los datos en bloques más pequeños (es decir, segmentos o datagramas) que son más fáciles de administrar y transportar.



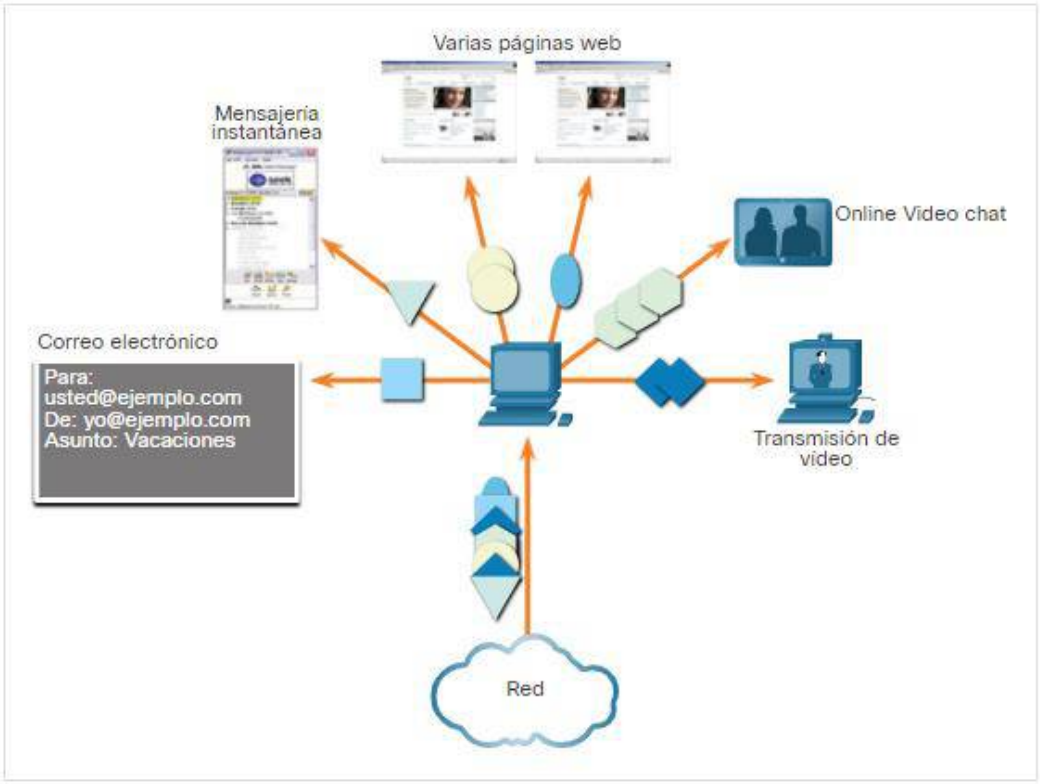
Seguimiento de conversaciones individuales | Segmentación de datos y rearmado de segmentos | **Agregar información de encabezado** | Identificación de las aplicaciones | Multiplexión de conversaciones

Agregar información de encabezado

El protocolo de capa de transporte también agrega información de encabezado que contiene datos binarios organizados en varios campos a cada bloque de datos. Los valores de estos campos permiten que los distintos protocolos de la capa de transporte lleven a cabo variadas funciones de administración de la comunicación de datos.

Por ejemplo, el host receptor utiliza la información de encabezado para volver a ensamblar los bloques de datos en un flujo de datos completo para el programa de capa de aplicación de recepción.

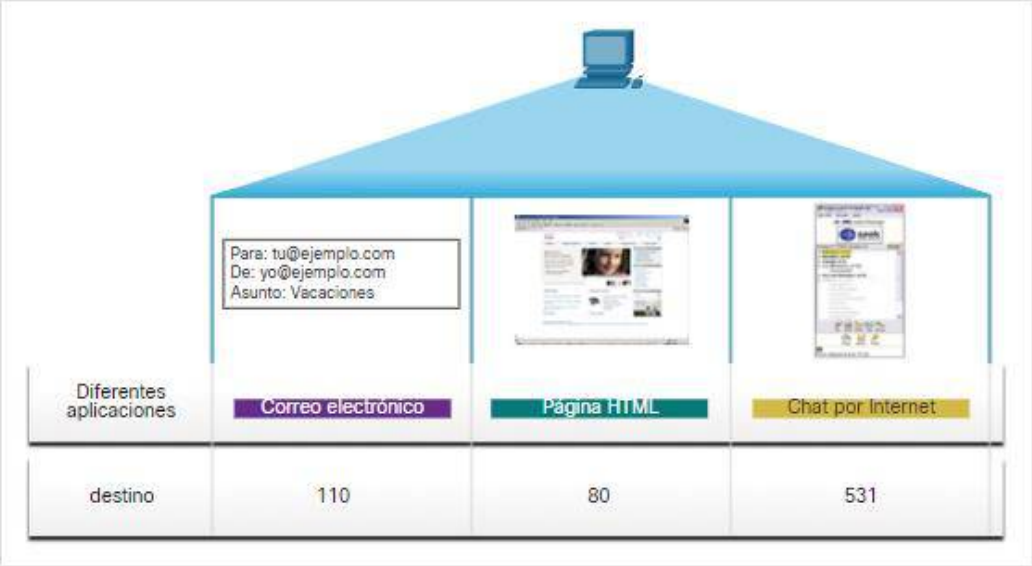
La capa de transporte garantiza que incluso con múltiples aplicaciones que se ejecutan en un dispositivo, todas las aplicaciones reciben los datos correctos.

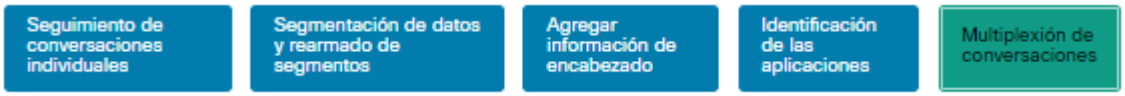


Seguimiento de conversaciones individuales | Segmentación de datos y rearmado de segmentos | Agregar información de encabezado | Identificación de las aplicaciones | Multiplexión de conversaciones

Identificación de las aplicaciones

La capa de transporte debe poder separar y administrar varias comunicaciones con diferentes necesidades de requisitos de transporte. Para pasar flujos de datos a las aplicaciones adecuadas, la capa de transporte identifica la aplicación de destino utilizando un identificador llamado número de puerto. Como se ilustra en la figura, a cada proceso de software que necesita acceder a la red se le asigna un número de puerto único para ese host.



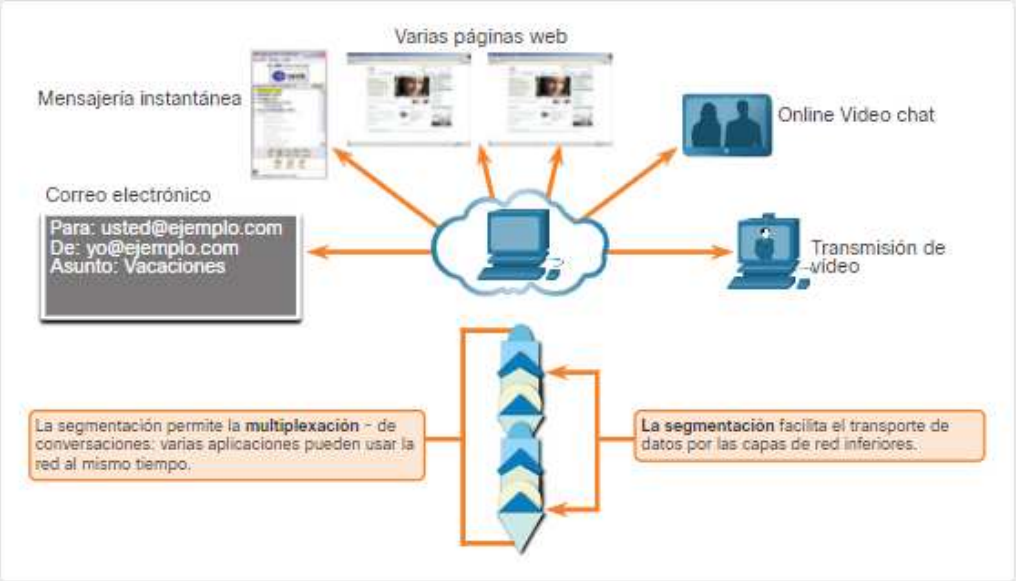


Multiplexión de conversaciones

El envío de algunos tipos de datos (por ejemplo, una transmisión de video) a través de una red, como una transmisión de comunicación completa, puede consumir todo el ancho de banda disponible. Esto evitaría que se produzcan otras conversaciones de comunicación al mismo tiempo. También podría dificultar la recuperación de errores y la retransmisión de datos dañados.

Como se muestra en la figura, la capa de transporte utiliza segmentación y multiplexación para permitir que diferentes conversaciones de comunicación se intercalen en la misma red.

La verificación de errores se puede realizar en los datos del segmento, para determinar si el segmento se modificó durante la transmisión.



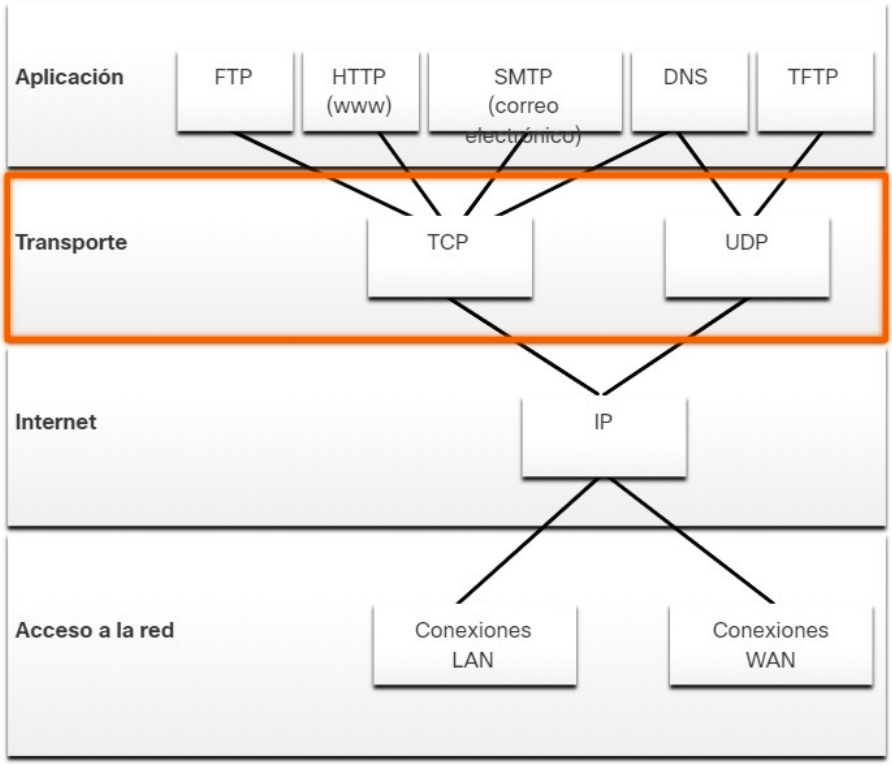
14.1.3

Protocolos de capa de transporte

IP se ocupa solo de la estructura, el direccionamiento y el routing de paquetes. IP no especifica la manera en que se lleva a cabo la entrega o el transporte de los paquetes.

Los protocolos de capa de transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de fiabilidad de una conversación. La capa de transporte incluye los protocolos TCP y UDP.

Las diferentes aplicaciones tienen diferentes requisitos de confiabilidad de transporte. Por lo tanto, TCP/IP proporciona dos protocolos de capa de transporte, como se muestra en la figura.



Muestra cómo los protocolos de capa de aplicación como FTP, HTTP, SMTP utilizan TCP en la capa de transporte y DNS y TFTP utilizan UDP. Cómo todos usan IP en la capa de Internet independientemente de si se conectan a una LAN o a una WAN en la capa de acceso a la red.

14.1.4

Protocolo de control de transmisión (TCP)

IP solo se refiere a la estructura, direccionamiento y enrutamiento de paquetes, desde el remitente original hasta el destino final. IP no es responsable de garantizar la entrega o determinar si es necesario establecer una conexión entre el remitente y el receptor.

El TCP se considera un protocolo de la capa de transporte confiable y completo, que garantiza que todos los datos lleguen al destino. TCP incluye campos que garantizan la entrega de los datos de la aplicación. Estos campos requieren un procesamiento adicional por parte de los hosts de envío y recepción.

Nota: TCP divide los datos en segmentos.

La función del protocolo de transporte TCP es similar al envío de paquetes de los que se hace un rastreo de origen a destino. Si se divide un pedido de envío en varios paquetes, un cliente puede verificar en línea para ver el orden de la entrega.

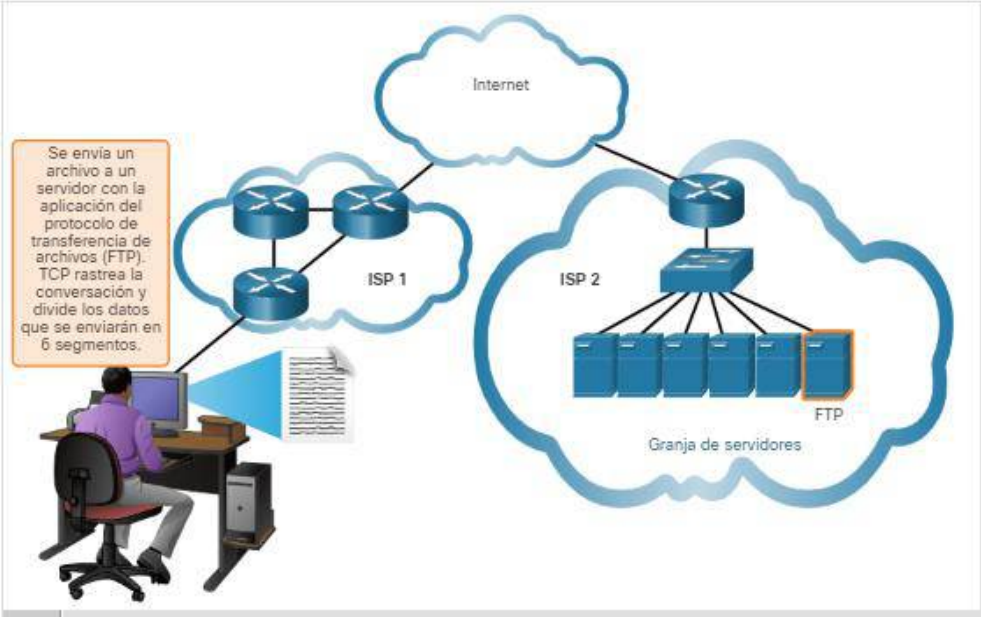
TCP proporciona confiabilidad y control de flujo mediante estas operaciones básicas:

- Numere y rastree segmentos de datos transmitidos a un host específico desde una aplicación específica
- Confirmar datos recibidos
- Vuelva a transmitir cualquier información no reconocida después de un cierto período de tiempo
- Datos de secuencia que pueden llegar en un orden incorrecto
- Enviar datos a una velocidad eficiente que sea aceptable por el receptor

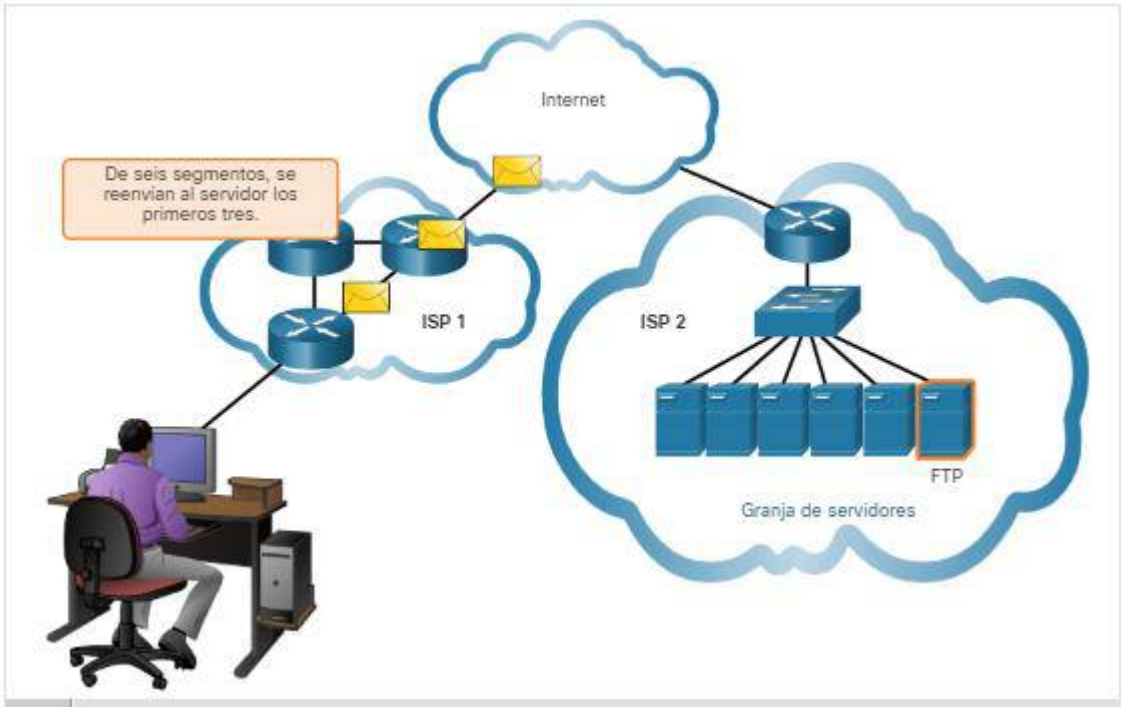
Para mantener el estado de una conversación y realizar un seguimiento de la información, TCP debe establecer primero una conexión entre el remitente y el receptor. Es por eso que TCP se conoce como un protocolo orientado a la conexión.

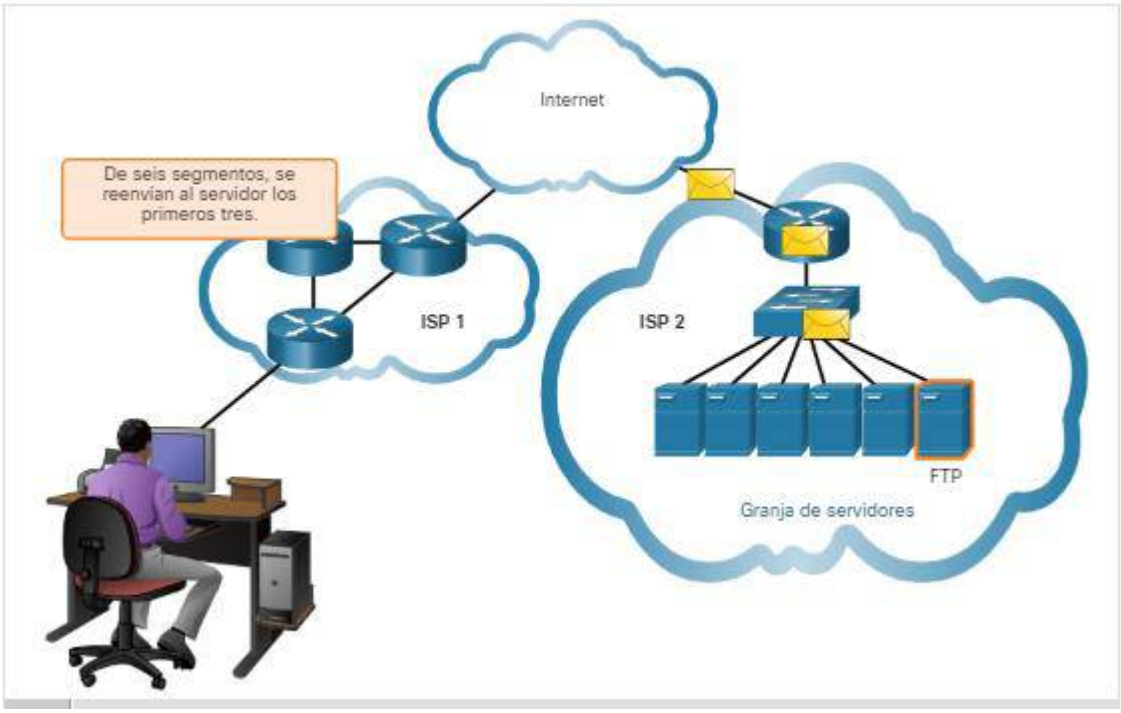
Haga clic en Reproducir en la figura para ver cómo los segmentos de TCP y los reconocimientos se transmiten entre el emisor y el receptor.

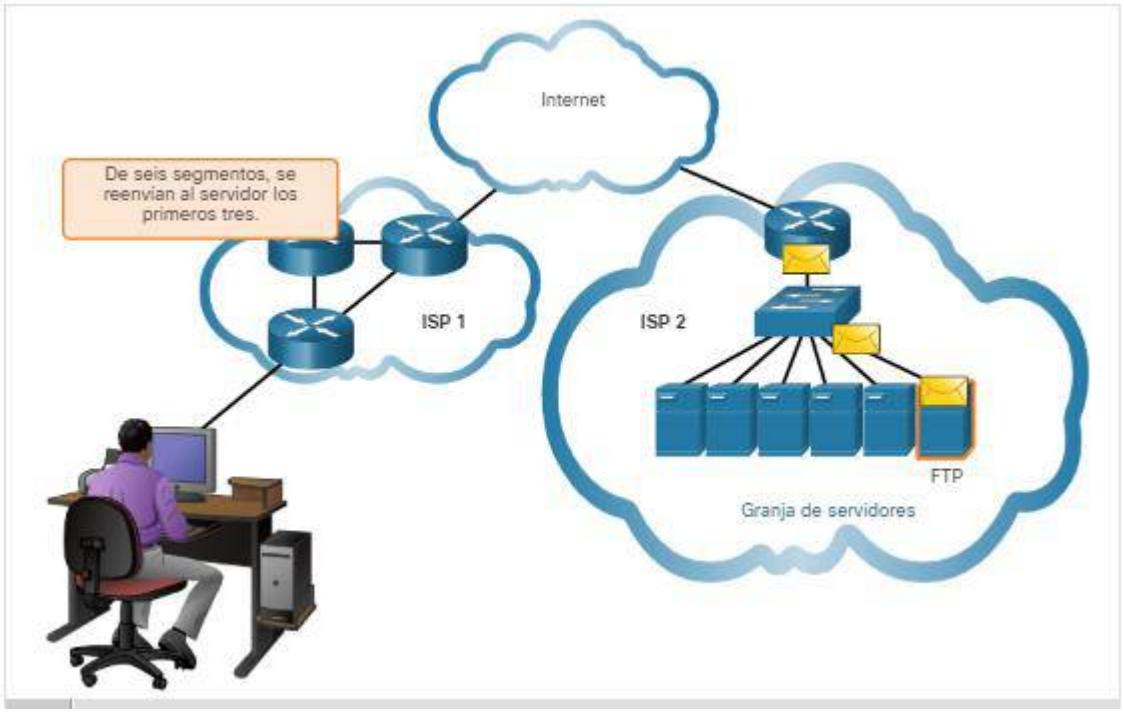
Se envía un archivo a un servidor con la aplicación del protocolo de transferencia de archivos (FTP). TCP rastrea la conversación y divide los datos que se enviarán en 6 segmentos.



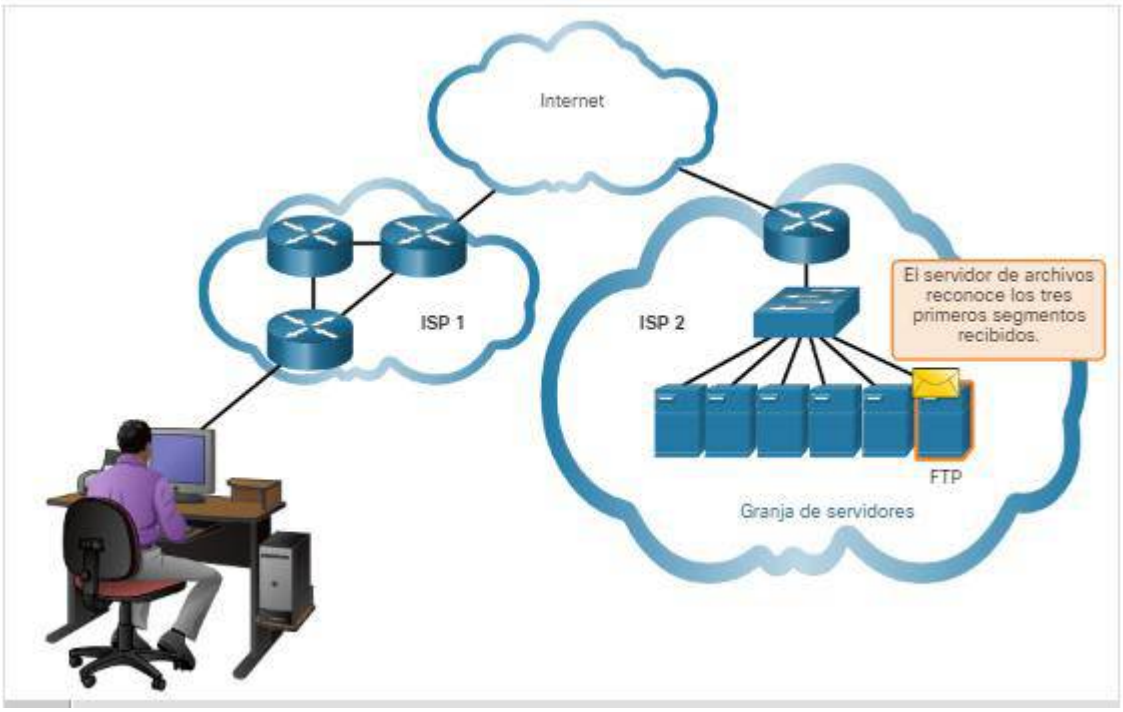
De seis segmentos, se reenvían al servidor los primeros tres.

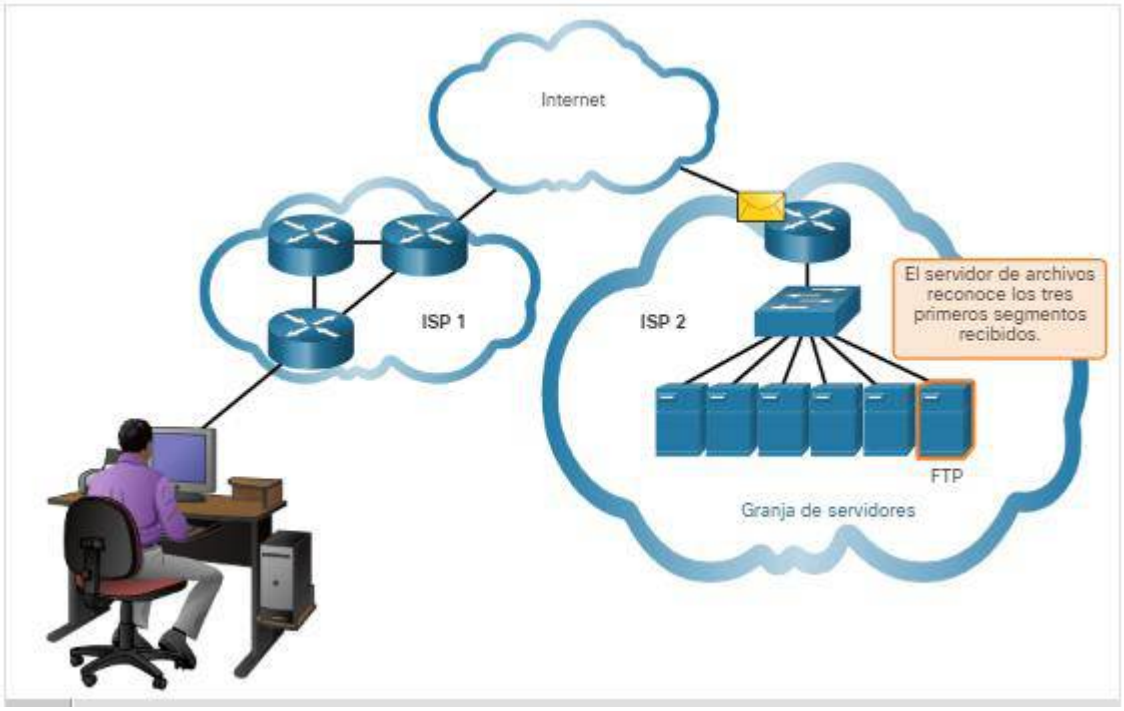

Internet
De seis segmentos, se reenvían al servidor los primeros tres.
ISP 1
ISP 2
FTP
Granja de servidores

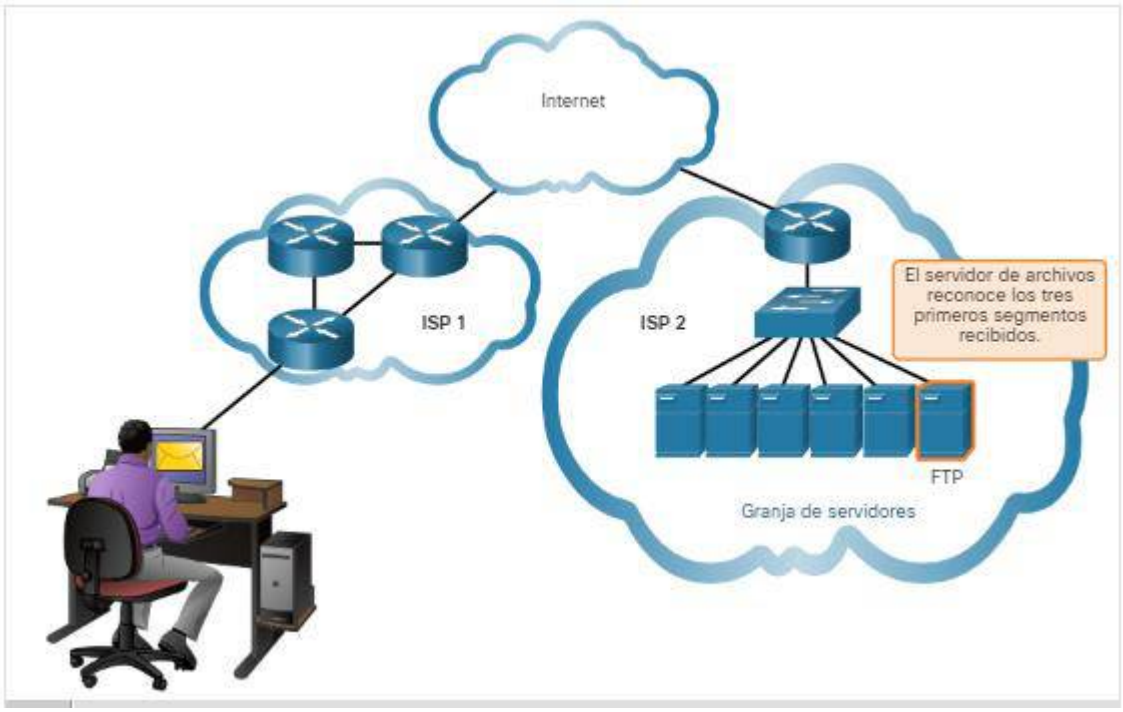

Internet
De seis segmentos, se reenvían al servidor los primeros tres.
ISP 1
ISP 2
FTP
Granja de servidores



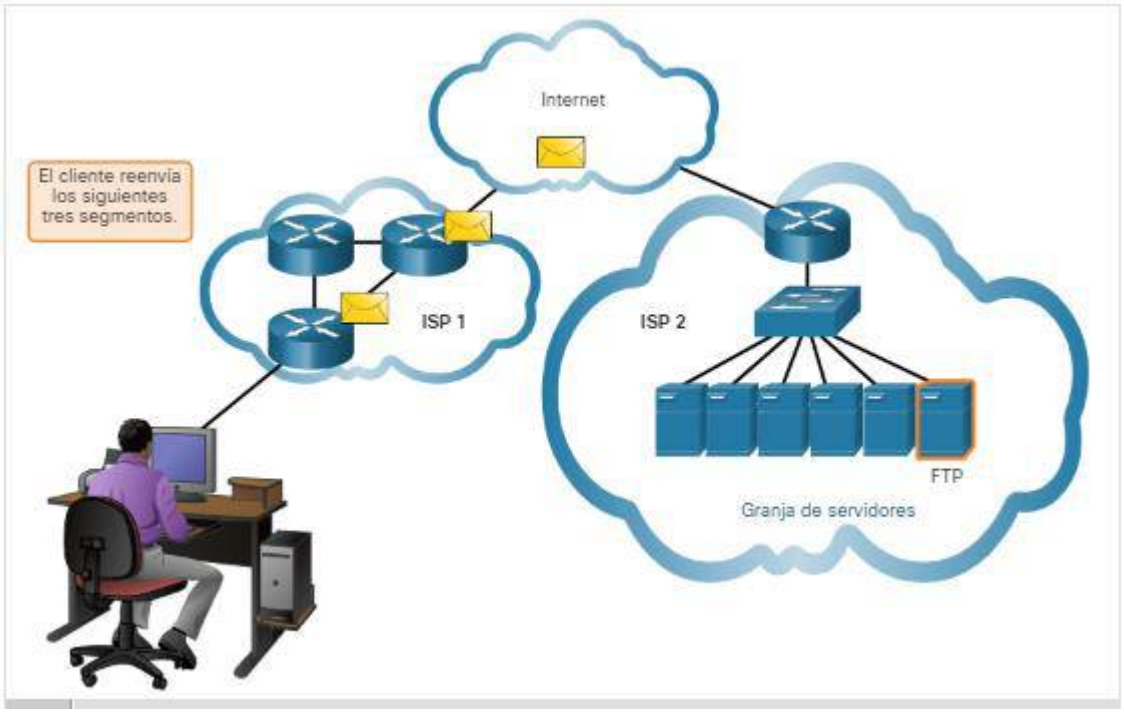
servidor de archivos reconoce los tres primeros segmentos recibidos.



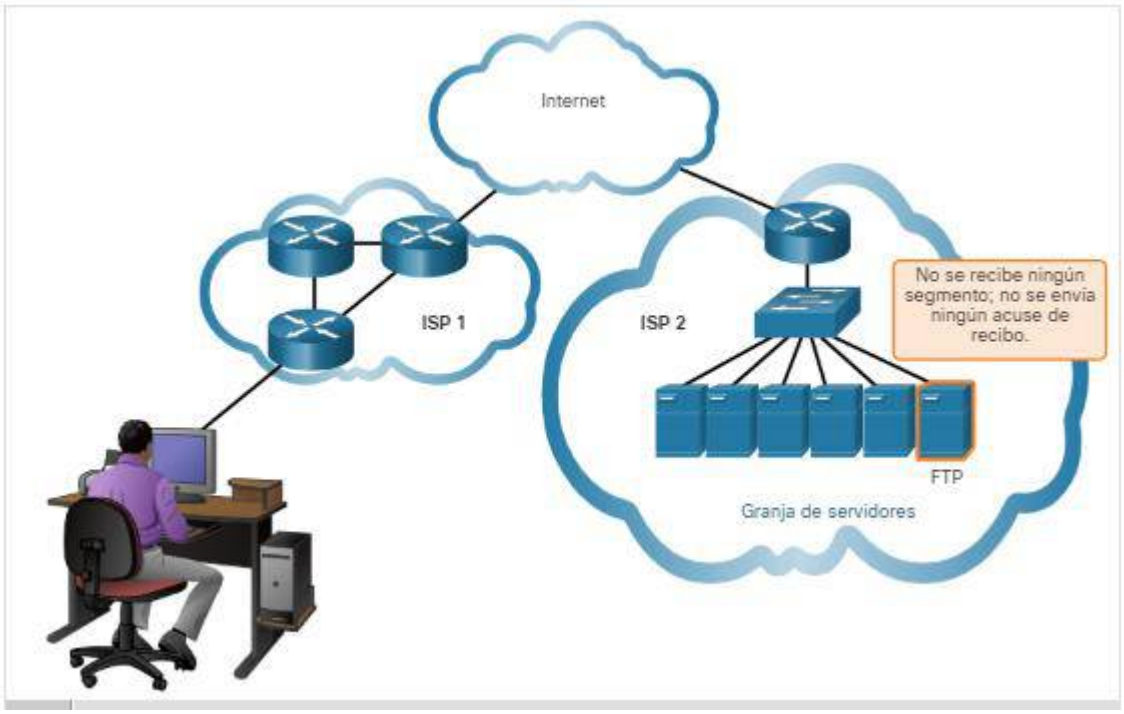




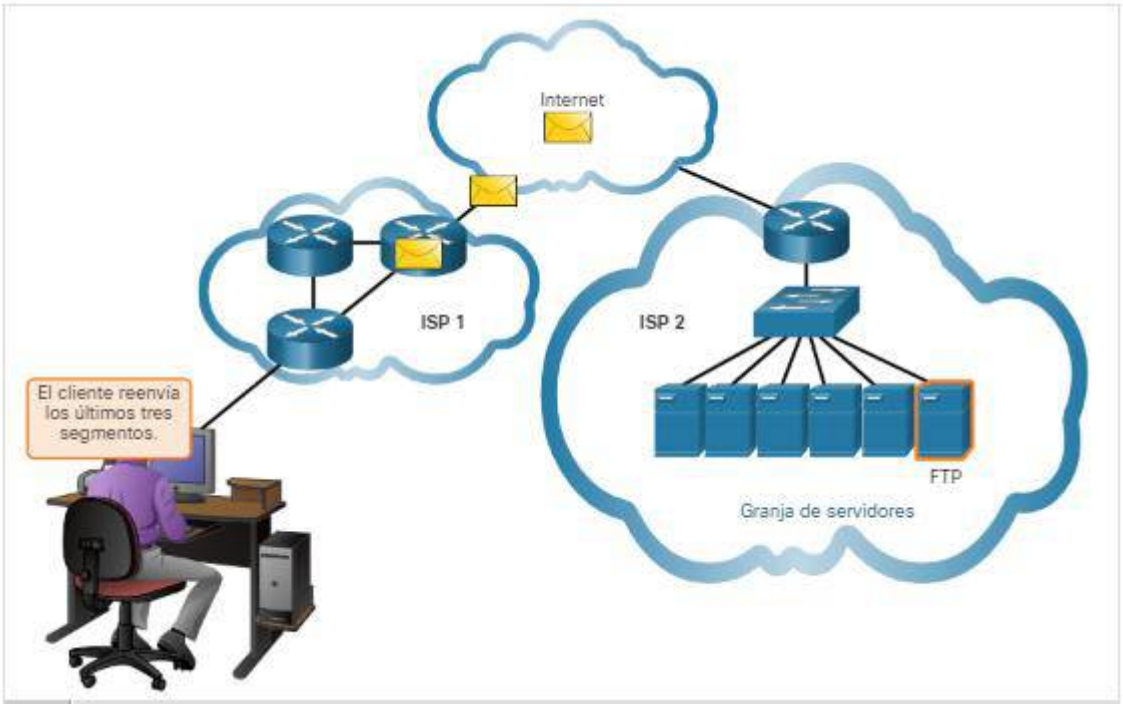
El cliente reenvía los siguientes tres segmentos.

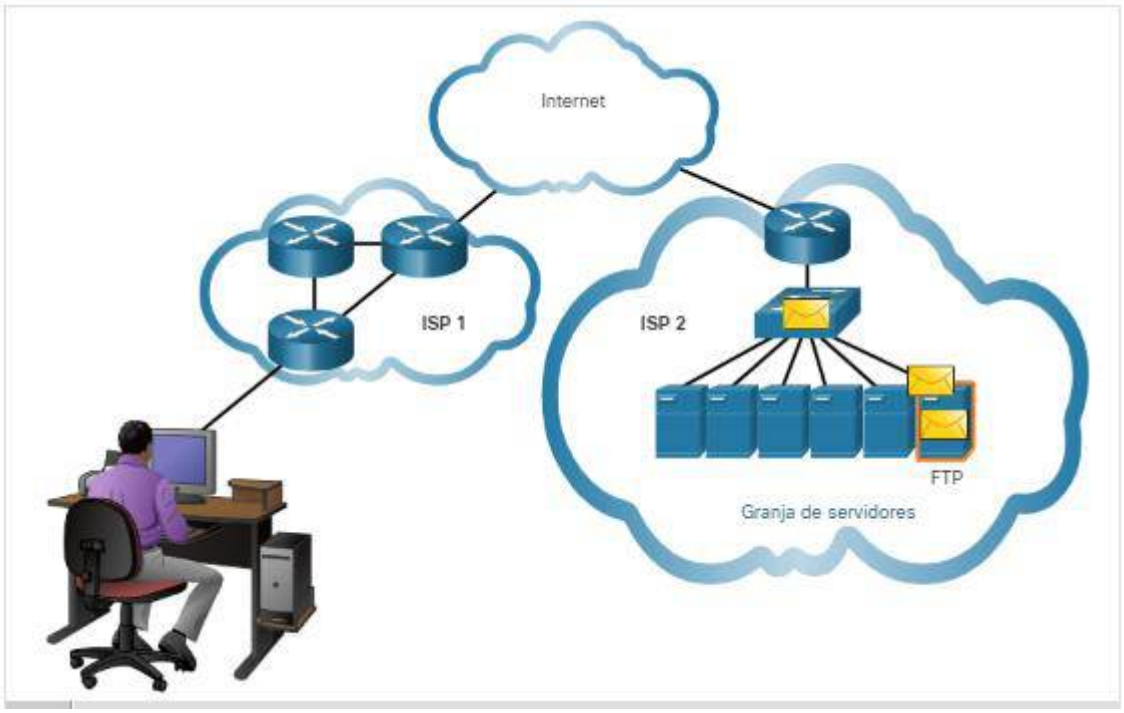


No se recibe ningún segmento; no se envía ningún acuse de recibo.

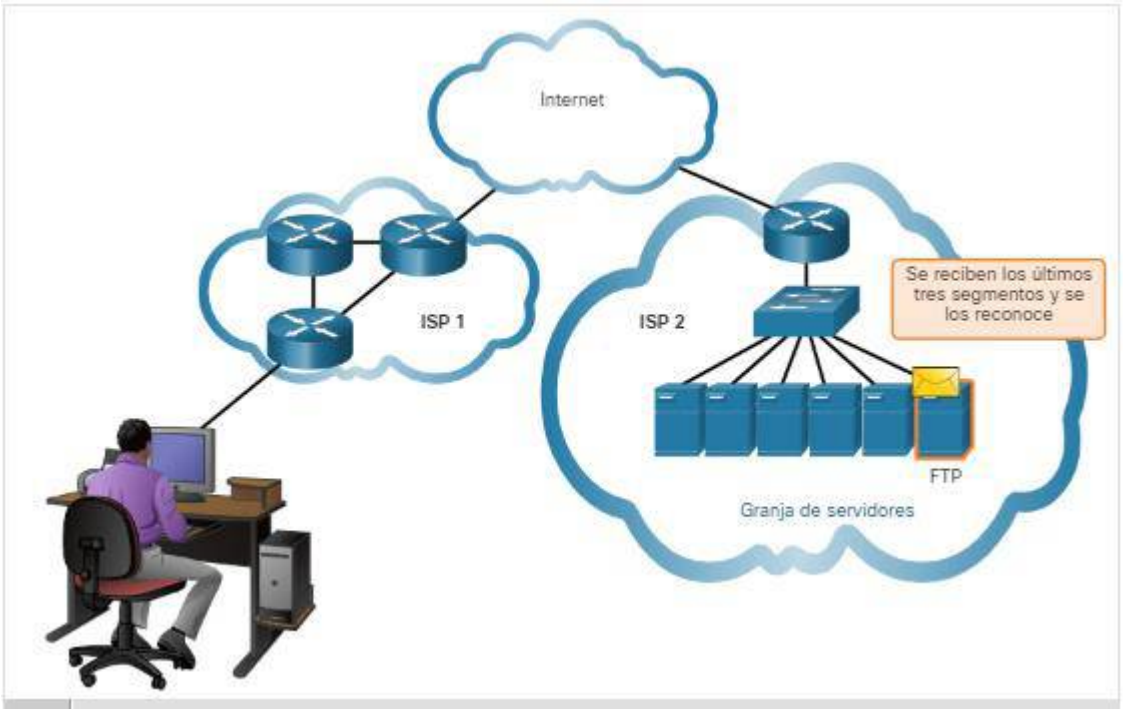


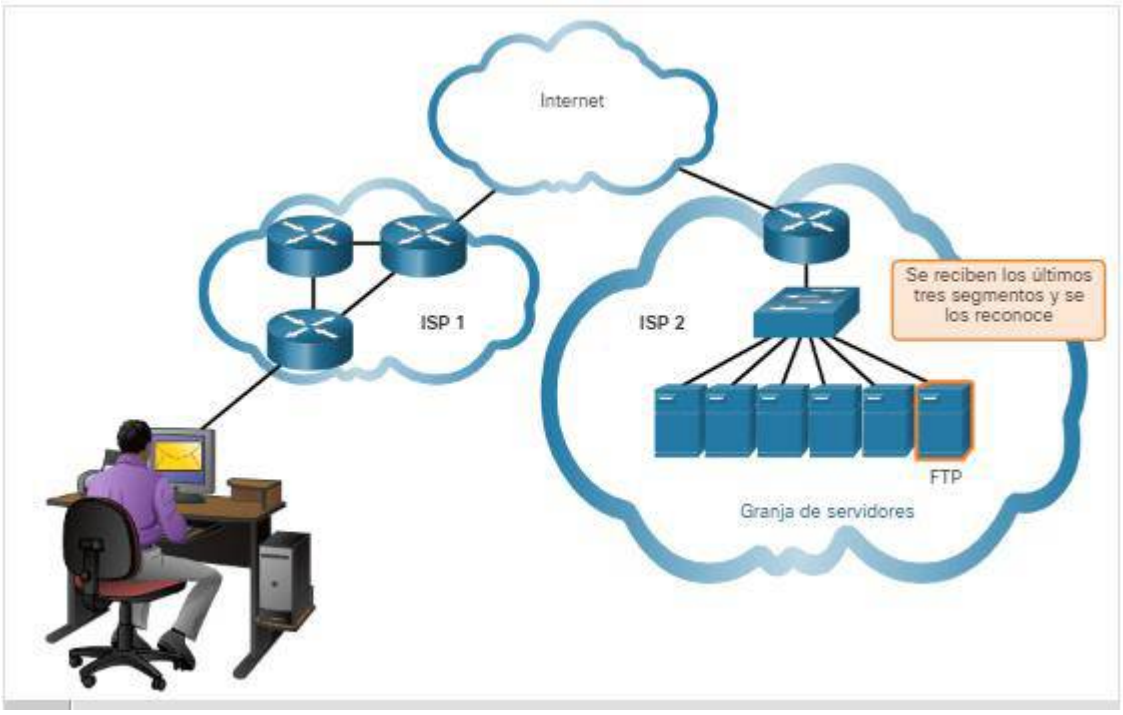
El cliente reenvía los últimos tres segmentos.





Se reciben los últimos tres segmentos y se los reconoce.





Muestra una conexión a un servidor FTP iniciada con un protocolo de enlace TCP de 3 vías y los segmentos de datos contabilizados mediante números de secuencia y confirmaciones.

14.1.5

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo de capa de transporte más simple que TCP. No proporciona confiabilidad y control de flujo, lo que significa que requiere menos campos de encabezado. Debido a que los procesos UDP remitente y receptor no tienen que administrar la confiabilidad y el control de flujo, esto significa que los datagramas UDP se pueden procesar más rápido que los segmentos TCP. El UDP proporciona las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos.

Nota: UDP divide los datos en datagramas que también se conocen como segmentos.

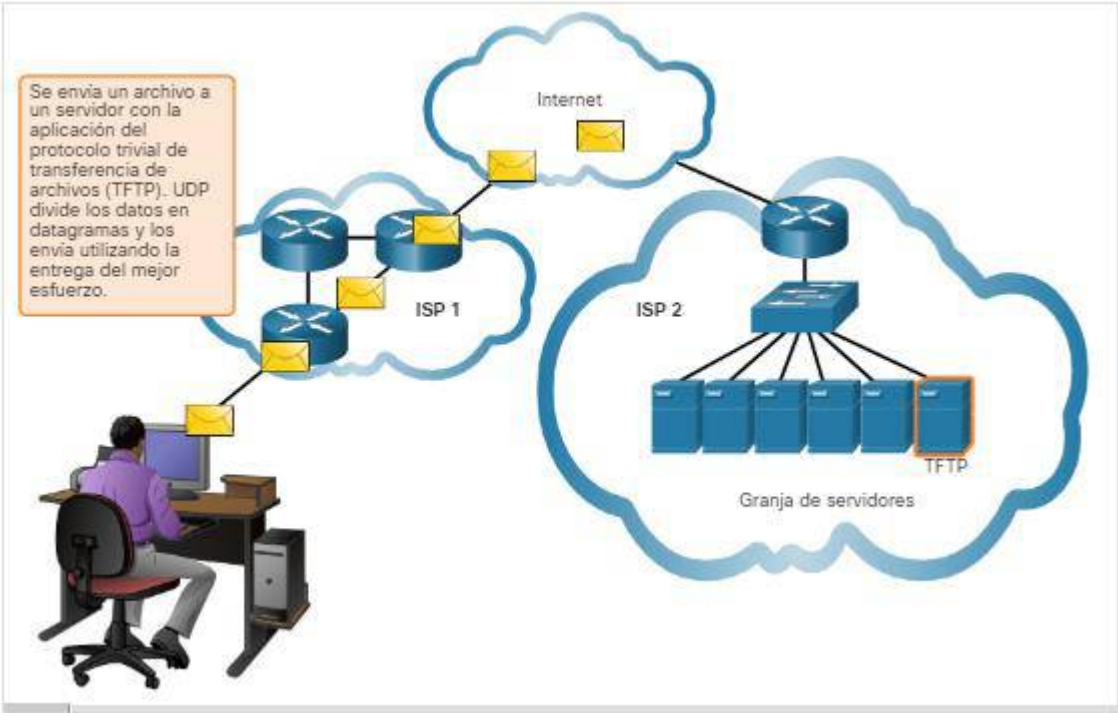
UDP es un protocolo sin conexión. Debido a que UDP no proporciona fiabilidad ni control de flujo, no requiere una conexión establecida. Debido a que UDP no realiza un seguimiento de la información enviada o recibida entre el cliente y el servidor, UDP también se conoce como protocolo sin estado.

UDP también se conoce como un protocolo de entrega de mejor esfuerzo porque no hay reconocimiento de que los datos se reciben en el destino. Con UDP, no existen procesos de capa de transporte que informen al emisor si la entrega se realizó correctamente.

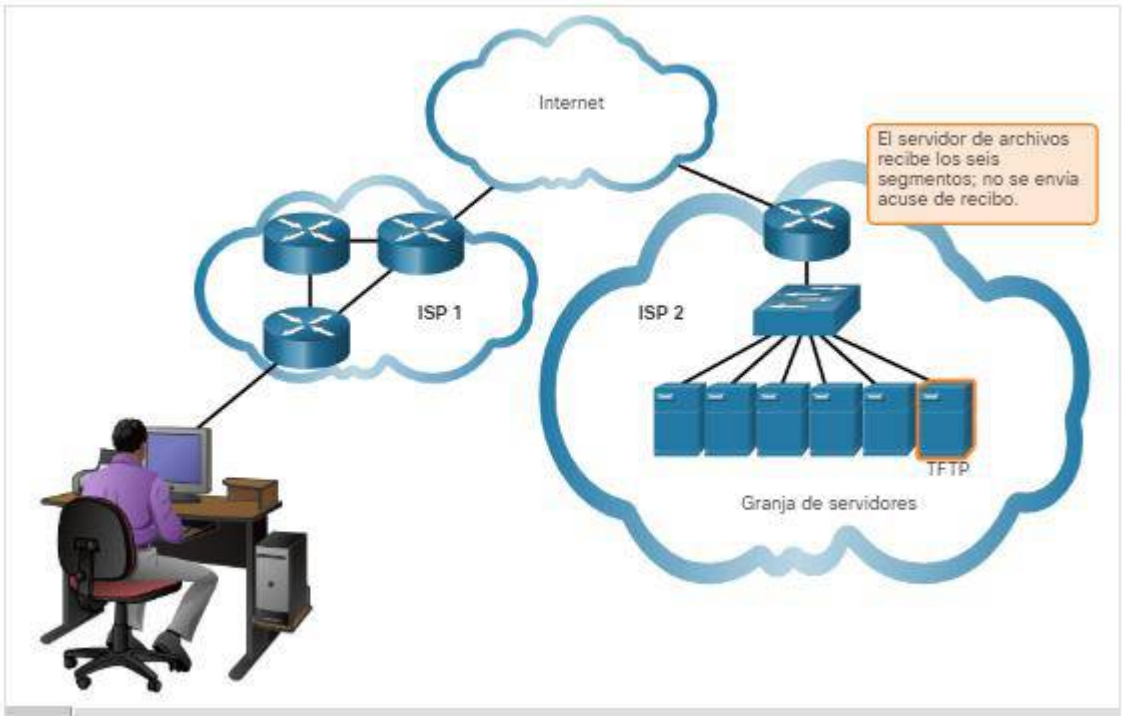
UDP es como colocar una carta regular, no registrada, en el correo. El emisor de la carta no conoce la disponibilidad del receptor para recibir la carta. Además, la oficina de correos tampoco es responsable de hacer un rastreo de la carta ni de informar al emisor si esta no llega a destino.

Haga clic en Reproducir en la figura para ver una animación de los datagramas UDP que se transmiten del remitente al receptor.

Se envía un archivo a un servidor con la aplicación del protocolo trivial de transferencia de archivos (TFTP). UDP divide los datos en datagramas y los envía utilizando la entrega del mejor esfuerzo.



El servidor de archivos recibe los seis segmentos; no se envía acuse de recibo.



Muestra una conexión a un servidor TFTP utilizando datagramas UDP que se envían sin números de secuencia o confirmaciones.

14.1.6

Protocolo de la capa de transporte correcto para la aplicación adecuada

Algunas aplicaciones pueden tolerar cierta pérdida de datos durante la transmisión a través de la red, pero los retrasos en la transmisión son inaceptables. Para estas aplicaciones, UDP es la mejor opción porque requiere menos sobrecarga de red. UDP es preferible para aplicaciones como Voz sobre IP (VoIP). Los reconocimientos y la retransmisión retrasarían la entrega y harían inaceptable la conversación de voz.

UDP también es utilizado por las aplicaciones de solicitud y respuesta donde los datos son mínimos, y la retransmisión se puede hacer rápidamente. Por ejemplo, el servicio de nombres de dominio (DNS) utiliza UDP para este tipo de transacción. El cliente solicita direcciones IPv4 e IPv6 para obtener un nombre de dominio conocido desde un servidor DNS. Si el cliente no recibe una respuesta en un período de tiempo predeterminado, simplemente envía la solicitud de nuevo.

Por ejemplo, si uno o dos segmentos de una transmisión de vídeo en vivo no llegan al destino, se interrumpe momentáneamente la transmisión. Esto puede manifestarse como distorsión en la imagen o el sonido, pero puede no ser perceptible para el usuario. Si el dispositivo de destino tuviera que dar cuenta de los datos perdidos, la transmisión se podría demorar mientras espera las retransmisiones, lo que ocasionaría que la imagen o el sonido se degraden considerablemente. En este caso, es mejor producir el mejor vídeo o audio posible con los segmentos recibidos y prescindir de la confiabilidad.

Para otras aplicaciones es importante que todos los datos lleguen y que puedan ser procesados en su secuencia adecuada. Para estos tipos de aplicaciones, TCP se utiliza como protocolo de transporte. Por ejemplo, las aplicaciones como las bases de datos, los navegadores web y los clientes de correo electrónico, requieren que todos los datos que se envían lleguen a destino en su formato original. Cualquier dato faltante podría corromper una comunicación, haciéndola incompleta o ilegible. Por ejemplo, cuando se accede a la información bancaria a través de la web, es importante asegurarse de que toda la información se envía y recibe correctamente.

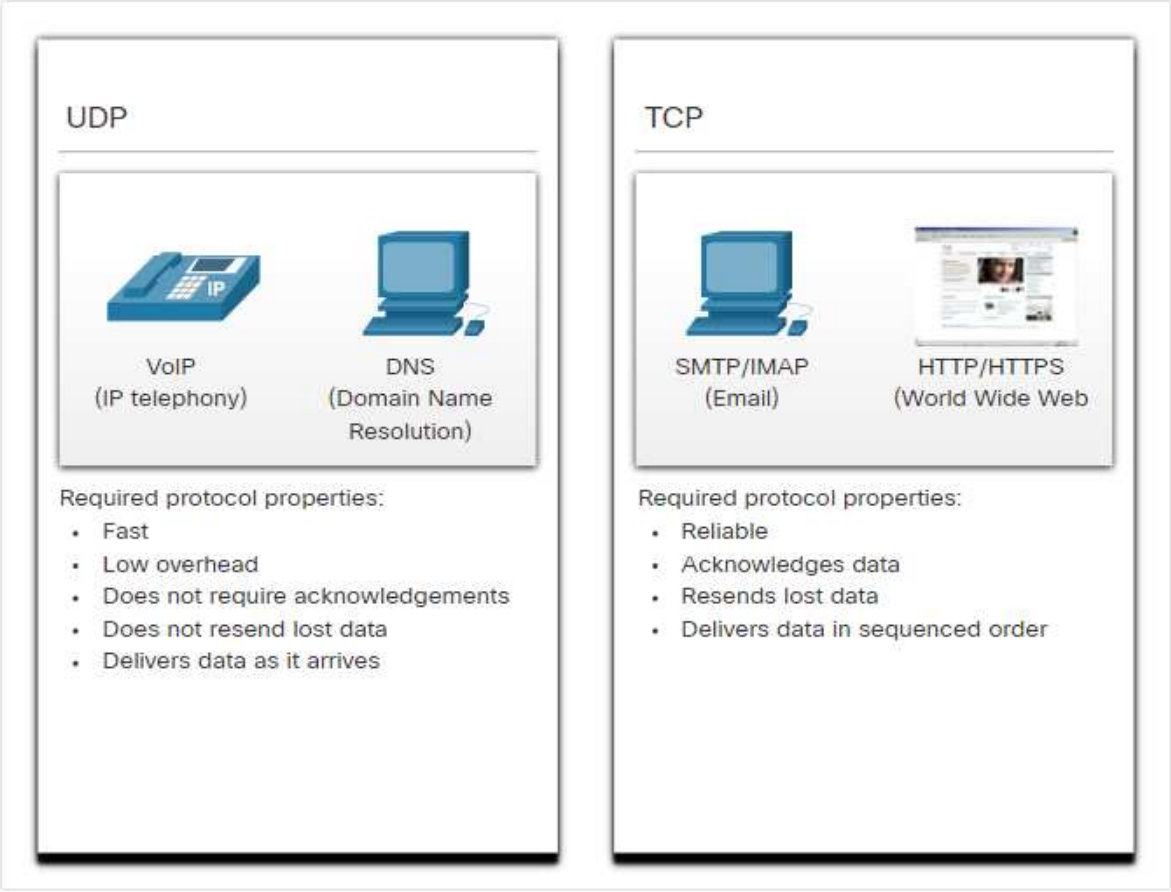
Los desarrolladores de aplicaciones deben elegir qué tipo de protocolo de transporte es adecuado según los requisitos de las aplicaciones. El vídeo puede enviarse a través de TCP o UDP. Las aplicaciones que transmiten audio y video almacenado generalmente usan TCP. La aplicación utiliza TCP para realizar buffering, sondeo de ancho de banda y control de congestión, con el fin de controlar mejor la experiencia del usuario.

El vídeo y la voz en tiempo real generalmente usan UDP, pero también pueden usar TCP, o tanto UDP como TCP. Una aplicación de videoconferencia puede usar UDP de forma

predeterminada, pero debido a que muchos firewalls bloquean UDP, la aplicación también se puede enviar a través de TCP.

Las aplicaciones que transmiten audio y video almacenado usan TCP. Por ejemplo, si de repente la red no puede admitir el ancho de banda necesario para ver una película a pedido, la aplicación detiene la reproducción. Durante la pausa, es posible que vea un mensaje de "almacenando en búfer..." mientras TCP intenta restablecer la transmisión. Cuando todos los segmentos están en orden y se restaura un nivel mínimo de ancho de banda, se reanuda la sesión TCP y se reanuda la reproducción de la película.

La figura resume las diferencias entre UDP y TCP.



Enumera las diferencias entre UDP: sobrecarga rápida, baja, sin confirmaciones, sin reenvío y TCP: confiable, reconoce datos, reenvía datos perdidos y entrega datos con números de secuencia.

14.1.7

Compruebe su comprensión - Transporte de datos

Verifique su comprensión de la capa de transporte eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La capa de transporte es responsable de establecer una sesión de comunicación temporal entre las aplicaciones host de origen y de destino.
2. La capa de transporte es responsable de la multiplexación de conversaciones, segmentación de datos y reensamblaje de segmentos, y seguimiento de conversaciones individuales.
3. UDP es un protocolo de entrega de mayor esfuerzo, mientras que TCP es un protocolo de transporte confiable.
4. UDP sería utilizado por aplicaciones VoIP sensibles al tiempo.

Has tenido 4 respuestas correctas de 4.

1. ¿Qué capa es responsable de establecer una sesión de comunicación temporal entre las aplicaciones host de origen y destino?

¡Lo tienes!

- ○ Capa de aplicación
- ○ Capa de enlace de datos
- ○ Capa de red
- ○ Capa física
- ◉ Capa de transporte

2. ¿Cuáles son las tres responsabilidades de la capa de transporte? (Escoja tres opciones).

¡Lo tienes!

- ☑ Multiplexión de conversaciones
- ☐ identificación de marcos
- ☐ identificación de información de enrutamiento
- ☑ segmentación de datos y reensamblado de segmentos
- ☑ Seguimiento de conversaciones individuales

3. ¿Qué declaración de protocolo de capa de transporte es verdadera?

¡Lo tienes!

- ○ TCP tiene menos campos que UDP.
- ○ TCP es más rápido que UDP.
- ◉ UDP es un protocolo de entrega de mejor esfuerzo.
- ○ UDP proporciona fiabilidad.

4. ¿Qué protocolo de capa de transporte se usaría para aplicaciones VoIP?

¡Lo tienes!

- ○ Protocolo de información de sesión (SIP)
- ○ Protocolo de control de transmisión (TCP)
- ◉ Protocolo de datagramas de usuario (UDP)
- ○ Protocolo de transferencia de VoIP

Correct

You have successfully identified the correct answers.

1. The transport layer is responsible for establishing a temporary communication session between the source and destination host applications.
2. The transport layer is responsible for conversation multiplexing, segmenting data and reassembling segments, and tracking individual conversations.
3. UDP is a best-effort delivery protocol while TCP is a reliable transport protocol.
4. UDP would be used by time sensitive VoIP applications.

You got 4 out of 4 questions correct.

1. Which layer is responsible for establishing a temporary communication session between the source and destination host applications?

You got it!

- ○ application layer
- ○ data link layer
- ○ network layer
- ○ physical layer
- ◉ transport layer

2. Which three are transport layer responsibilities? (Choose three.)

You got it!

- ☑ conversation multiplexing
- ☐ identifying frames
- ☐ identifying routing information
- ☑ segmenting data and reassembling segments
- ☑ tracking individual conversations

3. Which transport layer protocol statement is true?

You got it!

- ○ TCP has fewer fields than UDP.
- ○ TCP is faster than UDP.
- ◉ UDP is a best-effort delivery protocol.
- ○ UDP provides reliability.

4. Which transport layer protocol would be used for VoIP applications?

You got it!

- ○ Session Information Protocol (SIP)
- ○ Transmission Control Protocol (TCP)
- ◉ User Datagram Protocol (UDP)
- ○ VoIP Transfer Protocol

Descripción general de TCP

14.2.1

Características de TCP

En el tema anterior, aprendió que TCP y UDP son los dos protocolos de capa de transporte. Este tema proporciona más detalles sobre lo que hace TCP y cuándo es una buena idea usarlo en lugar de UDP.

Para comprender las diferencias entre TCP y UDP, es importante comprender cómo cada protocolo implementa funciones de confiabilidad específicas y cómo cada protocolo rastrea las conversaciones.

Además de admitir las funciones básicas de segmentación y reensamblado de datos, TCP también proporciona los siguientes servicios:

- **Establece una sesión -** -TCP es un protocolo orientado a la conexión que negocia y establece una conexión permanente (o sesión) entre los dispositivos de origen y destino antes de reenviar cualquier tráfico. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente.
- **Garantiza una entrega confiable: -** por muchas razones, es posible que un segmento se corrompa o se pierda por completo, ya que se transmite a través de la red. TCP asegura que cada segmento que envía la fuente llega al destino.
- **Proporciona entrega en el mismo pedido -** Debido a que las redes pueden proporcionar múltiples rutas que pueden tener diferentes velocidades de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, TCP garantiza que los segmentos se vuelvan a ensamblar en el orden correcto.
- **Admite control de flujo: -** los hosts de red tienen recursos limitados (es decir, memoria y potencia de procesamiento). Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a un cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la necesidad de retransmitir los datos cuando los recursos del host receptor se ven desbordados.

Para obtener más información sobre TCP, busque en Internet el RFC 793.

14.2.2

Encabezado TCP

TCP es un protocolo con estado, lo que significa que realiza un seguimiento del estado de la sesión de comunicación. Para hacer un seguimiento del estado de una sesión, TCP registra qué información se envió y qué información se reconoció. La sesión con estado comienza con el establecimiento de la sesión y termina con la finalización de la sesión.

Un segmento TCP agrega 20 bytes (es decir, 160 bits) de sobrecarga al encapsular los datos de la capa de aplicación. La figura muestra los campos en un encabezado TCP.

Muestra los campos en el encabezado TCP

14.2.3

Campos de encabezado TCP

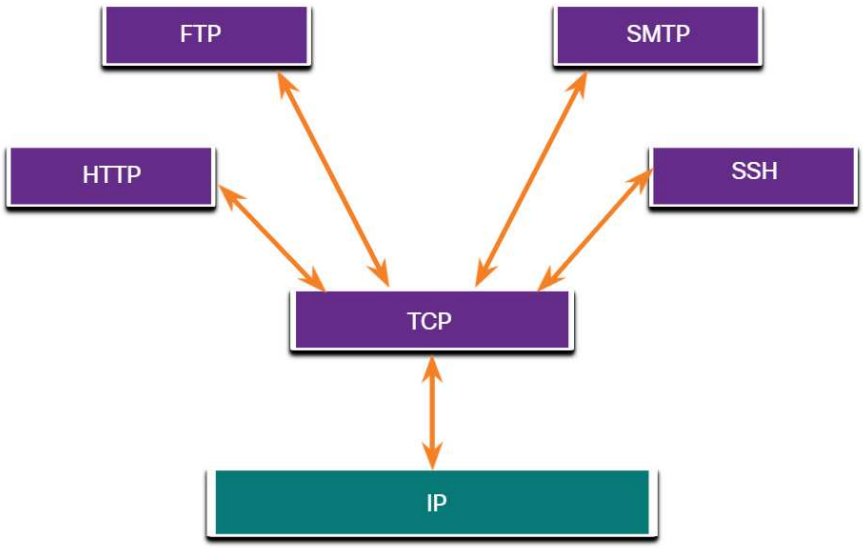
La tabla identifica y describe los diez campos de un encabezado TCP.

Campo de encabezado TCP	Descripción
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto.
Puerto de destino	Un campo de 16 bits utilizado para identificar la aplicación de destino por puerto específico.
Secuencia de números	Campo de 32 bits utilizado para reensamblar datos.
de 32 bits	Un campo de 32 bits utilizado para indicar que se han recibido datos y el siguiente byte esperado de la fuente.
Longitud del encabezado	Un campo de 4 bits conocido como «desplazamiento de datos» que indica la propiedad longitud del encabezado del segmento TCP.
Reservado	Un campo de 6 bits que está reservado para uso futuro.
Bits de control	Un campo de 6 bits utilizado que incluye códigos de bits, o indicadores, que indican la propiedad propósito y función del segmento TCP.
Tamaño de la ventana	Un campo de 16 bits utilizado para indicar el número de bytes que se pueden aceptar a la vez.
Suma de comprobación	A 16-bit field used for error checking of the segment header and data.
Urgente	Campo de 16 bits utilizado para indicar si los datos contenidos son urgentes.

14.2.4

Aplicaciones que utilizan TCP

TCP es un buen ejemplo de cómo las diferentes capas del conjunto de protocolos TCP / IP tienen roles específicos. TCP maneja todas las tareas asociadas con la división del flujo de datos en segmentos, proporcionando confiabilidad, controlando el flujo de datos y reordenando segmentos. TCP libera la aplicación de tener que administrar estas tareas. Las aplicaciones, como las que se muestran en la figura, simplemente puede enviar el flujo de datos a la capa de transporte y utilizar los servicios de TCP.



Muestra flechas que señalan ambas direcciones desde HTTP, FTP, SMTP y SSH a TCP y, a continuación, desde TCP a IP.

14.2.5

Verifique su comprensión - Descripción general de TCP

Compruebe su comprensión de TCP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El protocolo de capa de transporte TCP garantiza una entrega fiable del mismo pedido.
2. El encabezado TCP consta de 10 campos en un encabezado de 20 bytes.
3. FTP y HTTP requieren el uso del protocolo de capa de transporte TCP.

Has tenido 3 respuestas correctas de 3.

Correct

You have successfully identified the correct answers.

1. The TCP transport layer protocol ensures reliable same-order delivery.
2. The TCP header consists of 10 fields in a 20-byte header.
3. FTP and HTTP require the use of the TCP transport layer protocol.

You got 3 out of 3 questions correct.

1. ¿Qué protocolo de capa de transporte garantiza la entrega fiable del mismo pedido?

¡Lo tienes!

- ICMP
- IP
- (•) TCP
- UDP

2. ¿Qué enunciado de encabezado TCP es verdadero?

¡Lo tienes!

- Se compone de 4 campos en un encabezado de 8 bytes.
- Se compone de 8 campos en un encabezado de 10 bytes.
- (•) Se compone de 10 campos en un encabezado de 20 bytes.
- Se compone de 20 campos en un encabezado de 40 bytes.

3. ¿Qué dos aplicaciones usarían el protocolo de capa de transporte TCP? (Escoja dos opciones).

¡Lo tienes!

- [x] FTP
- [x] HTTP
- [ ] ICMP
- [ ] TFTP
- [ ] VoIP

1. Which transport layer protocol ensures reliable same-order delivery?

You got it!

- ICMP
- IP
- (•) TCP
- UDP

2. Which TCP header statement is true?

You got it!

- It consists of 4 fields in an 8-byte header.
- It consists of 8 fields in a 10-byte header.
- (•) It consists of 10 fields in a 20-byte header.
- It consists of 20 fields in a 40-byte header.

3. Which two applications would use the TCP transport layer protocol? (Choose two.)

You got it!

- [x] FTP
- [x] HTTP
- [ ] ICMP
- [ ] TFTP
- [ ] VoIP

Capa de transporte / Visión general de UDP

Visión general de UDP

14.3.1

Características de UDP

Este tema abarcará UDP, lo que hace y cuándo es una buena idea usarlo en lugar de TCP. UDP es un protocolo de transporte del mejor esfuerzo. UDP es un protocolo de transporte liviano que ofrece la misma segmentación y rearmado de datos que TCP, pero sin la confiabilidad y el control del flujo de TCP.

UDP es un protocolo tan simple que, por lo general, se lo describe en términos de lo que no hace en comparación con TCP.

Las características UDP incluyen lo siguiente:

- Los datos se reconstruyen en el orden en que se recibieron.
- Los segmentos perdidos no se vuelven a enviar.
- No hay establecimiento de sesión.
- El envío no está informado sobre la disponibilidad de recursos.

Para obtener más información sobre UDP, busque en Internet el RFC.

14.3.2

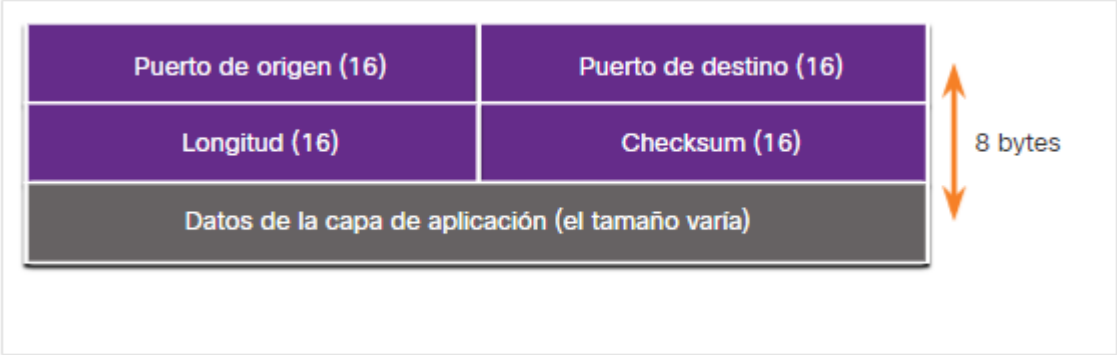
Encabezado UDP

UDP es un protocolo sin estado, lo que significa que ni el cliente ni el servidor rastrean el estado de la sesión de comunicación. Si se requiere confiabilidad al utilizar UDP como protocolo de transporte, a esta la debe administrar la aplicación.

Uno de los requisitos más importantes para transmitir vídeo en vivo y voz a través de la red es que los datos fluyan rápidamente. Las aplicaciones de vídeo y de voz en vivo pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible, y se adaptan perfectamente a UDP.

Los bloques de comunicación en UDP se denominan datagramas o segmentos. Estos datagramas se envían como el mejor esfuerzo por el protocolo de la capa de transporte.

El encabezado UDP es mucho más simple que el encabezado TCP porque solo tiene cuatro campos y requiere 8 bytes (es decir, 64 bits). La figura muestra los campos en un encabezado TCP.



El diagrama de datagramas UDP muestra 4 campos de encabezado: puerto de origen, puerto de destino, longitud y suma de comprobación, así como los datos de capa de aplicación sin encabezado.

14.3.3

Campos de encabezado UDP

La tabla identifica y describe los cuatro campos de un encabezado UDP.

Campo de encabezado UDP	Descripción
Puerto de origen	Campo de 16 bits utilizado para identificar la aplicación de origen por número de puerto.
Puerto de destino	Un campo de 16 bits utilizado para identificar la aplicación de destino por puerto específico.
Longitud	Campo de 16 bits que indica la longitud del encabezado del datagrama UDP.
Suma de comprobación	Campo de 16 bits utilizado para la comprobación de errores del encabezado y los datos del datagrama.

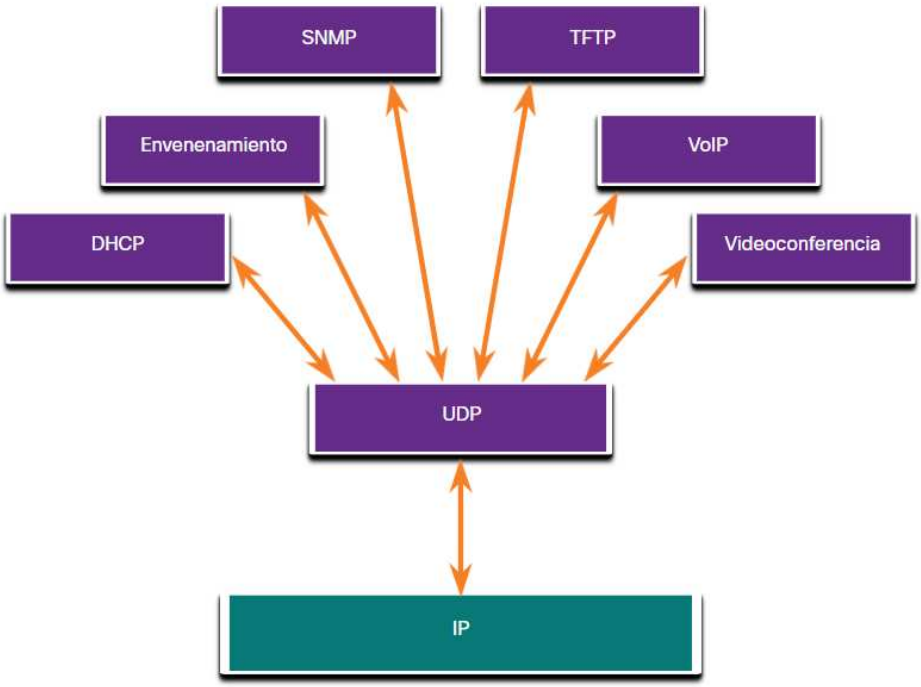
14.3.4

Aplicaciones que utilizan UDP

Existen tres tipos de aplicaciones que son las más adecuadas para UDP:

- **Aplicaciones de video y multimedia en vivo:** - estas aplicaciones pueden tolerar cierta pérdida de datos, pero requieren poco o ningún retraso. Los ejemplos incluyen VoIP y la transmisión de video en vivo.
- **Solicitudes simples de solicitud y respuesta:** - aplicaciones con transacciones simples en las que un host envía una solicitud y puede o no recibir una respuesta. Los ejemplos incluyen DNS y DHCP.
- **Aplicaciones que manejan la confiabilidad por sí mismas:** - comunicaciones unidireccionales donde el control de flujo, la detección de errores, los reconocimientos y la recuperación de errores no son necesarios o la aplicación puede manejarlos. Los ejemplos incluyen SNMP y TFTP.

La figura identifica las aplicaciones que requieren UDP.



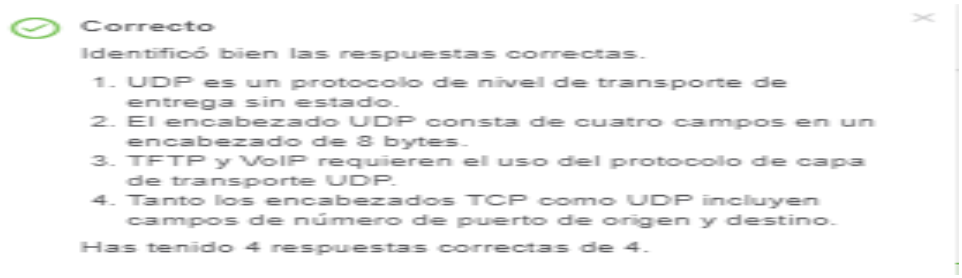
Muestra flechas que señalan ambas direcciones desde DHCP, DNS, SNMP, TFTP, VoIP e IPTV a UDP y, a continuación, desde UDP a IP.

Aunque DNS y SNMP utilizan UDP de manera predeterminada, ambos también pueden utilizar TCP. DNS utilizará TCP si la solicitud de DNS o la respuesta de DNS son más de 512 bytes, como cuando una respuesta de DNS incluye muchas resoluciones de nombre. Del mismo modo, en algunas situaciones, el administrador de redes puede querer configurar SNMP para utilizar TCP.

14.3.5

Verifique su comprensión - Descripción general de UDP

Verifique su comprensión de UDP eligiendo la MEJOR respuesta a las siguientes preguntas.



Correcto

Identificó bien las respuestas correctas.

1. UDP es un protocolo de nivel de transporte de entrega sin estado.
2. El encabezado UDP consta de cuatro campos en un encabezado de 8 bytes.
3. TFTP y VoIP requieren el uso del protocolo de capa de transporte UDP.
4. Tanto los encabezados TCP como UDP incluyen campos de número de puerto de origen y destino.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuál de los siguientes es un protocolo de nivel de transporte de entrega sin estado?

¡Lo tienes!

- ICMP
- IP
- TCP
- (•) UDP

2. ¿Qué declaración de encabezado UDP es verdadera?

¡Lo tienes!

- (•) Se compone de 4 campos en un encabezado de 8 bytes.
- Se compone de 8 campos en un encabezado de 10 bytes.
- Se compone de 10 campos en un encabezado de 20 bytes.
- Se compone de 20 campos en un encabezado de 40 bytes.

3. ¿Qué dos aplicaciones usarían el protocolo de capa de transporte UDP? (Escoja dos opciones).

¡Lo tienes!

- [ ] FTP
- [ ] HTTP
- [ ] ICMP
- [x] TFTP
- [x] VoIP

4. ¿Qué dos campos son los mismos en un encabezado TCP y UDP? (Escoja dos opciones).

¡Lo tienes!

- [ ] Bits de control
- [x] Número de puerto de destino
- [ ] Número de secuencia
- [x] Número de puerto de origen
- [ ] Número de puerto conocido

Correct

You have successfully identified the correct answers.

1. UDP is a stateless best-effort delivery transport layer protocol.
2. The UDP header consists of four fields in an 8-byte header.
3. TFTP and VoIP require the use of the UDP transport layer protocol.
4. Both TCP and UDP headers include a source and destination port number fields.

You got 4 out of 4 questions correct.

1. Which of the following is a stateless best-effort delivery transport layer protocol?

You got it!

- ( ) ICMP
- ( ) IP
- ( ) TCP
- (•) UDP

2. Which UDP header statement is true?

You got it!

- (•) It consists of 4 fields in an 8-byte header.
- ( ) It consists of 8 fields in a 10-byte header.
- ( ) It consists of 10 fields in a 20-byte header.
- ( ) It consists of 20 fields in a 40-byte header.

3. Which two applications would use the UDP transport layer protocol? (Choose two.)

You got it!

- [ ] FTP
- [ ] HTTP
- [ ] ICMP
- [x] TFTP
- [x] VoIP

4. Which two fields are the same in a TCP and UDP header? (Choose two.)

You got it!

- [ ] Control bits
- [x] Destination port number
- [ ] Sequence number
- [x] Source port number
- [ ] Well-known port number

Capa de transporte / Números de puerto

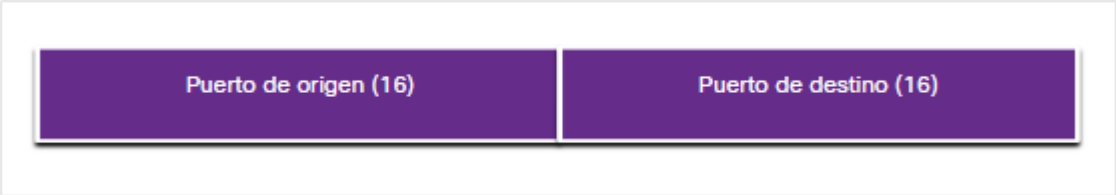
Números de puerto

14.4.1

Comunicaciones Múltiples Separadas

Como ha aprendido, hay algunas situaciones en las que TCP es el protocolo correcto para el trabajo, y otras situaciones en las que se debe usar UDP. Independientemente del tipo de datos que se transporten, tanto TCP como UDP utilizan números de puerto.

Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas. Como se muestra en la figura, los campos de encabezado TCP y UDP identifican un número de puerto de aplicación de origen y destino.



Muestra los campos de encabezado del puerto de origen y del puerto de destino que son de 2 bytes cada uno.

El número de puerto de origen está asociado con la aplicación de origen en el host local, mientras que el número de puerto de destino está asociado con la aplicación de destino en el host remoto.

Por ejemplo, supongamos que un host está iniciando una solicitud de página web desde un servidor web. Cuando el host inicia la solicitud de página web, el host genera dinámicamente el número de puerto de origen para identificar de forma exclusiva la conversación. Cada solicitud generada por un host utilizará un número de puerto de origen creado dinámicamente diferente. Este proceso permite establecer varias conversaciones simultáneamente.

En la solicitud, el número de puerto de destino es lo que identifica el tipo de servicio que se solicita del servidor web de destino. Por ejemplo, cuando un cliente especifica el puerto 80 en el puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios web.

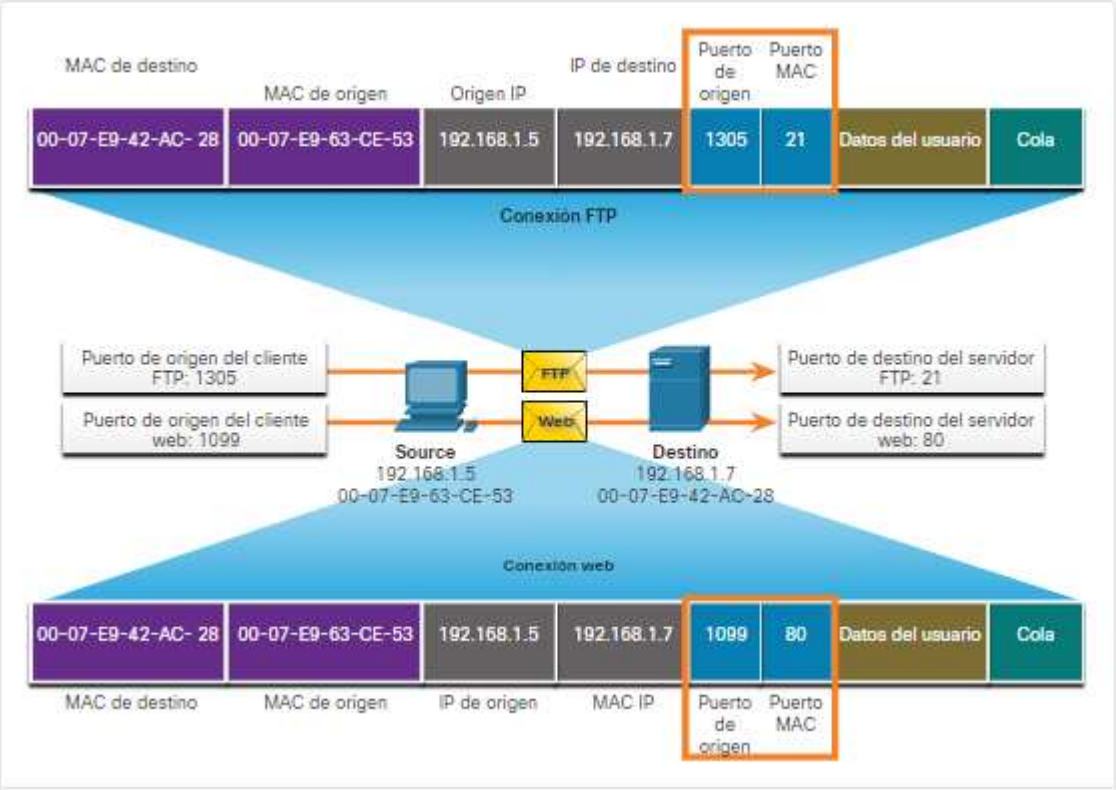
Un servidor puede ofrecer más de un servicio simultáneamente, como servicios web en el puerto 80, mientras que ofrece el establecimiento de conexión de Protocolo de transferencia de archivos (FTP) en el puerto 21.

14.4.2

Pares de enchufes

Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. Se conoce como socket a la combinación de la dirección IP de origen y el número de puerto de origen, o de la dirección IP de destino y el número de puerto de destino.

En el ejemplo de la figura, el PC está solicitando simultáneamente servicios FTP y web desde el servidor de destino.



Muestra un equipo que realiza tanto una solicitud web como una solicitud FTP a un servidor. Las solicitudes tienen números de puerto de origen y destino que identifican el PC host y el servicio de aplicación solicitado respectivamente.

En el ejemplo, la solicitud FTP generada por el PC incluye las direcciones MAC de Capa 2 y las direcciones IP de Capa 3. La solicitud también identifica el puerto de origen 1305 (es decir, generado dinámicamente por el host) y el puerto de destino, identificando los servicios FTP en el puerto 21. El host también ha solicitado una página web del servidor utilizando las mismas direcciones de Capa 2 y Capa 3. Sin embargo, está utilizando el número de puerto de origen 1099 (es decir, generado dinámicamente por el host) y el puerto de destino que identifica el servicio web en el puerto 80.

El socket se utiliza para identificar el servidor y el servicio que solicita el cliente. Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099.

El socket en un servidor web puede ser 192.168.1.7:80

Juntos, estos dos zócalos se combinan para formar un par de zócalos: 192.168.1.5:1099, 192.168.1.7:80

Los sockets permiten que los diversos procesos que se ejecutan en un cliente se distingan entre sí. También permiten la diferenciación de diferentes conexiones a un proceso de servidor.

El número de puerto de origen actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de transporte hace un seguimiento de este puerto y de la aplicación que generó la solicitud de manera que cuando se devuelva una respuesta, esta se envíe a la aplicación correcta.

14.4.3

Grupos de números de puerto

La Autoridad de Números Asignados de Internet (IANA) es la organización de estándares responsable de asignar varios estándares de direccionamiento, incluidos los números de puerto de 16 bits. Los 16 bits utilizados para identificar los números de puerto de origen y destino proporcionan un rango de puertos entre 0 y 65535.

La IANA ha dividido el rango de números en los siguientes tres grupos de puertos.

Grupo de puertos	Rango de números	Descripción
Puertos bien conocidos	0 to 1,023	• Estos números de puerto están reservados para servicios comunes o populares y aplicaciones como navegadores web, clientes de correo electrónico y acceso remoto clientes. • Los puertos conocidos definidos para aplicaciones de servidor comunes permiten para identificar fácilmente el servicio asociado requerido.
Puertos registrados	1,024 to 49,151	• Estos números de puerto son asignados por IANA a una entidad solicitante a utilizar con procesos o aplicaciones específicos. • Estos procesos son principalmente aplicaciones individuales que un usuario ha elegido instalar, en lugar de aplicaciones comunes que recibir un número de puerto conocido. • Por ejemplo, Cisco ha registrado el puerto 1812 para su servidor RADIUS proceso de autenticación
Privada and/or **puertos dinámicos**	49,152 to 65,535	• Estos puertos también se conocen como puertos *efímeros*. • El sistema operativo del cliente generalmente asigna números de puerto dinámicamente cuando se inicia una conexión a un servicio. • El puerto dinámico se utiliza para identificar la aplicación del cliente durante la comunicación

Nota: Algunos sistemas operativos de clientes pueden usar números de puerto registrados en lugar de números de puerto dinámicos para asignar puertos de origen.

La tabla muestra algunos números de puerto conocidos y sus aplicaciones asociadas.

Números de puerto conocidos

Número de puerto	Protocolo	Aplicación
20	TCP	Protocolo de transferencia de archivos (FTP) - Datos
21	TCP	Protocolo de transferencia de archivos (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo simple de transferencia de correo (SMTP)
53	UDP, TCP	Servicio de nombres de dominio (DNS, Domain Name Service)
67	UDP	Protocolo de configuración dinámica de host (DHCP): servidor
68	UDP	Protocolo de configuración dinámica de host: cliente
69	UDP	Protocolo trivial de transferencia de archivos (TFTP)
80	TCP	Protocolo de transferencia de hipertexto (HTTP)
110	TCP	Protocolo de oficina de correos, versión 3 (POP3)
143	TCP	Protocolo de acceso a mensajes de Internet (IMAP)
161	UDP	Protocolo simple de administración de redes (SNMP)
443	TCP	Protocolo seguro de transferencia de hipertexto (HTTPS)

Algunas aplicaciones pueden utilizar TCP y UDP. Por ejemplo, DNS utiliza UDP cuando los clientes envían solicitudes a un servidor DNS. Sin embargo, la comunicación entre dos servidores DNS siempre usa TCP.

Busque en el sitio web de IANA el registro de puertos para ver la lista completa de números de puerto y aplicaciones asociadas.

14.4.4

El comando netstat

Las conexiones TCP no descritas pueden representar una importante amenaza a la seguridad. Pueden indicar que algo o alguien está conectado al host local. A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Como se muestra a continuación, ingrese el comando **netstat** Como se muestra a continuación, ingrese el comando para enumerar los protocolos en uso, la dirección local y los números de puerto, la dirección extranjera y los números de puerto y el estado de la conexión.

```
C:\> netstat
Active Connections
Proto Dirección local Dirección extranjera Estado
TCP 192.168.1. 124:3126 192.168.0.2:netbios-ssn ESTABLECEDA
TCP 192.168.1. 124:3158 207.138.126.152:http ESTABLECED
TCP 192.168.1. 124:3159 207.138.126.169:http ESTABLECIDO
TCP 192.168.1. 124:3160 207.138.126.169:http ESTABLEZADO
TCP 192.168.1. 124:3161 sc.msn.com:http ESTABLECID
TCP 192.168.1. 124:3166 www.cisco.com:http ESTABLECIDADO
```

De manera predeterminada, el comando **netstat** intentará resolver las direcciones IP para nombres de dominio y números de puerto para aplicaciones conocidas. La **-n** opción se puede usar para mostrar las direcciones IP y los números de puerto en su forma numérica.

14.4.5

Verifique su comprensión - Números de puerto

Verifique su comprensión de los números de puerto eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El par de sockets para un host con dirección IP 10.1.1.10 que solicita servicios web de un servidor en 10.1.1.254 sería 10.1.1. 10:1099, 10.1.1. 254:80.
2. Los números de puerto de las aplicaciones FTP, HTTP y TFTP se definen en el grupo de números de puerto conocidos.
3. El comando de Windows **netstat** mostraría los protocolos en uso, la dirección local y los números de puerto, la dirección extranjera y los números de puerto y el estado de la conexión.

Has tenido 3 respuestas correctas de 3.

1. Supongamos que un host con dirección IP 10.1.1.10 desea solicitar servicios web desde un servidor en 10.1.1.254. ¿Cuál de los siguientes mostraría para corregir el par de socket?

¡Lo tienes!

- [ ] 1099:10 .1.1.10, 80:10 .1.1.254
- [ ] 10.1.1. 10:80, 10.1.1. 254:1099
- [x] 10.1.1. 10:1099, 10.1.1. 254:80
- [ ] 80:10 .1.1.10, 1099:10 .1.1.254

2. ¿Qué grupo de puertos incluye números de puerto para aplicaciones FTP, HTTP y TFTP?

¡Lo tienes!

- [ ] Puertos dinámicos
- [ ] Puertos privados
- [ ] Puertos registrados
- [x] Puertos bien conocidos

3. ¿Qué comando de Windows mostrará los protocolos en uso, la dirección local y los números de puerto, la dirección extranjera y los números de puerto y el estado de la conexión?

¡Lo tienes!

- ipconfig /all
- ping
- (•) netstat
- traceroute

Correct

You have successfully identified the correct answers.

1. The socket pair for a host with IP address 10.1.1.10 requesting web services from a server at 10.1.1.254 would be 10.1.1.10:1099, 10.1.1.254:80.
2. FTP, HTTP, and TFTP applications port numbers are defined in the well-known port numbers group.
3. The **netstat** windows command would display protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.

You got 3 out of 3 questions correct.

1. Assume a host with IP address 10.1.1.10 wants to request web services from a server at 10.1.1.254. Which of the following would display to correct socket pair?

You got it!

- 1099:10.1.1.10, 80:10.1.1.254
- 10.1.1.10:80, 10.1.1.254:1099
- (•) 10.1.1.10:1099, 10.1.1.254:80
- 80:10.1.1.10, 1099:10.1.1.254

2. Which port group includes port numbers for FTP, HTTP, and TFTP applications?

You got it!

- Dynamic ports
- Private ports
- Registered ports
- (•) Well-known ports

3. Which windows command would display the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state?

You got it!

- ipconfig /all
- ping
- (•) netstat
- traceroute

Proceso de comunicación TCP

14.5.1

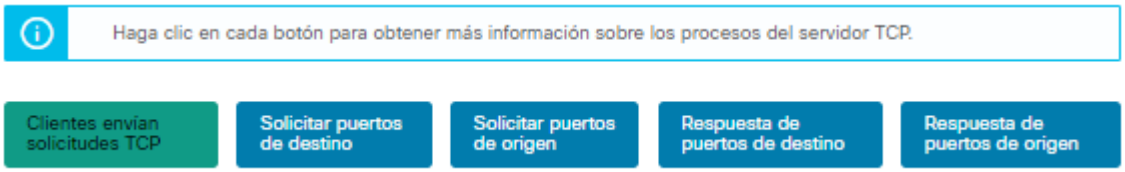
Procesos del servidor TCP

Ya conoces los fundamentos de TCP. Comprender el papel de los números de puerto le ayudará a comprender los detalles del proceso de comunicación TCP. En este tema, también aprenderá acerca de los procesos de enlace de tres vías TCP y terminación de sesión.

Cada proceso de aplicación que se ejecuta en el servidor para utilizar un número de puerto. El número de puerto es asignado automáticamente o configurado manualmente por un administrador del sistema.

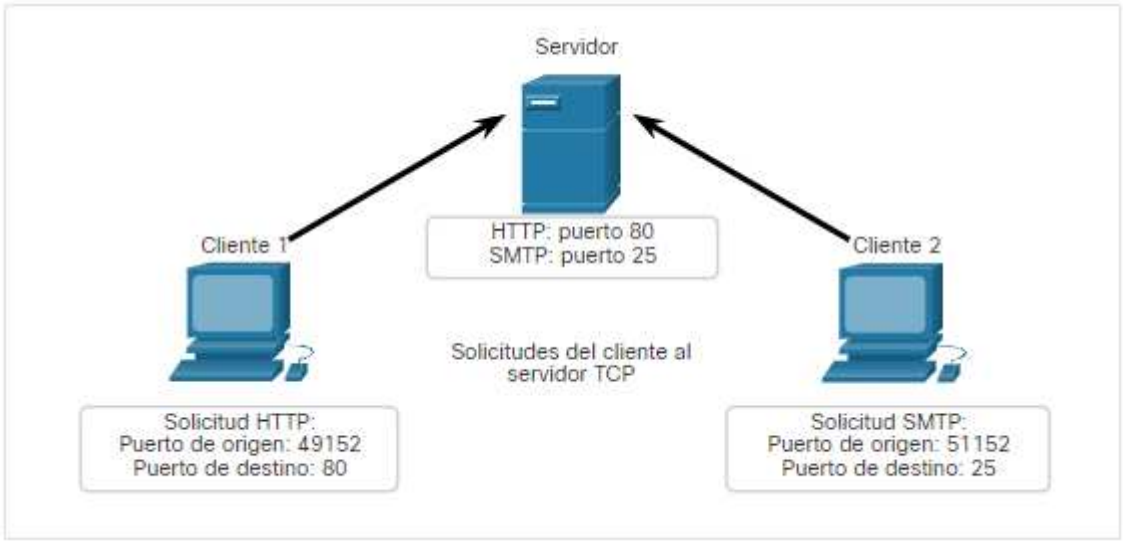
Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la capa de transporte. Por ejemplo, un host que ejecuta una aplicación de servidor web y una aplicación de transferencia de archivos no puede tener ambos configurados para usar el mismo puerto, como el puerto TCP 80.

Una aplicación de servidor activa asignada a un puerto específico se considera abierta, lo que significa que la capa de transporte acepta y procesa los segmentos dirigidos a ese puerto. Toda solicitud entrante de un cliente, direccionada al socket correcto es aceptada y los datos se envían a la aplicación del servidor. Pueden existir varios puertos abiertos simultáneamente en un servidor, uno para cada aplicación de servidor activa.



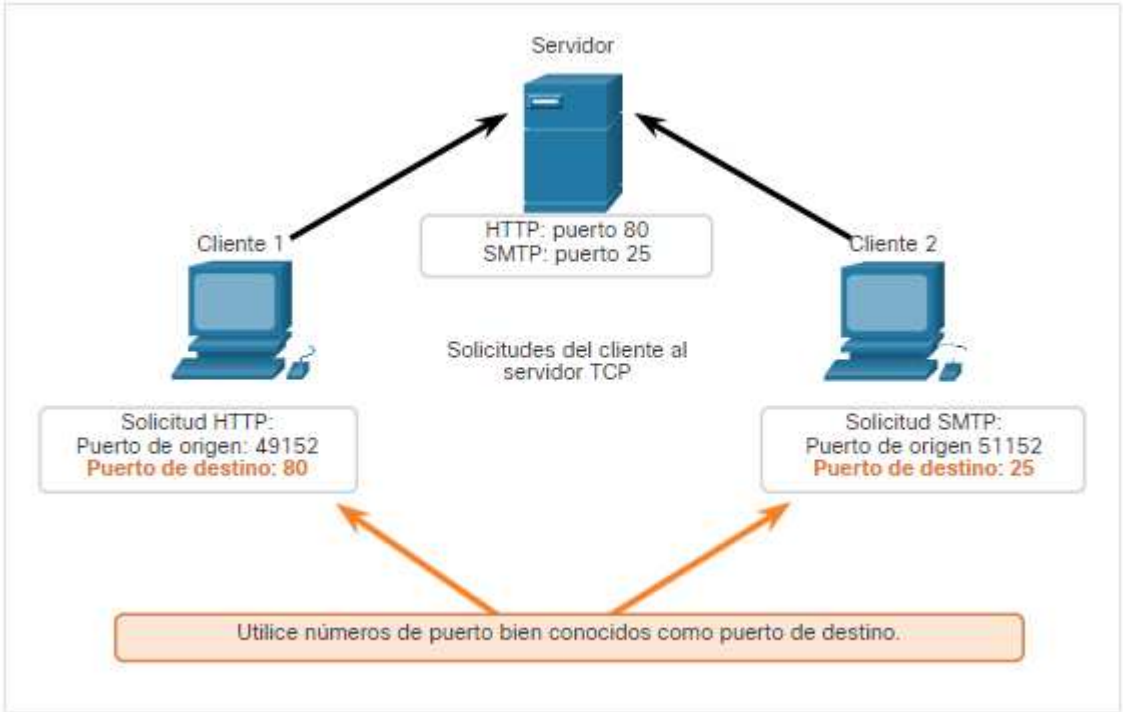
Clientes Mandando Solicitudes TCP

El cliente 1 solicita servicios web y el cliente 2 solicita servicio de correo electrónico utilizando puertos conocidos (es decir, servicios web = puerto 80, servicios de correo electrónico = puerto 25).



Solicitud de Puertos de Destino

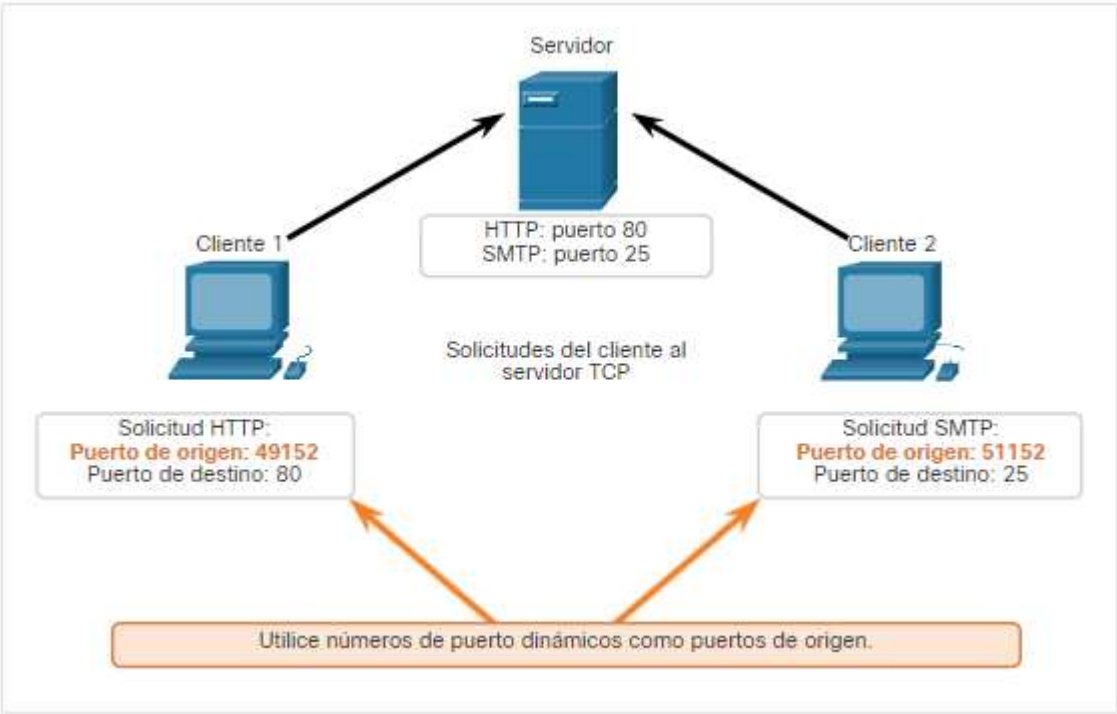
Las solicitudes generan dinámicamente un número de puerto de origen. En este caso, el cliente 1 está utilizando el puerto de origen 49152 y el cliente 2 está utilizando el puerto de origen 51152.



Clientes envían solicitudes TCP | Solicitar puertos de destino | Solicitar puertos de origen | Respuesta de puertos de destino | Respuesta de puertos de origen

Solicitud de Puertos de Origen

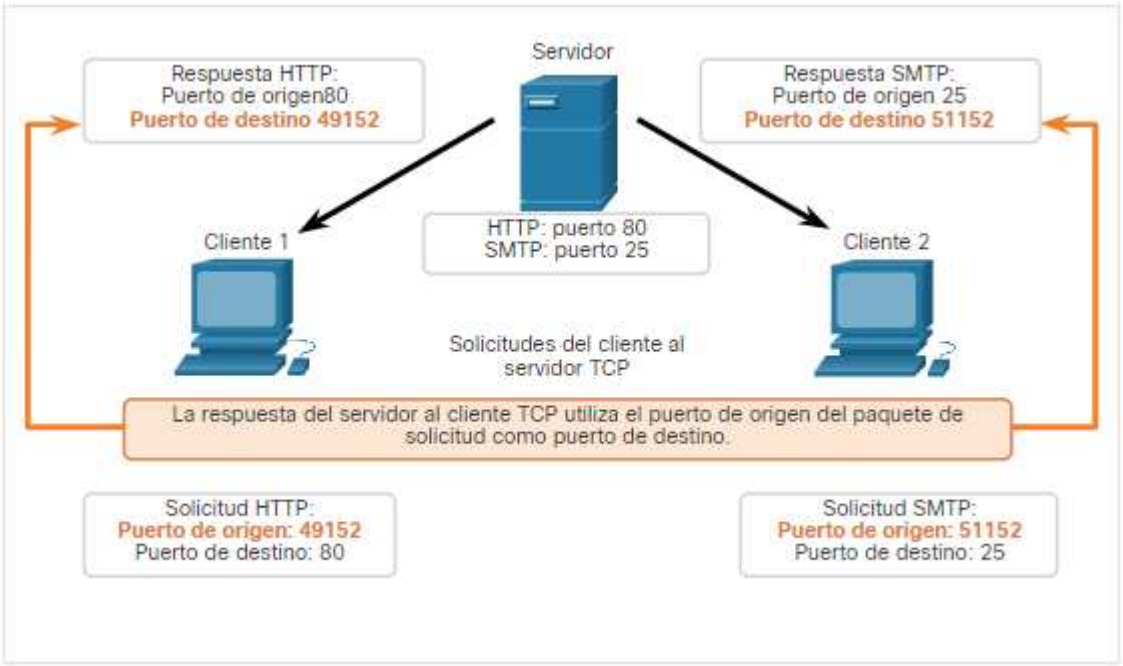
Cuando el servidor responde a las solicitudes del cliente, invierte los puertos de destino y origen de la solicitud inicial.



Clientes envían solicitudes TCP | Solicitar puertos de destino | Solicitar puertos de origen | Respuesta de puertos de destino | Respuesta de puertos de origen

Respuesta de Puertos de Destino

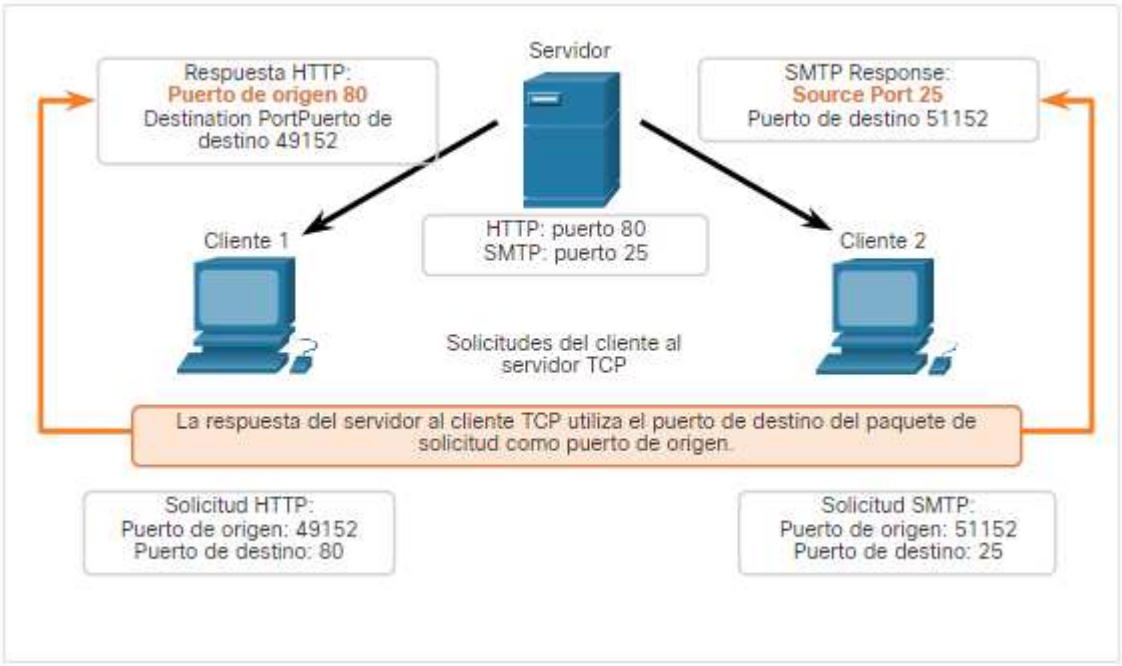
Observe que la respuesta del servidor a la solicitud web ahora tiene el puerto de destino 49152 y la respuesta de correo electrónico ahora tiene el puerto de destino 51152.



Clientes envían solicitudes TCP | Solicitar puertos de destino | Solicitar puertos de origen | Respuesta de puertos de destino | Respuesta de puertos de origen

Respuesta de Puertos de Origen

El puerto de origen en la respuesta del servidor es el puerto de destino original en las solicitudes iniciales.



14.5.2

Establecimiento de conexiones TCP

En algunas culturas, cuando dos personas se conocen, generalmente se saludan dándose la mano. Ambas partes entienden el acto de estrechar la mano como una señal de saludo amistoso. Las conexiones en la red son similares. En las conexiones TCP, el cliente host establece la conexión con el servidor mediante el proceso de enlace de tres vías.

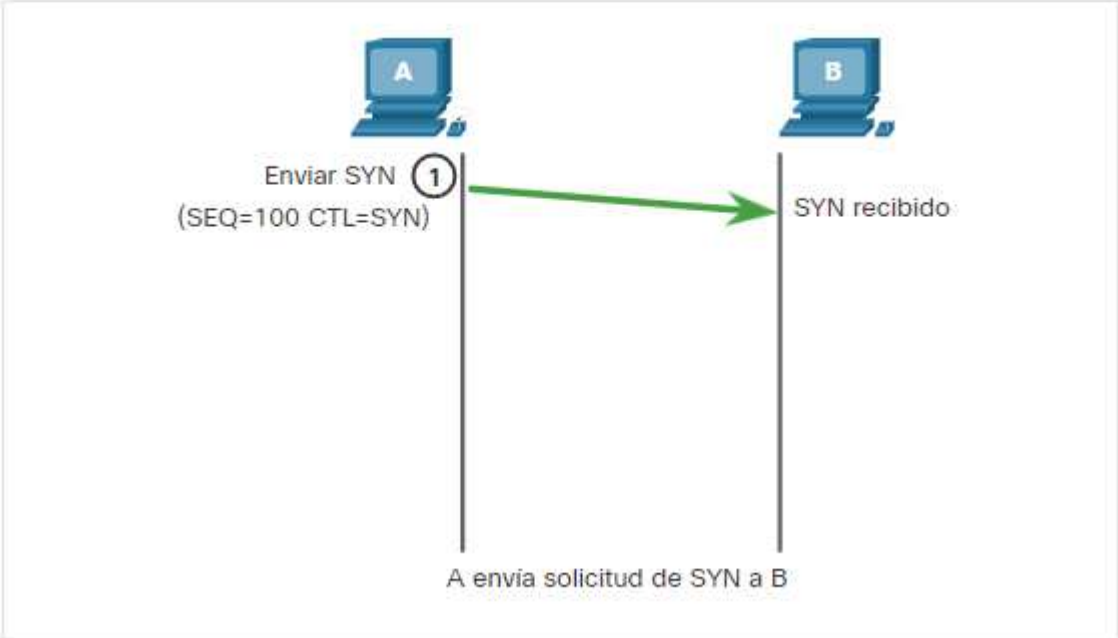
Haga clic en cada botón para obtener más información sobre cada paso de establecimiento de conexión TCP.

Paso 1. SYN | Paso 2. ACK y SYN | Paso 3. ACK

Paso 1. SYN

El cliente de origen solicita una sesión de comunicación con el servidor.

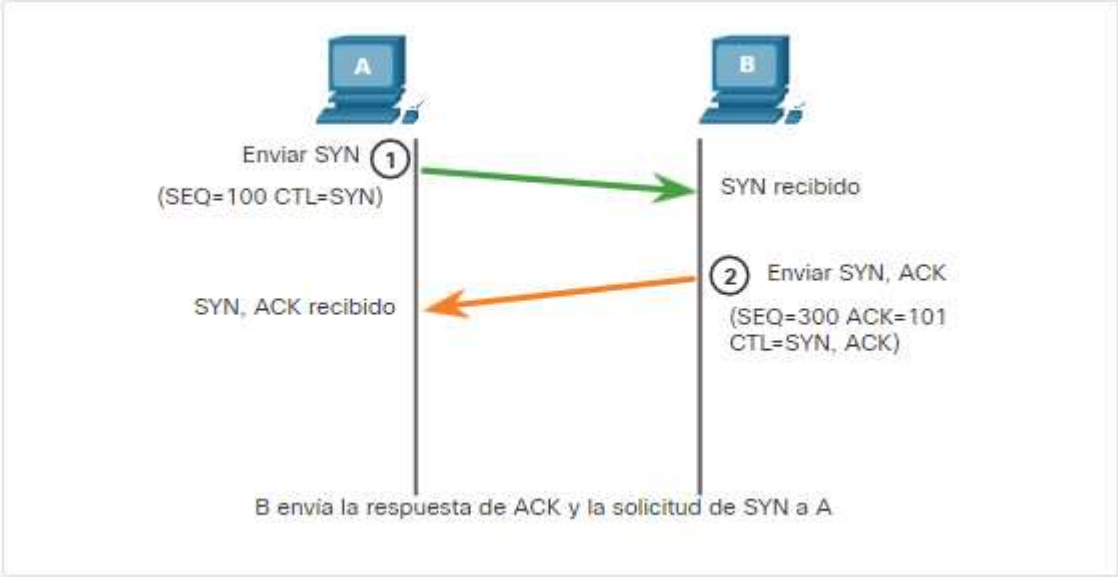
PCA inicia un apretón de manos de tres vías mediante el envío de un segmento syn a PCB.



Paso 1. SYN | Paso 2. ACK y SYN | Paso 3. ACK

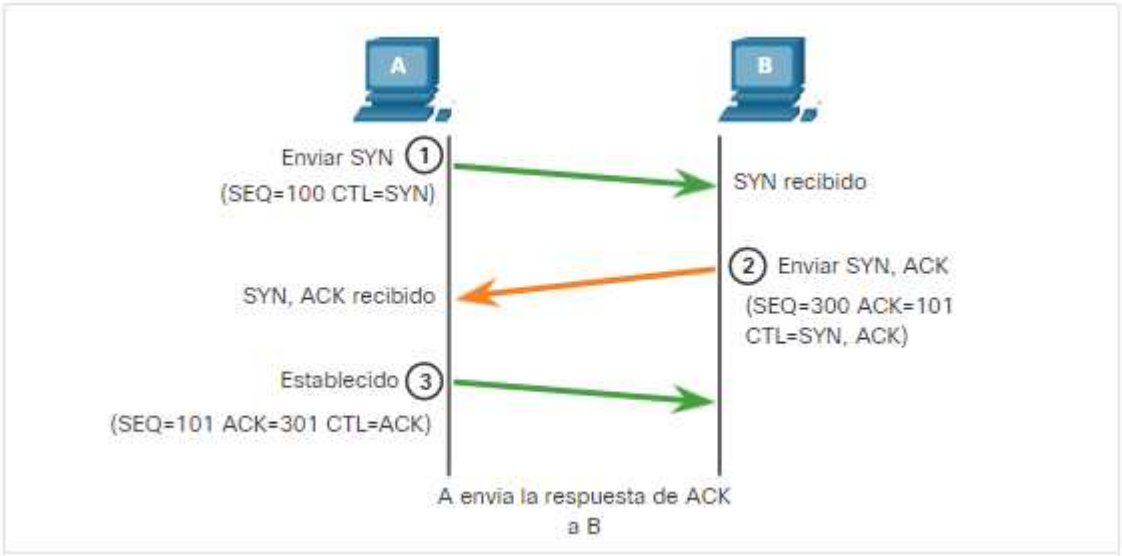
Paso 2. ACK y SYN

El servidor acusa recibo de la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.



Paso 3. ACK

El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.



El protocolo de enlace de tres vías valida que el host de destino esté disponible para comunicarse. En este ejemplo, el host A ha validado que el host B está disponible.

14.5.3

Terminación de sesión

Para cerrar una conexión, se debe establecer el marcador de control de finalización (FIN) en el encabezado del segmento. Para finalizar todas las sesiones TCP de una vía, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento de reconocimiento (ACK). Por lo tanto, para terminar una conversación simple admitida por TCP, se requieren cuatro intercambios para finalizar ambas sesiones. El cliente o el servidor pueden iniciar la terminación.

En el ejemplo, los términos cliente y servidor se utilizan como referencia por simplicidad, pero dos hosts que tengan una sesión abierta pueden iniciar el proceso de finalización.

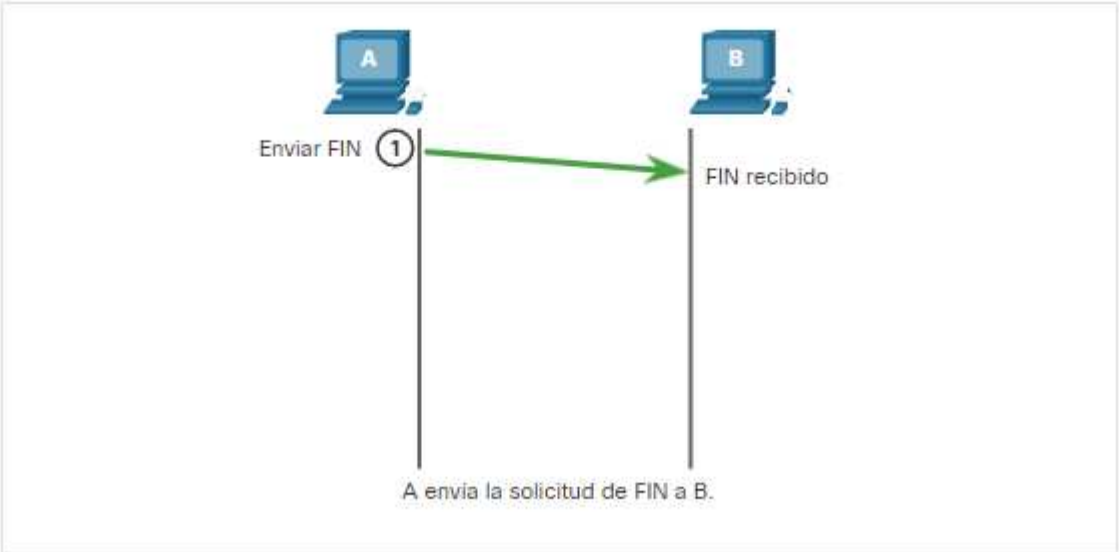
Haga clic en cada botón para obtener más información sobre los pasos de finalización de la sesión.

Paso 1. FIN | Paso 2. ACK | Paso 3. FIN | Paso 4. ACK

Paso 1. FIN

Cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el indicador FIN establecido.

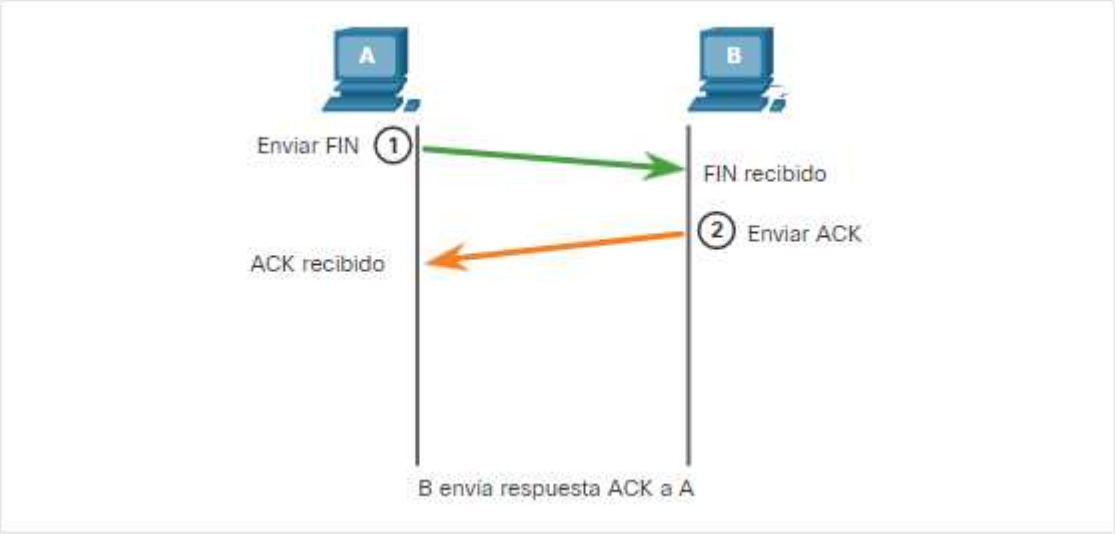
PCA envía un segmento de aleta a PCB para finalizar la sesión cuando no hay más datos para enviar



Paso 1. FIN | Paso 2. ACK | Paso 3. FIN | Paso 4. ACK

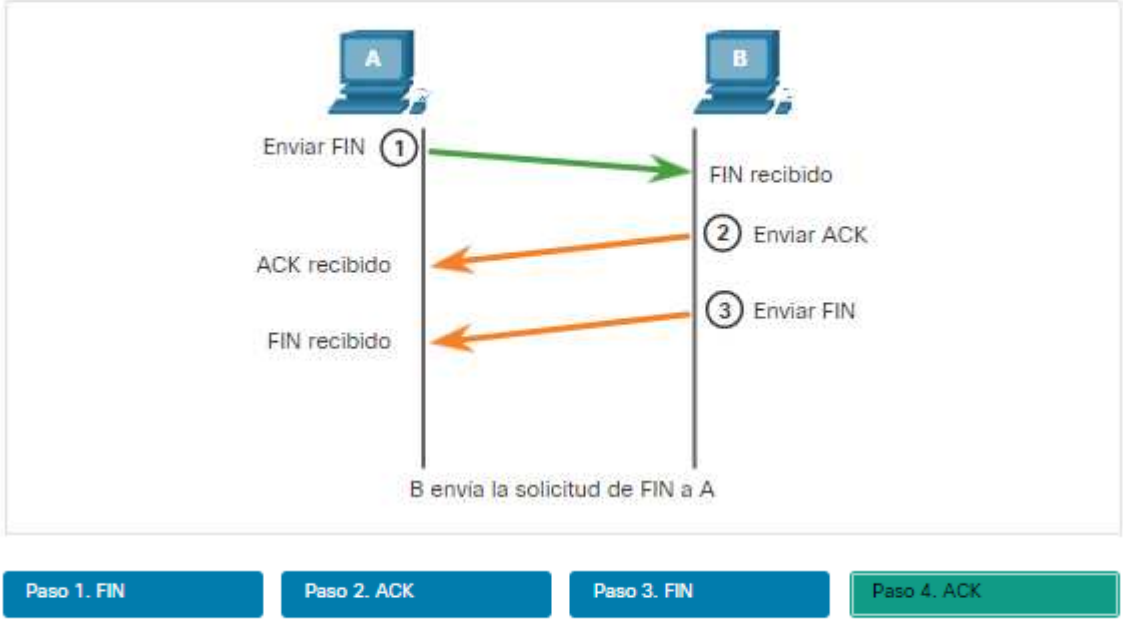
Paso 2. ACK

El servidor envía un ACK para acusar recibo del FIN para terminar la sesión de cliente a servidor.



Paso 3. FIN

El servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.



Paso 4. ACK

El cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.

Una vez reconocidos todos los segmentos, la sesión se cierra.

14.5.4

Análisis del enlace de tres vías de TCP

Los hosts mantienen el estado, rastrean cada segmento de datos dentro de una sesión e intercambian información sobre qué datos se reciben utilizando la información en el encabezado TCP. TCP es un protocolo full-duplex, donde cada conexión representa dos sesiones de comunicación unidireccionales. Para establecer la conexión, los hosts realizan un enlace de tres vías. Como se muestra en la figura, los bits de control en el encabezado TCP indican el progreso y el estado de la conexión.

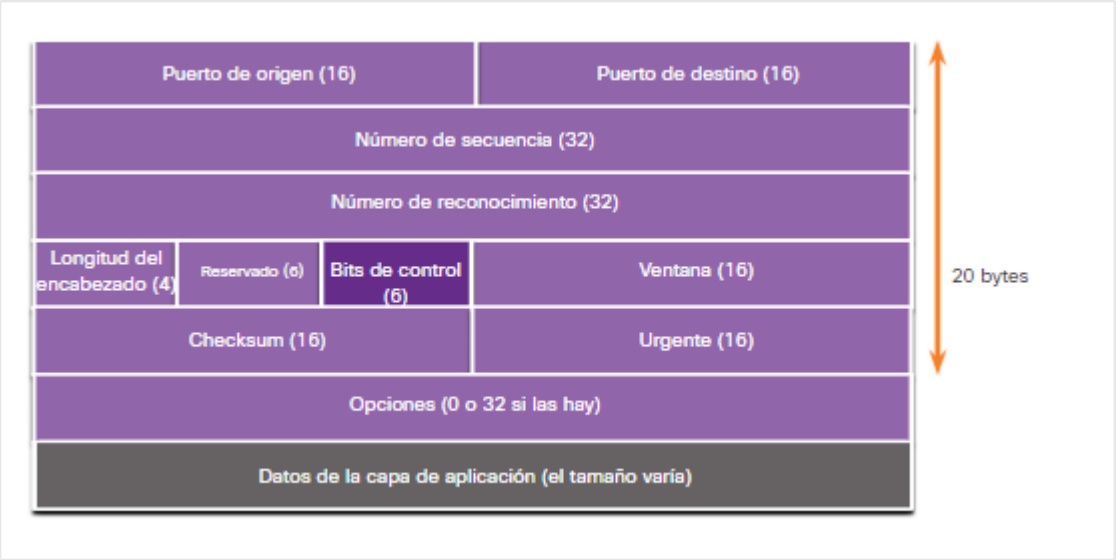
Estas son las funciones del apretón de manos de tres vías:

- Establece que el dispositivo de destino está presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y acepte solicitudes en el número de puerto de destino que el cliente de origen desea utilizar.
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto

Una vez completada la comunicación, las sesiones se cierran y la conexión finaliza. Los mecanismos de conexión y sesión permiten la función de confiabilidad TCP.

muestra los campos de encabezado del segmento tcp con el campo de bits de control de 6 bits resaltado

Campo de bits de control



Los seis bits del campo de bits de control del encabezado del segmento TCP también se conocen como marcadores. Una bandera es un bit que está activado o desactivado.

Los seis indicadores de bits de control son los siguientes:

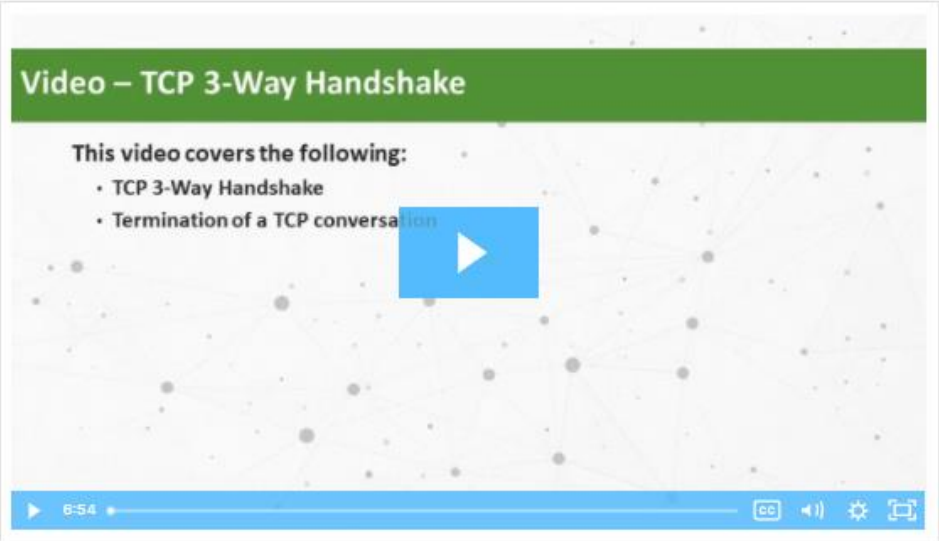
- **URG** - campo de puntero urgente significativo
- **ACK** - Indicador de acuse de recibo utilizado en el establecimiento de la conexión y la terminación de la sesión
- **PSH** - Función de empuje
- **RST** - restablece la conexión cuando se produce un error o un tiempo de espera
- **SYN** - Sincronizar números de secuencia utilizados en el establecimiento de conexión
- **FIN** - No más datos del remitente y se utilizan en la terminación de la sesión

Busque en Internet para obtener más información sobre las banderas PSH y URG.

14.5.5

Vídeo: Protocolo de enlace TCP de 3 vías

Haga clic en Reproducir en la figura para ver una demostración en video del protocolo de enlace TCP de 3 vías, utilizando Wireshark.



14.5.6

Compruebe su comprensión - Proceso de comunicación TCP

Verifique su comprensión del proceso de comunicación TCP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El puerto de destino es el puerto conocido para Simple Mail Transport Protocol, que es 25. Este es el puerto en el que el servidor de correo estará escuchando. El cliente solicitante selecciona dinámicamente el puerto de origen y puede ser 49152.
2. El protocolo de enlace de tres vías consta de tres intercambios de mensajes con los siguientes indicadores de bits de control: SYN, SYN ACK y ACK.
3. Hay cuatro intercambios para finalizar ambas sesiones entre dos hosts. (1) El host A envía una FIN. (2) El host B envía un ACK. (3) El host B envía un FIN. (4) El host A envía un ACK.

Has tenido 3 respuestas correctas de 3.

1. ¿Cuáles de los siguientes puertos serían válidos de origen y destino para un host que se conecta a un servidor de correo electrónico?

¡Lo tienes!

- Fuente: 25, Destino: 49152
- Fuente: 80, Destino: 49152
- (•) Fuente: 49152, Destino: 25
- Fuente: 49152, Destino: 80

2. ¿Qué indicadores de bits de control se utilizan durante el apretón de manos de tres vías?

¡Lo tienes!

- ACK y FIN
- FIN y RESET
- RESET y SYN
- (•) SYN y ACK

3. ¿Cuántos intercambios se necesitan para finalizar ambas sesiones entre dos hosts?

¡Lo tienes!

- un intercambio
- dos intercambios
- tres intercambios
- (•) cuatro intercambios
- cinco intercambios

Correct

You have successfully identified the correct answers.

1. The destination port is the well-known port for Simple Mail Transport Protocol, which is 25. This is the port that the mail server will be listening on. The source port is dynamically selected by the requesting client and can be 49152.
2. The three-way handshake consists of a three message exchanges with the following control bit flags: SYN, SYN ACK, and ACK.
3. There are four exchanges to end both sessions between two hosts. (1) Host A sends a FIN. (2) Host B sends an ACK. (3) Host B sends a FIN. (4) Host A sends an ACK.

You got 3 out of 3 questions correct.

1. Which of the following would be valid source and destination ports for a host connecting to an email server?

You got it!

- ○ Source: 25, Destination: 49152
- ○ Source: 80, Destination: 49152
- ◉ Source: 49152, Destination: 25
- ○ Source: 49152, Destination: 80

2. Which control bit flags are used during the three-way handshake?

You got it!

- ○ ACK and FIN
- ○ FIN and RESET
- ○ RESET and SYN
- ◉ SYN and ACK

3. How many exchanges are needed to end both sessions between two hosts?

You got it!

- ○ one exchange
- ○ two exchanges
- ○ three exchanges
- ◉ four exchanges
- ○ five exchanges

Capa de transporte / Confiabilidad y control de flujo

Confiabilidad y control de flujo

14.6.1

Fiabilidad de TCP: entrega garantizada y ordenada

La razón por la que TCP es el mejor protocolo para algunas aplicaciones es porque, una diferencia de UDP, reenviar paquetes descartados y números paquetes para indicar su orden correcto antes de la entrega. TCP también puede ayudar a mantener el flujo de paquetes para que los dispositivos no se sobrecarguen. En este tema se tratan detalladamente estas características de TCP.

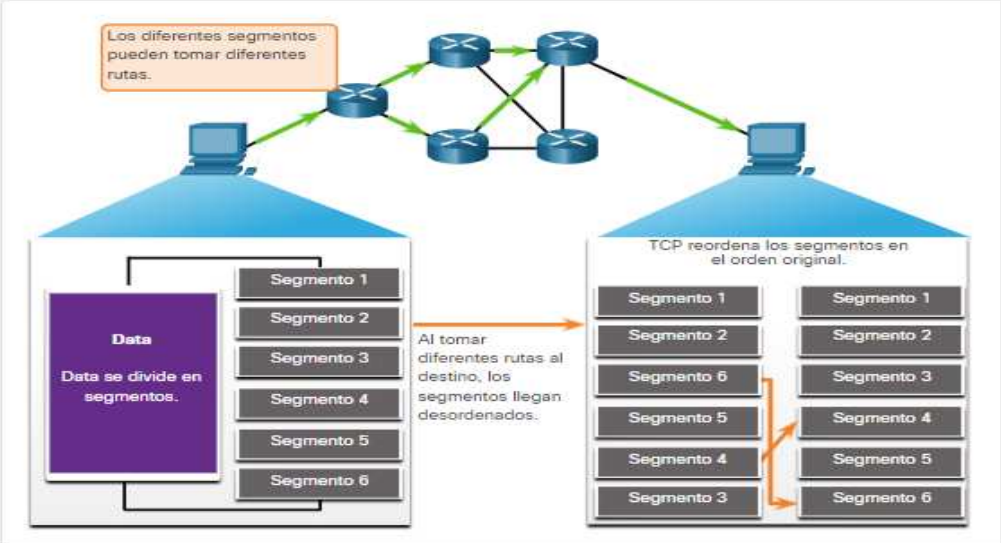
Puede haber momentos en que los segmentos TCP no llegan a su destino. Otras veces, los segmentos TCP podrían llegar fuera de servicio. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se vuelven a ensamblar en el orden original. Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete. El número de secuencia representa el primer byte de datos del segmento TCP.

Durante la configuración de la sesión, se establece un número de secuencia inicial (ISN). Este ISN representa el valor inicial de los bytes que se transmiten a la aplicación receptora. A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa según el número de bytes que se han transmitido. Este seguimiento de bytes de datos permite identificar y reconocer cada segmento de manera exclusiva. A partir de esto, se pueden identificar segmentos perdidos.

El ISN no comienza en uno, pero es efectivamente un número aleatorio. Esto permite evitar ciertos tipos de ataques maliciosos. Para mayor simplicidad, usaremos un ISN de 1 para los ejemplos de este capítulo.

Los números de secuencia de segmento indican cómo reensamblar y reordenar los segmentos recibidos, como se muestra en la figura.

Los segmentos TCP se vuelven a ordenar en el destino



La figura muestra que, aunque los segmentos pueden tomar diferentes rutas y llegar fuera de servicio en el destino, TCP tiene la capacidad de reordenar los segmentos.

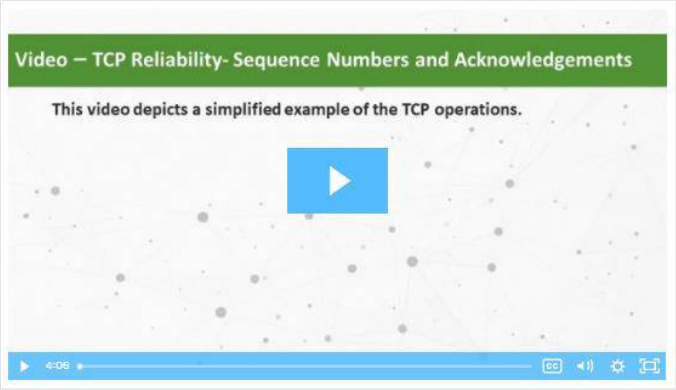
El proceso TCP receptor coloca los datos del segmento en un búfer de recepción. Los segmentos se colocan en el orden de secuencia adecuado y se pasan a la capa de aplicación cuando se vuelven a montar. Todos los segmentos que lleguen con números de secuencia desordenados se retienen para su posterior procesamiento. A continuación, cuando llegan los segmentos con bytes faltantes, tales segmentos se procesan en orden.

14.6.2

Video: Confiabilidad de TCP: números de secuencia y acuses de recibo

Una de las funciones de TCP es garantizar que cada segmento llegue a su destino. Los servicios TCP en el host de destino reconocen los datos que ha recibido la aplicación de origen.

Haga clic en Reproducir en la figura para ver una lección acerca de los reconocimientos y los números de secuencia TCP.

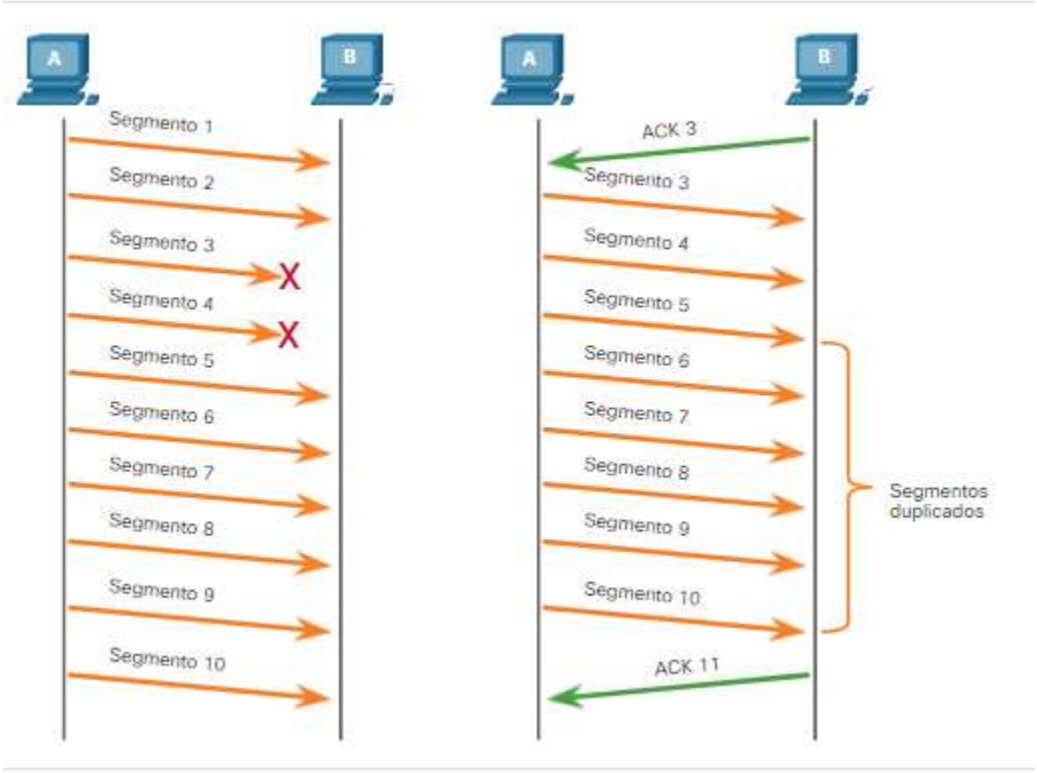


14.6.3

Fiabilidad de TCP: pérdida y retransmisión de datos

No importa cuán bien diseñada esté una red, ocasionalmente se produce la pérdida de datos. TCP proporciona métodos para administrar la pérdida de segmentos. Entre estos está un mecanismo para retransmitir segmentos para los datos sin reconocimiento.

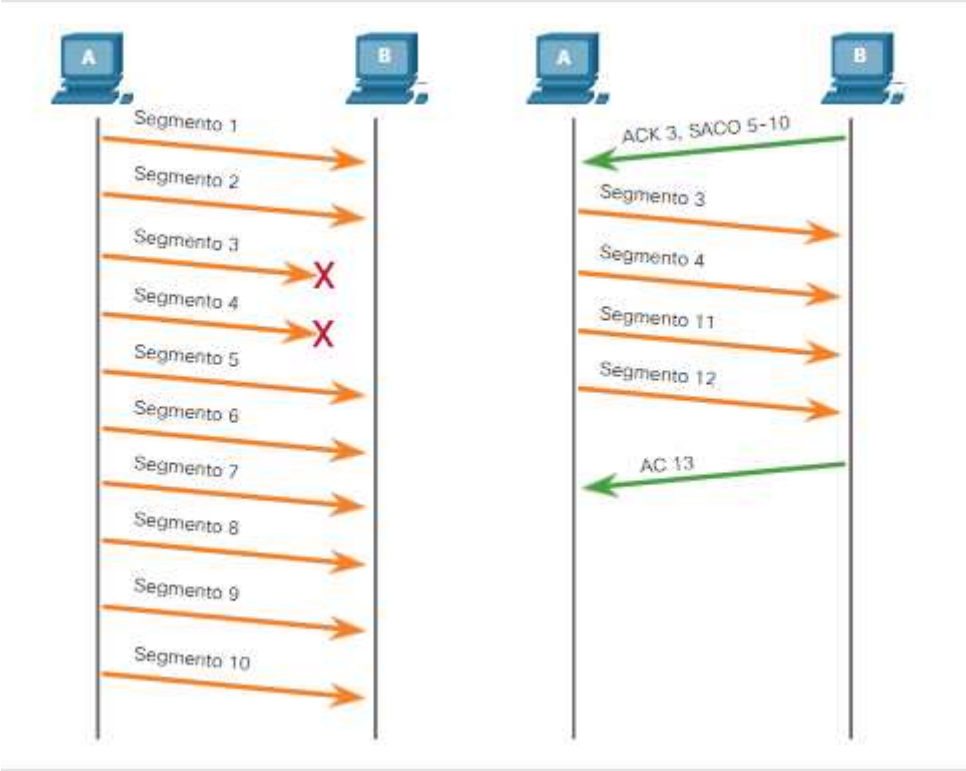
Antes de mejoras posteriores, TCP solo podía reconocer el siguiente byte esperado. Por ejemplo, en la figura, utilizando números de segmento para simplificar, el host A envía los segmentos del 1 al 10 al host B. Si llegan todos los segmentos excepto los segmentos 3 y 4, el host B respondería con acuse de recibo especificando que el siguiente segmento esperado es el segmento 3. El anfitrión A no tiene idea de si algún otro segmento llegó o no. Por lo tanto, el host A reenviaría los segmentos 3 a 10. Si todos los segmentos de reenvío llegan correctamente, los segmentos 5 a 10 serían duplicados. Esto puede provocar retrasos, congestión e ineficiencias.



Muestra PCA enviando 10 segmentos a PCB, pero los segmentos 3 y 4 no llegan. Así que a partir del segmento 3, PCA vuelve a enviar los segmentos 3 a 10, aunque la PCB solo necesitaba los segmentos 3 y 4.

Los sistemas operativos host actualmente suelen emplear una característica TCP opcional llamada reconocimiento selectivo (SACK), negociada durante el protocolo de enlace de tres vías. Si ambos hosts admiten SACK, el receptor puede reconocer explícitamente qué segmentos (bytes) se recibieron, incluidos los segmentos discontinuos. Por lo tanto, el host remitente solo necesitaría retransmitir los datos faltantes. Por ejemplo, en la siguiente figura, utilizando de nuevo números de segmento para simplificar, el host A envía los segmentos 1 a 10 al host B. Si llegan todos los segmentos excepto los segmentos 3 y 4, el host B puede

reconocer que ha recibido los segmentos 1 y 2 (ACK 3) y reconocer selectivamente los segmentos 5 a 10 (SACK 5-10). El host A solo necesitaría reenviar los segmentos 3 y 4.



Muestra PCA enviando 10 segmentos a PCB, pero los segmentos 3 y 4 no llegan. Esta vez PCB envía un ack 3 y un saco 5-10 para que PCA sepa reenviar los segmentos faltantes 3 y 4 y continuar con el segmento 11.

Nota: TCP normalmente envía ACK para cada otro paquete, pero otros factores más allá del alcance de este tema pueden alterar este comportamiento.

TCP utiliza temporizadores para saber cuánto tiempo debe esperar antes de reenviar un segmento. En la figura, reproduzca el vídeo y haga clic en el enlace para descargar el archivo PDF. El vídeo y el archivo PDF examinan la pérdida y la retransmisión de datos.

14.6.4

Video: Confiabilidad de TCP: Pérdida y retransmisión de datos

Haga clic en Reproducir en la figura para ver una lección acerca de la retransmisión TCP.

14.6.5

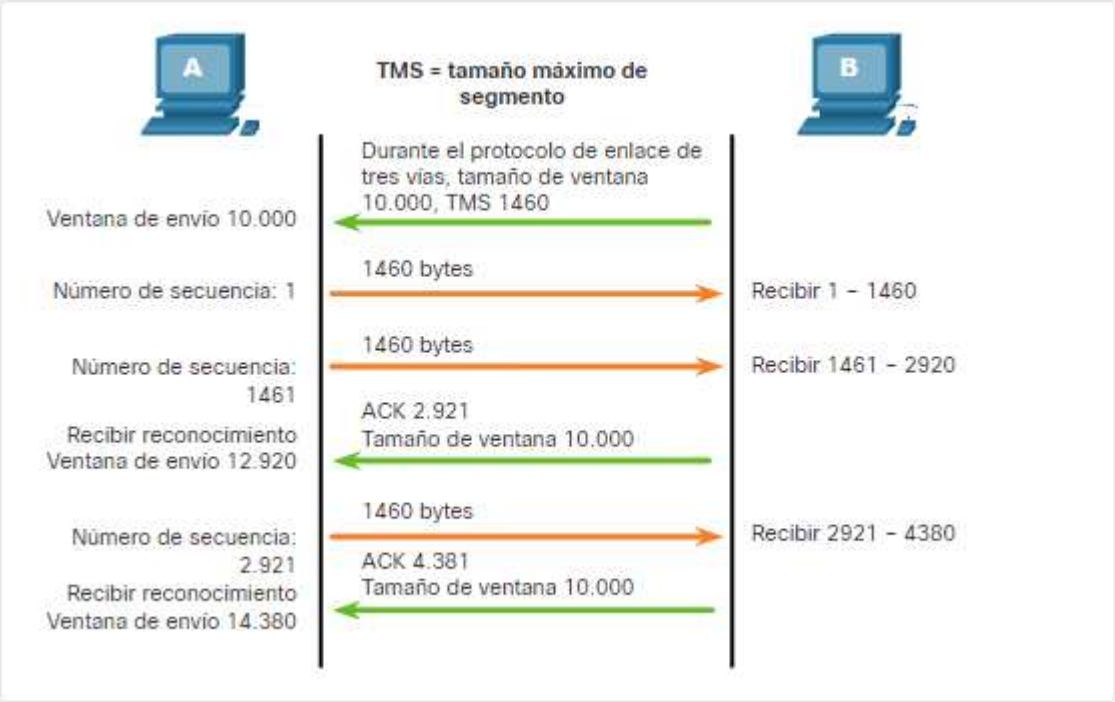
Control de flujo de TCP: tamaño de la ventana y reconocimientos

TCP también proporciona mecanismos para el control de flujo. El control de flujo es la cantidad de datos que el destino puede recibir y procesar de manera confiable. El control de flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada. Para lograr esto, el encabezado TCP incluye un campo de 16 bits llamado “tamaño de la ventana”.

En la figura, se muestra un ejemplo de tamaño de ventana y reconocimientos.

muestra el PCB que envía PCA un tamaño de ventana negociado de 10.000 bytes y un tamaño máximo de segmento de 1.460 bytes. PCA comienza a enviar segmentos comenzando con la secuencia número 1. Se puede enviar una confirmación de PCB sin esperar hasta que se alcance el tamaño de la ventana y el tamaño de la ventana se puede ajustar mediante PCA creando una ventana deslizante

Ejemplo de tamaño de ventana de TCP



El tamaño de la ventana determina la cantidad de bytes que se pueden enviar para recibir un reconocimiento. El número de reconocimiento es el número del siguiente byte esperado.

El tamaño de ventana es la cantidad de bytes que el dispositivo de destino de una sesión TCP puede aceptar y procesar al mismo tiempo. En este ejemplo, el tamaño de la ventana inicial de la PC B para la sesión TCP es de 10,000 bytes. A partir del primer byte, el byte1, el último byte que la PC A puede enviar sin recibir un reconocimiento es el byte 10000. Esto se conoce como la ventana de envío de la PC A. El tamaño de la ventana se incluye en cada segmento TCP para que el destino pueda modificar el tamaño de la ventana en cualquier momento dependiendo de la disponibilidad del búfer.

El tamaño inicial de la ventana se acuerda cuando se establece la sesión TCP durante la realización del enlace de tres vías. El dispositivo de origen debe limitar el número de bytes enviados al dispositivo de destino en función del tamaño de la ventana del destino. El dispositivo de origen puede continuar enviando más datos para la sesión solo cuando obtiene un reconocimiento de los bytes recibidos. Por lo general, el destino no esperará que se reciban todos los bytes de su tamaño de ventana antes de contestar con un acuse de recibo. A medida que se reciben y procesan los bytes, el destino envía reconocimientos para informar al origen que puede continuar enviando bytes adicionales.

Por ejemplo, es típico que la PC B no espere hasta que se hayan recibido los 10,000 bytes antes de enviar un acuse de recibo. Esto significa que la PC A puede ajustar su ventana de envío a medida que recibe confirmaciones de la PC B. Como se muestra en la figura, cuando

la PC A recibe una confirmación con el número de confirmación 2,921, que es el siguiente byte esperado. La ventana de envío de PC A incrementará 2.920 bytes. Esto cambia la ventana de envío de 10.000 bytes a 12.920. Esto significa que la PC A puede ajustar su ventana de envío a medida que recibe confirmaciones de la PC B. Como se muestra en la figura, cuando la PC A recibe una confirmación con el número de confirmación 2,921, que es el siguiente byte esperado.

Un destino que envía confirmaciones a medida que procesa los bytes recibidos, y el ajuste continuo de la ventana de envío de origen, se conoce como ventanas deslizantes. En el ejemplo anterior, la ventana de envío del PC A aumenta o se desliza sobre otros 2.921 bytes de 10.000 a 12.920.

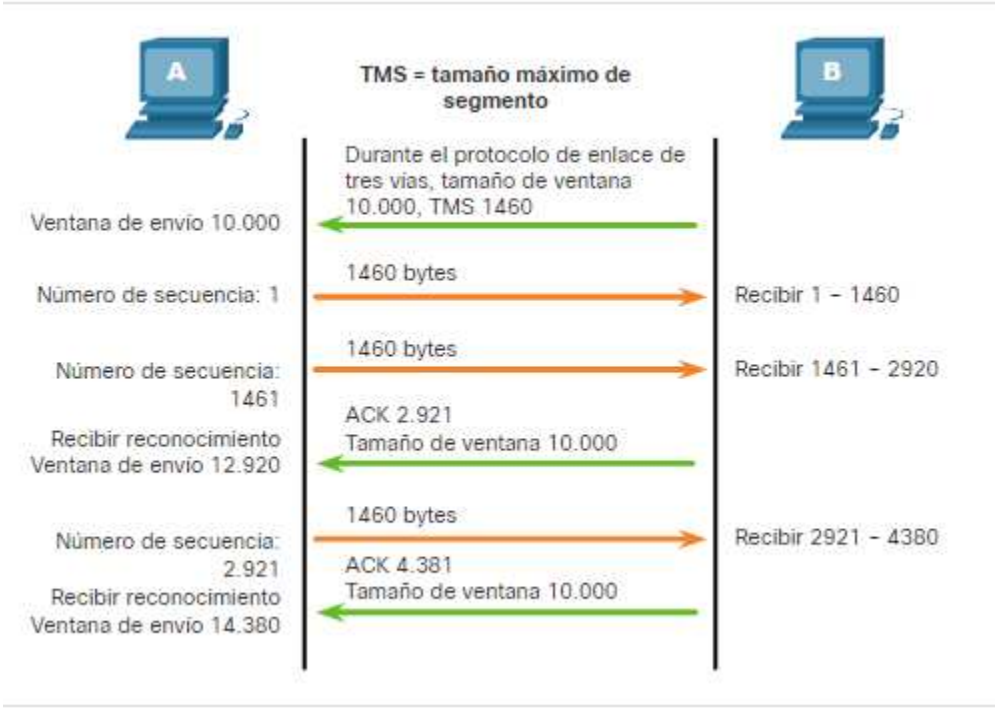
Si disminuye la disponibilidad de espacio de búfer del destino, puede reducir su tamaño de ventana para informar al origen que reduzca el número de bytes que debe enviar sin recibir un reconocimiento.

Nota: Los dispositivos de hoy usan el protocolo de ventanas deslizantes. El receptor generalmente envía un acuse de recibo después de cada dos segmentos que recibe. El número de segmentos recibidos antes de que se acuse recibo puede variar. La ventaja de las ventanas deslizantes es que permiten que el emisor transmita continuamente segmentos mientras el receptor está acusando recibo de los segmentos anteriores. Los detalles de las ventanas deslizantes exceden el ámbito de este curso.

14.6.6

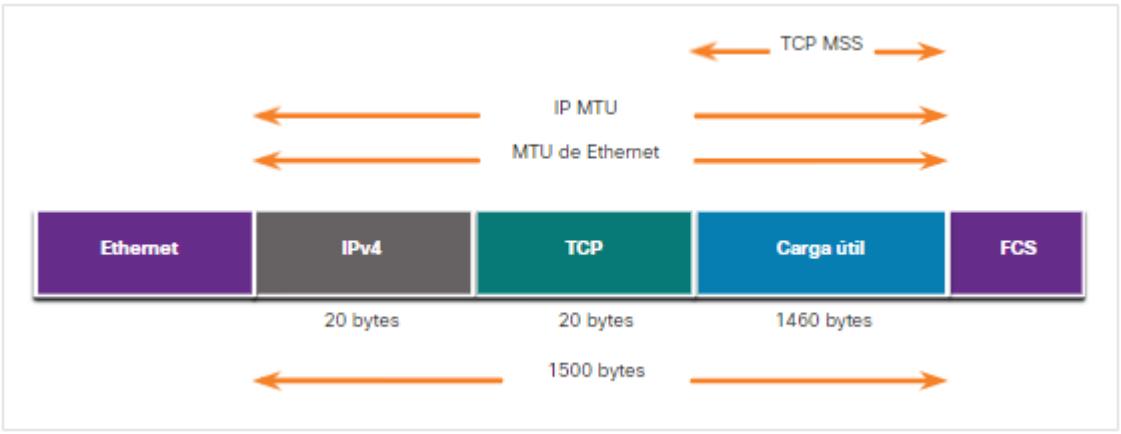
Control de flujo TCP - Tamaño máximo de segmento (MSS)

En la figura, la fuente está transmitiendo 1.460 bytes de datos dentro de cada segmento TCP. Normalmente, es el tamaño máximo de segmento (MSS) que puede recibir el dispositivo de destino. El MSS forma parte del campo de opciones del encabezado TCP que especifica la mayor cantidad de datos, en bytes, que un dispositivo puede recibir en un único segmento TCP. El tamaño MSS no incluye el encabezado TCP. El MSS se incluye normalmente durante el apretón de manos de tres vías.



Muestra el mismo diagrama que antes, pero el énfasis está en el MSS de tamaño máximo de segmento de 1460.

Un MSS común es de 1.460 bytes cuando se usa IPv4. Un host determina el valor de su campo de MSS restando los encabezados IP y TCP de unidad máxima de transmisión (MTU) de Ethernet. En una interfaz de Ethernet, el MTU predeterminado es de 1500 bytes. Restando el encabezado IPv4 de 20 bytes y el encabezado TCP de 20 bytes, el tamaño predeterminado de MSS será 1460 bytes, como se muestra en la figura.



Muestra un diagrama de un marco Ethernet completo del cual la MTU es 1500 bytes, con 20 bytes siendo el encabezado IP, y 20 bytes siendo el encabezado TCP, esto deja 1460 bytes que es el tamaño máximo del segmento TCP MSS.

14.6.7

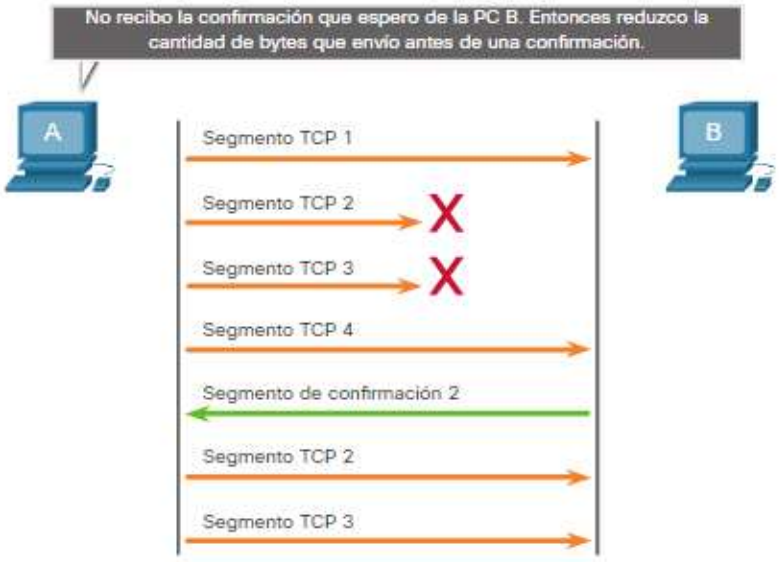
Control de flujo de TCP: prevención de congestiones

Cuando se produce congestión en una red, el router sobrecargado comienza a descartar paquetes. Cuando los paquetes que contienen segmentos TCP no llegan a su destino, se dejan sin confirmar. Mediante la determinación de la tasa a la que se envían pero no se reconocen los segmentos TCP, el origen puede asumir un cierto nivel de congestión de la red.

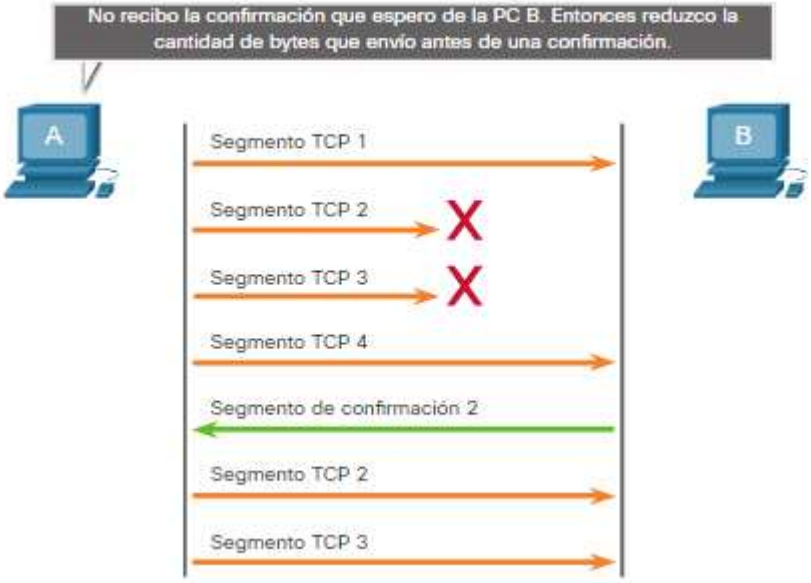
Siempre que haya congestión, se producirá la retransmisión de los segmentos TCP perdidos del origen. Si la retransmisión no se controla adecuadamente, la retransmisión adicional de los segmentos TCP puede empeorar aún más la congestión. No sólo se introducen en la red los nuevos paquetes con segmentos TCP, sino que el efecto de retroalimentación de los segmentos TCP retransmitidos que se perdieron también se sumará a la congestión. Para evitar y controlar la congestión, TCP emplea varios mecanismos, temporizadores y algoritmos de manejo de la congestión.

Si el origen determina que los segmentos TCP no están siendo reconocidos o que sí son reconocidos pero no de una manera oportuna, entonces puede reducir el número de bytes que envía antes de recibir un reconocimiento. Como se ilustra en la figura, PC A detecta que hay congestión y, por lo tanto, reduce el número de bytes que envía antes de recibir un acuse de recibo de PC B.

Control de congestión de TCP



Muestra PCA enviando segmentos a PCB donde los segmentos perdidos y la retransmisión pueden causar congestión.



Los números de acuse de recibo corresponden al siguiente byte esperado y no a un segmento. Los números de segmentos utilizados se simplifican con fines ilustrativos.

Tenga en cuenta que es el origen el que está reduciendo el número de bytes sin reconocimiento que envía y no el tamaño de ventana determinado por el destino.

Nota: Las explicaciones de los mecanismos reales de manejo de congestión, temporizadores y algoritmos están más allá del alcance de este curso.

14.6.8

Compruebe su comprensión - Fiabilidad y control de flujo

Compruebe su comprensión de la fiabilidad TCP y el proceso de control de flujo eligiendo la mejor respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El host de destino utiliza el campo de número de secuencia para volver a ensamblar segmentos en el orden original.
2. El campo Tamaño de ventana se utiliza para proporcionar control de flujo.
3. Cuando un host de envío detecta congestión, reduce el número de bytes que envía antes de recibir una confirmación del host de destino.

Has tenido 3 respuestas correctas de 3.

1. ¿Qué campo utiliza el host de destino para volver a ensamblar segmentos en el orden original?

¡Lo tienes!

- ( ) Bits de control
- ( ) Puerto de destino
- (•) Número de secuencia
- ( ) Puerto de origen
- ( ) Tamaño de la ventana

2. ¿Qué campo se utiliza para proporcionar control de flujo?

¡Lo tienes!

- ( ) Bits de control
- ( ) Puerto de destino
- ( ) Número de secuencia
- ( ) Puerto de origen
- (•) Tamaño de la ventana

3. ¿Qué sucede cuando un host de envío detecta que hay congestión?

¡Lo tienes!

- ( ) El host receptor aumenta el número de bytes que envía antes de recibir una confirmación del host remitente.
- ( ) El host receptor reduce el número de bytes que envía antes de recibir una confirmación del host remitente.
- ( ) El host de envío aumenta el número de bytes que envía antes de recibir una confirmación del host de destino.
- (•) El host de envío reduce el número de bytes que envía antes de recibir una confirmación del host de destino.

Correct

You have successfully identified the correct answers.

1. The sequence number field is used by the destination host to reassemble segments into the original order.
2. The Window Size field is used to provide flow control.
3. When a sending host senses congestion, it reduces the number of bytes it sends before receiving an acknowledgment from the destination host.

You got 3 out of 3 questions correct.

1. What field is used by the destination host to reassemble segments into the original order?

You got it!

- ○ Control Bits
- ○ Destination Port
- ◉ Sequence Number
- ○ Source Port
- ○ Window Size

2. What field is used to provide flow control?

You got it!

- ○ Control Bits
- ○ Destination Port
- ○ Sequence Number
- ○ Source Port
- ◉ Window Size

3. What happens when a sending host senses there is congestion?

You got it!

- ○ The receiving host increases the number of bytes it sends before receiving an acknowledgment from the sending host.
- ○ The receiving host reduces the number of bytes it sends before receiving an acknowledgment from the sending host.
- ○ The sending host increases the number of bytes it sends before receiving an acknowledgment from the destination host.
- ◉ The sending host reduces the number of bytes it sends before receiving an acknowledgment from the destination host.

Comunicación UDP

14.7.1

Comparación de baja sobrecarga y confiabilidad de UDP

Como se explicó anteriormente, UDP es perfecto para comunicaciones que necesitan ser rápidas, como VoIP. Este tema explica en detalle por qué UDP es perfecto para algunos tipos de transmisiones. Como se muestra en la figura, UDP no establece una conexión. UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.

Muestra un remitente de host que necesita enviar datos de voz y vídeo que se envían con UDP que no requiere una conexión negociada previa.

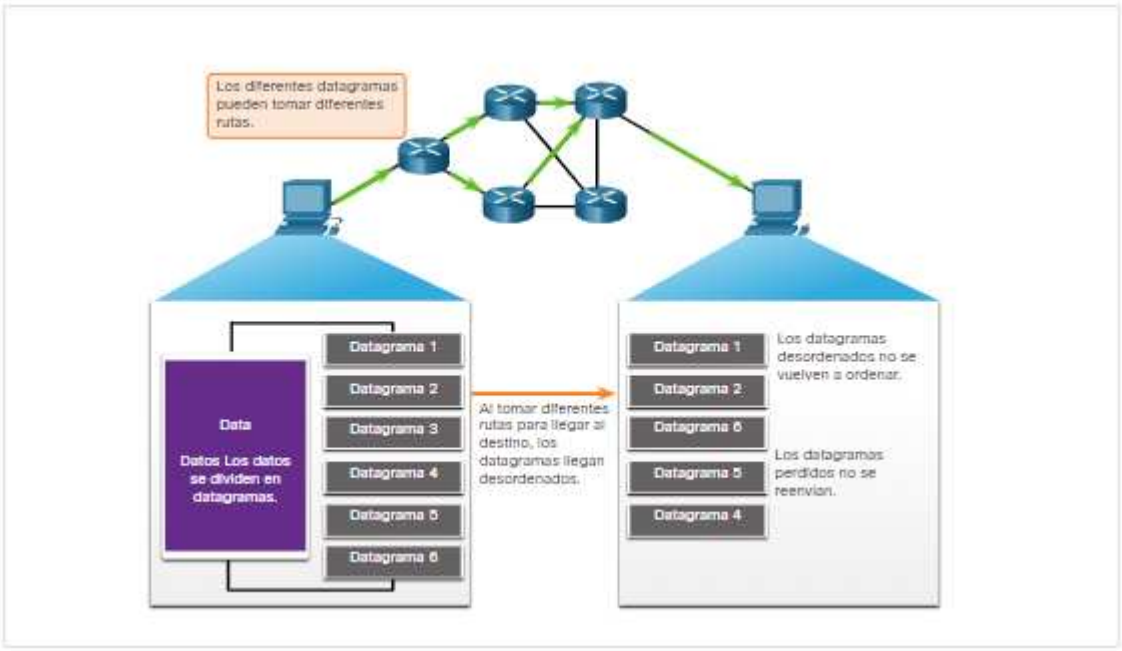
14.7.2

Reensamblaje de datagramas de UDP

Tal como los segmentos con TCP, cuando se envían datagramas UDP a un destino, a menudo toman diferentes rutas y llegan en el orden equivocado. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no tiene forma de reordenar datagramas en el orden en que se transmiten, como se muestra en la ilustración.

Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de datos es importante para la aplicación, esta debe identificar la secuencia adecuada y determinar cómo se deben procesar los datos.

UDP: sin conexión y poco confiable



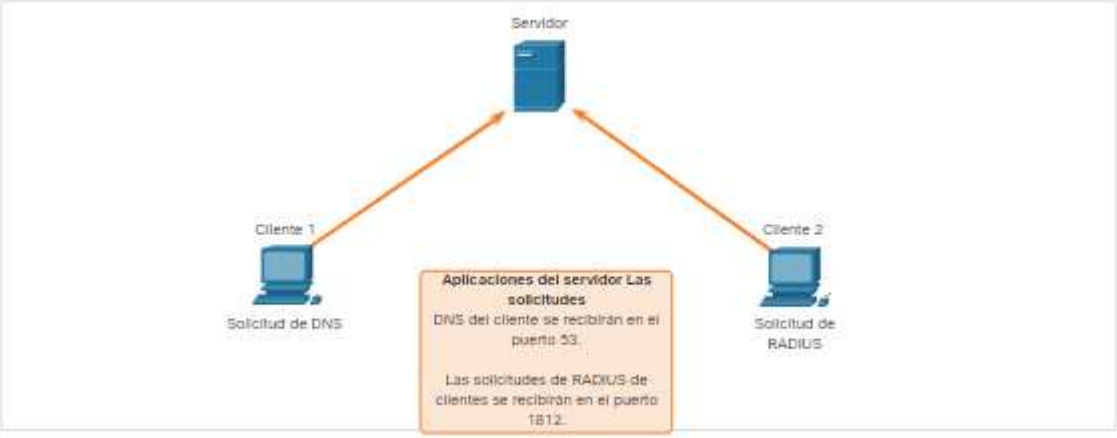
Muestra los datagramas UDP enviados en orden pero que llegan fuera de servicio debido a la posibilidad de diferentes rutas para llegar al destino.

14.7.3

Procesos y solicitudes del servidor UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asignan números de puerto conocidos o registrados, como se muestra en la figura. Cuando estas aplicaciones o estos procesos se ejecutan en un servidor, aceptan los datos que coinciden con el número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.

Servidor UDP a la escucha de solicitudes



Muestra que una aplicación de servidor RADIUS utiliza UDP para escuchar solicitudes en el puerto 53.

Nota: El servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) que se muestra en la figura proporciona servicios de autenticación, autorización y contabilidad para administrar el acceso de los usuarios. El funcionamiento de RADIUS está más allá del alcance de este curso.

14.7.4

Procesos de cliente UDP

Como en TCP, la comunicación cliente-servidor es iniciada por una aplicación cliente que solicita datos de un proceso de servidor. El proceso de cliente UDP selecciona dinámicamente un número de puerto del intervalo de números de puerto y lo utiliza como puerto de origen para la conversación. Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor.

Después de que un cliente ha seleccionado los puertos de origen y destino, se utiliza el mismo par de puertos en el encabezado de todos los datagramas en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

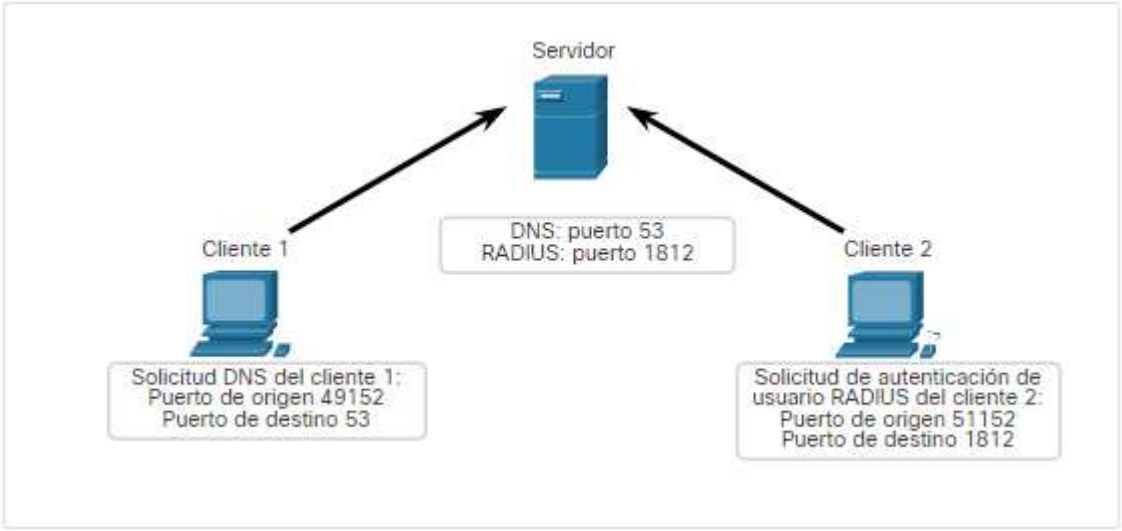
Haga clic en cada botón para obtener una ilustración de dos hosts que solicitan servicios del servidor de autenticación DNS y RADIUS.

Clientes que envían solicitudes UDP | Puertos de destino de solicitud UDP | Puertos de origen de solicitud UDP | Destino de respuesta UDP | Puertos de origen de respuesta UDP

Clientes Mandando Solicitudes UDP

El cliente 1 está enviando una solicitud DNS utilizando el conocido puerto 53, mientras que el cliente 2 solicita servicios de autenticación RADIUS mediante el puerto registrado 1812.

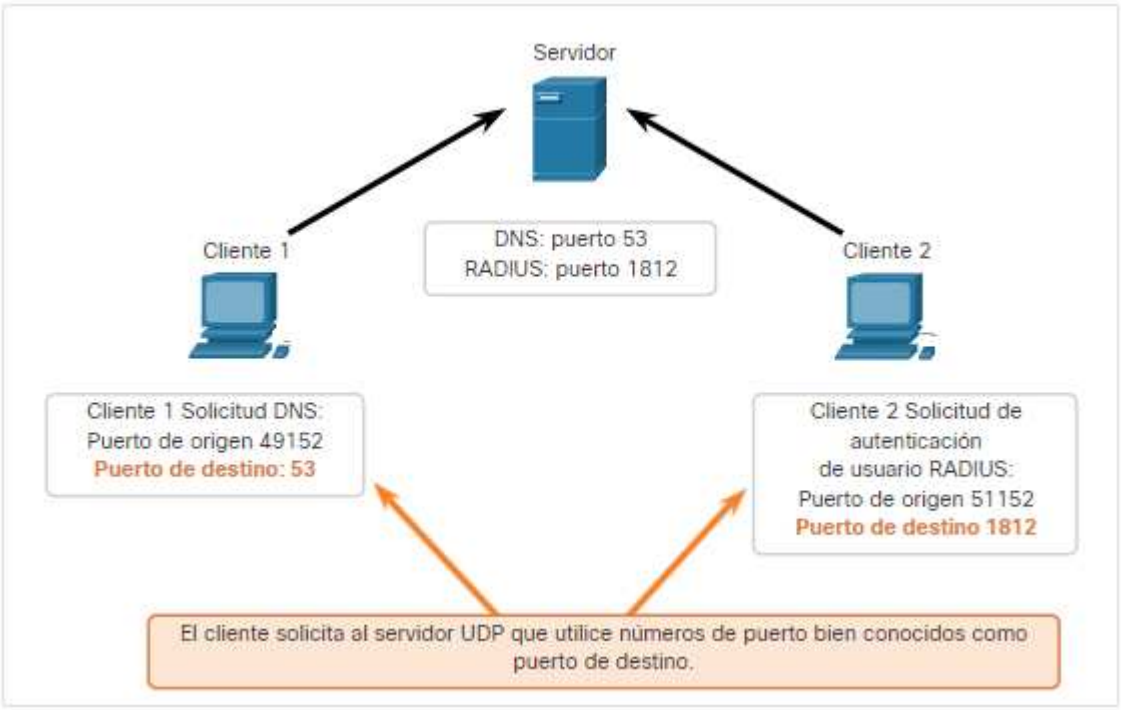
Dos clientes de PC diferentes necesitan realizar una solicitud a un servidor DNS



Clientes que envían solicitudes UDP | Puertos de destino de solicitud UDP | Puertos de origen de solicitud UDP | Destino de respuesta UDP | Puertos de origen de respuesta UDP

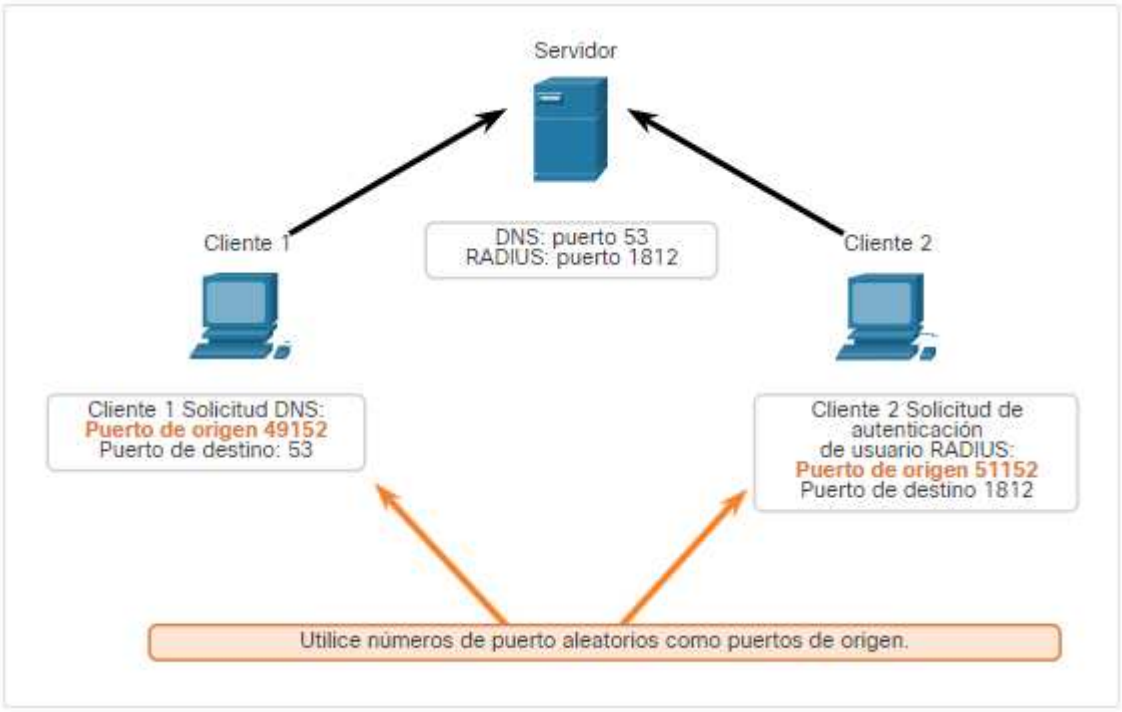
Solicitud UDP de Puertos de Origen

Las solicitudes de los clientes generan dinámicamente números de puerto de origen. En este caso, el cliente 1 está utilizando el puerto de origen 49152 y el cliente 2 está utilizando el puerto de origen 51152.



UDP Solicitud de Puertos de Origen

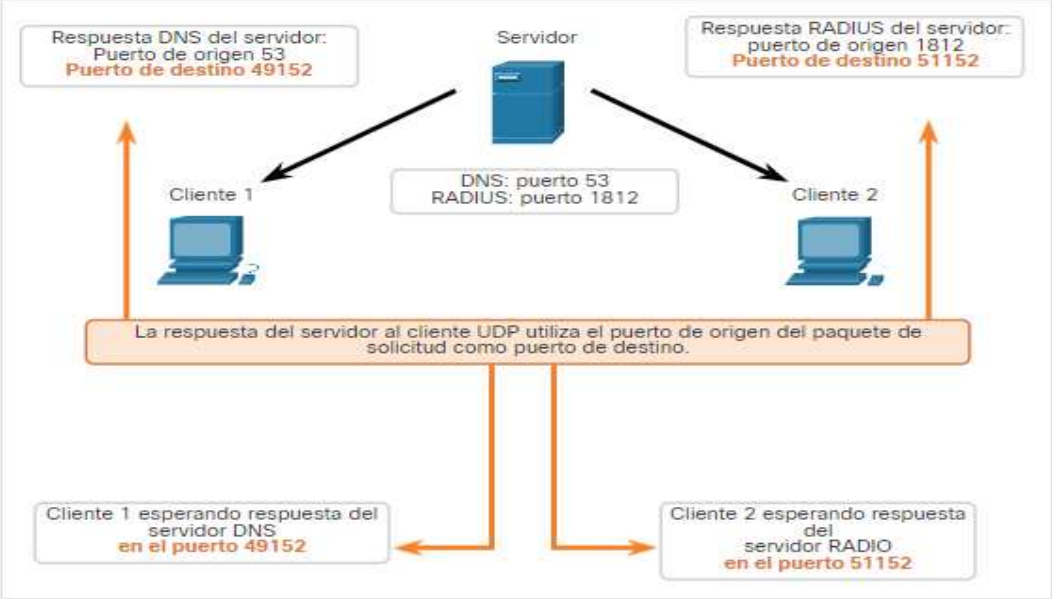
Cuando el servidor responde a las solicitudes del cliente, invierte los puertos de destino y origen de la solicitud inicial.



Clientes que envían solicitudes UDP | Puertos de destino de solicitud UDP | Puertos de origen de solicitud UDP | **Destino de respuesta UDP** | Puertos de origen de respuesta UDP

Destino de respuesta UDP

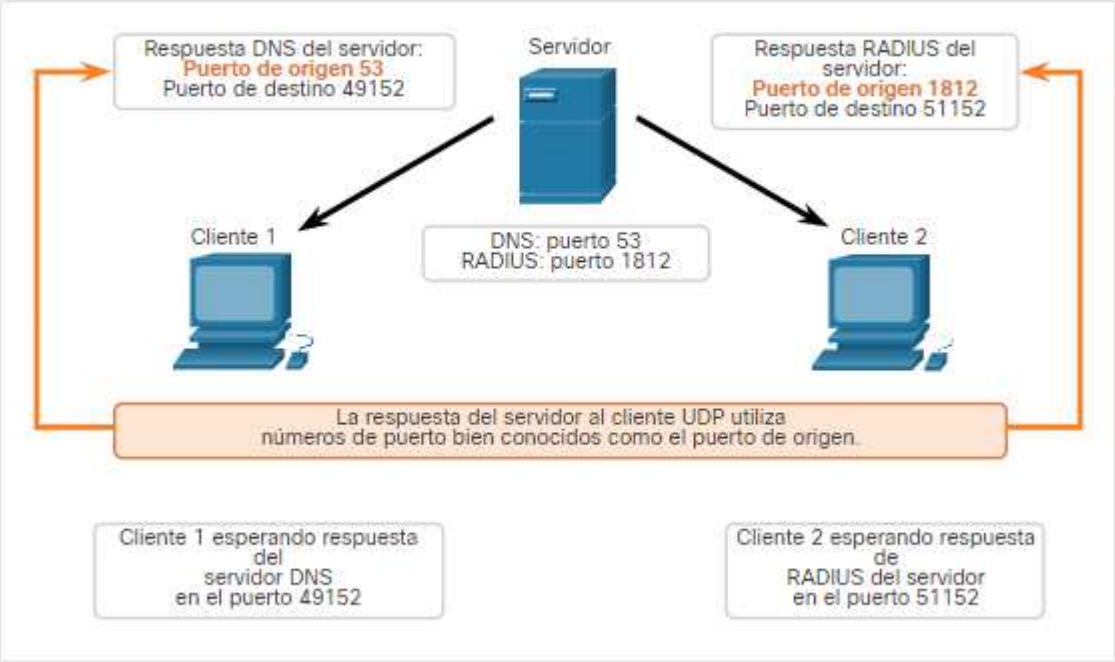
En la respuesta del servidor a la solicitud DNS ahora es el puerto de destino 49152 y la respuesta de autenticación RADIUS ahora es el puerto de destino 51152.



Clientes que envían solicitudes UDP	Puertos de destino de solicitud UDP	Puertos de origen de solicitud UDP	Destino de respuesta UDP	Puertos de origen de respuesta UDP

UDP Respuesta de Puertos de Origen

Los puertos de origen en la respuesta del servidor son los puertos de destino originales en las solicitudes iniciales.



14.7.5

Compruebe su comprensión - Comunicación UDP

Compruebe su comprensión de la comunicación UDP eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. UDP es deseable para los protocolos que realizan transacciones simples de solicitud y respuesta debido a su baja sobrecarga.
2. UDP vuelve a ensamblar los datos en el orden en que fueron recibidos.
3. Los puertos de origen y destino válidos correctos para un host que solicita el servicio DNS es Origen: 49152, Destino: 53.

Has tenido 3 respuestas correctas de 3.

1. ¿Por qué es conveniente UDP para los protocolos que hacen una simple solicitud y responden transacciones?

¡Lo tienes!

- ○ Control de flujo
- ◉ Baja sobrecarga
- ○ Confianza
- ○ Entrega en el mismo pedido

2. ¿Qué declaración de reensamblaje de datagramas UDP es verdadera?

¡Lo tienes!

- ○ UDP no vuelve a ensamblar los datos.
- ◉ UDP vuelve a ensamblar los datos en el orden en que fueron recibidos.
- ○ UDP vuelve a ensamblar los datos utilizando bits de control.
- ○ UDP vuelve a ensamblar los datos utilizando números de secuencia.

3. ¿Cuáles de los siguientes puertos serían válidos de origen y destino para un host que se conecta a un servidor DNS?

¡Lo tienes!

- ○ Fuente: 53, Destino: 49152
- ○ Fuente: 1812, Destino: 49152
- ◉ Fuente: 49152, Destino: 53
- ○ Fuente: 49152, Destino: 1812

Correct

You have successfully identified the correct answers.

1. UDP is desirable for protocols that make simple request and reply transactions because of its low overhead.
2. UDP reassembles the data in the order that it was received.
3. The correct valid source and destination ports for a host requesting DNS service is Source: 49152, Destination: 53.

You got 3 out of 3 questions correct.

1. Why is UDP desirable for protocols that make a simple request and reply transactions?

You got it!

- ○ Flow Control
- ◉ Low overhead
- ○ Reliability
- ○ Same-order delivery

2. Which UDP datagram reassembly statement is true?

You got it!

- ○ UDP does not reassemble the data.
- ◉ UDP reassembles the data in the order that it was received.
- ○ UDP reassembles the data using control bits.
- ○ UDP reassembles the data using sequence numbers.

3. Which of the following would be valid source and destination ports for a host connecting to a DNS server?

You got it!

- ○ Source: 53, Destination: 49152
- ○ Source: 1812, Destination: 49152
- ◉ Source: 49152, Destination: 53
- ○ Source: 49152, Destination: 1812

Capa de transporte / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

14.8.1

Packet Tracer: Comunicaciones de TCP y UDP

En esta actividad, explorará la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función de los números de puerto para determinar qué aplicación local solicitó los datos o los envía.

Comunicaciones de TCP y UDP

Comunicaciones de TCP y UDP

14.8.2

¿Qué aprenderé en este módulo?

Transportation of Data

La capa de transporte es el enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión a través de la red. La capa de transporte es responsable de las comunicaciones lógicas entre aplicaciones que se ejecutan en diferentes hosts. La capa de transporte incluye los protocolos TCP y UDP. Los protocolos de capa de transporte especifican cómo transferir mensajes entre hosts y es responsable de administrar los requisitos de fiabilidad de una conversación. La capa de transporte es responsable del seguimiento de conversaciones (sesiones), la segmentación de datos y el reensamblaje de segmentos, la adición de información de encabezado, la identificación de aplicaciones y la multiplexación de conversaciones. TCP is stateful, reliable, acknowledges data, resends lost data, and delivers data in sequenced order. Utilice TCP para el correo electrónico y la web. UDP no tiene estado, es rápido, tiene una sobrecarga baja, no requiere acuses de recibo, no reenvía los datos perdidos y entrega los datos en el orden en que llegan. Use UDP para VoIP y DNS.

Revisar TCP

TCP establece sesiones, asegura confiabilidad, proporciona entrega del mismo pedido y admite control de flujo. Un segmento TCP agrega 20 bytes de sobrecarga como información de encabezado al encapsular los datos de capa de aplicación. Los campos de encabezado TCP son los puertos de origen y destino, número de secuencia, número de reconocimiento, longitud del encabezado, reservado, bits de control, tamaño de ventana, suma de verificación y urgente. Las aplicaciones que usan TCP son HTTP, FTP, SMTP y Telnet.

Revisar UDP

UDP reconstruye los datos en el orden en que se reciben, los segmentos perdidos no se vuelven a enviar, no se establece la sesión y UPD no informa al remitente de la disponibilidad de recursos. Los campos de encabezado UDP son puertos de origen y destino, longitud y suma de verificación. Las aplicaciones que utilizan UDP son DHCP, DNS, SNMP, TFTP, VoIP y videoconferencias.

Número de Puertos

Los protocolos de capa de transporte TCP y UDP utilizan números de puerto para administrar múltiples conversaciones simultáneas. Esta es la razón por la que los campos de encabezado TCP y UDP identifican un número de puerto de aplicación de origen y destino. Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. Se conoce como socket a la combinación de la dirección IP de origen y el número de puerto de origen, o de la dirección IP de destino y el número de puerto de destino. El socket se utiliza para identificar el servidor y el servicio que solicita el cliente. Hay un rango de números de puerto entre 0 y 65535. Esta gama se divide en grupos: Puertos conocidos, Puertos Registrados, Puertos Privados y/o Dinámicos. Hay algunos números de puerto conocidos que están reservados para aplicaciones comunes como FTP, SSH, DNS, HTTP y otros. A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones.

Proceso de Comunicación TCP

Cada proceso de aplicación que se ejecuta en el servidor para utilizar un número de puerto. El número de puerto es asignado automáticamente o configurado manualmente por un administrador del sistema. Los procesos del servidor TCP son los siguientes: clientes que envían solicitudes TCP, solicitan puertos de destino, solicitan puertos de origen, responden a solicitudes de puerto de destino y puerto de origen. Para terminar una conversación simple admitida por TCP, se requieren cuatro intercambios para finalizar ambas sesiones. El cliente o el servidor pueden iniciar la terminación. El protocolo de enlace de tres vías establece que el dispositivo de destino está presente en la red, verifica que el dispositivo de destino tiene un servicio activo y acepta solicitudes en el número de puerto de destino que el cliente iniciador pretende utilizar, e informa al dispositivo de destino que el cliente de origen tiene la intención de establecer una sesión de comunicación sobre ese número de puerto. Los seis indicadores de bits de control son: URG, ACK, PSH, RST, SYN y FIN.

Fiabilidad y Control de Flujo

Para que el receptor comprenda el mensaje original, los datos en estos segmentos se vuelven a ensamblar en el orden original. Se asignan números de secuencia en el encabezado de cada paquete. No importa cuán bien diseñada esté una red, ocasionalmente se produce la pérdida de datos. TCP proporciona formas de administrar pérdidas de segmentos. Hay un mecanismo para retransmitir segmentos para datos no reconocidos. Los sistemas operativos host actualmente suelen emplear una característica TCP opcional llamada reconocimiento selectivo (SACK), negociada durante el protocolo de enlace de tres vías. Si ambos hosts admiten SACK, el receptor puede reconocer explícitamente qué segmentos (bytes) se recibieron, incluidos los segmentos discontinuos. Por lo tanto, el host emisor solo necesitaría retransmitir los datos faltantes. El control de flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino. Para lograr esto, el encabezado TCP incluye un campo de 16 bits llamado “tamaño de la ventana”. El proceso en el que el destino envía reconocimientos a medida que procesa los bytes recibidos y el ajuste continuo de la ventana de envío del origen se conoce como ventanas deslizantes. El origen está transmitiendo 1460 bytes de datos dentro de cada

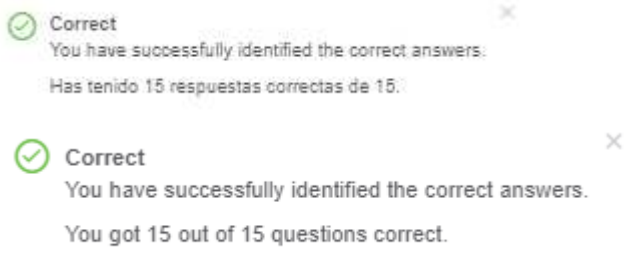
segmento TCP. Este es el MSS típico que puede recibir un dispositivo de destino. Para evitar y controlar la congestión, TCP emplea varios mecanismos de manejo de congestión. Es la fuente la que está reduciendo el número de bytes no reconocidos que envía y no el tamaño de ventana determinado por el destino.

Comunicación UDP

UDP es un protocolo simple que proporciona las funciones básicas de la capa de transporte. Cuando los datagramas UDP se envían a un destino, a menudo toman caminos diferentes y llegan en el orden incorrecto. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no puede reordenar los datagramas en el orden de la transmisión. UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de datos es importante para la aplicación, esta debe identificar la secuencia adecuada y determinar cómo se deben procesar los datos. A las aplicaciones de servidor basadas en UDP se les asignan números de puerto conocidos o registrados. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto. El proceso de cliente UDP selecciona dinámicamente un número de puerto del intervalo de números de puerto y lo utiliza como puerto de origen para la conversación. Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor. Después de que un cliente ha seleccionado los puertos de origen y destino, se utiliza el mismo par de puertos en el encabezado de todos los datagramas utilizados en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

14.8.3

Módulo Quiz - Capa de transporte



1. ¿Qué acción realiza un cliente al establecer la comunicación con un servidor mediante el uso de UDP en la capa de transporte?

Tema 14.7.0 - Dado que no es necesario establecer una sesión para UDP, el cliente selecciona un puerto de origen aleatorio para iniciar una conexión. El número de puerto aleatorio seleccionado se inserta en el campo de puerto de origen del encabezado UDP.

- El cliente establece el tamaño de ventana para la sesión.
- (•) El cliente envía un ISN al servidor para iniciar el protocolo de enlace de 3 vías.
- El cliente selecciona aleatoriamente un número de puerto de origen.
- El cliente envía un segmento de sincronización para comenzar la sesión.

2. ¿Qué entidad de capa de transporte se utiliza para garantizar el establecimiento de la sesión?

Tema 14.5.0 - TCP utiliza el protocolo de enlace de 3 vías.UDP no utiliza esta función. El protocolo de enlace de 3 vías garantiza la conectividad entre los dispositivos de origen y destino antes de que se produzca la transmisión.

- Indicador ACK UDP
- (•) Protocolo de enlace TCP de 3 vías
- Número de secuencia UDP
- Número de puerto TCP

3. ¿Cuál es la gama completa de puertos TCP y UDP conocidos?

Tema 14.4.0 - Hay tres rangos de puertos TCP y UDP. El rango bien conocido de números de puerto es de 0 a 1023.

- Entre 0 y 255
- (•) Entre 0 y 1023
- the combination of the source and destination sequence and acknowledgment numbers
- the combination of the source and destination sequence numbers and port numbers

4. ¿Qué es un socket?

Tema 14.4.0: un socket es una combinación de la dirección IP de origen y el puerto de origen o la dirección IP de destino y el número de puerto de destino.

- la combinación de la dirección IP de origen y destino y la dirección Ethernet de origen y destino
- (•) La combinación de una dirección IP de origen y un número de puerto o una dirección IP de destino y un número de puerto
- la combinación de la secuencia de origen y destino y los números de acuse de recibo
- la combinación de los números de secuencia de origen y destino y los números de puerto

5. ¿Cómo administra un servidor en red las solicitudes de varios clientes para diferentes servicios?

Tema 14.4.0 - Cada servicio proporcionado por un servidor, como el correo electrónico o las transferencias de archivos, utiliza un número de puerto específico. El número de puerto de origen de una solicitud de servicio identifica al cliente que solicita servicios. El número de puerto de destino identifica el servicio específico. Los servidores no utilizan información de direcciones para proporcionar servicios. Los enrutadores y conmutadores utilizan información de direccionamiento para mover el tráfico a través de la red.

- ○ El servidor envía todas las solicitudes a través de una puerta de enlace predeterminada.
- ○ A cada solicitud se les asignan números de puerto de origen y destino.
- ◉ El servidor utiliza direcciones IP para identificar diferentes servicios.
- ○ Cada solicitud se realiza un seguimiento a través de la dirección física del cliente.

6. ¿Cuáles son los dos servicios o protocolos que usan el protocolo UDP preferido para obtener transmisiones veloces y baja sobrecarga? Elija dos opciones.

Tema 14.3.0: tanto DNS como VoIP utilizan UDP para proporcionar bajos servicios generales dentro de una implementación de red.

- ◉ applications that are sensitive to delay
- ○ applications that need reliable delivery
- ○ applications that require retransmission of lost segments
- ○ applications that are sensitive to packet loss

7. ¿Cuál es el propósito de usar un número de puerto de origen en una comunicación TCP?

Tema 14.4.0 - El número de puerto de origen en un encabezado de segmento se utiliza para realizar un seguimiento de varias conversaciones entre dispositivos. También se utiliza para mantener una entrada abierta para la respuesta del servidor. Las opciones incorrectas están más relacionadas con el control de flujo y la entrega garantizada.

- ◉ para notificar al dispositivo remoto que la conversación ha terminado
- ○ para ensamblar los segmentos que llegaron fuera de servicio
- ○ para realizar un seguimiento de múltiples conversaciones entre dispositivos
- ○ para consultar un segmento no recibido

8. ¿Qué número o conjunto de números representa un socket?

Tema 14.4.0 - Un socket se define mediante la combinación de una dirección IP y un número de puerto, e identifica de forma única una comunicación en particular.

- ☐ identifying the applications
- ☑ acknowledging received data
- ☐ identifying individual conversations
- ☑ retransmitting any unacknowledged data
- ☐ reconstructing data in the order received

9. ¿Qué dos indicadores en el encabezado TCP se utilizan en un protocolo de enlace de tres vías TCP para establecer conectividad entre dos dispositivos de red? (Escoja dos opciones).

Tema 14.5.0 - TCP utiliza los indicadores SYN y ACK para establecer conectividad entre dos dispositivos de red.

- ○ to notify the remote device that the conversation is over
- ○ to assemble the segments that arrived out of order
- ◉ to keep track of multiple conversations between devices
- ○ to inquire for a nonreceived segment

10. ¿Qué sucede si parte de un mensaje FTP no se entrega al destino?

Tema 14.6.0 - Debido a que FTP utiliza TCP como protocolo de capa de transporte, los números de secuencia y confirmación identificarán los segmentos que faltan, que se volverán a enviar para completar el mensaje.

- ☑ El mensaje se pierde porque FTP no utiliza un método de entrega fiable.
- ☐ El host de origen FTP envía una consulta al host de destino.
- ☐ Se vuelve a enviar la parte del mensaje FTP que se perdió.
- ☐ Se vuelve a enviar el mensaje FTP completo.
- ☑ SYN
- ☐ URG

11. ¿Qué tipos de aplicaciones son los más adecuados para el uso de UDP?

Tema 14.3.0: UDP no es un protocolo orientado a la conexión y no proporciona mecanismos de retransmisión, secuenciación o control de flujo. Proporciona funciones básicas de capa de transporte con mucha menos sobrecarga que TCP. Una sobrecarga menor hace que UDP sea una aplicación adecuada para las aplicaciones sensibles a las demoras.

- ○ Las aplicaciones sensibles a las demoras
- ○ Las aplicaciones que necesitan una entrega confiable
- ○ Las aplicaciones que requieren la retransmisión de segmentos perdidos
- ◉ Las aplicaciones sensibles a la pérdida de paquetes

12. La congestión de la red hizo que el emisor Nota la pérdida de segmentos TCP que se enviaron a destino. ¿Cuál de las siguientes es una forma en la que el protocolo TCP intenta solucionar este problema?

Tema 14.6.0: si la fuente determina que los segmentos TCP no se reconocen o no se reconocen de manera oportuna, entonces puede reducir el número de bytes que envía antes de recibir un reconocimiento. En este proceso, no se modifica el tamaño de ventana en el encabezado del segmento. El origen no reduce el tamaño de ventana que se envía en el encabezado del segmento. El host de destino ajusta el tamaño de ventana en el encabezado del segmento cuando recibe datos más rápido de lo que los puede procesar, no cuando hay congestión de red.

- ○ El origen reduce la cantidad de datos que transmite antes de recibir un acuse de recibo del destino.
- ○ El origen reduce el tamaño de la ventana para reducir la velocidad de transmisión del destino.
- ◉ El destino reduce el tamaño de la ventana.
- ○ El destino envía menos cantidad de mensajes de acuse de recibo para conservar el ancho de banda.

13. ¿Qué dos operaciones son proporcionadas por TCP pero no por UDP? (Escoja dos opciones).

Tema 14.1.0 - Numeración y seguimiento de segmentos de datos, reconocimiento de datos recibidos y retransmisión de datos no reconocidos son operaciones de fiabilidad para garantizar que todos los datos lleguen al destino. UDP no proporciona confiabilidad. Tanto TCP como UDP identifican las aplicaciones y realizan un seguimiento de conversaciones individuales. UDP no cuenta los segmentos de datos y reconstruye los datos en el orden en que se reciben.

- [ ] Identificación de las aplicaciones
- [x] Acuse de recibo de los datos recibidos
- [ ] Seguimiento de conversaciones individuales
- [ ] Retransmisión de cualquier dato sin acuse de recibo.
- [x] reconstruir los datos en el orden recibido

14. ¿Cuál es el mecanismo TCP que se utiliza para evitar la congestión?

Tema 14.6.0: TCP utiliza ventanas para intentar administrar la velocidad de transmisión al flujo máximo que la red y el dispositivo de destino pueden soportar mientras minimiza la pérdida y las retransmisiones. Cuando está saturado de datos, el destino puede enviar una solicitud para reducir el tamaño de la ventana. Este método para evitar la congestión se denomina "ventanas deslizantes".

- ( ) Protocolo de enlace de tres vías
- ( ) Par de sockets
- (•) Protocolo de enlace de dos vías
- ( ) Ventana deslizante

15. ¿Cuál es la responsabilidad de los protocolos de capa de transporte?

Tema 14.1.0 - Hay tres responsabilidades principales para los protocolos de capa de transporte TCP y UDP:
- Seguimiento de conversaciones individuales
- Segmentación de datos y reensamblado de segmentos
- Identificación de las aplicaciones.

- ( ) proporcionar acceso a la red
- (•) Seguimiento de conversaciones individuales
- ( ) determinar la mejor ruta para reenviar un paquete
- ( ) traducción de direcciones IP privadas a direcciones IP públicas

1. Which transport layer feature is used to establish a connection-oriented session?

Topic 14.5.0 – TCP uses the 3-way handshake. UDP does not use this feature. The 3-way handshake ensures there is connectivity between the source and destination devices before transmission occurs.

- ○ UDP ACK flag
- ◉ TCP 3-way handshake
- ○ UDP sequence number
- ○ TCP port number

2. What is the complete range of TCP and UDP well-known ports?

Topic 14.4.0 – There are three ranges of TCP and UDP ports. The well-know range of port numbers is from 0 – 1023.

- ○ 0 to 255
- ◉ 0 to 1023
- ○ 256 – 1023
- ○ 1024 – 49151

3. What is a socket?

Topic 14.4.0 – A socket is a combination of the source IP address and source port or the destination IP address and the destination port number.

- ○ the combination of the source and destination IP address and source and destination Ethernet address
- ◉ the combination of a source IP address and port number or a destination IP address and port number
- ○ the combination of the source and destination sequence and acknowledgment numbers
- ○ the combination of the source and destination sequence numbers and port numbers

4. How does a networked server manage requests from multiple clients for different services?

Topic 14.4.0 – Each service provided by a server, such as email or file transfers, uses a specific port number. The source port number of a service request identifies the client that is requesting services. The destination port number identifies the specific service. Servers do not use address information to provide services. Routers and switches use addressing information to move traffic through the network.

- ○ The server sends all requests through a default gateway.
- ◉ Each request has a combination of source and destination port numbers, coming from a unique IP address.
- ○ The server uses IP addresses to identify different services.
- ○ Each request is tracked through the physical address of the client.

5. What happens if part of an FTP message is not delivered to the destination?

Topic 14.6.0 – Because FTP uses TCP as its transport layer protocol, sequence and acknowledgment numbers will identify the missing segments, which will be re-sent to complete the message.

- ○ The message is lost because FTP does not use a reliable delivery method.
- ○ The FTP source host sends a query to the destination host.
- ◉ The part of the FTP message that was lost is re-sent.
- ○ The entire FTP message is re-sent.

6. What type of applications are best suited for using UDP?

Topic 14.3.0 – UDP is not a connection-oriented protocol and does not provide retransmission, sequencing, or flow control mechanisms. It provides basic transport layer functions with a much lower overhead than TCP. Lower overhead makes UDP suitable for applications which are sensitive to delay.

- ◉ applications that are sensitive to delay
- ○ applications that need reliable delivery
- ○ applications that require retransmission of lost segments
- ○ applications that are sensitive to packet loss

7. Network congestion has resulted in the source learning of the loss of TCP segments that were sent to the destination. What is one way that the TCP protocol addresses this?

Topic 14.6.0 – If the source determines that the TCP segments are either not being acknowledged or are not acknowledged in a timely manner, then it can reduce the number of bytes it sends before receiving an acknowledgment. This does not involve changing the window in the segment header. The source does not decrease the window that is sent in the segment header. The window in the segment header is adjusted by the destination host when it is receiving data faster than it can process it, not when network congestion is encountered.

- (●) The source decreases the amount of data that it transmits before it receives an acknowledgement from the destination.
- ( ) The source decreases the window size to decrease the rate of transmission from the destination.
- ( ) The destination decreases the window size.
- ( ) The destination sends fewer acknowledgement messages in order to conserve bandwidth.

8. Which two operations are provided by TCP but not by UDP? (Choose two.)

Topic 14.1.0 – Numbering and tracking data segments, acknowledging received data, and retransmitting any unacknowledged data are reliability operations to ensure that all of the data arrives at the destination. UDP does not provide reliability. Both TCP and UDP identify the applications and track individual conversations. UDP does not number data segments and reconstructs data in the order that it is received.

- [ ] identifying the applications
- [x] acknowledging received data
- [ ] identifying individual conversations
- [x] retransmitting any unacknowledged data
- [ ] reconstructing data in the order received

9. What is the purpose of using a source port number in a TCP communication?

Topic 14.4.0 – The source port number in a segment header is used to keep track of multiple conversations between devices. It is also used to keep an open entry for the response from the server. The incorrect options are more related to flow control and guaranteed delivery.

- ( ) to notify the remote device that the conversation is over
- ( ) to assemble the segments that arrived out of order
- (●) to keep track of multiple conversations between devices
- ( ) to inquire for a nonreceived segment

10. Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)

Topic 14.5.0 – TCP uses the SYN and ACK flags in order to establish connectivity between two network devices.

- [x] ACK
- [ ] FIN
- [ ] PSH
- [ ] RST
- [x] SYN
- [ ] URG

11. What TCP mechanism is used to enhance performance by allowing a device to continuously send a steady stream of segments as long as the device is also receiving necessary acknowledgements?

Topic 14.6.0 – TCP uses windows to attempt to manage the rate of transmission to the maximum flow that the network and destination device can support while minimizing loss and retransmissions. When overwhelmed with data, the destination can send a request to reduce the of the window. The process of the destination sending acknowledgments as it processes bytes received and the continual adjustment of the source send window is known as sliding windows.

- ( ) three-way handshake
- ( ) socket pair
- ( ) two-way handshake
- (●) sliding window

12. Which action is performed by a client when establishing communication with a server via the use of UDP at the transport layer?

Topic 14.7.0 - Because a session does not have to be established for UDP, the client selects a random source port to begin a connection. The random port number selected is inserted into the source port field of the UDP header.

- ○ The client sets the window size for the session.
- ○ The client sends an ISN to the server to start the 3-way handshake.
- ◉ The client randomly selects a source port number.
- ○ The client sends a synchronization segment to begin the session.

13. Which two services or protocols use the preferred UDP protocol for fast transmission and low overhead? (Choose two)

Topic 14.3.0 - Both DNS and VoIP use UDP to provide low overhead services within a network implementation.

- ☐ FTP
- ☑ DNS
- ☐ HTTP
- ☐ POP3
- ☑ VoIP

14. Which number or set of numbers represents a socket?

Topic 14.4.0 - A socket is defined by the combination of an IP address and a port number, and uniquely identifies a particular communication.

- ○ 01-23-45-67-89-AB
- ○ 21
- ◉ 192.168.1.1:80
- ○ 10.1.1.15

15. What is a responsibility of transport layer protocols?

Topic 14.1.0 - There are three main responsibilities for transport layer protocols TCP and UDP:
- Tracking individual conversations
- Segmenting data and reassembling segments
- Identifying the applications

- ○ providing network access
- ◉ tracking individual conversations
- ○ determining the best path to forward a packet
- ○ translating private IP addresses to public IP addresses

Capítulo 15_Capa de aplicación

Introducción

15.0.1

¿Por qué debería tomar este módulo?

Bienvenido a la Capa de aplicación

Como ha aprendido, la capa de transporte es donde los datos se mueven realmente de un host a otro. Pero antes de que eso pueda tener lugar, hay muchos detalles que deben determinarse para que este transporte de datos ocurra correctamente. Esta es la razón por la que hay una capa de aplicación tanto en los modelos OSI como en los modelos TCP/IP. Como ejemplo, antes de que hubiera streaming de vídeo a través de Internet, teníamos que ver películas caseras de una variedad de otras maneras. Imagina que grabaste algún partido de fútbol de tu hijo. Tus padres, en otra ciudad, sólo tienen un videograbador. Tienes que copiar el vídeo de tu cámara en el tipo correcto de casete para enviarlos. Tu hermano tiene un reproductor de DVD, por lo que transfieres tu video a un DVD para enviarlo. De esto se trata la capa de aplicación, asegurándose de que los datos estén en un formato que el dispositivo receptor pueda usar. ¡Vamos a bucear!

15.0.2

¿Qué aprenderé en este módulo?

**Título del módulo: Capa de aplicación

Objetivos del módulo: Explique el funcionamiento de los protocolos de la capa de aplicación en cuanto a dar soporte a las aplicaciones de usuario final.

Título del tema	Objetivo del tema
Aplicación, presentación y sesión	Explicar cómo las funciones de la capa de aplicación, capa de presentación, y la capa de sesión trabajan juntos para proporcionar servicios de red al usuario final aplicaciones de SP y empresariales.
Entre pares	Explique cómo funcionan las aplicaciones de usuario final en una red punto a punto.
Protocolos web y de correo electrónico	Explique la forma en que funcionan los protocolos web y de correo electrónico.

Título del tema	Objetivo del tema
Servicios de direccionamiento IP	Explique cómo funcionan de DNS y DHCP.
Servicios de intercambio de archivos	Explique la forma en que funcionan los protocolos de transferencia de archivos.

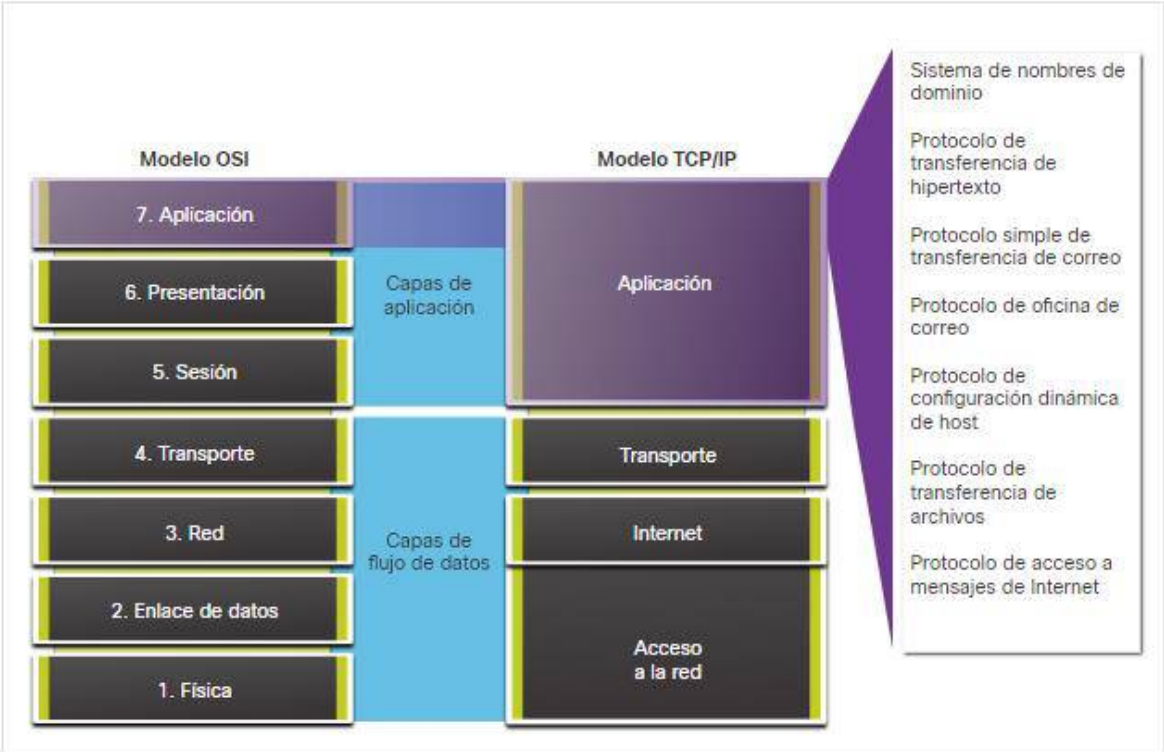
Capa de aplicación / Aplicación, presentación y sesión

Aplicación, presentación y sesión

15.1.1

Capa de aplicación

En los modelos OSI y TCP/IP La capa de aplicación es la más cercana al usuario final. Como se muestra en la figura, es la capa que proporciona la interfaz entre las aplicaciones utilizada para la comunicación y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino.



La figura es una comparación de las capas de modelo OSI y TCP/IP. El modelo OSI se muestra a la izquierda. De arriba a abajo se encuentran los siguientes números de capa y nombres: 7) Aplicación, 6) Presentación, 5) Sesión, 4) Transporte, 3) Red, 2) Enlace de datos y 1) Física. El modelo TCP/IP se muestra a la derecha. De arriba a abajo, los nombres de capa y los números de capa del modelo OSI asociados son: Aplicación (Capas OSI 7, 6 y 5), Transporte (Capa OSI 4), Internet (Capa OSI 3) y Acceso de red (Capas OSI 2 y 1). El texto al pie de la figura dice que Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en el que se relacionan con las capas que están por encima y por debajo de cada capa. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork. La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes. Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores. Entre las aplicaciones de ejemplo de la capa de aplicación del modelo OSI se incluyen el sistema de nombres de dominio, el protocolo de transferencia de hipertexto, el protocolo simple de transferencia de correo, el protocolo de oficina de correos, el protocolo de configuración dinámica de host, el protocolo de transferencia de archivo y el protocolo de acceso a mensajes de Internet.

Basado en el modelo TCP/IP Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) definen funciones de la capa de aplicación TCP/IP única.

Existen muchos protocolos de capa de aplicación, y están en constante desarrollo. Algunos de los protocolos de capa de aplicación más conocidos incluyen el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP), el protocolo trivial de transferencia de archivos (TFTP), el protocolo de acceso a mensajes de Internet (IMAP) y el protocolo del sistema de nombres de dominios (DNS).

15.1.2

Capa de presentación y sesión

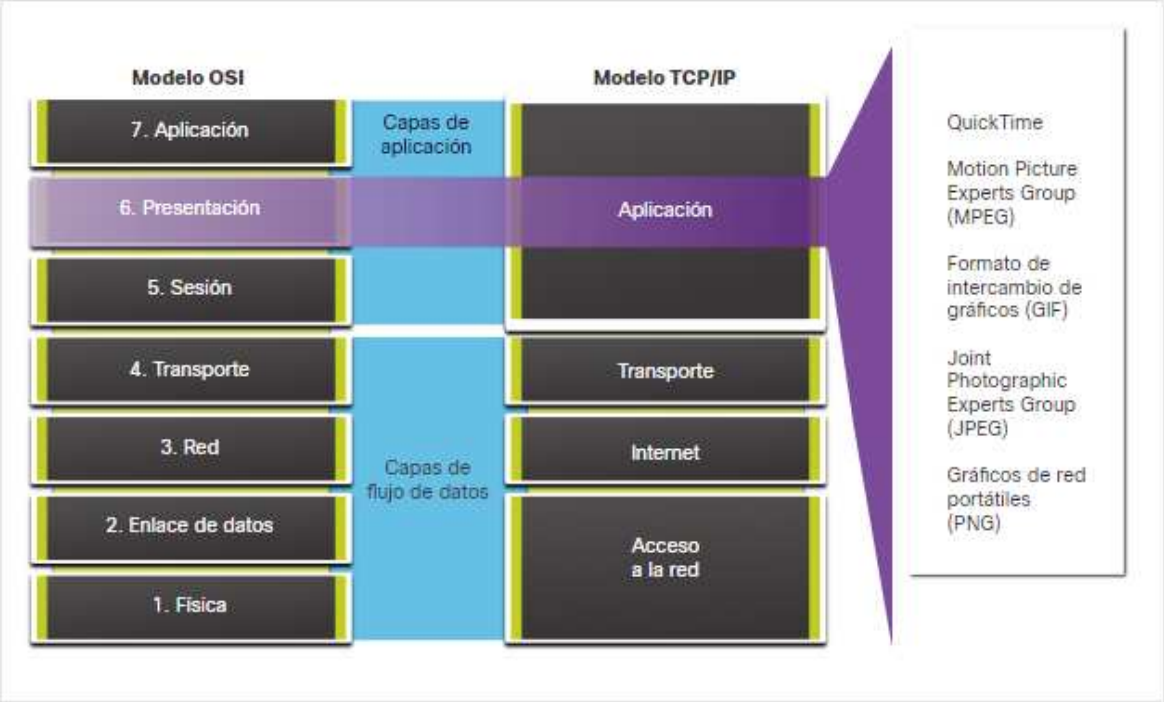
Presentation Layer

La capa de presentación tiene tres funciones principales:

- Dar formato a los datos del dispositivo de origen, o presentarlos, en una forma compatible para que lo reciba el dispositivo de destino.
- Comprimir los datos de forma tal que los pueda descomprimir el dispositivo de destino.

- Cifrar los datos para transmitirlos y descifrarlos al recibirlos.

Como se muestra en la ilustración, la capa de presentación da formato a los datos para la capa de aplicación y establece estándares para los formatos de archivo. Dentro de los estándares más conocidos para vídeo encontramos QuickTime y el Grupo de expertos en películas (MPEG). Entre los formatos gráficos de imagen conocidos que se utilizan en redes, se incluyen los siguientes: formato de intercambio de gráficos (GIF), formato del Joint Photographic Experts Group (JPEG) y formato de gráficos de red portátiles (PNG).



La figura es una comparación de las capas de modelo OSI y TCP/IP. El modelo OSI se muestra a la izquierda. De arriba a abajo se encuentran los siguientes números de capa y nombres: 7) Aplicación, 6) Presentación, 5) Sesión, 4) Transporte, 3) Red, 2) Enlace de datos y 1) Física. El modelo TCP/IP se muestra a la derecha. De arriba a abajo, los nombres de capa y los números de capa del modelo OSI asociados son: Aplicación (Capas OSI 7, 6 y 5), Transporte (Capa OSI 4), Internet (Capa OSI 3) y Acceso de red (Capas OSI 2 y 1). El texto al pie de la figura dice que Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en el que se relacionan con las capas que están por encima y por debajo de cada capa. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork. La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes. Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente

en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores. Entre los ejemplos para la capa de presentación del modelo OSI, se incluyen Quick Time, Motion Picture Experts Group (MPEG), formato de intercambio de gráficos (GIF), Joint Photographic Experts Group (JPEG) y gráficos de red portátiles (PNG).

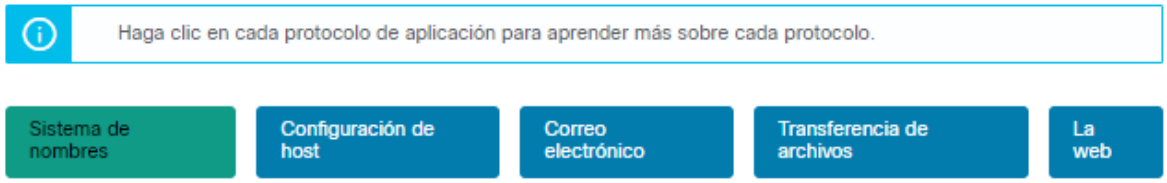
Capa de Sesión

Como su nombre lo indica, las funciones de la capa de sesión crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado.

15.1.3

Protocolos de capa de aplicación de TCP/IP

Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet. Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones se lleven a cabo correctamente, los protocolos de capa de aplicación que se implementaron en los hosts de origen y de destino deben ser compatibles.



Name System

DNS - Domain Name System (or Service)

- TCP, UDP cliente 53
- Traduce los nombres de dominio tales como cisco.com a direcciones IP

Host Config

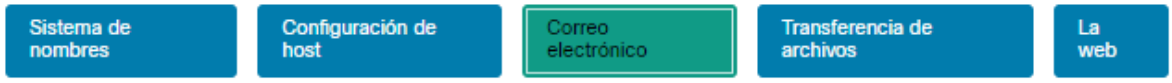
BOOTP - Bootstrap Protocol

Cliente* UDP 68, servidor 67

- Permite que una estación de trabajo sin disco obtenga su propia dirección IP, la dirección IP de un servidor BOOTP en la red y un archivo que se debe cargar en la memoria para arrancar la máquina.
- El protocolo DHCP reemplaza al protocolo BOOTP.

DHCP - Dynamic Host Configuration Protocol

- Cliente UDP 68, servidor 67
- Permite que las direcciones vuelvan a utilizarse cuando ya no son necesarias



Email

SMTP - Simple Mail Transfer Protocol

- TCP 25
- Permite a los clientes enviar correo electrónico a un servidor de correo.
- Permite a los servidores enviar correo electrónico a otros servidores.

POP3 - Post Office Protocol

- TCP 110
- Permite a los clientes recibir correo electrónico de un servidor de correo.
- Descarga el correo electrónico a la aplicación de correo local del cliente

IMAP - Internet Message Access Protocol

- TCP 143
- Permite que los clientes accedan a correos electrónicos almacenados en un servidor de correo.
- Mantiene el correo electrónico en el servidor.

File Transfer

FTP - File Transfer Protocol

- TCP 20 a 21
- Establece las reglas que permiten a un usuario en un host acceder y transferir archivos hacia y desde otro host a través de una red.
- FTP Es un protocolo confiable de entrega de archivos, orientado a la conexión y con acuse de recibo.

TFTP - Trivial File Transfer Protocol

Cliente* UDP 69

- Un protocolo de transferencia de archivos simple y sin conexión con entrega de archivos sin reconocimiento y sin el máximo esfuerzo
- Utiliza menos sobrecarga que FTP.

Web

HTTP - Hypertext Transfer Protocol

- TCP 80, 8080
- Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.

HTTPS - HTTP Secure

- TCP, UDP 443
- El navegador usa cifrado para proteger las comunicaciones HTTP.
- Autentica el sitio web al que se conecta el navegador.

15.1.4

Compruebe su comprensión - Aplicación, sesión, presentación

Verifique su comprensión de routers eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La capa de aplicación del modelo OSI es la más cercana al usuario final. Proporciona una interfaz entre protocolos de aplicación que intercambian datos entre hosts.
2. La capa de presentación se ocupa del formato y la presentación de datos en un formato compatible con el dispositivo de destino. Ejemplos de estándares de capa de presentación son MKV, GIF, JPG, MOV y PNG.
3. Las tres capas superiores del modelo OSI; aplicación, presentación y sesión definen funciones de la capa de aplicación TCP/IP.
4. La capa de aplicación del modelo OSI proporciona una interfaz entre protocolos de aplicaciones que intercambian datos entre hosts. Los protocolos de la capa de aplicación incluyen HTTP, DNS, HTML, IMAP, FTP y SMTP.
5. La capa de sesión del modelo OSI crea y mantiene los diálogos, o sesiones, entre dos hosts comunicantes.

Has tenido 5 respuestas correctas de 5.

1. Esta capa del modelo OSI se refiere a los protocolos que intercambian datos entre programas que se ejecutan en hosts.

¡Lo tienes!

- (•) Aplicación
- ( ) Transporte
- ( ) Red
- ( ) Fisica

2. Los estándares MKV, GIF y JPG están asociados con qué capa OSI?

¡Lo tienes!

- ( ) Aplicación
- (•) Presentación
- ( ) Sesión
- ( ) Transporte

3. Estas tres capas OSI definen las mismas funciones que la capa de aplicación del modelo TCP/IP.

¡Lo tienes!

- [x] Aplicación
- [x] Presentación
- [x] Sesión
- [ ] Transporte
- [ ] Red
- [ ] Enlace de datos

4. ¿Cuáles son los dos protocolos que pertenecen a la capa de aplicación OSI?

¡Lo tienes!

- [ ] PNG
- [x] Envenenamiento
- [x] SMTP
- [ ] QuickTime

5. Esta es una función de la capa de sesión OSI.

¡Lo tienes!

- ( ) comprimir y descomprimir datos
- ( ) proporcionar una interfaz entre aplicaciones
- ( ) formato de datos para la capa de aplicación
- (•) intercambio de información para iniciar el diálogo entre pares

Correct

You have successfully identified the correct answers.

1. The application layer of the OSI model is the layer that is closest to the end user. It provides an interface between application protocols exchanging data between hosts.
2. The presentation layer is concerned with formatting and presenting data in a format that is compatible with the destination device. Examples of presentation layer standards are MKV, GIF, JPG, MOV, and PNG.
3. The upper three OSI layers; application, presentation, and session, define the application layer functions of the TCP/IP model.
4. The application layer of the OSI model provides an interface between applications protocols exchanging data between hosts. Protocols at the application layer include DNS, HTTP, SMTP, FTP, and IMAP.
5. The session layer of the OSI model creates and maintains the dialogs, or sessions, between two communicating hosts.

You got 5 out of 5 questions correct.

1. This layer of the OSI model is concerned with the protocols that exchange data between programs running on hosts.

You got it!

- (•) application
- ( ) transport
- ( ) network
- ( ) physical

2. MKV, GIF, and JPG standards are associated with which OSI layer?

You got it!

- ( ) application
- (•) presentation
- ( ) session
- ( ) transport

3. These three OSI layers define the same functions as the TCP/IP model application layer.

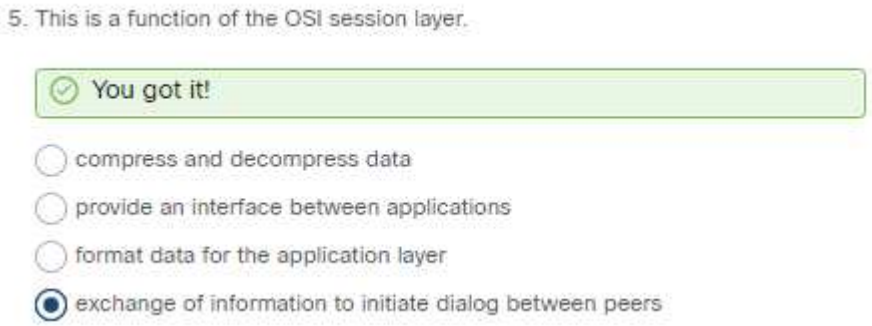
You got it!

- [x] application
- [x] presentation
- [x] session
- [ ] transport
- [ ] network
- [ ] data link

4. Which two are protocols that belong in the OSI application layer?

You got it!

- [ ] PNG
- [x] DNS
- [x] SMTP
- [ ] QuickTime



Capa de aplicación / Punto a punto

Punto a punto

15.2.1

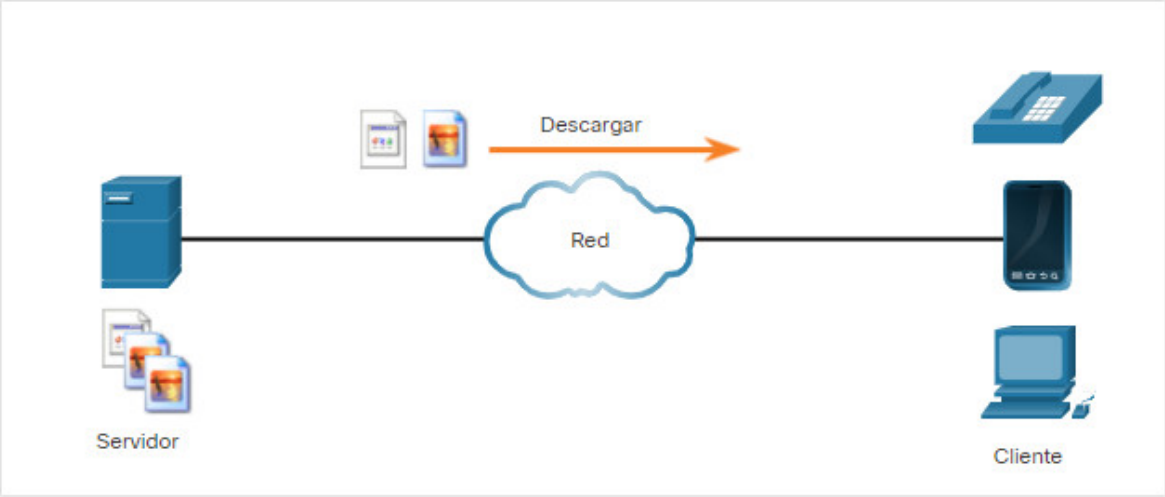
Modelo cliente-servidor

En el tema anterior, aprendió que los protocolos de capa de aplicación TCP/IP implementados tanto en el host de origen como en el de destino deben ser compatibles. En este tema aprenderá sobre el modelo cliente/servidor y los procesos utilizados, que se encuentran en la capa de aplicación. Lo mismo ocurre con una red Cliente a Servidor. En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”. El cliente es una combinación de hardware/software que las personas utilizan para acceder directamente a los recursos que se almacenan en el servidor.

Los procesos de cliente y servidor se consideran parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más flujos de datos al cliente. Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio también puede requerir la autenticación del usuario y la identificación de un archivo de datos que se vaya a transferir.

Un ejemplo de una red cliente-servidor es el uso del servicio de correo electrónico de un ISP para enviar, recibir y almacenar correo electrónico. El cliente de correo electrónico en una PC doméstica emite una solicitud al servidor de correo electrónico del ISP para que se le envíe todo correo no leído. El servidor responde enviando al cliente el correo electrónico solicitado. La transferencia de datos de un cliente a un servidor se conoce como “carga” y la transferencia de datos de un servidor a un cliente se conoce como “descarga”.

Como se muestra en la figura los archivos se descargan del servidor al cliente.



La figura representa el modelo de servidor cliente. Un cliente que se representa como un teléfono celular, computadora o teléfono VoIP está conectado a un servidor y descarga archivos desde el servidor.

15.2.2

Redes entre pares

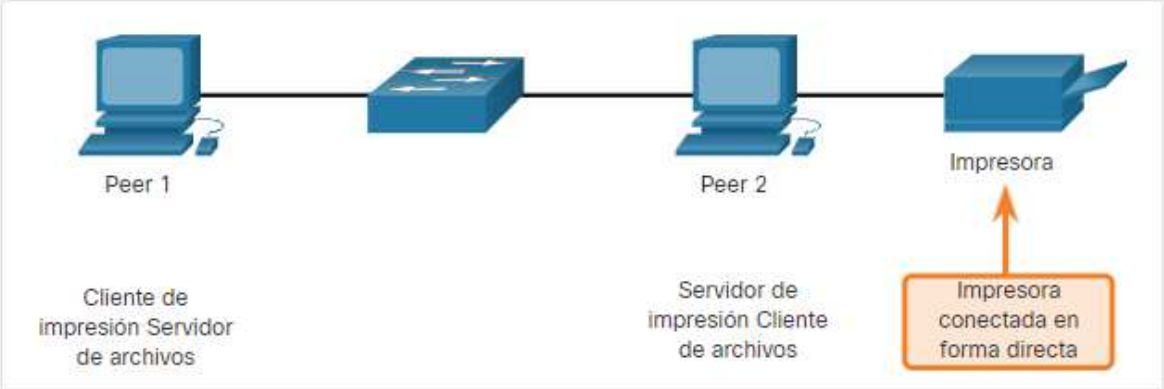
En el modelo de red entre pares (P2P), se accede a los datos de un dispositivo par sin utilizar un servidor dedicado.

El modelo de red P2P consta de dos partes: las redes P2P y las aplicaciones P2P. Ambas partes tienen características similares, pero en la práctica son muy diferentes.

En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Todo terminal conectado puede funcionar como servidor y como cliente. Un equipo puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud.

Además de compartir archivos, una red como esta permitiría que los usuarios habiliten juegos en red o compartan una conexión a Internet.

En un intercambio entre pares, ambos dispositivos se consideran iguales en el proceso de comunicación. El par 1 tiene archivos que se comparten con el par 2 y puede acceder a la impresora compartida que está conectada directamente al par 2 para imprimir archivos. El par 2 comparte la impresora conectada directamente con el par 1 mientras accede a los archivos compartidos en el par 1, como se muestra en la figura.



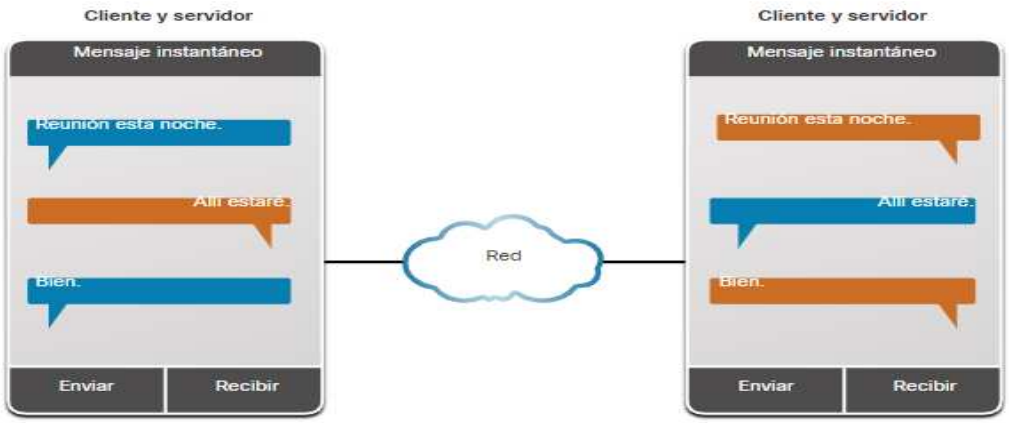
La figura representa el modelo de par a par. Dos computadoras están conectadas por un conmutador y se comunican directamente entre sí. Además, una impresora es compartida por uno de los equipos y puede ser accedida por cualquiera de los equipos de la figura.

15.2.3

Peer-to-Peer Applications

Una aplicación P2P permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación, como se muestra en la figura. En este modelo, cada cliente es un servidor y cada servidor es un cliente. Las aplicaciones P2P requieren que cada terminal proporcione una interfaz de usuario y ejecute un servicio en segundo plano.

Algunas aplicaciones P2P utilizan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices que apuntan a las ubicaciones de los recursos están almacenados en un directorio centralizado. En un sistema híbrido, cada punto accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro punto.



La figura muestra una aplicación P2P que es una versión híbrida del modelo peer to peer con dos aplicaciones de mensajería instantánea que se comunican con cada una a través de la red donde ambas aplicaciones actúan como clientes y servidores.

Ambos clientes inician y reciben mensajes simultáneamente.

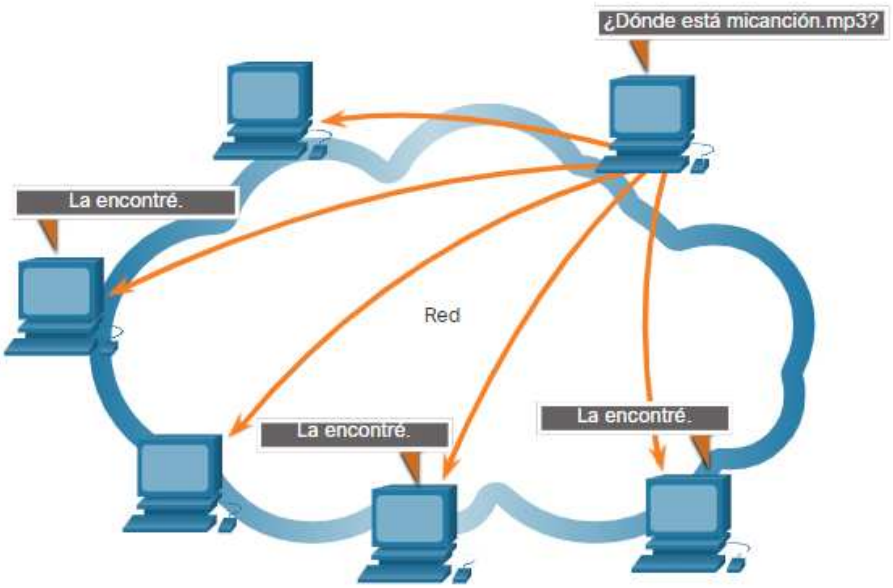
15.2.4

Aplicaciones P2P comunes

Con las aplicaciones P2P, cada PC de la red que ejecuta la aplicación puede funcionar como cliente o como servidor para las otras PC en la red que ejecutan la aplicación. Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Conexión directa
- eDonkey
- Freenet

Algunas aplicaciones P2P se basan en el protocolo Gnutella, con el que cada usuario comparte archivos enteros con otros usuarios. Como se muestra en la ilustración, el software de cliente compatible con Gnutella permite a los usuarios conectarse a los servicios Gnutella a través de Internet, además de ubicar los recursos compartidos por otros puntos Gnutella y acceder a dichos recursos. Muchas aplicaciones cliente de Gnutella están disponibles, incluyendo µTorrent, BitComet, DC++, Deluge y emule.



Gnutella permite que las aplicaciones P2P busquen recursos compartidos entre puntos.

La figura muestra una aplicación P2P que busca recursos compartidos. La application P2P está preguntando a sus pers si tiene el recurso en este caso mysong.mp3.

Muchas aplicaciones P2P permiten que los usuarios compartan partes de varios archivos con otro usuario a la vez. Los clientes utilizan un pequeño archivo llamado archivo torrent para localizar a otros usuarios que tienen las piezas que necesitan y conectarse directamente a ellos. Este archivo también contiene información sobre los equipos de seguimiento que realizan el seguimiento de qué usuarios tienen qué archivos. Los clientes piden partes de varios usuarios al mismo tiempo. Esta tecnología se denomina BitTorrent. BitTorrent tiene su propio cliente. pero existen muchos clientes BitTorrent, incluidos uTorrent, Deluge,y qBittorrent.

Nota: Cualquier tipo de archivo se puede compartir entre los usuarios. Muchos de estos archivos están protegidos por derechos de autor, lo que significa que sólo el creador tiene el derecho de utilizarlos y distribuirlos. Es contrario a la ley descargar o distribuir archivos protegidos por derechos de autor sin el permiso del titular de los derechos de autor. La violación de los derechos de autor puede ocasionar cargos penales y demandas civiles.

15.2.5

Verifique su comprensión Cliente a Servidor

Verifique su comprensión de Cliente a Servidor eligiendo la mejor respuesta a las siguientes preguntas:

Correcto

Identificó bien las respuestas correctas.

1. La respuesta correcta es falso. En el modelo de punto a punto, los clientes pueden compartir recursos sin utilizar un servidor dedicado.
2. La respuesta correcta es verdadero. Una red de punto a punto no requiere un servidor dedicado porque cada par puede funcionar como cliente y como servidor.
3. Los clientes BitTorrent utilizan un archivo torrent para localizar a otros clientes que comparten fragmentos de archivos necesarios. De esta manera, muchos archivos se pueden compartir entre clientes al mismo tiempo.
4. Gnutella es un protocolo Cliente a Servidor que permite a los usuarios compartir archivos enteros con otros usuarios.

Has tenido 4 respuestas correctas de 4.

1. ¿Verdadero o falso? El modelo de red Cliente a Servidor requiere la implementación de un servidor dedicado para el acceso a los datos.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

2. ¿Verdadero o falso? En un entorno de red de punto a punto, cada par puede funcionar como cliente y servidor.

¡Lo tienes!

- ◉ Verdadero
- ○ Falso

3. Cual aplicación P2P permite que los usuarios compartan partes de varios archivos con otro usuario a la vez?

¡Lo tienes!

- ○ Híbrido
- ○ Gnutella
- ◉ BitTorrent

4. ¿Cuál de los siguientes es una característica del protocolo Gnutella?

¡Lo tienes!

- ◉ Los usuarios pueden compartir archivos completos con otros usuarios.
- ○ Los usuarios pueden compartir fragmentos de archivos con otros usuarios.
- ○ Los usuarios pueden acceder a un servidor de índices para obtener la ubicación de los recursos compartidos por otros usuarios.

Correct

You have successfully identified the correct answers.

1. The correct answer is False. In the peer-to-peer model, clients can share resources without using a dedicated server.
2. The correct answer is True. A peer-to-peer network does not require a dedicated server because each peer can function as both a client and as a server.
3. BitTorrent clients use a torrent file to locate other clients that are sharing pieces of needed files. In this way, many files can be shared between clients at the same time.
4. Gnutella is a peer-to-peer protocol that allows users to share whole files with other users.

You got 4 out of 4 questions correct.

1. True or false? The peer-to-peer networking model requires the implementation of a dedicated server for data access.

You got it!

- ○ True
- ◉ False

2. True or false? In a peer-to-peer network environment every peer can function as both a client and a server.

You got it!

- ◉ True
- ○ False

3. Which peer-to-peer application allows users to share pieces of many files with each other at the same time?

You got it!

- ○ Hybrid
- ○ Gnutella
- ◉ BitTorrent

4. Which of the following is a feature of the Gnutella protocol?

You got it!

- ◉ Users can share whole files with other users.
- ○ Users can share pieces of files with other users.
- ○ Users can access an index server to get the location of resources shared by other users.

Capa de aplicación / Protocolos web y de correo electrónico

Protocolos web y de correo electrónico

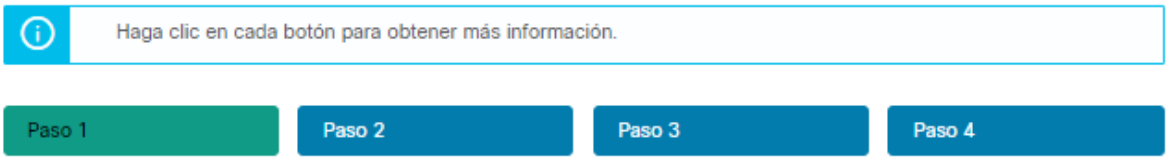
15.3.1

Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

Existen protocolos específicos de la capa de aplicación diseñados para usos comunes, como la navegación web y el correo electrónico. El primer tema le dio una visión general de estos protocolos. Este tema entra en más detalle.

Cuando se escribe una dirección web o un localizador uniforme de recursos (URL) en un navegador web, el navegador establece una conexión con el servicio web. El servicio web se está ejecutando en el servidor que está utilizando el protocolo HTTP. Los nombres que la mayoría de las personas asocia con las direcciones web son URL e identificador uniforme de recursos (URI).

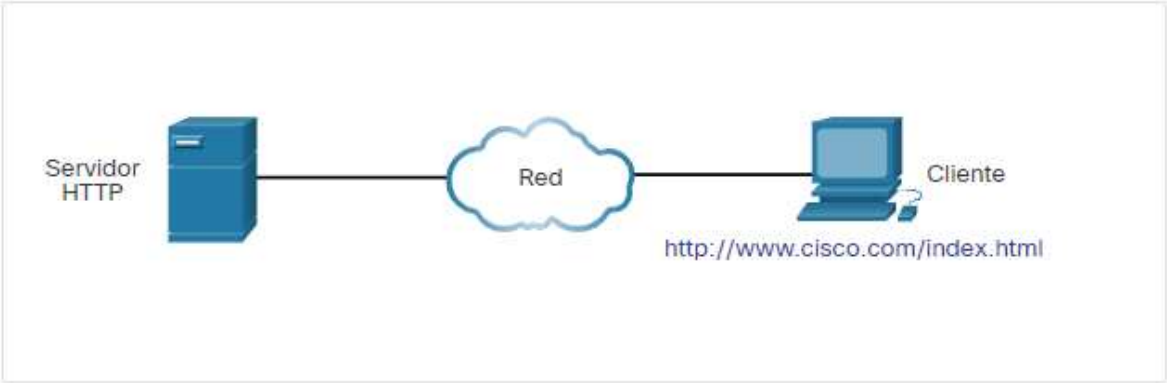
Para comprender mejor cómo interactúa el navegador web con el servidor web, podemos analizar cómo se abre una página web en un navegador. Para este ejemplo, utilice el URL http://www.cisco.com/index.html.



Paso 1

El explorador interpreta las tres partes del URL:

- http (el protocolo o esquema)
- www.cisco.com (el nombre del servidor)
- index.html (el nombre de archivo específico solicitado)

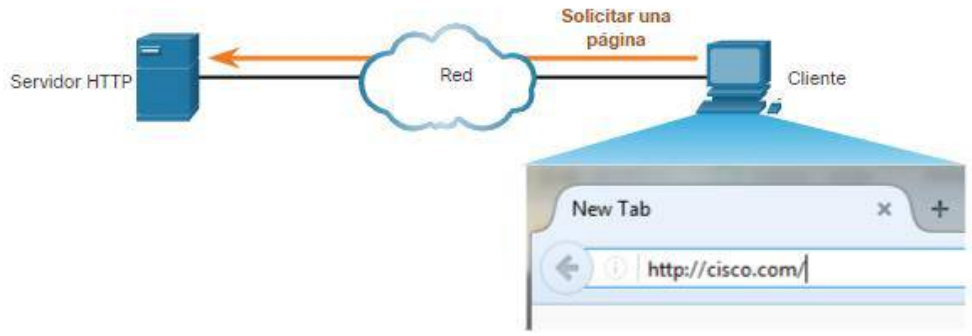


Muestra un servidor http conectado a través de Internet a un equipo cliente. El equipo cliente está solicitando la URL www.cisco.com que es el servidor HTTP.

Paso 1 | Paso 2 | Paso 3 | Paso 4

Paso 2

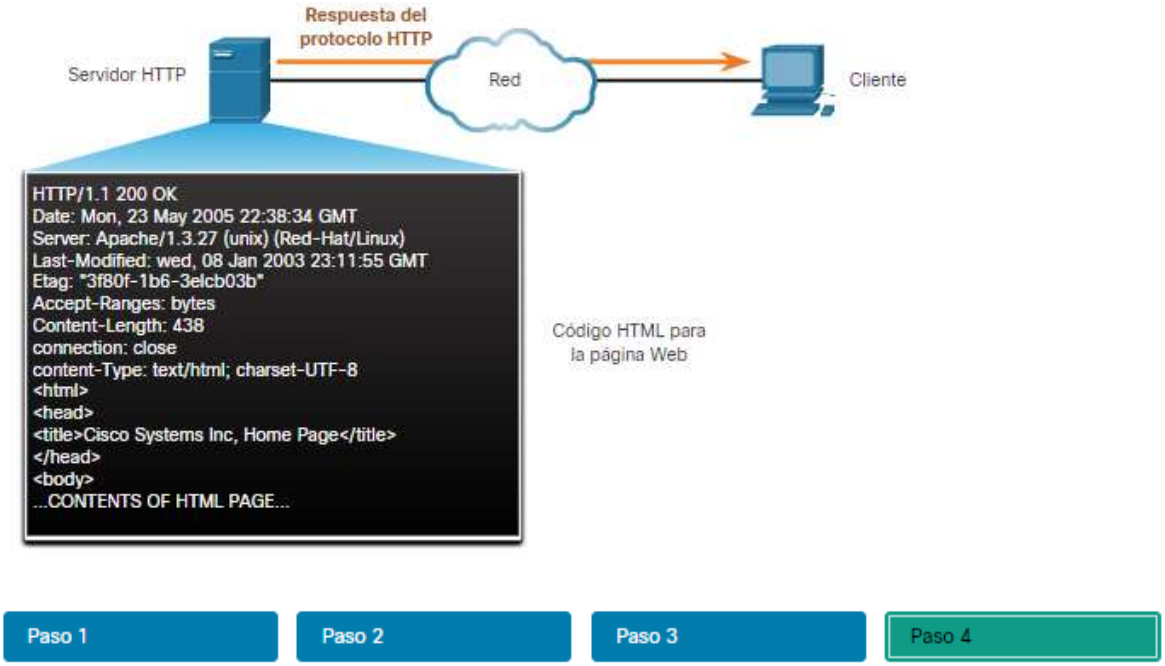
El navegador luego verifica con un Servidor de nombres de dominio (DNS) para convertir a www.cisco.com en una dirección numérica que utiliza para conectarse con el servidor. El cliente inicia una solicitud HTTP a un servidor enviando una solicitud GET al servidor y solicita el archivo index.html.



Paso 1 | Paso 2 | Paso 3 | Paso 4

Paso 3

En respuesta a la solicitud, el servidor envía el código HTML de esta página web al navegador.



Paso 4

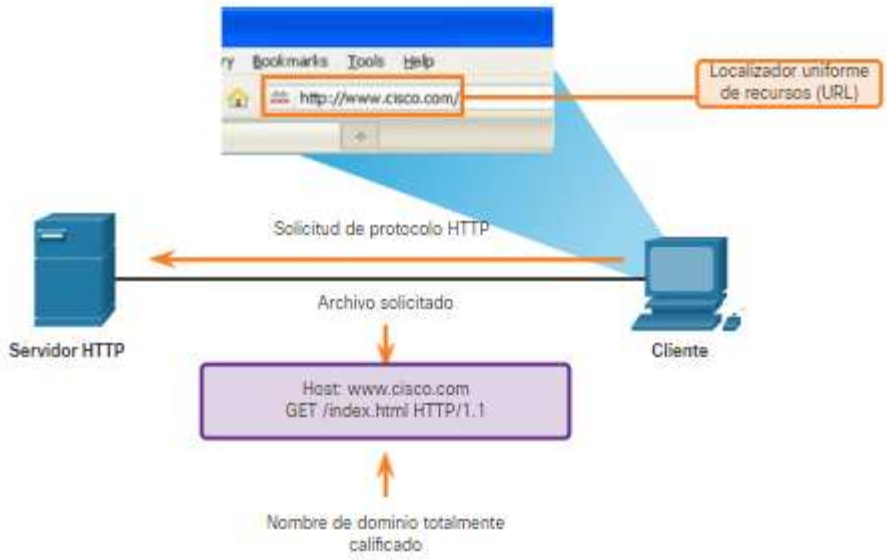
El navegador descifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del navegador.

15.3.2

HTTP y HTTPS

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un navegador web, envía una solicitud a un servidor web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son GET, POST y PUT (consulte la figura):

- **GET** - solicitud de datos por parte del cliente. Un cliente (navegador web) envía el mensaje GET al servidor web para solicitar las páginas HTML.
- **POST** - carga archivos de datos, como los datos de formulario, al servidor web. .* **PUT** - carga los recursos o el contenido, como por ejemplo una imagen, en el servidor web.



La figura muestra a un cliente que realiza una solicitud HTTP a un servidor HTTP. El archivo solicitado es un nombre de dominio completo. La solicitud utiliza un Get para recuperar la página web. El campo URL se muestra en el equipo cliente como una solicitud http://www.cisco.com.

Aunque HTTP es sumamente flexible, no es un protocolo seguro. Los mensajes de solicitud envían información al servidor en texto sin formato que puede ser interceptado y leído. Las respuestas del servidor, generalmente páginas HTML, también están sin cifrar.

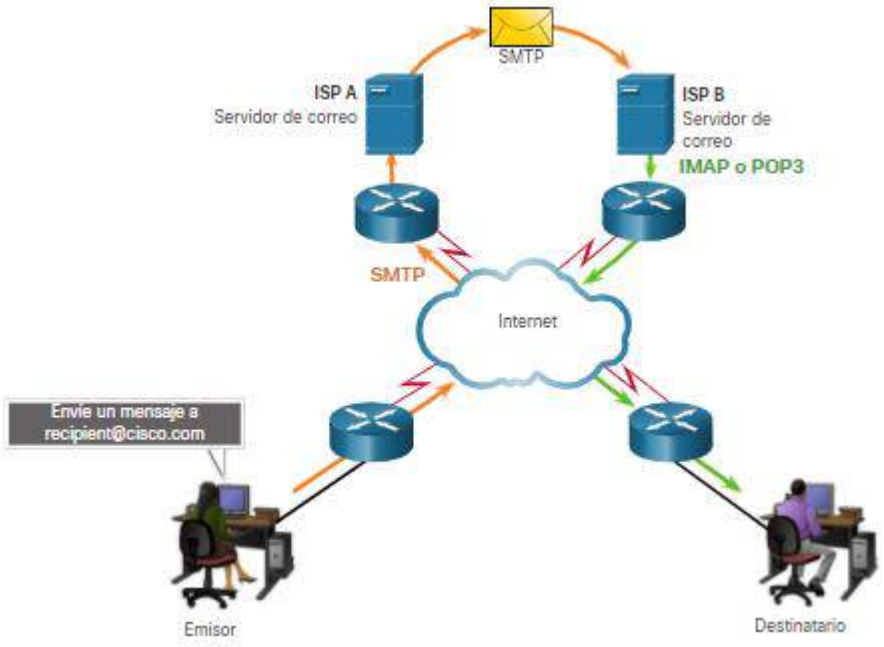
Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS). HTTPS utiliza autenticación y cifrado para proteger los datos mientras viajan entre el cliente y el servidor. HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del

servidor que HTTP, pero el flujo de datos se cifra con capa de sockets seguros (SSL) antes de transportarse a través de la red.

15.3.3

Protocolos de correo electrónico

Uno de los principales servicios que un ISP ofrece es hosting de correo electrónico. Para ejecutar el correo electrónico en una PC o en otro terminal, se requieren varios servicios y aplicaciones, como se muestra en la figura. El correo electrónico es un método de guardado y desvío que se utiliza para enviar, guardar y recuperar mensajes electrónicos a través de una red. Los mensajes de correo electrónico se guardan en bases de datos en servidores de correo.



La figura muestra una transacción de correo electrónico de un remitente mediante el protocolo SMTP que envía un correo electrónico a recipient@cisco.com a través de un servidor de correo ISP A que llega a los destinatarios del servidor de correo electrónico ISP B y el destinatario que lee el correo electrónico mediante el protocolo IMAP o POP.

Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir correo electrónico. Los servidores de correo se comunican con otros servidores de correo para transportar mensajes desde un dominio a otro. Un cliente de correo electrónico no se comunica directamente con otro cliente de correo electrónico cuando envía un correo electrónico. En cambio, ambos clientes dependen del servidor de correo para transportar los mensajes.

El correo electrónico admite tres protocolos diferentes para su funcionamiento: el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina de correos (POP) e IMAP. El proceso de capa de aplicaciones que envía correo utiliza el SMTP. Un cliente recupera el correo electrónico mediante uno de los dos protocolos de capa de aplicaciones: el POP o el IMAP.

15.3.4

SMTP, POP e IMAP

Haga clic en cada botón para obtener más información.

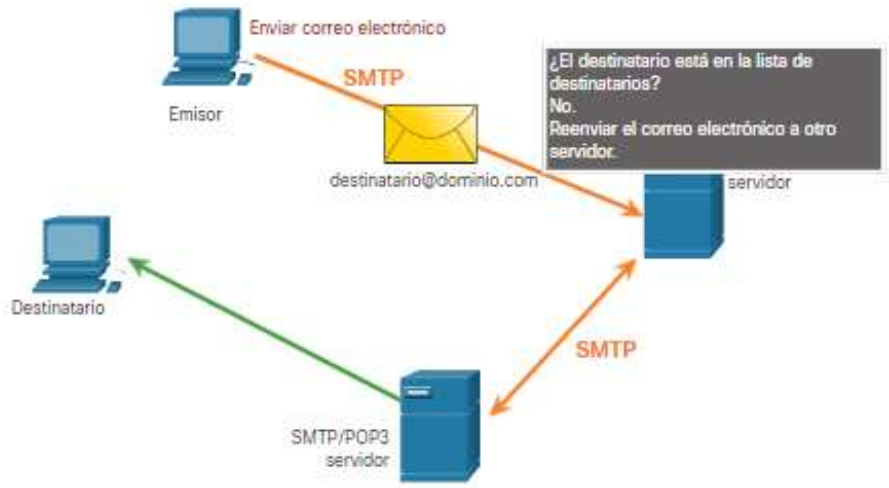
SMTP | POP | IMAP

SMTP

Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo del mensaje puede contener la cantidad de texto que se desee, el encabezado debe contar con una dirección de correo electrónico de destinatario correctamente formateada y una dirección de emisor.

Cuando un cliente envía correo electrónico, el proceso SMTP del cliente se conecta a un proceso SMTP del servidor en el puerto bien conocido 25. Después de que se establece la conexión, el cliente intenta enviar el correo electrónico al servidor a través de esta. Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía a otro servidor de correo para su entrega.

El servidor de correo electrónico de destino puede no estar en línea, o estar muy ocupado, cuando se envían los mensajes. Por lo tanto, el SMTP pone los mensajes en cola para enviarlos posteriormente. El servidor verifica periódicamente la cola en busca de mensajes e intenta enviarlos nuevamente. Si el mensaje aún no se ha entregado después de un tiempo predeterminado de expiración, se devolverá al emisor como imposible de entregar.



Esta es una figura con un equipo remitente y un equipo destinatario. Dos servidores SMTP/POP3 están conectados entre ambos. Se envía un mensaje de correo desde el equipo remitente con la etiqueta recipient@domain.com mediante el protocolo smtp. El primer SMTP/POP3 recibe el mensaje del remitente y pregunta ¿Está el destinatario en mi lista de destinatarios? No. Reenviar correo electrónico a otro servidor. El segundo servidor SMTP/POP3 recibe el mensaje a través del protocolo SMTP y reenvía el mensaje al destinatario.

15.3.5

Verifique su comprensión: Web y protocolos de correo electrónico

Verifique su comprensión de Web y protocolos de correo electrónico eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. HTTP utiliza el mensaje POST para cargar archivos de datos a un servidor web. Los clientes utilizan el mensaje GET para solicitar datos y el mensaje PUT se utiliza para cargar contenido como imágenes.
2. Los exploradores web se conectan a servidores web a través de HTTP. IMAP y SMTP son protocolos de correo electrónico. SSL es un protocolo de cifrado utilizado con HTTPS.
3. Los clientes de correo electrónico se conectan a servidores SMTP a través del puerto 25 para enviar correo electrónico. POP e IMAP son utilizados por los clientes para recibir correo electrónico. HTTP se utiliza entre navegadores web y servidores web.
4. IMAP es un protocolo para que los clientes recuperen copias de mensajes de correo electrónico desde un servidor IMAP. Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente.
5. La respuesta correcta es falso. HTTP envía información en texto sin formato y no se considera seguro. Si se desea seguridad, se debe utilizar HTTP Secure (HTTPS).

Has tenido 5 respuestas correctas de 5.

1. Este tipo de mensaje se utiliza al cargar archivos de datos en un servidor web.

¡Lo tienes!

- ○ GET
- ◉ POST
- ○ PUT

2. Este protocolo es utilizado por un navegador web para establecer una conexión con un servidor web.

¡Lo tienes!

- ◉ HTTP
- ○ SSL
- ○ IMAP
- ○ SMTP

3. Este protocolo es utilizado por un cliente para enviar correo electrónico a un servidor de correo.

¡Lo tienes!

- ○ POP
- ◉ SMTP
- ○ IMAP
- ○ HTTP

4. ¿Cuál es una característica de IMAP?

¡Lo tienes!

- ○ Carga mensajes de correo electrónico a un servidor.
- ○ Escucha pasivamente en el puerto 110 para las solicitudes de los clientes.
- ◉ Descarga una copia de los mensajes de correo electrónico dejando el original en el servidor.

5. ¿Verdadero o falso? HTTP es un protocolo seguro.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

Correct

You have successfully identified the correct answers.

1. HTTP uses the POST message to upload data files to a web server. The GET message is used by clients to request data and the PUT message is used to upload content such as images.
2. Web browsers connect to web servers over HTTP. IMAP and SMTP are email protocols. SSL is an encryption protocol used with HTTPS.
3. Email clients connect to SMTP servers over port 25 to send email. POP and IMAP are used by clients to receive email. HTTP is used between web browsers and web servers.
4. IMAP is a protocol for clients to retrieve copies of email messages from an IMAP server. The original messages remain on the server until manually deleted.
5. The correct answer is False. HTTP sends information in plaintext and is not considered secure. If security is desired, HTTP Secure (HTTPS) should be used.

You got 5 out of 5 questions correct.

1. This message type is used when uploading data files to a web server.

You got it!

- ○ GET
- ◉ POST
- ○ PUT

2. This protocol is used by a web browser to establish a connection to a web server.

You got it!

- ◉ HTTP
- ○ SSL
- ○ IMAP
- ○ SMTP

3. This protocol is used by a client to send email to a mail server.

You got it!

- ○ POP
- ◉ SMTP
- ○ IMAP
- ○ HTTP

1. Capa de aplicación
2. Servicios de direccionamiento IP

Servicios de direccionamiento IP

15.4.1

Servicio de nombres de dominios

Existen otros protocolos específicos de capa de aplicación diseñados para facilitar la obtención de direcciones para dispositivos de red. Estos servicios son esenciales porque llevaría mucho tiempo recordar direcciones IP en lugar de direcciones URL o configurar manualmente todos los dispositivos de una red mediana a grande. El primer tema de este módulo le dio una visión general de estos protocolos. En este tema se detallan los servicios de direccionamiento IP, DNS y DHCP.

En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

En Internet, los nombres de dominio, como http://www.cisco.com, son mucho más fáciles de recordar para las personas que 198.133.219.25, que es la dirección IP numérica real para este servidor. Si Cisco decide cambiar la dirección numérica de www.cisco.com, esto no afecta al usuario, porque el nombre de dominio se mantiene. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad.

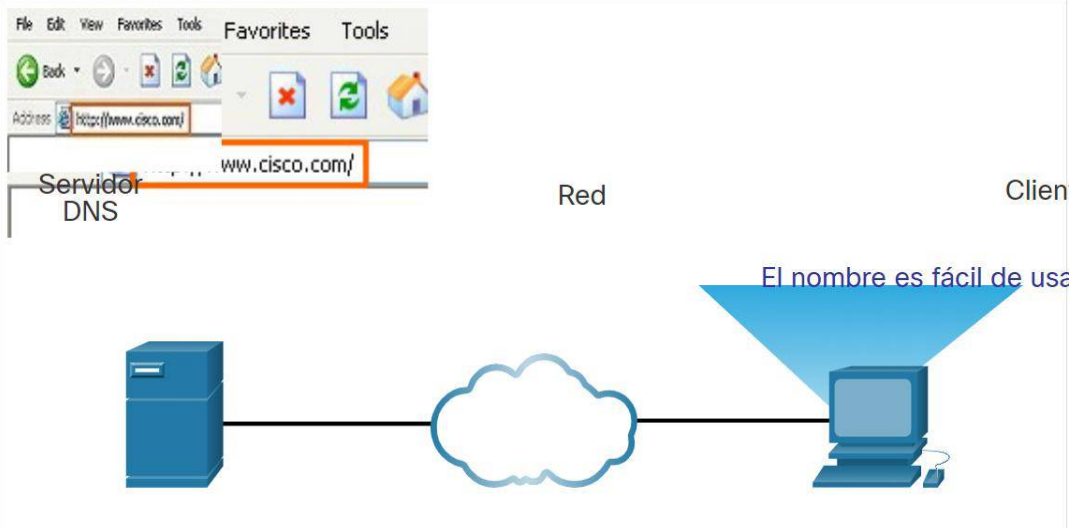
El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye el formato de consultas, respuestas y datos. Las comunicaciones del protocolo DNS utilizan un único formato llamado "mensaje". Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Haga clic en cada botón para obtener más información.

Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5

Paso 1

El usuario escribe un FQDN en un campo Dirección de aplicación del explorador.

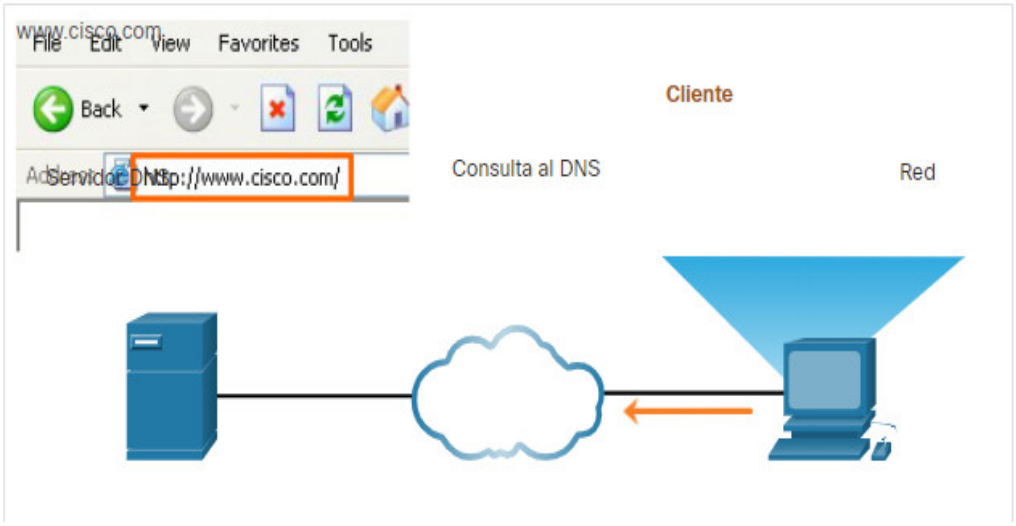


Esta es una figura con un cliente, que se pone en contacto con un servidor DNS a través de la red, con un FQDN escrito en un campo URL del navegador porque el nombre de un sitio web es más fácil de usar para las personas.

Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5

Paso 2

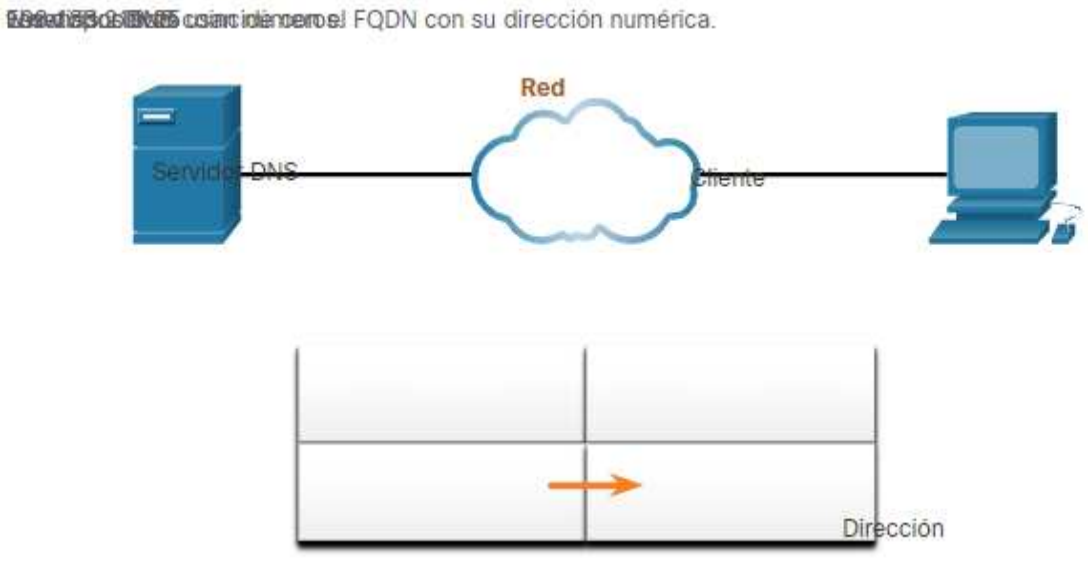
Se envía una consulta DNS al servidor DNS designado para el equipo cliente.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5

Paso 3

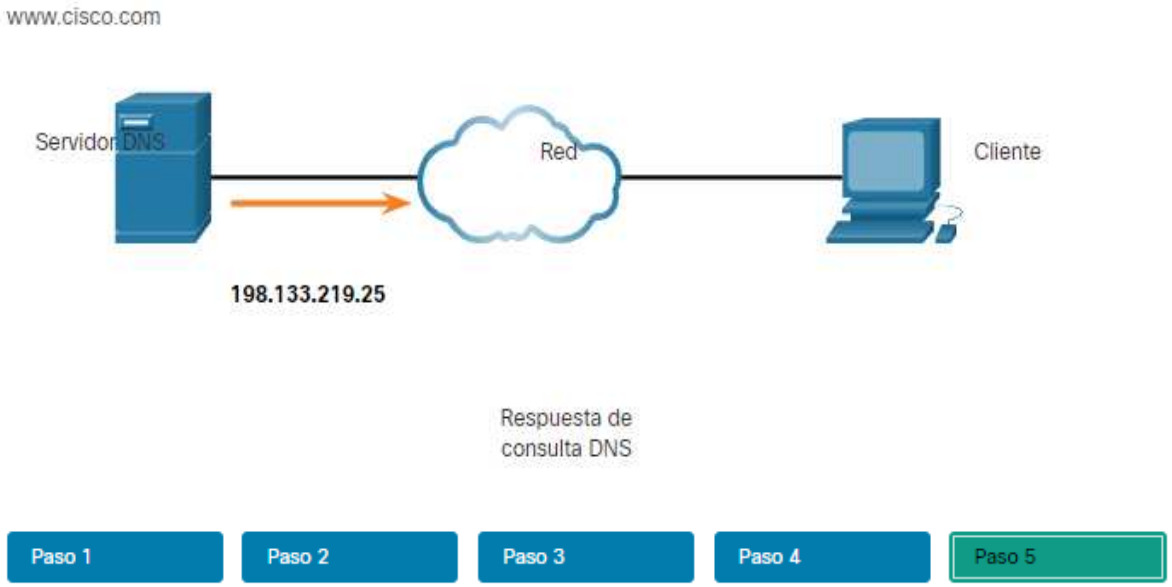
El servidor DNS coincide con el FQDN con su dirección IP.



Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5

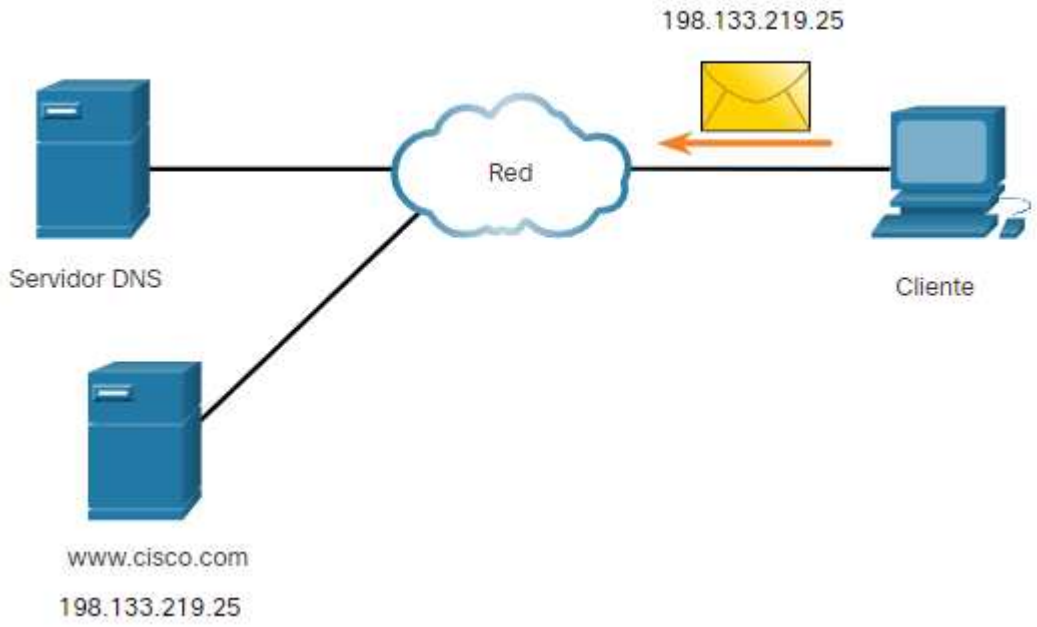
Paso 4

La respuesta de consulta DNS se envía de nuevo al cliente con la dirección IP del FQDN.



Paso 5

El equipo cliente utiliza la dirección IP para realizar solicitudes del servidor.



Formato de mensaje DNS

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro. Algunos de estos tipos de registros son los siguientes:

- **A** - una dirección IPv4 de terminal
- **NS** - un servidor de nombre autoritativo
- **AAAA** - una dirección IPv6 de terminal (pronunciada quad-A)
- **MX** - un registro de intercambio de correo

Cuando un cliente realiza una consulta, el proceso DNS del servidor observa primero sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente la dirección numerada por si se vuelve a solicitar el mismo nombre.

El servicio del cliente DNS en los equipos Windows también almacena los nombres resueltos previamente en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas de DNS en caché.

Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Sección de mensajes DNS	Descripción
Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional

15.4.3

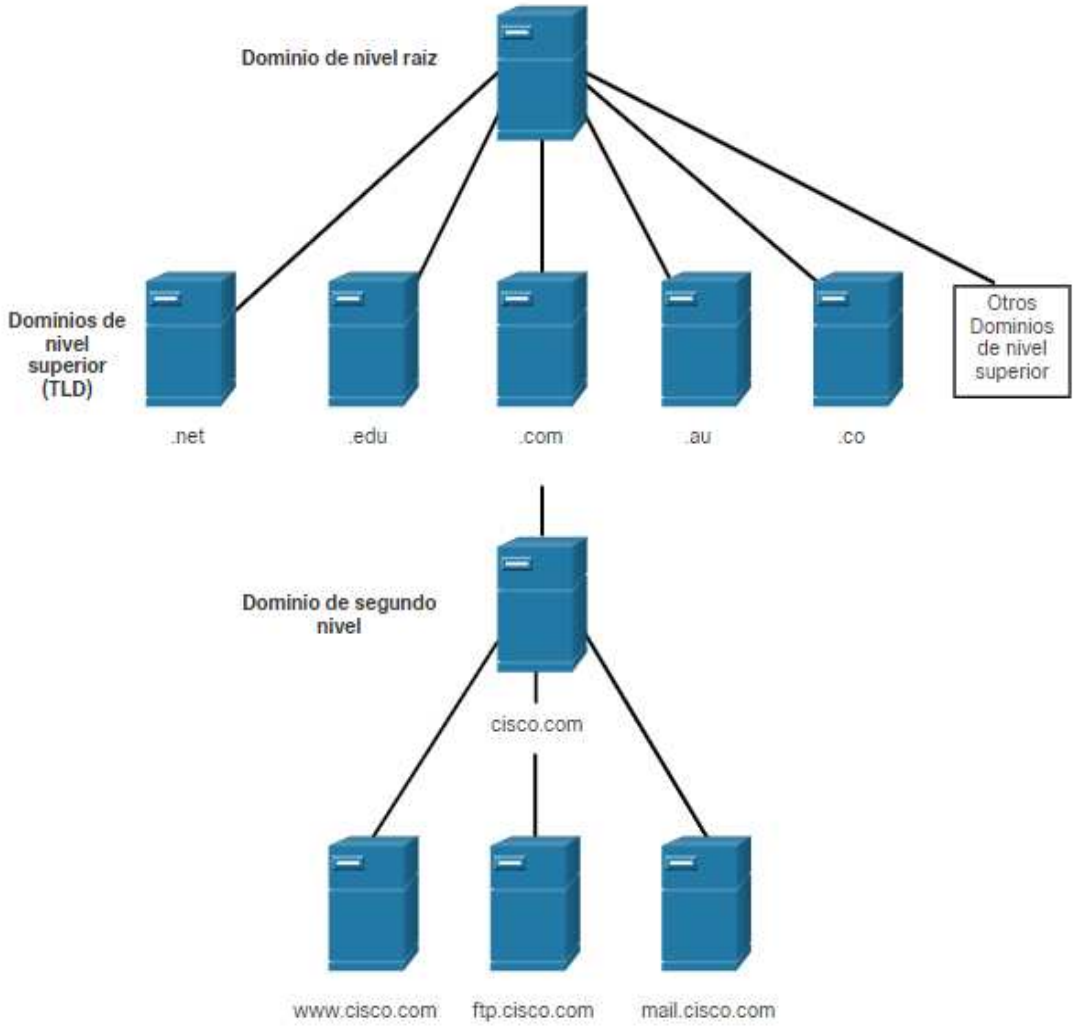
Jerarquía DNS

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres, como se muestra en la figura. DNS utiliza nombres de domino para formar la jerarquía.

La estructura de nomenclatura se divide en zonas pequeñas y manejables. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción. DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Algunos ejemplos de dominios de nivel superior son los siguientes:

- **.com** - una empresa o industria
- **.org** - una organización sin fines de lucro
- **.au** - Australia
- **.co** - Colombia



En la figura, se muestra la jerarquía DNS. En la parte superior está el dominio de nivel raíz con los dominios de nivel superior (TLD) conectados debajo del dominio de nivel raíz. Los TLD son .net, .edu, .com, .au, .co y otros doamins de nivel superior. Bajo el TLD .com está el dominio de segundo nivel www.cisco.com y bajo cisco.com son www.cisco.com, ftp.cisco.com y mail.cisco.com.

15.4.4

El comando nslookup

Al configurar un dispositivo de red, se proporcionan una o más direcciones de servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet (ISP) suministra las direcciones para utilizar con los servidores DNS. Cuando la aplicación del usuario pide conectarse a un dispositivo remoto por nombre, el cliente DNS solicitante consulta al servidor de nombres para resolver el nombre para una dirección numérica.

Los sistemas operativos informáticos también cuentan con una herramienta llamada nslookup que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En esta figura **nslookup** cuando se ejecuta el comando, se muestra el servidor DNS predeterminado configurado para su host. El nombre de un host o de un dominio se puede introducir en el **nslookup** prompt. La utilidad nslookup tiene muchas opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS.

```
C:\Users > nslookup
Servidor predeterminado: dns-sj.cisco.com
Dirección: 171.70.168.183
> www.cisco.com
Servidor: dns-sj.cisco.com
Dirección: 171.70.168.183
Nombre: origin-www.cisco.com
dirección: 2001:420:1101:1::a
          173.37.145.84
Alias: www.cisco.com
> cisco.netacad.net
Servidor: dns-sj.cisco.com
Dirección: 171.70.168.183
Nombre: cisco.netacad.net
Dirección: 72.163.6.223
>
```

15.4.5

Comprobador de sintaxis - El comando nslookup

Practique la introducción del comando nslookup tanto en Windows como en Linux.

En el símbolo del sistema de Windows, introduzca el comando **nslookup** para iniciar una consulta manual de los servidores de nombres.

```
C:\>nslookup
Default Server: Unknown
Address: 10.10.10.1
```

The output lists the name and IP address of the DNS server configured in the client. Note that the DNS server address can be manually configured, or dynamically learned, through DHCP. You are now in **nslookup** mode. Enter the domain name www.cisco.com.

```
>www.cisco.com
Server:  UnKnown
Address:  10.10.10.1
Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2600:1404:a:395::b33
          2600:1404:a:38e::b33
          172.230.155.162
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

The output lists the 'www.cisco.com' related IP addresses that the server 'e2867' currently has in its database. Notice that IPv6 addresses are also listed. In addition, various aliases are shown that will resolve to 'www.cisco.com'.

Enter the **exit** command to leave nslookup mode and return to the Windows command line.

```
>exit
```

You can directly query the DNS servers by simply adding the domain name to the **nslookup** command.

Enter **nslookup www.google.com**.

```
C:\>nslookup www.google.com
Server:  UnKnown
Address:  10.10.10.1
Non-authoritative answer:
Name:    www.google.com
```

```
Addresses:  2607:f8b0:4000:80f::2004
          172.217.12.36


=======================================
```

You are now working from Linux command prompt. The nslookup command is the same.

- Enter the **nslookup** command to begin a manual query of the name servers.
- Enter **www.cisco.com** at the > prompt.
- Enter the **exit** command to leave nslookup mode and return to the Linux command line.

```
user@cisconetacad$nslookup
Server: 127.0.1.1
Address: 127.0.1.1#53
>www.cisco.com
Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical name =
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name =
e144.dscb.akamaiedge.net.
Name: e144.dscb.akamaiedge.net
Address: 23.60.112.170
>exit
```

As in Windows, you can directly query the DNS servers by simply adding the domain name to the **nslookup** command. Enter **nslookup www.google.com**.

```
user@cisconetacad$nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.6.164
Name:   www.google.com
Address: 2607:f8b0:4000:812::2004
You successfully used the **nslookup** command to verify the status of
domain names.
```

15.4.6

Protocolo de configuración dinámica de host

El protocolo DHCP del servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, gateways y otros parámetros de redes IPv4. Esto se denomina “direccionamiento dinámico”. La alternativa al direccionamiento dinámico es el direccionamiento estático. Al

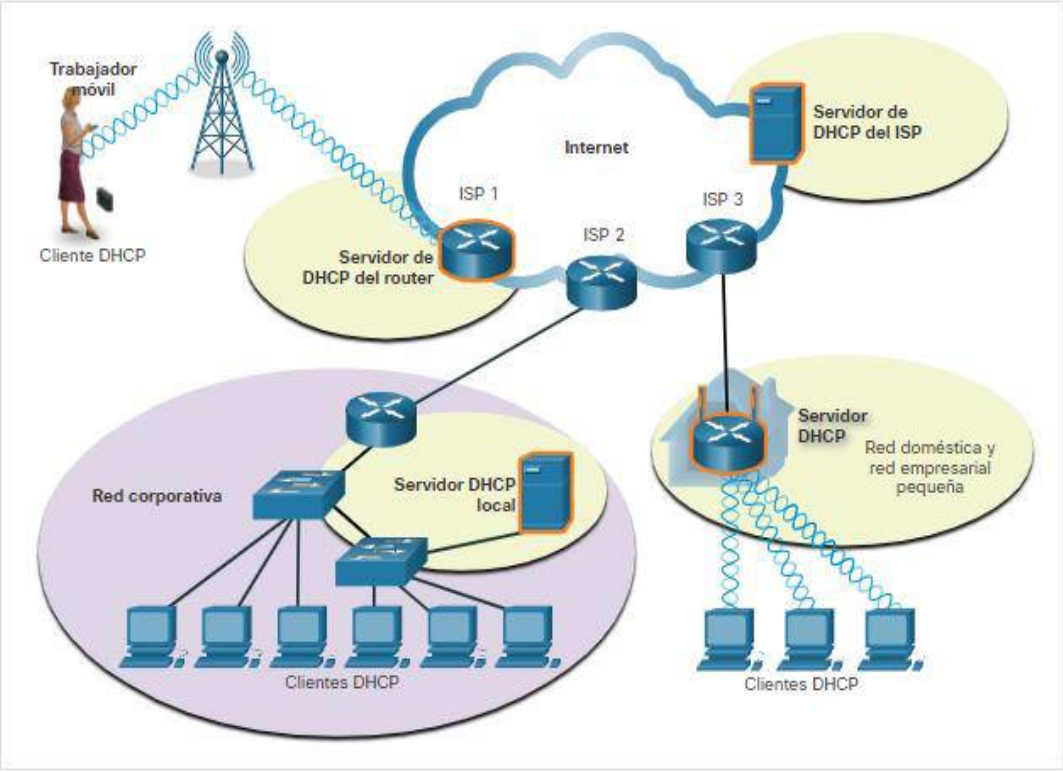
utilizar el direccionamiento estático, el administrador de redes introduce manualmente la información de la dirección IP en los hosts.

Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado grupo y la asigna (concede) al host.

En redes más grandes, o donde los usuarios cambian con frecuencia, se prefiere asignar direcciones con DHCP. Es posible que los nuevos usuarios necesiten conexiones; otros pueden tener PC nuevas que deben estar conectadas. En lugar de usar asignación de direcciones estáticas para cada conexión, es más eficaz que las direcciones IPv4 se asignen automáticamente mediante DHCP.

DHCP puede asignar direcciones IP durante un período de tiempo configurable, denominado período de concesión. El período de concesión es una configuración DHCP importante. Cuando caduca el período de concesión o el servidor DHCP recibe un mensaje DHCPRELASE, la dirección se devuelve al grupo DHCP para su reutilización. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer con facilidad las conexiones de red por medio de DHCP.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores DHCP. En la mayoría de las redes medianas a grandes, el servidor DHCP suele ser un servidor local y dedicado con base en una PC. En las redes domésticas, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al ISP.



En la figura se muestra un servidor DHCP ISP conectado a Internet con tres routers ISP con la etiqueta ISP1, ISP2, ISP #. Cada router ISP está conectado a una red diferente. ISP1 se conecta a una antena inalámbrica a un trabajador móvil que es el cliente DCHP. ISP2 está conectado a un router de red corporativa que se conecta a una LAN corporativa con su propio servidor DHCP local conectado a un switch conectado a seis clientes DHCP. ISP3 está conectado a un servidor DHCP inalámbrico para una red doméstica y pequeña empresa a los tres clientes DHCP conectados.

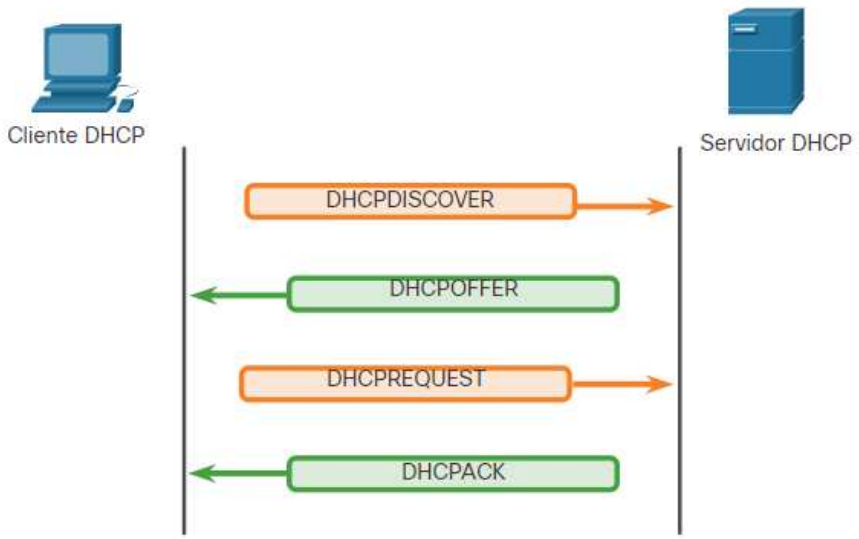
Muchas redes utilizan tanto el direccionamiento estático como DHCP. DHCP se utiliza para hosts de propósito general, tales como los dispositivos de usuario final. El direccionamiento estático se utiliza para los dispositivos de red, tales como gateways, switches, servidores e impresoras.

DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Una diferencia importante es que DHCPv6 no brinda una dirección de gateway predeterminado. Esto sólo se puede obtener de forma dinámica a partir del anuncio de router del propio router.

15.4.7

Funcionamiento de DHCP

Como se muestra en la ilustración, cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. El mensaje de oferta contiene la dirección IPv4 y la máscara de subred que se deben asignar, la dirección IPv4 del servidor DNS y la dirección IPv4 del gateway predeterminado. La oferta de concesión también incluye la duración de esta.



La figura muestra una escala de protocolo con un cliente DHCP en un lado y un cliente DHCP en el otro. El cliente DHCP envía un mensaje DHCPDISCOVER al servidor DHCP. El servidor de DHCPv4 envía el mensaje DHCPOFFER asignado al cliente DHCP. El cliente DHCP envía un mensaje DHCPREQUEST en response al DHCPOFFER desde el servidor DHCP. El servidor DHCP envía un mensaje DHCPACK de vuelta al cliente DHCP. El proceso se llama DORA.

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local. Por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.

Suponiendo que la dirección IPv4 solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de reconocimiento de DHCP (DHCPACK) que le informa al cliente que finalizó la concesión. Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo de DHCP (DHCPNAK). Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

El servidor DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes.

DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.

15.4.8

Laboratorio: Observar la resolución de nombres DNS

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Observar la conversión de un URL en una dirección IP mediante DNS
- Parte 2: Observar la búsqueda DNS mediante el **nslookup** comando en un sitio web
- Parte 3: Observar la búsqueda DNS mediante el**nslookup** comando nslookup en servidores de correo

Observe la resolución de nombres DNS

15.4.9

Compruebe su comprensión — Servicios de direccionamiento IP

Elija la MEJOR repuesta para las siguientes preguntas y compruebe su conocimiento sobre servicios de direccionamiento IP.

Correcto

Identificó bien las respuestas correctas.

1. Los registros AAAA DNS se utilizan para resolver nombres en direcciones IPv6.
2. La respuesta correcta es falso. Cuando un servidor DNS recibe una solicitud de resolución de nombres para un nombre que no está dentro de su zona, el servidor reenviará la solicitud a otro servidor DNS.
3. Al **nslookup** ejecutar el comando, se muestra el servidor DNS predeterminado configurado.
4. Los registros NS resuelven los servidores de nombres autorizados. Los registros DNS A resuelven direcciones IPv4. Los registros AAAA resuelven direcciones IPv6 y los registros MX resuelven servidores de intercambio de correo.
5. La respuesta correcta es falso. Hay cuatro mensajes DHCP intercambiados entre clientes y servidores. El cliente inicia el proceso DHCP con un mensaje de detección DHCP a los servidores DHCP disponibles.

Has tenido 5 respuestas correctas de 5.

1. ¿Cuál de los siguientes tipos de registros DNS se utiliza para resolver direcciones IPv6?

¡Lo tienes!

- servidor
- NS
- (•) AAAA
- MX

2. ¿Verdadero o falso? Un servidor DNS que recibe una solicitud de resolución de nombres que no está dentro de su zona DNS enviará un mensaje de error al cliente solicitante.

¡Lo tienes!

- Verdadero
- (•) Falso

3. ¿Cuál de los siguientes es mostrado por la utilidad nslookup?

¡Lo tienes!

- (•) el servidor DNS predeterminado configurado
- la dirección IP del dispositivo final
- todas las entradas DNS almacenadas en caché

4. ¿Cuál de los siguientes tipos de registros de recursos DNS resuelve los servidores de nombres autorizados?

¡Lo tienes!

- (•) NS
- servidor
- MX
- AAAA

5. ¿Verdadero o falso? Los clientes DHCP envían un mensaje de solicitud DHCP a los servidores DHCP disponibles.

¡Lo tienes!

- Verdadero
- (•) Falso

Correct

You have successfully identified the correct answers.

1. DNS AAAA records are used to resolve names to IPv6 addresses.
2. The correct answer is False. When a DNS server receives a name resolution request for a name not within its zone, the serve will forward the request to another DNS server.
3. By issuing the **nslookup** command, the default DNS server that is configured is displayed.
4. NS records resolve authoritative name servers. DNS A records resolve IPv4 addresses. AAAA records resolve IPv6 addresses, and MX records resolve mail exchange servers.
5. The correct answer is False. There are four DHCP messages exchanged between clients and servers. The client initiates the DHCP process with a DHCP discover message to available DHCP servers.

You got 5 out of 5 questions correct.

1. Which of the following DNS record types is used to resolve IPv6 addresses?

You got it!

- ○ A
- ○ NS
- ◉ AAAA
- ○ MX

2. True or false? A DNS server that receives a request for a name resolution that is not within its DNS zone will send a failure message to the requesting client.

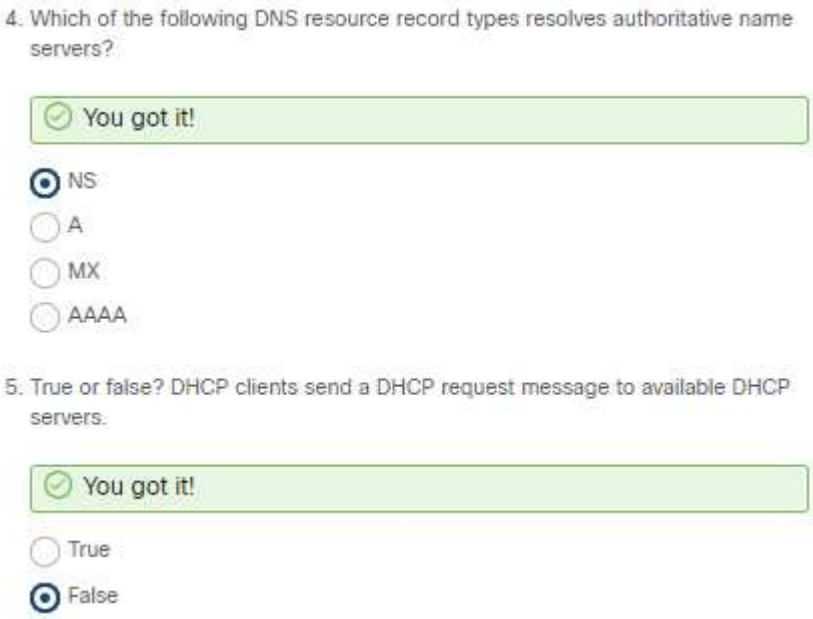
You got it!

- ○ True
- ◉ False

3. Which of the following is displayed by the nslookup utility?

You got it!

- ◉ the configured default DNS server
- ○ the IP address of the end device
- ○ all cached DNS entries



Capa de aplicación / Servicios de intercambio de archivos

Servicios de intercambio de archivos

15.5.1

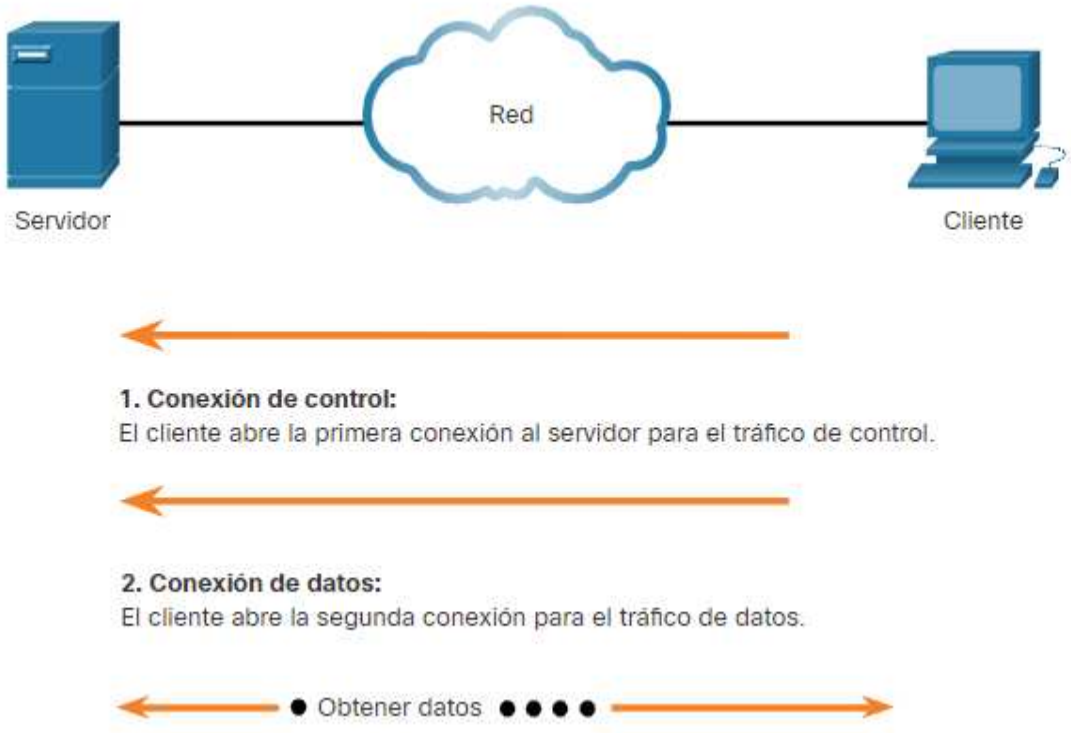
Protocolo de transferencia de archivos

Como aprendió en temas anteriores, en el modelo cliente/servidor, el cliente puede cargar datos a un servidor y descargar datos desde un servidor, si ambos dispositivos utilizan un protocolo de transferencia de archivos (FTP). Al igual que los protocolos HTTP, correo electrónico y direccionamiento, FTP es comúnmente utilizado protocolo de capa de aplicación. En este tema se analiza el FTP con más detalle.

El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.

La figura representa una transacción FTP. Un cliente se pone en contacto con un servidor a través de una red. Conexión de control: El cliente abre la primera conexión al servidor para el tráfico de control. El segundo mensaje del cliente es una conexión de datos: el cliente abre

una segunda conexión para datos borradores. El cliente solicita datos del servidor mediante el comando Get Data.



De acuerdo con el comando enviado a través de la conexión de control, los datos pueden descargarse desde el servidor o subirse desde el cliente.

El cliente establece la primera conexión al servidor para controlar el tráfico en el puerto TCP 21. El tráfico consiste en comandos de cliente y respuestas de servidor.

El cliente establece la segunda conexión al servidor para la transferencia de datos propiamente dicha por medio del puerto 20 de TCP. Esta conexión se crea cada vez que hay datos para transferir.

La transferencia de datos se puede producir en ambas direcciones. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos).

15.5.2

Bloque de mensajes del servidor

El bloque de mensajes del servidor (SMB) es un protocolo de intercambio de archivos cliente/servidor que describe la estructura de los recursos de red compartidos, como archivos, directorios, impresoras y puertos serie. Es un protocolo de solicitud-respuesta. Todos los

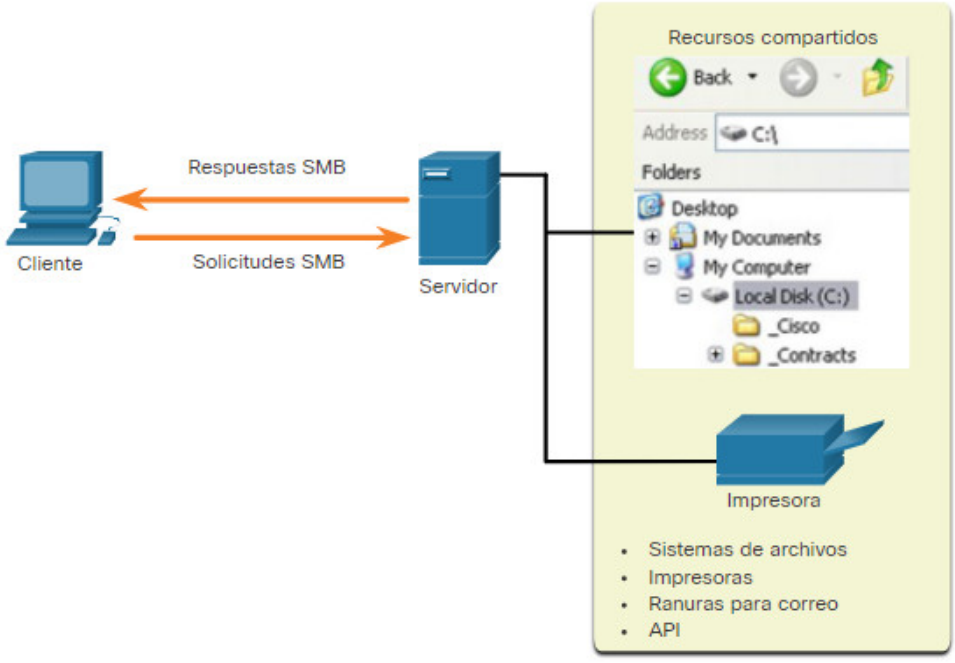
mensajes SMB comparten un mismo formato. Este formato utiliza un encabezado de tamaño fijo seguido de un parámetro de tamaño variable y un componente de datos.

Aquí hay tres funciones de mensajes SMB:

- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a los archivos y a las impresoras
- Autorizar una aplicación para enviar o recibir mensajes para o de otro dispositivo

Los servicios de impresión y transferencia de archivos SMB se han transformado en el pilar de las redes de Microsoft. Con la presentación de la serie de software Windows 2000, Microsoft cambió la estructura subyacente para el uso de SMB. En versiones anteriores de los productos de Microsoft, los servicios de SMB utilizaban un protocolo que no es TCP/IP para implementar la resolución de nombres. A partir de Windows 2000, todos los productos subsiguientes de Microsoft utilizan la convención de nomenclatura DNS, que permite que los protocolos TCP/IP admitan directamente el uso compartido de recursos de SMB, como se muestra en la figura.

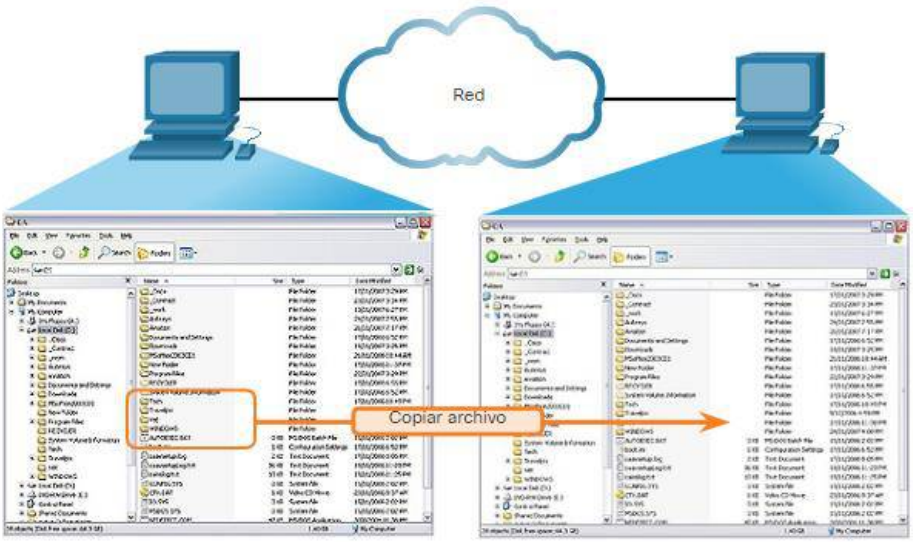
SMB es un protocolo del tipo cliente-servidor, solicitud-respuesta. Los servidores pueden hacer que sus recursos estén disponibles en la red para que los usen los clientes.



La figura muestra un recurso compartido de Microsoft Windows de Mis documentos con solicitudes de cliente de un servidor Mis documentos. El cliente envía una solicitud SMB y recibe una respuesta SMB del recurso compartido Mis documentos. Los recursos

compartidos incluyen sistemas de archivos, Printers mostrados como un icono, ranuras de correo y API.

El proceso de intercambio de archivos de SMB entre equipos Windows se muestra en la siguiente figura:



Se puede copiar un archivo de una PC a otra con Windows Explorer y usando el protocolo SMB.

La figura representa un archivo de copia que tiene lugar entre dos equipos Windows que forman un sistema de archivos al otro a través de la red.

A diferencia del protocolo para compartir archivos admitido por FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de establecer la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

Los sistemas operativos LINUX y UNIX también proporcionan un método de intercambio de recursos con redes de Microsoft mediante una versión del SMB llamado SAMBA. Los sistemas operativos Macintosh de Apple también admiten recursos compartidos utilizando el protocolo SMB.

15.5.3

Verifique sus conocimientos: servicios de compatir archivos

Elija la MEJOR repuesta para las siguientes preguntas y compruebe su conocimiento sobre servicios de compartir archivos.

Correcto

Identificó bien las respuestas correctas.

1. FTP requiere dos conexiones entre el cliente y el servidor. Una conexión está a través del puerto 21 para comandos de cliente y respuestas de servidor. La otra conexión es a través del puerto 20 para la transferencia de datos.
2. La respuesta correcta es verdadero. La transferencia de datos a través de FTP puede tener lugar en cualquier dirección, cargas de cliente a servidor o descargas de servidor a cliente.
3. Los puertos 20 y 21 son utilizados por FTP.
4. La respuesta correcta es falso. El uso compartido de recursos a través de SMB también es compatible con Apple Macintosh. Los sistemas operativos Linux y Unix utilizan una versión de SMB llamada SAMBA.

Has tenido 4 respuestas correctas de 4.

1. ¿Cuántas conexiones requiere FTP entre el cliente y el servidor?

¡Lo tienes!

- ○ 1
- ◉ 2
- ○ 3
- ○ 4

2. ¿Verdadero o falso? Las transferencias de datos FTP tienen lugar de cliente a servidor (push) y de servidor a cliente (pull).

¡Lo tienes!

- ◉ Verdadero
- ○ Falso

3. ¿Cuáles de estos puertos son utilizados por FTP? (Escoja dos opciones).

¡Lo tienes!

- ☑ 20
- ☑ 21
- ☐ 25
- ☐ 110

4. ¿Verdadero o falso? El uso compartido de recursos a través de SMB solo se admite en los sistemas operativos de Microsoft.

¡Lo tienes!

- ○ Verdadero
- ◉ Falso

Correct

You have successfully identified the correct answers.

1. FTP requires two connections between the client and the server. One connection is over port 21 for client commands and server replies. The other connection is over port 20 for data transfer.
2. The correct answer is True. Data transfer over FTP can take place in either direction, uploads from client to server, or downloads from server to client.
3. Ports 20 and 21 are used by FTP.
4. The correct answer is False. Resource sharing over SMB is also supported by Apple Macintosh. Linux and Unix operating systems use a version of SMB called SAMBA.

You got 4 out of 4 questions correct.

1. How many connections are required by FTP between client and server?

You got it!

- ○ 1
- ◉ 2
- ○ 3
- ○ 4

2. True or false? FTP data transfers take place from client to server (push) and from server to client (pull).

You got it!

- ◉ True
- ○ False

3. Which of these ports are used by FTP? (Choose two.)

You got it!

- ☑ 20
- ☑ 21
- ☐ 25
- ☐ 110

4. True or false? Resource sharing over SMB is only supported on Microsoft operating systems.

You got it!

- ○ True
- ◉ False

Práctica del Módulo y Cuestionario

15.6.1

¿Qué aprenderé en este módulo?

Aplicación, Presentación y Sesión

En los modelos OSI y TCP/IP La capa de aplicación es la más cercana al usuario final. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. La capa de presentación tiene tres funciones principales: formatear o presentar datos en el dispositivo de origen en un formulario compatible para recibirlos por el dispositivo de destino, comprimir los datos de forma que el dispositivo de destino pueda descomprimir y cifrar los datos para su transmisión y descifrar los datos al recibirlos - Sí. La capa de sesión crea y mantiene diálogos entre las aplicaciones de origen y de destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado. Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet. Los protocolos son utilizados tanto por los dispositivos de origen como de destino durante una sesión. Los protocolos implementados tanto en el host de origen como en el de destino deben ser compatibles.

Cliente a Servidor

En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más flujos de datos al cliente. En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos sin tener un servidor dedicado. Todo terminal conectado puede funcionar como servidor y como cliente. Un equipo puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las aplicaciones P2P requieren que cada terminal proporcione una interfaz de usuario y ejecute un servicio en segundo plano. Algunas aplicaciones P2P utilizan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices que apuntan a las ubicaciones de los recursos están almacenados en un directorio centralizado. Muchas aplicaciones P2P permiten que los usuarios compartan partes de varios archivos con otro usuario a la vez. Los clientes utilizan un pequeño archivo llamado archivo torrent para localizar a otros usuarios que tienen las piezas que necesitan y conectarse directamente a ellos. Este archivo también contiene información sobre los equipos de seguimiento que realizan el seguimiento de qué usuarios tienen qué archivos.

Protocolos de Correo y WEB

Cuando se escribe una dirección web o un localizador uniforme de recursos (URL) en un navegador web, el navegador establece una conexión con el servicio web. El servicio web se está ejecutando en el servidor que está utilizando el protocolo HTTP. HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un navegador web, envía una solicitud a un servidor web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son GET, POST y PUT HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el flujo de datos se cifra con capa de sockets seguros (SSL) antes de transportarse a través de la red. El correo electrónico soporta tres protocolos separados para funcionar: SMTP, POP e IMAP. El proceso de capa de aplicaciones que envía correo utiliza el SMTP. Un cliente recupera el correo electrónico mediante POP o IMAP. Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo del mensaje puede contener la cantidad de texto que se desee, el encabezado debe contar con una dirección de correo electrónico de destinatario correctamente formateada y una dirección de emisor. POP es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo. Con POP, el correo se descarga desde el servidor al cliente y después se elimina en el servidor. Con IMAP a diferencia de POP, cuando el usuario se conecta a un servidor con capacidad IMAP, se descargan copias de los mensajes a la aplicación cliente. Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente.

Servicios de Direccionamiento IP

El protocolo del DNS define un servicio automatizado que coincide con los nombres de recursos que tienen la dirección de red numérica solicitada. El protocolo de comunicaciones DNS utiliza un formato de mensaje para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores. DNS utiliza nombres de domino para formar la jerarquía. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. La utilidad nslookup permite que el usuario consulte manualmente los servidores de nombres para resolver un nombre de host determinado. DHCP para IPv4 este servicio automatiza la asignación de direcciones IPv4, máscaras de subred, gateway y otros parámetros de redes IPv4. DHCPv6 proporciona servicios similares para clientes IPv6, excepto que no proporciona una dirección de puerta de enlace predeterminada. Cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.

Servicios de Compartir Archivos

Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP. El cliente establece la primera conexión al servidor para controlar el tráfico en el puerto TCP 21. El cliente establece la segunda

conexión al servidor para la transferencia de datos propiamente dicha por medio del puerto 20 de TCP. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos). Aquí hay tres funciones de los mensajes SMB pueden iniciar, autenticar y terminar sesiones, controlar el acceso a archivos e impresoras, y permitir que una aplicación envíe mensajes a otro dispositivo o los reciba de él. A diferencia del protocolo para compartir archivos admitido por FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de establecer la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

15.6.2

Módulo Quiz - Capa de aplicación

Correct

You have successfully identified the correct answers.

Has tenido 15 respuestas correctas de 15.

1. ¿Qué protocolo se puede usar para transferir mensajes de un servidor de correo electrónico a un cliente de correo electrónico?

Tema 15.3.0 - SMTP se usa para enviar correos del cliente al servidor, mientras que POP3 se usa para descargar el correo del servidor al cliente. Los protocolos HTTP y SNMP no están relacionados con el correo electrónico.

- a dedicated file server
- a home router
- an ISP DHCP server
- a DNS server

2. Cuando se recuperan mensajes de correo electrónico, ¿qué protocolo permite un almacenamiento y una copia de seguridad sencillos y centralizados de los correos electrónicos que sería deseable para una pequeña y mediana empresa?

Tema 15.3.0 - IMAP es preferido para pequeñas y medianas empresas, ya que IMAP permite el almacenamiento centralizado y la copia de seguridad de correos electrónicos, con copias de los correos electrónicos que se envían a los clientes. POP entrega los correos electrónicos a los clientes y los elimina en el servidor de correo electrónico. SMTP se utiliza para enviar correos electrónicos y no para recibirlos. HTTPS no se utiliza para la navegación web segura.

- .com
- www
- http
- index

3. ¿Cuál protocolo de la capa de aplicación se utiliza para permite a las aplicaciones de Microsoft el uso compartido de archivos y los servicios de impresión?

Tema 15.5.0 - SMB se utiliza para el uso compartido de archivos y los servicios de impresión. El sistema operativo Linux también proporciona un método de intercambio de recursos con redes de Microsoft mediante una versión de SMB llamada SAMBA.

- [ ] responsibility for logical addressing
- [ ] responsibility for physical addressing
- [x] the creation and maintenance of dialogue between source and destination applications
- [x] closest to the end user
- [ ] the establishing of window size

4. Un autor está cargando el documento de un capítulo de una computadora personal al servidor de archivos de una editorial. ¿Qué papel toma la computadora personal en este modelo de red?

Tema 15.2.0 - En el modelo de red de cliente/servidor, un dispositivo de red toma el papel del servidor para proporcionar un servicio particular, como la transferencia y el almacenamiento de archivos. El dispositivo que solicita el servicio toma el papel del cliente. Si hay presente un servidor exclusivo, el modelo de red será el de cliente/servidor aunque no sea necesario utilizarlo. En cambio, el modelo de red entre pares no tiene un servidor exclusivo.

- (•) Cliente
- ( ) Maestro
- ( ) Servidor
- ( ) Esclavo

5. ¿Qué afirmación sobre FTP es verdadera?

Tema 15.5.0 - FTP es un protocolo cliente/servidor. FTP requiere dos conexiones entre el cliente y el servidor y utiliza TCP para proporcionar conexiones confiables. Con FTP la transferencia de datos se puede producir en ambas direcciones. El cliente puede descargar (extraer) datos del servidor o cargar (insertar) datos al servidor.

- ( ) El cliente puede elegir si FTP va a establecer una o dos conexiones con el servidor.
- (•) El cliente puede descargar (extraer) datos del servidor o cargar (insertar) datos al servidor.
- ( ) FTP e una aplicacio Cliente a Servidor.
- ( ) FTP no proporciona fiabilidad durante la transmisión de datos.

6. Un host inalámbrico debe solicitar una dirección IP. ¿Qué protocolo se utilizaría para procesar la solicitud?

Tema 15.4.0 - El protocolo DHCP se utiliza para solicitar, emitir y administrar la información de asignación de direcciones IP. CSMA/CD es el método de acceso que se utiliza con redes Ethernet por cable. ICMP se utiliza para probar la conectividad. SNMP se utiliza con la administración de redes, y FTP se utiliza para la transferencia de archivos.

- ( ) HTTP
- ( ) SMTP
- ( ) DHCP
- (•) SMB

7. ¿Qué capa del modelo TCP/IP es la más cercana al usuario final?

Tema 15.1.0 - Los usuarios finales usan aplicaciones para interactuar con la red y utilizarla. La capa de aplicación del modelo TCP/IP es la más cercana al usuario final. Los protocolos de capa de aplicación se usan para comunicar e intercambiar mensajes con otras aplicaciones y dispositivos de red. Las capas del modelo TCP/IP son, de arriba abajo, aplicación, transporte, Internet y acceso a la red (regla mnemotécnica ATIA).

- [ ] Aplicación
- [x] Internet
- [x] Acceso a la red
- [x] Transporte
- [ ] IP
- [ ] UDP

8. ¿Cuáles son los tres protocolos o estándares que se usan en la capa de aplicación del modelo TCP/IP? Elija tres opciones.

Tema 15.1.0 - HTTP, MPEG y GIF funcionan en las capas de la aplicación del modelo TCP/IP. TCP y UDP funcionan en la capa de transporte. IP funciona en la capa de Internet.

- ( ) Large networks send more requests for domain to IP address resolution than do smaller networks.
- ( ) DHCP uses a reliable transport layer protocol.
- ( ) It prevents sharing of files that are copyrighted.
- (•) It is a more efficient way to manage IPv4 addresses than static address assignment is.
- ( ) Hosts on large networks require more IPv4 addressing configuration settings than do hosts on small networks.

9. ¿Qué protocolo utiliza cifrado?

Tema 15.1.0 - HTTPS utiliza Secure Socket Layer (SSL) para cifrar el tráfico al que se accede desde un servidor web.

- (•) client
- ( ) master
- ( ) server
- ( ) slave
- ( ) transient

10. ¿Por qué se prefiere el uso de DHCP en redes grandes?

Tema 15.4.0 - La asignación de direcciones IP estáticas, se requiere personal que configure manualmente las direcciones de red en cada host de red. Las redes grandes pueden cambiar con frecuencia y tienen muchos más hosts para configurar que las redes pequeñas. DHCP proporciona una forma mucho más eficaz de configurar y administrar las direcciones IP en redes grandes que la asignación de direcciones estáticas.

- ( ) Las redes grandes envían más solicitudes de resolución de dominio a dirección IP que las redes pequeñas.
- (•) DHCP usa un protocolo de capa de transporte confiable.
- ( ) Evita que se compartan archivos que tienen derechos de autor.
- ( ) Es una forma más eficaz de administrar direcciones IP que la asignación de direcciones estáticas.

11. ¿Cuáles son las dos tareas que puede realizar un servidor DNS local? Elija dos opciones.

Tema 15.4.0 - Dos funciones importantes del DNS son proporcionar direcciones IP para nombres de dominio (como www.cisco.com) y reenviar las solicitudes que no se pueden resolver a otros servidores a fin de proporcionar nombres de dominio para la traducción de direcciones IP.DHCP proporciona información de asignación de direcciones IP a los dispositivos locales. Un protocolo de transferencia de archivos, como FTP, SFTP o TFTP, proporciona servicios de transferencia de archivos. IMAP y POP se pueden utilizar para recuperar un mensaje de correo electrónico de un servidor.

- ◯ Proporcionar direcciones IP a los hosts locales.
- ◯ Permitir la transferencia de datos entre dos dispositivos de red.
- ◉ Asignar nombres a direcciones IP para los hosts internos.
- ◯ Reenviar solicitudes de resolución de nombres entre servidores.
- ◯ Recuperar mensajes de correo electrónico.

12. En una red doméstica, ¿qué dispositivo tiene más posibilidades de proporcionar una asignación de direcciones IP dinámica a los clientes en dicha red?

Tema 15.4.0 - En una red doméstica, un router doméstico suele funcionar como servidor DHCP. El router doméstico se encarga de la asignación dinámica de direcciones IP a los clientes de la red doméstica. Los ISP también usan DHCP, pero este suele asignar direcciones IP a la interfaz de Internet del router doméstico, no a los clientes de la red doméstica. En las redes comerciales, es habitual que haya un servidor de archivos u otro servidor exclusivo para que proporcione servicios DHCP a la red. Por último, un servidor DNS se encarga de buscar la dirección IP para un URL, no de proporcionar una asignación dinámica de direcciones a los clientes de una red.

- ◉ Un servidor de archivos exclusivo
- ◯ Un router doméstico
- ◯ Un servidor DHCP del ISP
- ◯ Un servidor DNS

13. ¿Qué parte del URL http://www.cisco.com/index.html representa el dominio DNS de nivel superior?

Tema 15.4.0 - Los componentes del URL http://www.cisco.com/index.htm son los siguientes: -http = protocolo
-www = parte del nombre del servidor
-cisco = parte del nombre de dominio
-index = nombre de archivo
-com = dominio de nivel superior

- ◉ IMAP
- ◯ POP
- ◯ SMTP
- ◯ HTTPS

14. ¿Cuáles de las siguientes son dos características de la capa de aplicación del modelo TCP/IP? Elija dos opciones.

Tema 15.1.0 - La capa de aplicación del modelo TCP/IP es la que se encuentra más cerca del usuario final y proporciona la interfaz entre aplicaciones. Es responsable de dar formato a los datos, comprimirlos y cifrarlos, y se utiliza para crear y mantener diálogos entre las aplicaciones de origen y de destino.

- ◯ Es responsable de asignar direcciones lógicas.
- ◯ Es responsabilidad de asignar direcciones físicas.
- ◯ Crea y mantiene diálogos entre las aplicaciones de origen y de destino.
- ◉ Es la capa más cercana al usuario final.

15. ¿Qué tipo de mensaje utiliza un cliente HTTP para solicitar datos desde un servidor web?

Tema 15.3.0 - Los clientes HTTP envían mensajes GET para solicitar datos desde servidores web.

- [ ] providing IP addresses to local hosts
- [ ] allowing data transfer between two network devices
- [x] mapping name-to-IP addresses for internal hosts
- [x] forwarding name resolution requests between servers
- [ ] retrieving email messages

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. On a home network, which device is most likely to provide dynamic IPv4 addressing to clients on the home network?

Topic 15.4.0 - On a home network, a home router usually serves as the DHCP server. The home router is responsible for dynamically assigning IPv4 addresses to clients on the home network. ISPs also use DHCP, but it usually assigns an IPv4 address to the Internet interface of the home router, not the clients on the home network. In businesses, it is common to have a file or other dedicated server provide DHCP services to the network. Finally, a DNS server is responsible for finding the IP address for a URL, not for providing dynamic addressing to network clients.

- ( ) a dedicated file server
- (•) a home router
- ( ) an ISP DHCP server
- ( ) a DNS server

2. What part of the URL, http://www.cisco.com/index.html, represents the top-level DNS domain?

Topic 15.4.0 - The components of the URL http://www.cisco.com/index.htm are as follows:

- http = protocol
- www = part of the server name
- cisco = part of the domain name
- index = file name
- com = the top-level domain

- (•) .com
- ( ) www
- ( ) http
- ( ) index

3. What are two characteristics of the application layer of the TCP/IP model? (Choose two.)

Topic 15.1.0 - The application layer of the TCP/IP model is the layer that is closest to the end user, providing the interface between the applications. It is responsible for formatting, compressing, and encrypting data, and is used to create and maintain dialog between source and destination applications.

- [ ] responsibility for logical addressing
- [ ] responsibility for physical addressing
- [x] the creation and maintenance of dialogue between source and destination applications
- [x] closest to the end user
- [ ] the establishing of window size

4. What message type is used by an HTTP client to request data from a web server?

Topic 15.3.0 - HTTP clients send GET messages to request data from web servers.

- (•) GET
- ( ) POST
- ( ) PUT
- ( ) ACK

5. Which protocol can be used to transfer messages from an email server to an email client?

Topic 15.3.0 - SMTP is used to send mail from the client to the server but POP3 is used to download mail from the server to the client. HTTP and SNMP are protocols that are unrelated to email.

- ( ) SMTP
- (•) POP3
- ( ) SNMP
- ( ) HTTP

6. Which application layer protocol is used to provide file-sharing and print services to Microsoft applications?

Topic 15.5.0 - SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.

- ( ) HTTP
- ( ) SMTP
- ( ) DHCP
- (•) SMB

7. Which three protocols or standards are used at the application layer of the TCP/IP model? (Choose three.)

Topic 15.1.0 – HTTP, MPEG, and GIF operate at the application layer of the TCP/IP model. TCP and UDP operate at the transport layer. IP operates at the internet layer.

- [ ] TCP
- [x] HTTP
- [x] MPEG
- [x] GIF
- [ ] IP
- [ ] UDP

8. Why is DHCP for IPv4 preferred for use on large networks?

Topic 15.4.0 – Static IPv4 address assignment requires personnel to configure each network host with addresses manually. Large networks can change frequently and have many more hosts to configure than do small networks. DHCP provides a much more efficient means of configuring and managing IPv4 addresses on large networks than does static address assignment.

- ( ) Large networks send more requests for domain to IP address resolution than do smaller networks.
- ( ) DHCP uses a reliable transport layer protocol.
- ( ) It prevents sharing of files that are copyrighted.
- (•) It is a more efficient way to manage IPv4 addresses than static address assignment is.
- ( ) Hosts on large networks require more IPv4 addressing configuration settings than do hosts on small networks.

9. An author is uploading one chapter document from a personal computer to a file server of a book publisher. What role is the personal computer assuming in this network model?

Topic 15.2.0 – In the client/server network model, a network device assumes the role of server in order to provide a particular service such as file transfer and storage. The device requesting the service assumes the role of client. In the client/server network model, a dedicated server does not have to be used, but if one is present, the network model being used is the client/server model. In contrast, the peer-to-peer network model does not have a dedicated server.

- (•) client
- ( ) master
- ( ) server
- ( ) slave
- ( ) transient

10. Which statement is true about FTP?

Topic 15.5.0 – FTP is a client/server protocol. FTP requires two connections between the client and the server and uses TCP to provide reliable connections. With FTP, data transfer can happen in either direction. The client can download (pull) data from the server or upload (push) data to the server.

- ( ) The client can choose if FTP is going to establish one or two connections with the server.
- (•) The client can download data from or upload data to the server.
- ( ) FTP is a peer-to-peer application.
- ( ) FTP does not provide reliability during data transmission.

11. A wireless host needs to request an IPv4 address. What protocol would be used to process the request?

Topic 15.4.0 – The DHCP protocol is used to request, issue, and manage IP addressing information. CSMA/CD is the access method used with wired Ethernet. ICMP is used to test connectivity. SNMP is used with network management and FTP is used for file transfer.

- ◯ FTP
- ◯ HTTP
- ◉ DHCP
- ◯ ICMP
- ◯ SNMP

12. Which TCP/IP model layer is closest to the end user?

Topic 15.1.0 – End users use applications to interact with and use the network. The application layer of the TCP/IP model is closest to the end user. Application layer protocols are used to communicate and exchange messages with other network devices and applications. The layers of the TCP/IP model are from top to bottom (memory aid – ATIN): application, transport, internet, network access

- ◉ application
- ◯ internet
- ◯ network access
- ◯ transport

13. When retrieving email messages, which protocol allows for easy, centralized storage and backup of emails that would be desirable for a small- to medium-sized business?

Topic 15.3.0 – IMAP is preferred for small-to medium-sized businesses as IMAP allows centralized storage and backup of emails, with copies of the emails being forwarded to clients. POP delivers the emails to the clients and deletes them on the email server. SMTP is used to send emails and not to receive them. HTTPS is not used for secure web browsing.

- ◉ IMAP
- ◯ POP
- ◯ SMTP
- ◯ HTTPS

14. Which protocol uses encryption?

Topic 15.1.0 - HTTPS uses Secure Socket Layer (SSL) to encrypt traffic accessed from a web server.

- ◯ DHCP
- ◯ DNS
- ◯ FTP
- ◉ HTTPS

15. Which two tasks can be performed by a local DNS server? (Choose two.)

Topic 15.4.0 - Two important functions of DNS are to (1) provide IP addresses for domain names such as www.cisco.com, and (2) forward requests that cannot be resolved to other servers in order to provide domain name to IP address translation. DHCP provides IP addressing information to local devices. A file transfer protocol such as FTP, SFTP, or TFTP provides file sharing services. IMAP or POP can be used to retrieve an email message from a server.

- [ ] providing IP addresses to local hosts
- [ ] allowing data transfer between two network devices
- [x] mapping name-to-IP addresses for internal hosts
- [x] forwarding name resolution requests between servers
- [ ] retrieving email messages

Capítulo 16_Fundamentos de seguridad de la red

Introducción

16.0.1

¿Por qué debería tomar este módulo?

¡Bienvenido a Network Security Fundamentals!

Es posible que ya haya configurado una red o que esté preparándose para hacerlo. Aquí hay algo en lo que pensar. Establecer una red sin asegurarla es como abrir todas las puertas y ventanas de tu casa y luego ir de vacaciones. Cualquiera podría venir, ganar entrada, robar o romper objetos, o simplemente hacer un desastre. Como han visto en las noticias, es posible entrar en *cualquier* red! Como administrador de red, es parte de su trabajo dificultar el acceso a su red a los actores de amenazas. Este módulo le ofrece una visión general de los tipos de ataques de red y lo que puede hacer para reducir las posibilidades de éxito de un actor de amenazas. También cuenta con actividades Packet Tracer que le permiten practicar algunas técnicas básicas para la seguridad de la red. Si tiene una red, pero no es lo más segura posible, ¡entonces querrá leer este módulo ahora mismo!

16.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Fundamentos de seguridad de la red

Objetivos del módulo: Configure switches y routers con características de protección de dispositivos para mejorar la seguridad.

Título del tema	Objetivo del tema
Vulnerabilidades y amenazas a la seguridad	Explique por qué son necesarias las medidas básicas de seguridad en los dispositivos de red.
Ataques a la red	Identifique las vulnerabilidades de seguridad.
Mitigación de los ataques a la red	Identifique las técnicas generales de mitigación.
Seguridad de los dispositivos	Configure dispositivos de red con funciones de refuerzo de dispositivos para mitigar amenazas de seguridad.

Fundamentos de seguridad de la red / Vulnerabilidades y amenazas a la seguridad

Vulnerabilidades y amenazas a la seguridad

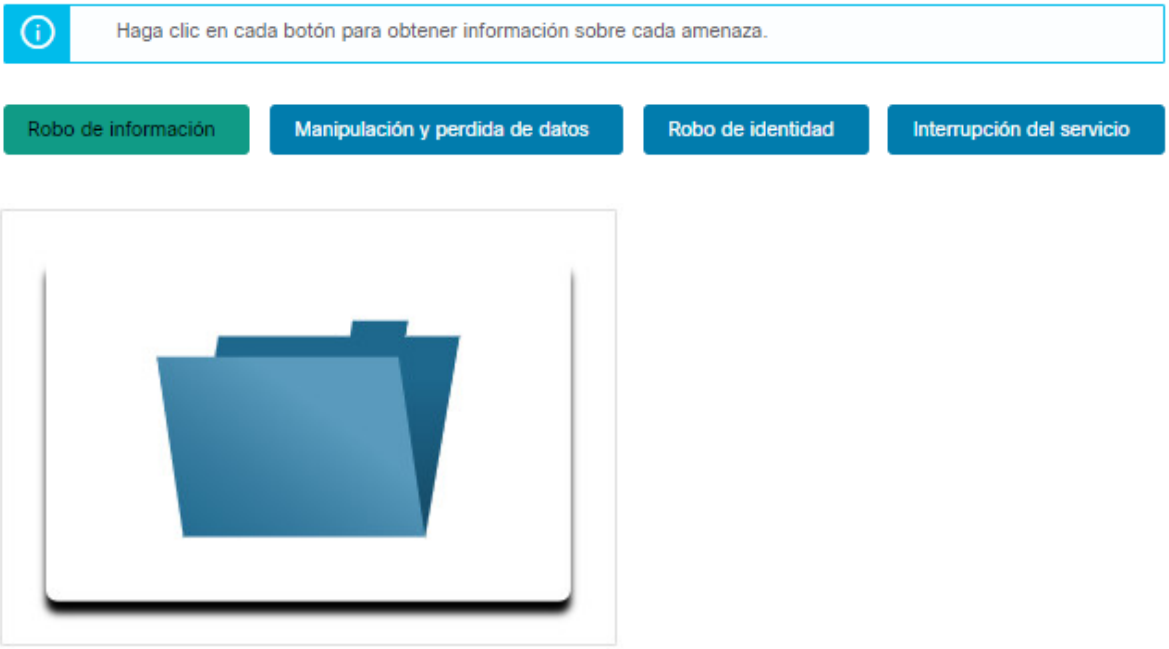
16.1.1

Tipos de amenazas

Las redes de computadoras cableadas e inalámbricas son esenciales para las actividades cotidianas. Tanto las personas como las organizaciones dependen de las computadoras y de las redes. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden resultar en una pérdida de tiempo y dinero debido a daños o robo de información o activos importantes.

Los intrusos pueden obtener acceso a una red a través de vulnerabilidades de software, ataques de hardware o adivinando el nombre de usuario y la contraseña de alguien. Los intrusos que obtienen acceso modificando software o explotando vulnerabilidades de software se denominan actores de amenazas.

Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas.



Robo de información is breaking into a computer to obtain confidential information. Information can be used or sold for various purposes. Example: robar la información de propiedad de una organización, como datos de investigación y desarrollo.

Manipulación y perdida de datos está entrando en una computadora para destruir o alterar los registros de datos. Un ejemplo de pérdida de datos es un actor de amenaza que envía un

virus que formatea el disco duro de una computadora. Un ejemplo de manipulación de datos es irrumpir en un sistema de registros para cambiar información, como el precio de un artículo.

Robo de información | Manipulación y perdida de datos | Robo de identidad | Interrupción del servicio

Robo de identidad es una forma de robo de información en la que se roba información personal con el fin de apoderarse de la identidad de alguien. Con esta información, un actor de amenazas puede obtener documentos legales, solicitar crédito y realizar compras en línea no autorizadas. Identificar el robo es un problema creciente que cuesta miles de millones de dólares por año.

Robo de información | Manipulación y perdida de datos | Robo de identidad | Interrupción del servicio

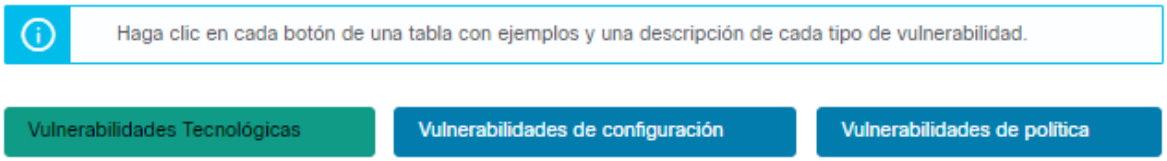
Servicio de Disrupción is preventing legitimate users from accessing services to which they are entitled. Examples: ataques de denegación de servicio (DoS) en servidores, dispositivos de red o enlaces de comunicaciones de red.

16.1.2

Tipos de vulnerabilidades

La vulnerabilidad es el grado de debilidad en una red o un dispositivo. Algún grado de vulnerabilidad es inherente a los enrutadores, conmutadores, equipos de escritorio, servidores e incluso dispositivos de seguridad. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales: política tecnológica, de configuración y de seguridad. Las tres fuentes de vulnerabilidades pueden dejar una red o dispositivo abierto a varios ataques, incluidos ataques de código malicioso y ataques de red.



Vulnerabilidades Tecnológicas

Vulnerabilidad	Descripción
Debilidad del protocolo TCP/IP	• Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), y el Protocolo de mensajes de control de Internet (ICMP) son inherentes inseguro. • Simple Network Management Protocol (SNMP) y Simple Mail Transfer Protocolo (SMTP) están relacionados con la estructura inherentemente insegura en el que se diseñó TCP.
Debilidades de los sistemas operativos	• Cada sistema operativo tiene problemas de seguridad que deben abordarse. • UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 • Están documentados en el Equipo de respuesta ante emergencias informáticas (CERT) archivos en http://www.cert.org
Debilidad de los equipos de red	Varios tipos de equipos de red, como enrutadores, firewalls y tienen debilidades de seguridad que deben reconocerse y protegerse en contra. Sus debilidades incluyen la protección con contraseña, la falta de autenticación, protocolos de enrutamiento y agujeros de firewall.

Vulnerabilidades de configuración

Vulnerabilidad	Descripción
Cuentas de usuario no seguras	La información de la cuenta de usuario puede transmitirse de forma insegura a través de la , exponiendo nombres de usuario y contraseñas a actores de amenazas.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común es el resultado de contraseñas de usuario mal creadas.
Servicios de internet mal configurados	Activar JavaScript en navegadores web permite ataques mediante JavaScript controlado por actores de amenazas al acceder a sitios que no son de confianza. Otras posibles fuentes de deficiencias incluyen una terminal mal configurada servicios, FTP o servidores web (por ejemplo, Microsoft Internet Information Servicios (IIS) y Apache HTTP Server.
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que crean o habilitan agujeros en de texto claro.
Equipos de red mal configurados	Las configuraciones incorrectas del equipo en sí pueden causar una seguridad significativa del switch. Por ejemplo, listas de acceso mal configuradas, protocolos de enrutamiento o Las cadenas de comunidad SNMP pueden crear o habilitar agujeros en la seguridad.

Vulnerabilidades Tecnológicas | Vulnerabilidades de configuración | Vulnerabilidades de política

Vulnerabilidades de política

Vulnerabilidad	Descripción
Falta de políticas de seguridad por escrito	Una política de seguridad no se puede aplicar o hacer cumplir consistentemente si es no escrito.
Políticas	Las batallas políticas y las guerras territoriales pueden dificultar la implementación de una política de seguridad coherente.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, fácilmente descifradas o predeterminadas pueden permitir acceso no autorizado a la red.
Controles de acceso lógico no aplicados	El monitoreo y la auditoría inadecuados permiten ataques y uso no autorizado para continuar, desperdiciando los recursos de la empresa. Esto podría dar lugar a acciones legales o terminación contra técnicos de TI, administración de TI, o incluso la empresa liderazgo que permite que estas condiciones inseguras persistan.
La instalación de software y hardware y los cambios no respetan la política	Cambios no autorizados a la topología de red o instalación de aplicación no aprobada crear o habilitar agujeros en la seguridad.
No existe plan de recuperación tras un desastre	La falta de un plan de recuperación ante desastres permite el caos, el pánico y la confusión. cuando se produce un desastre natural o un actor de amenaza ataca a la enterprise.

16.1.3

Seguridad física

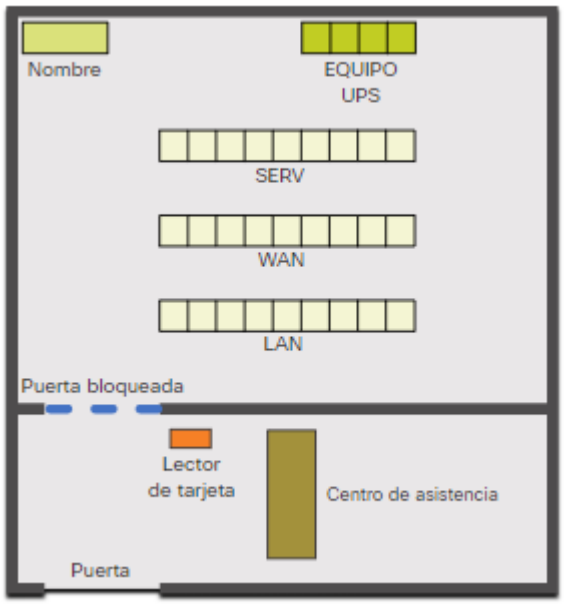
Un área vulnerable igualmente importante de la red a considerar es la seguridad física de los dispositivos. Si los recursos de la red pueden verse comprometidos físicamente, un actor de amenazas puede negar el uso de los recursos de la red.

Las cuatro clases de amenazas físicas son las siguientes:

- **Amenazas de Hardware -** Esto incluye daños físicos a servidores, enrutadores, conmutadores, planta de cableado y estaciones de trabajo.
- **Amenazas del Entorno -** Esto incluye temperaturas extremas (demasiado calor o demasiado frío) o temperaturas extremas (demasiado húmedo o demasiado seco).
- **Amenazas Eléctricas -** Esto incluye picos de voltaje, voltaje de suministro insuficiente (caídas de voltaje), energía no condicionada (ruido) y pérdida total de energía.
- **Amenazas de Mantenimiento -** Esto incluye un manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado deficiente y etiquetado deficiente.

Se debe crear e implementar un buen plan de seguridad física para abordar estos problemas. La figura muestra un ejemplo de plan de seguridad física.

Planifique la seguridad física para limitar el daño al equipo



- Sala de informática segura.
- Implemente seguridad física para limitar el daño al equipo.

Paso 1. Mantenga los equipos bajo llave y evite el acceso no autorizado por puertas, techos, pisos elevados, ventanas, canales y conductos de ventilación.

Paso 2. Controle la entrada del armario con registros electrónicos.

Paso 3. Utilice cámaras de seguridad.

La figura es un cuadrado que representa una sala de computadoras. Dentro de la sala de ordenadores en la esquina superior izquierda, es un pequeño rectángulo etiquetado, AC. Arriba a la derecha esquina, cuatro cuadrados están conectados y etiquetados, UPS BAY. En el centro de la hay tres filas de cuadrados, servidores etiquetados, WAN y LAN. La parte inferior de la sala de computadoras se divide para crear una habitación separada. Existe es una sección punteada del divisor etiquetada, puerta cerrada. Dentro de la es un escritorio de ayuda, un lector de tarjetas, así como otra puerta en el exterior.

16.1.4

Verifique su comprensión - Amenazas y vulnerabilidades de seguridad

Verifique su comprensión de las amenazas y vulnerabilidades de seguridad eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

1. Enviar un virus que formateará el disco duro de una computadora es un ejemplo de pérdida de datos o amenaza de manipulación.
2. El uso de información de identidad o crédito robado para realizar compras ilegales en línea es un ejemplo de robo de identidad.
3. La interrupción de los ataques de servicio se produce cuando se impide a los usuarios legítimos acceder a los datos y servicios.
4. Robar datos de investigación o información propietaria es un ejemplo de robo de información.
5. La interrupción de los ataques de servicio se produce cuando se impide a los usuarios legítimos acceder a los datos y servicios o a la red.
6. Alterar registros de datos es un ejemplo de pérdida o manipulación de datos.
7. Robar registros de datos o información propietaria es un ejemplo de robo de información.
8. Usar información de identidad para hacerse pasar por alguien para obtener crédito es un ejemplo de robo de identidad.

Has tenido 8 respuestas correctas de 8.

Correct

1. Sending a virus that will format the hard drive of a computer is an example of data loss or manipulation threat.
2. Using stolen credit or identity information to make illegal online purchases is an example of identity theft.
3. Disruption of service attacks occur when legitimate users are prevented from accessing data and services.
4. Stealing research data or proprietary information is an example of information theft.
5. Disruption of service attacks occur when legitimate users are prevented from accessing data and services or the network.
6. Altering data records is an example of data loss or manipulation.
7. Stealing data records or proprietary information is an example of information theft.
8. Using identity information to impersonate someone to obtain credit is an example of identity theft.

You got 8 out of 8 questions correct.

1. ¿Qué tipo de amenaza se describe cuando un actor de amenazas le envía un virus que puede reformatear su disco duro?

¡Lo tienes!

- (●) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- ( ) el robo de identidad
- ( ) Robo de información

2. ¿Qué tipo de amenaza se describe cuando un actor de amenazas realiza compras ilegales en línea utilizando información de crédito robada?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- (●) el robo de identidad
- ( ) Robo de información

3. ¿Qué tipo de amenaza se describe cuando un actor de amenazas impide que los usuarios legales accedan a los servicios de datos?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- (●) Interrupción del servicio
- ( ) el robo de identidad
- ( ) Robo de información

4. ¿Qué tipo de amenaza se describe cuando un actor de amenaza roba datos de investigación científica?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- ( ) el robo de identidad
- (●) Robo de información

5. ¿Qué tipo de amenaza se describe cuando un actor de amenazas sobrecarga una red para denegar el acceso a la red a otros usuarios?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- (●) Interrupción del servicio
- ( ) el robo de identidad
- ( ) Robo de información

6. ¿Qué tipo de amenaza se describe cuando un actor de amenazas altera los registros de datos?

¡Lo tienes!

- (●) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- ( ) el robo de identidad
- ( ) Robo de información

7. ¿Qué tipo de amenaza se describe cuando un actor de amenazas está robando la base de datos de usuarios de una empresa?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- ( ) el robo de identidad
- (●) Robo de información

8. ¿Qué tipo de amenaza se describe cuando un actor de amenaza se hace pasar por otra persona para obtener información crediticia sobre esa persona?

¡Lo tienes!

- ( ) pérdida o manipulación de datos
- ( ) Interrupción del servicio
- (●) el robo de identidad
- ( ) Robo de información

1. What kind of threat is described when a threat actor sends you a virus that can reformat your hard drive?

You got it!

- (●) data loss or manipulation
- ( ) disruption of service
- ( ) identify theft
- ( ) information theft

2. What kind of threat is described when a threat actor makes illegal online purchases using stolen credit information?

You got it!

- ( ) data loss or manipulation
- ( ) disruption of service
- (●) identify theft
- ( ) information theft

3. What kind of threat is described when a threat actor prevents legal users from accessing data services?

You got it!

- ○ data loss or manipulation
- ◉ disruption of service
- ○ identify theft
- ○ information theft

4. What kind of threat is described when a threat actor steals scientific research data?

You got it!

- ○ data loss or manipulation
- ○ disruption of service
- ○ identify theft
- ◉ information theft

5. What kind of threat is described when a threat actor overloads a network to deny other users network access?

You got it!

- ○ data loss or manipulation
- ◉ disruption of service
- ○ identify theft
- ○ information theft

6. What kind of threat is described when a threat actor alters data records?

You got it!

- ◉ data loss or manipulation
- ○ disruption of service
- ○ identify theft
- ○ information theft

7. What kind of threat is described when a threat actor is stealing a company's user database?

You got it!

- ○ data loss or manipulation
- ○ disruption of service
- ○ identify theft
- ◉ information theft

8. What kind of threat is described when a threat actor impersonates another person to obtain credit information about that person?

You got it!

- ○ data loss or manipulation
- ○ disruption of service
- ◉ identify theft
- ○ information theft

Fundamentos de seguridad de la red / Ataques de red

Ataques de red

16.2.1

Tipos de malware

En el tema anterior se explicaban los tipos de amenazas de red y las vulnerabilidades que hacen posibles las amenazas. En este tema se detalla más detalladamente cómo los actores de amenazas obtienen acceso a la red o restringen el acceso a los usuarios autorizados.

Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones "malas" o ilegítimas en los datos, hosts o redes. Los virus, gusanos y caballos de Troya son tipos de malware.

Viruses

Un virus informático es un tipo de malware que se propaga mediante la inserción de una copia de sí mismo en otro programa, del que pasa a formar parte. Se propaga de una computadora a otra, dejando infecciones a medida que viaja. La gravedad de los virus puede variar desde causar efectos ligeramente molestos hasta dañar datos o software y causar condiciones de denegación de servicio (DoS). Casi todos los virus se adjuntan a un archivo ejecutable, lo que significa que el virus puede existir en un sistema, pero no estará activo ni será capaz de propagarse hasta que un usuario ejecute o abra el archivo o programa host malicioso. Cuando se ejecuta el código del host, el código viral se ejecuta también. Normalmente, el programa host sigue funcionando después de que el virus lo infecta. Sin embargo, algunos virus sobrescriben otros programas con copias de sí mismos, lo que destruye el programa host por completo. Los virus se propagan cuando el software o documento al que están adjuntos se transfiere de una computadora a otra mediante la red, un disco, el intercambio de archivos o archivos adjuntos de correo electrónico infectados.

Worms

Los gusanos informáticos son similares a los virus en que se replican en copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo host infectado, los gusanos son software independiente y no requieren de un programa host ni de la ayuda humana para propagarse. Un gusano no necesita unirse a un programa para infectar un host y entrar en una computadora a través de una vulnerabilidad en el sistema. Los gusanos se aprovechan de las características del sistema para viajar a través de la red sin ayuda.

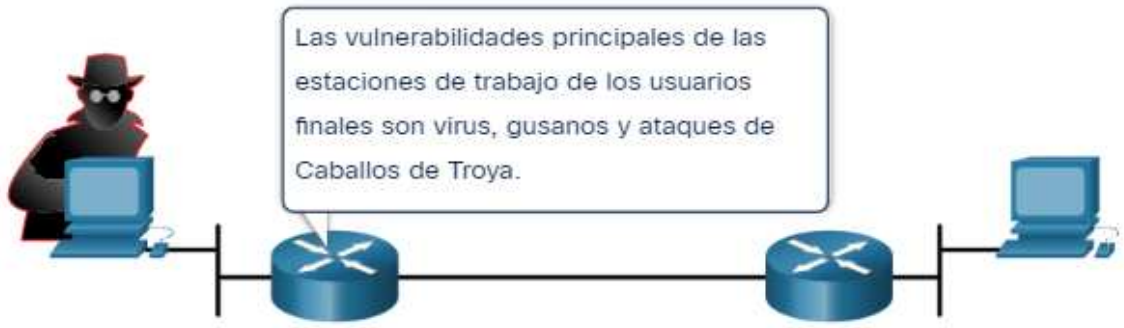
Trojan Horses

Un caballo de Troya es otro tipo de malware que lleva el nombre del caballo de madera que los griegos utilizaron para infiltrarse en Troya. Es una pieza de software dañino que parece legítimo. Los usuarios suelen ser engañados para cargarlo y ejecutarlo en sus sistemas. Después de activarse, puede lograr cualquier número de ataques al host, desde irritar al usuario (con

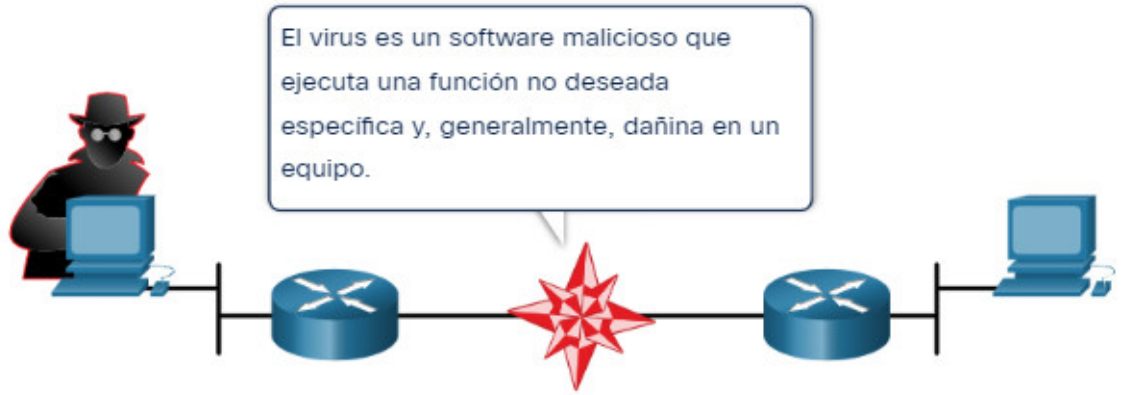
ventanas emergentes excesivas o cambiar el escritorio) hasta dañar el host (eliminar archivos, robar datos o activar y difundir otro malware, como los virus). Los caballos de Troya también son conocidos por crear puertas traseras para que usuarios maliciosos puedan acceder al sistema.

A diferencia de los virus y gusanos, los caballos de Troya no se reproducen al infectar otros archivos. Se autoreplican. Los caballos de Troya deben extenderse a través de la interacción del usuario, como abrir un archivo adjunto de correo electrónico o descargar y ejecutar un archivo de Internet.

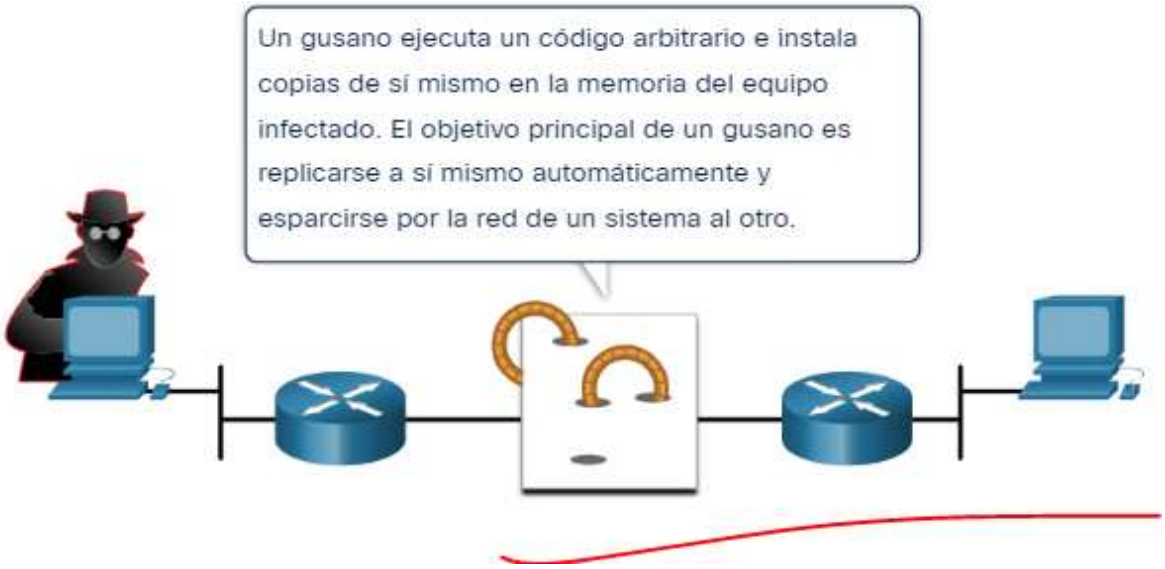
Haga clic en Reproducir en la figura para ver una explicación animada de los tres tipos de malware.



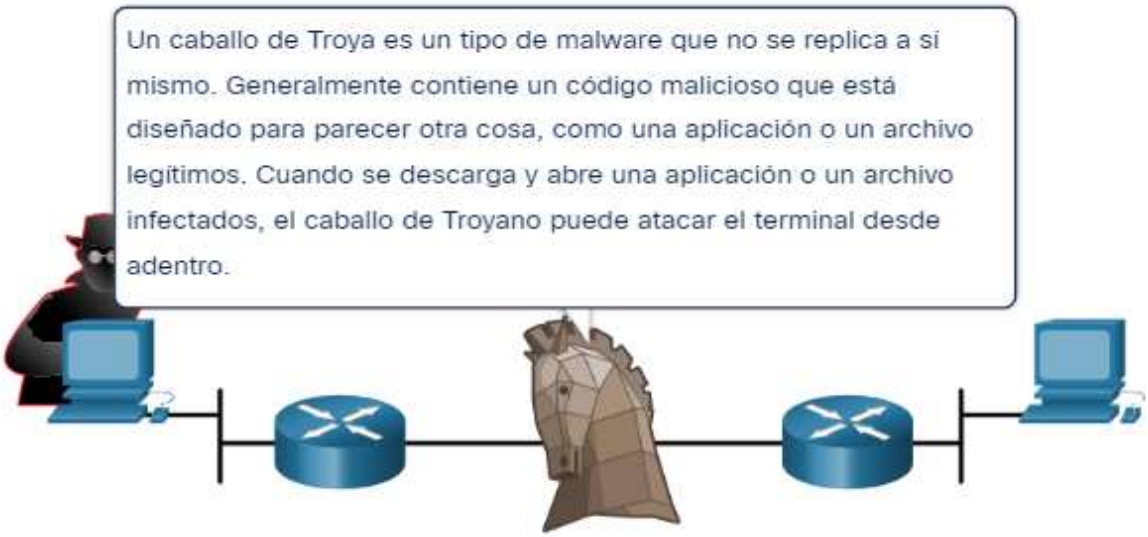
Las vulnerabilidades principales de las estaciones de trabajo de los usuarios finales son virus, gusanos y ataques de Caballos de Troya.



El virus es un software malicioso que ejecuta una función no deseada específica y, generalmente, dañina en un equipo.



Un gusano ejecuta un código arbitrario e instala copias de sí mismo en la memoria del equipo infectado. El objetivo principal de un gusano es replicarse a sí mismo automáticamente y esparcirse por la red de un sistema al otro.



Un caballo de Troya es un tipo de malware que no se replica a sí mismo. Generalmente contiene un código malicioso que está diseñado para parecer otra cosa, como una aplicación o un archivo legítimos. Cuando se descarga y abre una aplicación o un archivo infectados, el caballo de Troyano puede atacar el terminal desde adentro.

16.2.2

Ataques de reconocimiento

Además de los ataques de código malintencionado, es posible que las redes sean presa de diversos ataques de red. Los ataques de red pueden clasificarse en tres categorías principales:

- **Ataques de reconocimiento** \ - El descubrimiento y mapeo de sistemas, servicios o vulnerabilidades.
- **Ataques de acceso** \ - La manipulación no autorizada de datos, acceso al sistema o privilegios de usuario.
- **Denegación de servicio** \ - La desactivación o corrupción de redes, sistemas o servicios.

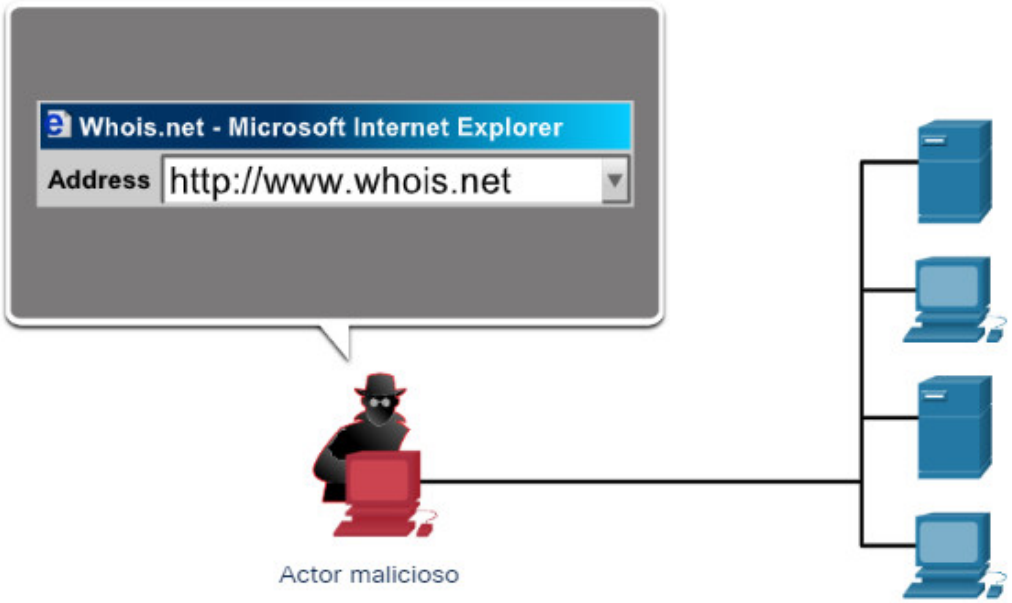
Para los ataques de reconocimiento, los actores de amenazas externas pueden usar herramientas de Internet, **nslookup** como los servicios públicos, **whois** para determinar fácilmente el espacio de direcciones IP asignado a una determinada corporación o entidad. Una vez que se determina el espacio de la dirección IP, un actor de amenazas puede hacer ping a las direcciones IP disponibles públicamente para identificar las direcciones que están activas. Para ayudar a automatizar este paso, un actor de amenazas puede usar una herramienta de barrido de ping, como **fping** o **gping**. Esto hace ping sistemáticamente a todas las direcciones de red en un rango o subred dado. Esto es similar a revisar una sección de una guía telefónica y llamar a cada número para ver quién atiende.

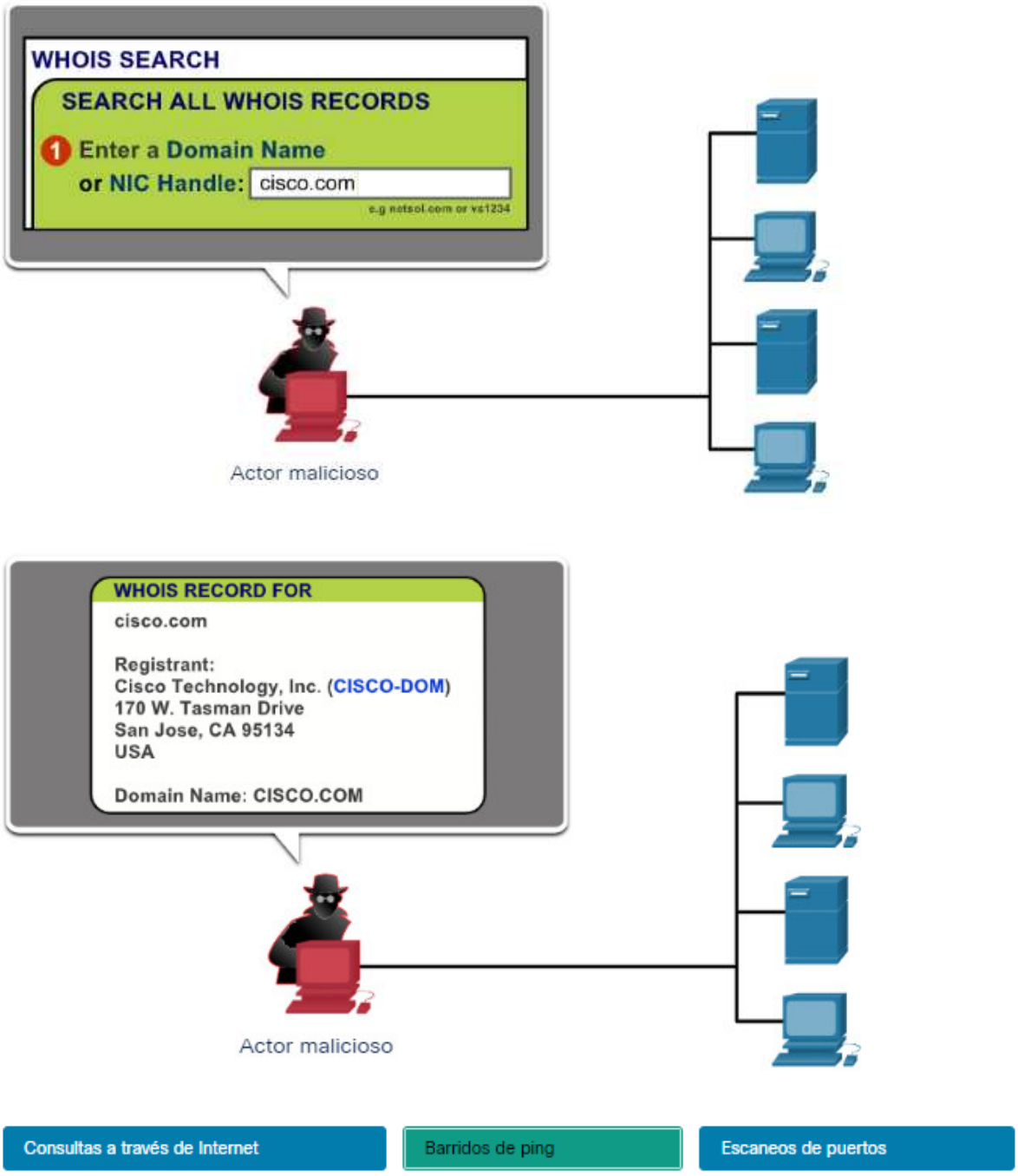
Haga clic en cada tipo de herramienta de ataque de reconocimiento para ver una animación del ataque.

Consultas a través de Internet | Barridos de ping | Escaneos de puertos

Consultas a través de Internet (Internet Queries)

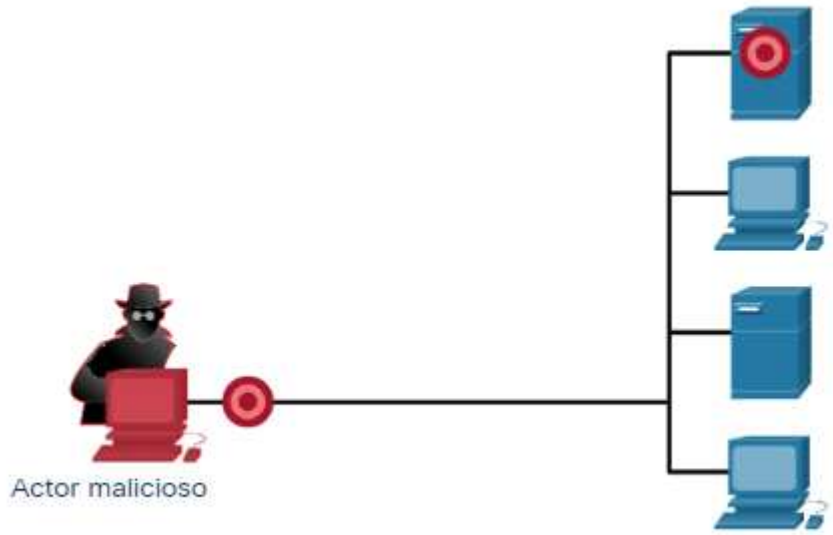
Haga clic en Reproducir en la figura para ver una animación. El actor de la amenaza está buscando información inicial sobre un objetivo. Se pueden usar varias herramientas, incluida la búsqueda de Google, los sitios web de las organizaciones, quién es y más.

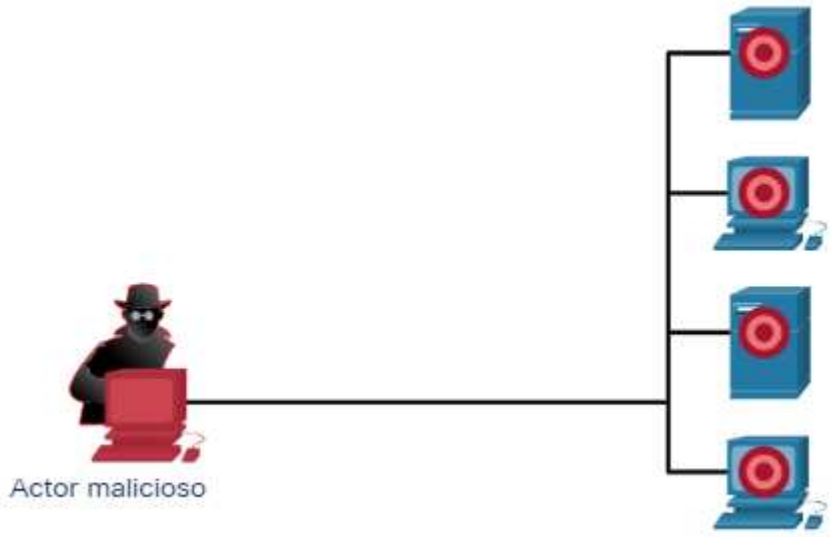


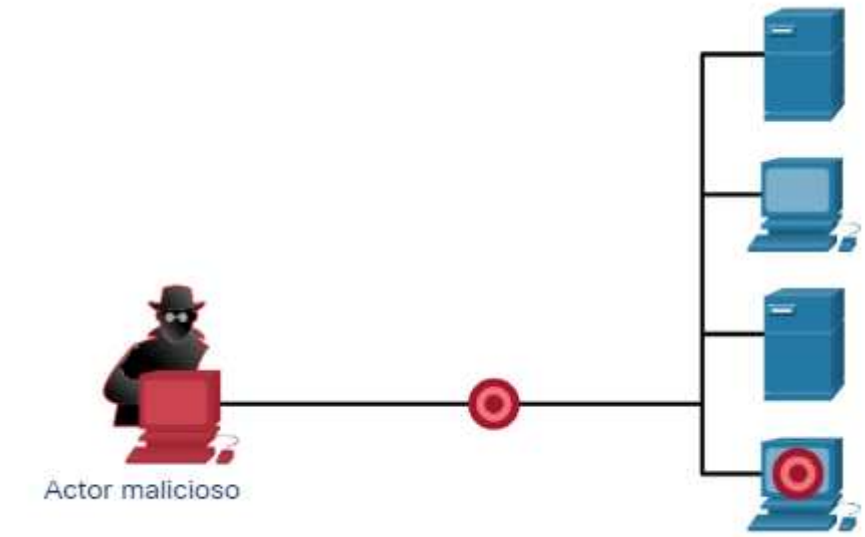


Barridos de Ping (Ping Sweeps)

Haga clic en Reproducir en la figura para ver una animación. El actor de la amenaza inicia un barrido de ping para determinar qué direcciones IP están activas.


Actor malicioso

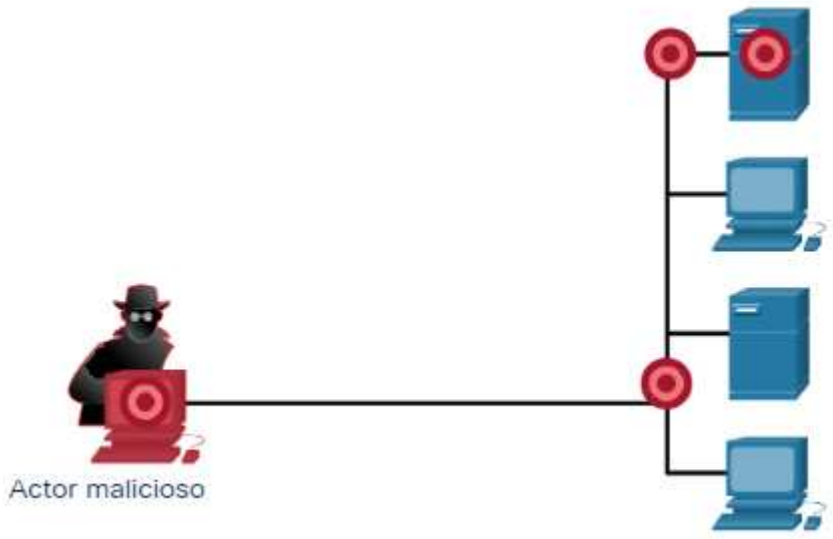

Actor malicioso

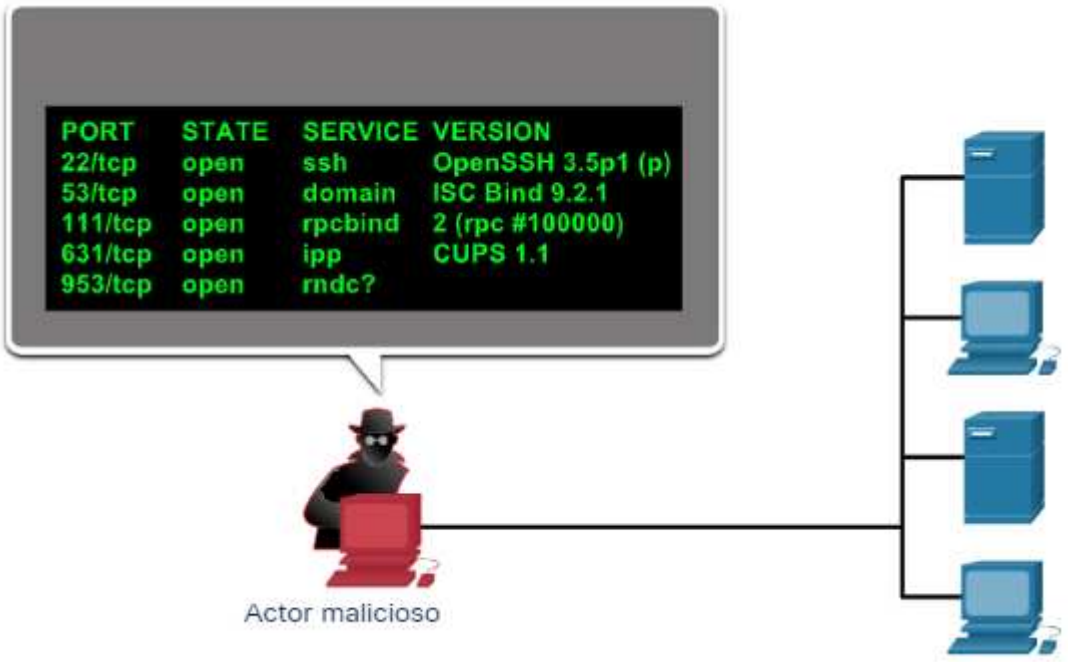


Consultas a través de Internet | Barridos de ping | Escaneos de puertos

Escaneos de puertos (Port Scans)

Haga clic en Reproducir en la figura para ver una animación de un actor de amenazas que realiza un escaneo de puertos en las direcciones IP activas descubiertas.

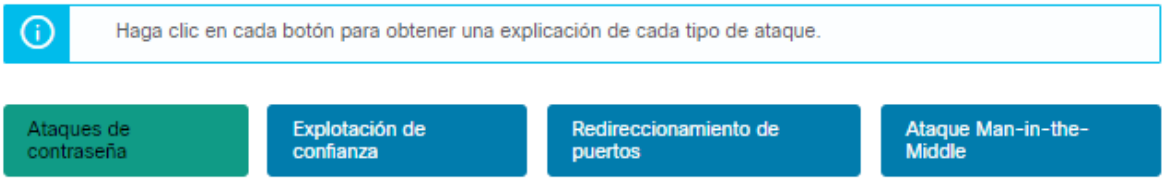




16.2.3

Ataques con acceso

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios FTP y los servicios Web para obtener acceso a las cuentas Web, a las bases de datos confidenciales y demás información confidencial. Un ataque de acceso permite a las personas obtener acceso no autorizado a información que no tienen derecho a ver. Los ataques de acceso se pueden clasificar en cuatro tipos: ataques de contraseña, explotación de confianza, redirección de puertos y man-in-the middle.

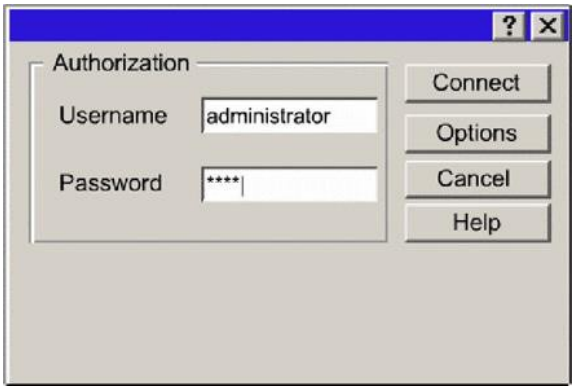


Ataques de contraseña

Los actores de amenazas pueden implementar ataques de contraseña utilizando varios métodos diferentesds:

- Ataques por fuerza bruta Ataques de caballos de* Troya
- Programas detectores de paquetes

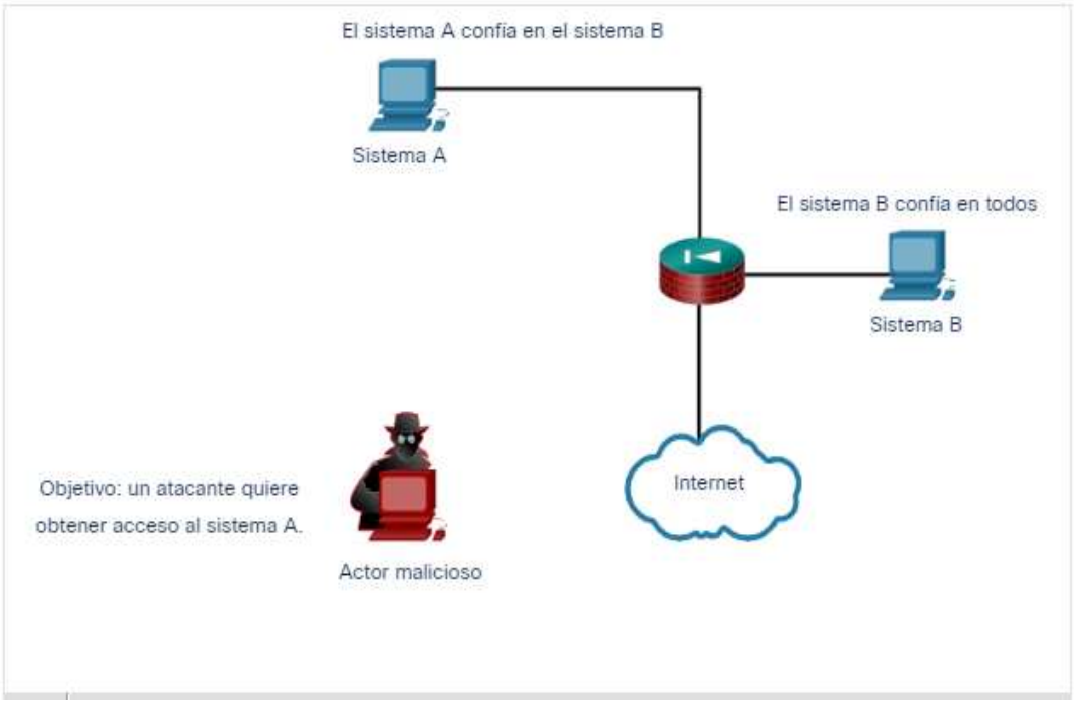
La primera figura muestra un cuadro de solicitud de inicio de sesión con el nombre de usuario, administrador y la contraseña, ****.



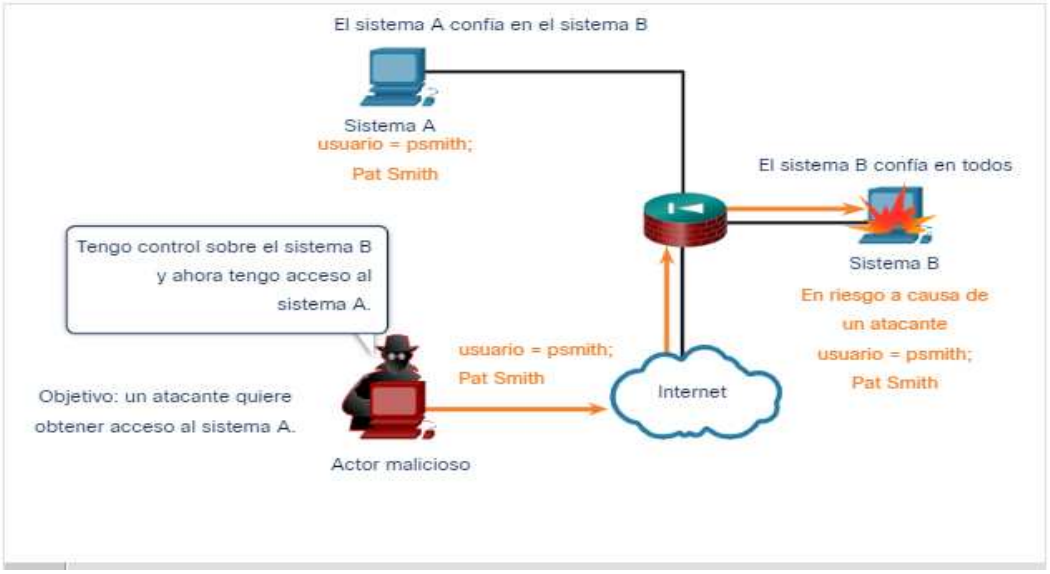
Ataques de contraseña | Explotación de confianza | Redireccionamiento de puertos | Ataque Man-in-the-Middle

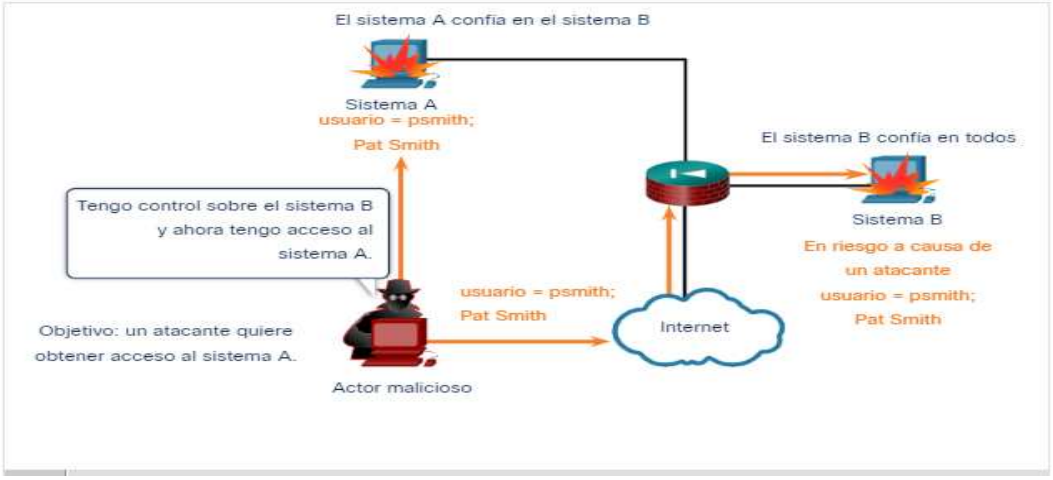
Explotación de confianza

En un ataque de explotación de confianza, un actor de amenazas utiliza privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo el objetivo. En la Figura 1, haga clic en Reproducir en la animación para ver un ejemplo de ataque de host de confianza.



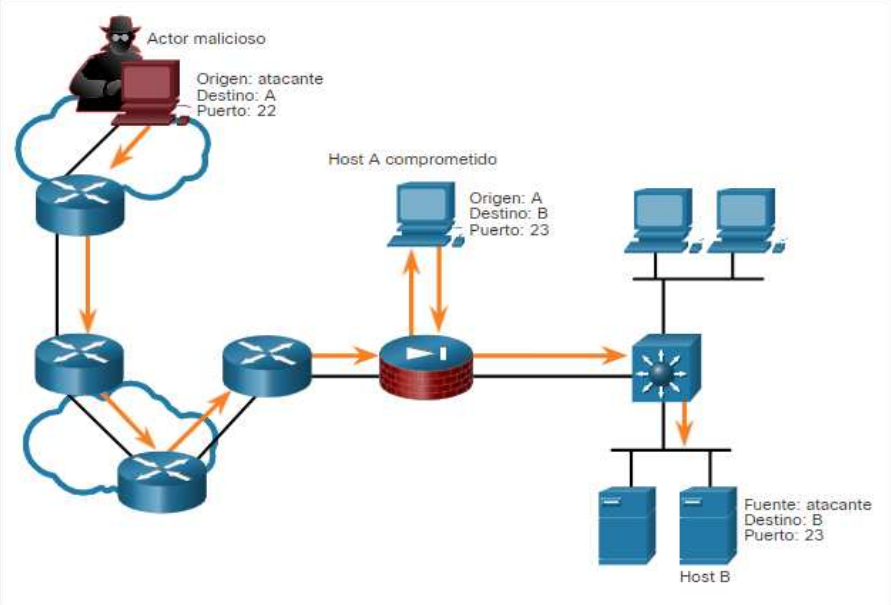
El sistema A confía en el sistema B
Sistema A
usuario = psmith;
Pat Smith
El sistema B confía en todos
Sistema B
En riesgo a causa de
un atacante
usuario = psmith;
Pat Smith
No puedo obtener acceso al sistema A, pero el sistema B está abierto.
usuario = psmith;
Pat Smith
Internet
Objetivo: un atacante quiere obtener acceso al sistema A.
Actor malicioso

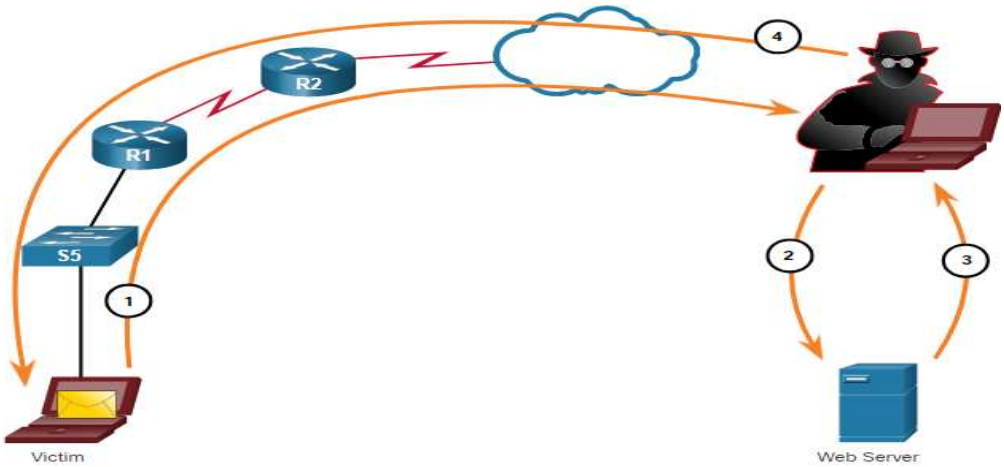

El sistema A confía en el sistema B
Sistema A
usuario = psmith;
Pat Smith
El sistema B confía en todos
Sistema B
En riesgo a causa de
un atacante
usuario = psmith;
Pat Smith
Tengo control sobre el sistema B y ahora tengo acceso al sistema A.
usuario = psmith;
Pat Smith
Internet
Objetivo: un atacante quiere obtener acceso al sistema A.
Actor malicioso


El sistema A confía en el sistema B
Sistema A
usuario = psmith;
Pat Smith
El sistema B confía en todos
Sistema B
En riesgo a causa de
un atacante
usuario = psmith;
Pat Smith
Tengo control sobre el sistema B y ahora tengo acceso al sistema A.
usuario = psmith;
Pat Smith
Internet
Objetivo: un atacante quiere obtener acceso al sistema A.
Actor malicioso

Redireccionamiento de puertos

Redireccionamiento de puertos: esto ocurre cuando un agente de amenaza utiliza un sistema en atacado como base para ataques contra otros objetivos. El ejemplo de la figura muestra un actor de amenaza que usa SSH (puerto 22) para conectarse a un host A comprometido. El host B confía en el host A y, por lo tanto, el actor de amenaza puede usar Telnet (puerto 23) para acceder a él.





Paso 1. Cuando una víctima solicita una página web, la solicitud se dirige a la computyadora del actor de la amenaza.

Paso 2. La computadora del actor de amenza recibe la solicitud y recupera la págiina real del sito web legítimo.

Paso 3. El actor de amenzas puede alterar la página web legítima y realizar los cambios en los datos.

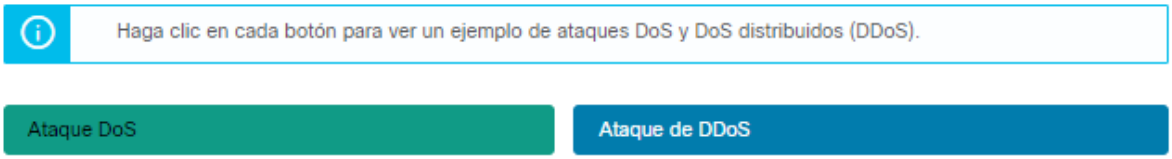
Paso 4. El actor de la amenaza reenvía la página solicitada a la víctima.

16.2.4

Ataques de denegación de servicio

Los ataques de denegación de servicio (DoS) son la forma de ataque más publicitada y una de las más difíciles de eliminar. Sin embargo, debido a su facilidad de implementación y daño potencialmente significativo, los ataques DoS merecen una atención especial por parte de los administradores de seguridad.

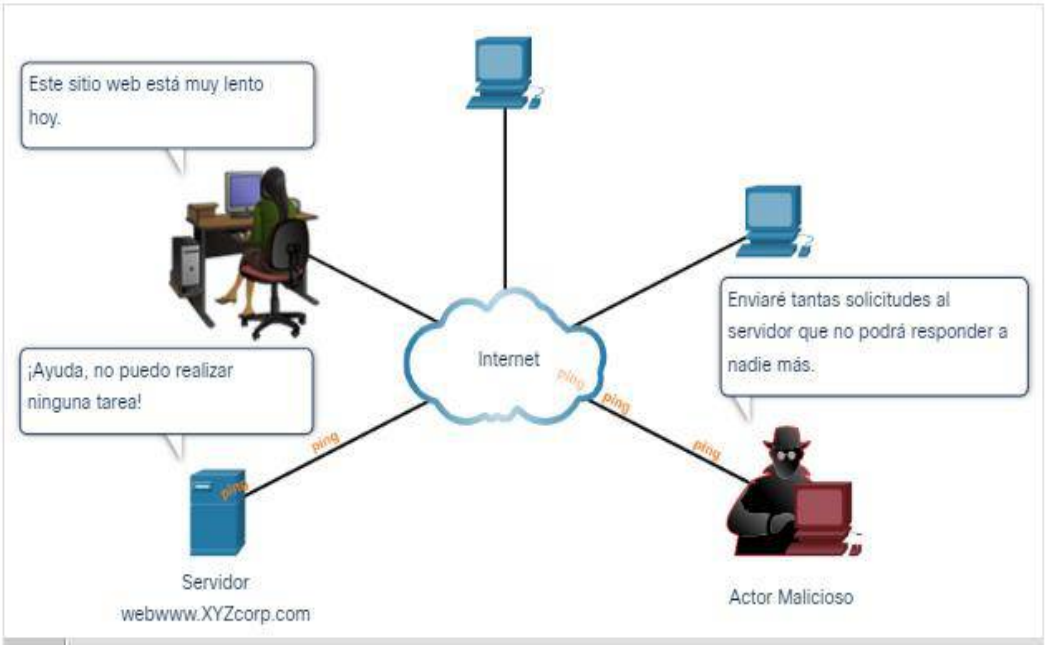
Los ataques DoS tienen muchas formas. Fundamentalmente, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema. Para prevenir los ataques de DoS es importante estar al día con las actualizaciones de seguridad más recientes de los sistemas operativos y las aplicaciones.



Ataque DoS

Los ataques de DoS son un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de ejecutar, incluso si lo hace un agente de amenaza inexperto.

Haga clic en Reproducir en la figura para ver las animaciones de un ataque DDoS.

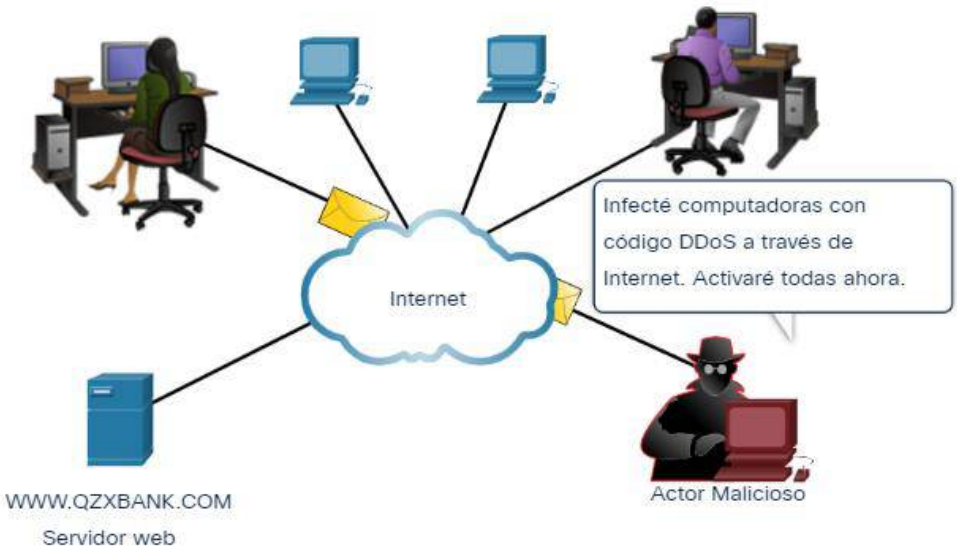


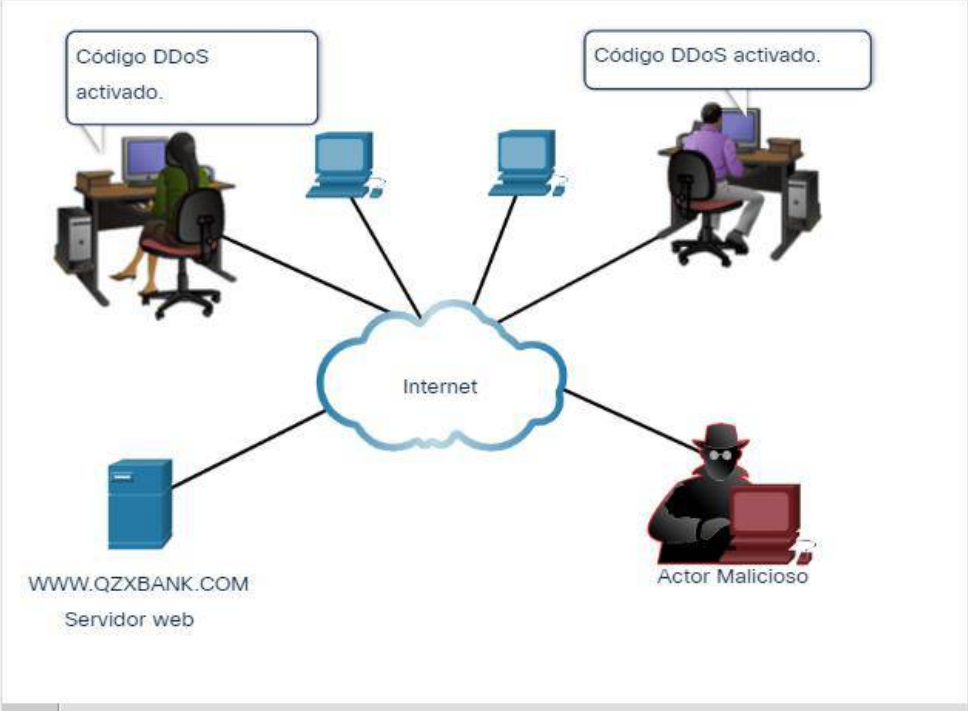
Ataque DoS | Ataque de DDoS

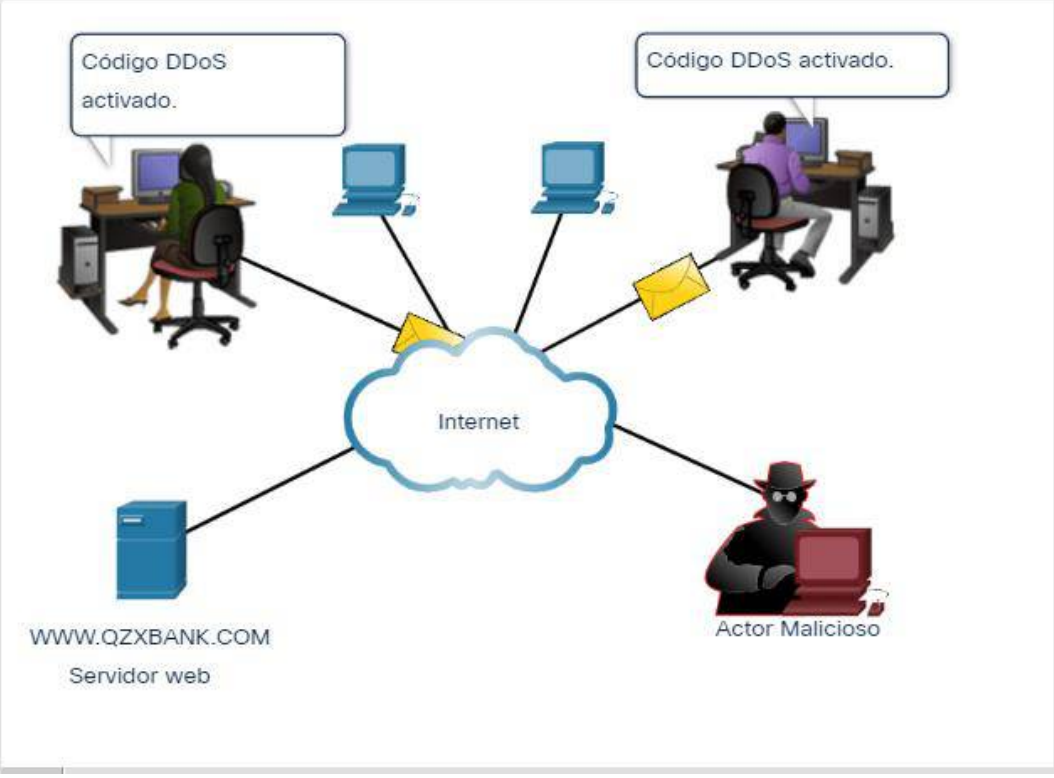
Ataque DDoS

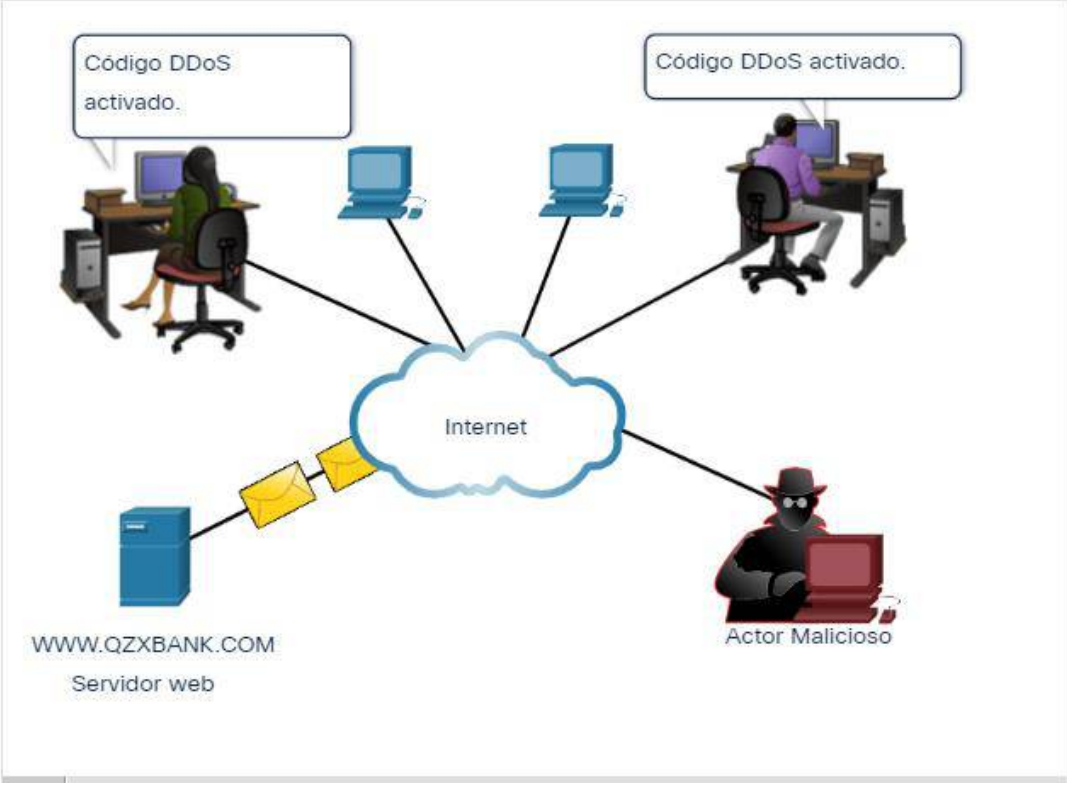
A DDoS is similar to a Ataque DoS, but it originates from multiple, coordinated sources. Por ejemplo, un actor de amenazas construye una red de hosts infectados, conocidos como zombies. Una red de zombies se llama botnet. El actor de amenazas utiliza un programa de comando y control (CNC) para instruir a la botnet de zombies para llevar a cabo un ataque DDoS.

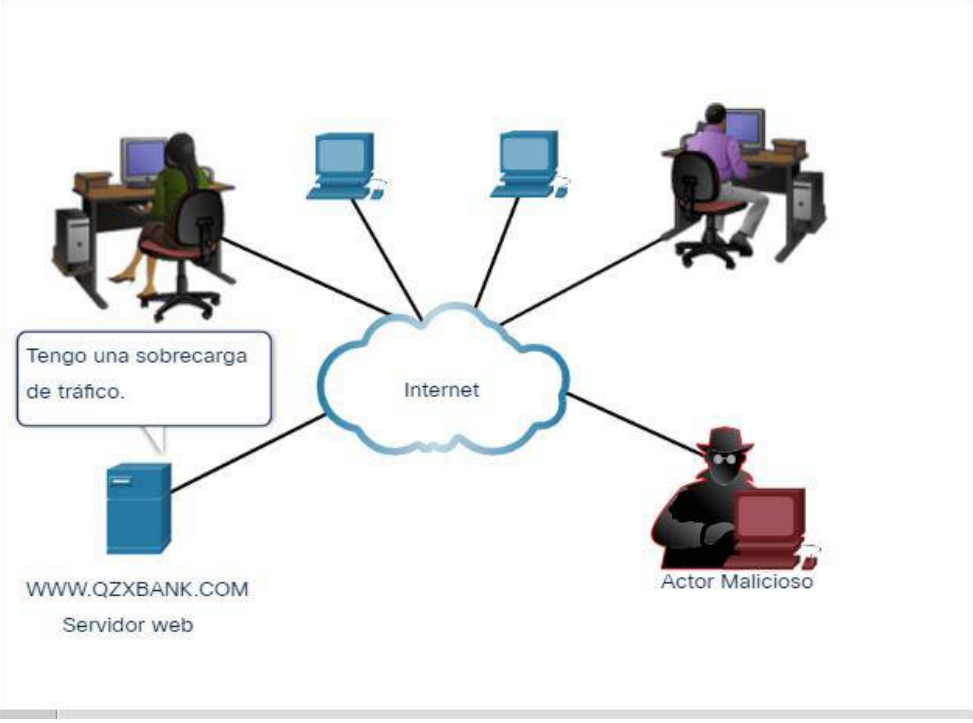
Haga clic en Reproducir en la figura para ver la animación de un ataque DDoS.




Código DDoS activado.
Código DDoS activado.
Internet
WWW.QZXBANK.COM
Servidor web
Actor Malicioso


Código DDoS activado.
Código DDoS activado.
Internet
WWW.QZXBANK.COM
Servidor web
Actor Malicioso


Código DDoS activado.
Código DDoS activado.
Internet
WWW.QZXBANK.COM
Servidor web
Actor Malicioso


Tengo una sobrecarga de tráfico.
Internet
WWW.QZXBANK.COM
Servidor web
Actor Malicioso

16.2.5

Verifique su comprensión: ataques de red

Verifique su comprensión de los ataques a la red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

1. Un ataque de denegación de servicio (DoS), si tiene éxito, impide que los usuarios autorizados accedan a los recursos del sistema.
2. Un ataque de acceso, si tiene éxito, aprovecha las vulnerabilidades conocidas. Estos ataques pueden permitir que un actor de amenazas obtenga acceso a recursos a los que no tienen derechos de acceso.
3. Los ataques demalware incluyen virus, gusanos y caballos de Troya. Estos tipos de ataques pueden provocar un fallo en los sistemas y archivos borrados o dañados.
4. Los ataques demalware incluyen virus, gusanos y caballos de Troya. Estos tipos de ataques pueden permitir que un actor de amenazas tome el control de un sistema infectado.
5. Un ataque de denegación de servicio (DoS), si tiene éxito, impide que los usuarios autorizados accedan a los recursos del sistema.
6. En un ataque de reconocimiento, el actor de amenazas puede sondear un sistema para averiguar qué puertos están abiertos y qué servicios se están ejecutando.

Has tenido 6 respuestas correctas de 6.

Correct

1. A denial of service (DoS) attack, if successful, prevents authorized users from accessing system resources.
2. An access attack, if successful, exploits known vulnerabilities. These attacks can allow a threat actor to gain access to resources they have no rights to access.
3. Malware attacks include viruses, worms, and Trojan horses. These types of attacks can result in crashed systems and deleted or corrupted files.
4. Malware attacks include viruses, worms, and Trojan horses. These types of attacks can allow a threat actor to take control of an infected system.
5. A denial of service (DoS) attack, if successful, prevents authorized users from accessing system resources.
6. In a reconnaissance attack, the threat actor can probe a system to find what ports are open, and what services are running.

You got 6 out of 6 questions correct.

1. Angela, miembro del personal de TI de ACME Inc., notó que la comunicación con el servidor web de la empresa era muy lenta. Después de investigar, determina que la causa de la respuesta lenta es una computadora en Internet que envía una gran cantidad de solicitudes web con formato incorrecto al servidor web de ACME. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ◯ Ataque de acceso
- ◉ ataque denegación de servicio (DoS)
- ◯ ataque de malware
- ◯ Ataque de reconocimiento

2. George tenía que compartir un video con un colega. Debido al gran tamaño del archivo de video, decidió ejecutar un servidor FTP simple en su estación de trabajo para enviarle el archivo de video a su colega. Para facilitar las cosas, George creó una cuenta con la contraseña simple de "archivo" y se la proporcionó a su compañero de trabajo el viernes. Sin las medidas de seguridad adecuadas o una contraseña segura, el personal de TI no se sorprendió al enterarse el lunes de que la estación de trabajo de George se había visto comprometida y estaba tratando de cargar documentos relacionados con el trabajo en Internet. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ◉ Ataque de acceso
- ◯ ataque denegación de servicio (DoS)
- ◯ ataque de malware
- ◯ Ataque de reconocimiento

3. Jeremiah estaba navegando en Internet desde su computadora personal cuando un sitio web aleatorio ofreció un programa gratuito para limpiar su sistema. Después de que el ejecutable se descargó y se ejecutó, el sistema operativo se bloqueó. Se habían corrompido archivos esenciales relacionados con el sistema operativo, y Jeremiah tuvo que formatear todo el disco y reinstalar el sistema operativo. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ◯ Ataque de acceso
- ◯ ataque denegación de servicio (DoS)
- ◉ ataque de malware
- ◯ Ataque de reconocimiento

4. Arianna encontró una unidad flash en el pavimento de un estacionamiento del centro comercial. Preguntó alrededor pero no pudo encontrar al dueño. Decidió conservarlo y lo conectó a su computadora portátil, solo para encontrar una carpeta de fotos. Arianna sintió curiosidad y abrió algunas fotos antes de formatear la unidad flash para usarla solo ella. Luego, Arianna notó que su cámara portátil estaba activa. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ○ Ataque de acceso
- ○ ataque denegación de servicio (DoS)
- ◉ ataque de malware
- ○ Ataque de reconocimiento

5. ACME Inc. usa una computadora como servidor de impresión. El personal de TI no ha hecho actualizaciones de seguridad en la computadora durante más de 60 días. Ahora el servidor de impresión funciona lentamente y envía una gran cantidad de paquetes maliciosos a su NIC. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ○ Ataque de acceso
- ◉ ataque denegación de servicio (DoS)
- ○ ataque de malware
- ○ Ataque de reconocimiento

6. Sharon, una pasante de TI en ACME Inc., descubrió algunos paquetes extraños mientras revisaba los registros de seguridad generados por el firewall. Un puñado de direcciones IP en Internet enviaban paquetes con formato incorrecto a varias direcciones IP diferentes, en varios números de puerto aleatorios diferentes dentro de ACME Inc. ¿Qué tipo de ataque se describe en este escenario?

¡Lo tienes!

- ○ Ataque de acceso
- ○ ataque denegación de servicio (DoS)
- ○ ataque de malware
- ◉ Ataque de reconocimiento

1. Angela, an IT staff member at ACME Inc., notices that communication with the company's web server is very slow. After investigating, she determines that the cause of the slow response is a computer on the internet sending a very large number of malformed web requests to ACME'S web server. What type of attack is described in this scenario?

You got it!

- ○ access attack
- ◉ denial of service (DoS) attack
- ○ malware attack
- ○ reconnaissance attack

2. George needed to share a video with a co-worker. Because of the large size of the video file, he decided to run a simple FTP server on his workstation to serve the video file to his co-worker. To make things easier, George created an account with the simple password of "file" and provided it to his co-worker on Friday. Without the proper security measures or a strong password, the IT staff was not surprised to learn on Monday that George's workstation had been compromised and was trying to upload work related documents to the internet. What type of attack is described in this scenario?

You got it!

- ◉ access attack
- ○ denial of service (DoS) attack
- ○ malware attack
- ○ reconnaissance attack

3. Jeremiah was browsing the internet from his personal computer when a random website offered a free program to clean his system. After the executable was downloaded and running, the operating system crashed. Crucial operating system related files had been corrupted and Jeremiah's computer required a full disk format and operating system re-installation. What type of attack is described in this scenario?

You got it!

- ○ access attack
- ○ denial of service (DoS) attack
- ◉ malware attack
- ○ reconnaissance attack

4. Arianna found a flash drive lying on the pavement of a mall parking lot. She asked around but could not find the owner. She decided to keep it and plugged it into her laptop, only to find a photo folder. Feeling curious, Arianna opened a few photos before formatting the flash drive for her own use. Afterwards, Arianna noticed that her laptop camera was active. What type of attack is described in this scenario?

You got it!

- ○ access attack
- ○ denial of service (DoS) attack
- ◉ malware attack
- ○ reconnaissance attack

5. A computer is used as a print server for ACME Inc. The IT staff failed to apply security updates to this computer for over 60 days. Now the print server is operating slowly, and sending a high number of malicious packets to its NIC. What type of attack is described in this scenario?

You got it!

- ○ access attack
- ◉ denial of service (DoS) attack
- ○ malware attack
- ○ reconnaissance attack

6. Sharon, an IT intern at ACME Inc., noticed some strange packets while revising the security logs generated by the firewall. A handful of IP addresses on the internet were sending malformed packets to several different IP addresses, at several different random port numbers inside ACME Inc. What type of attack is described in this scenario?

You got it!

- ○ access attack
- ○ denial of service (DoS) attack
- ○ malware attack
- ◉ reconnaissance attack

16.2.6

Laboratorio - Investigación de amenazas de seguridad de red

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: ExploreExplore el sitio web de SANS the SANS Website
- Parte 2: Identificar amenazas de seguridad de red recientes
- Parte 3: Detalle una amenaza de seguridad de red específica

Investigación de amenazas de seguridad de red

Fundamentos de seguridad de la red / Mitigaciones de ataque a la red

Mitigaciones de ataque a la red

16.3.1

Enfoque de Defensa en Profundidad

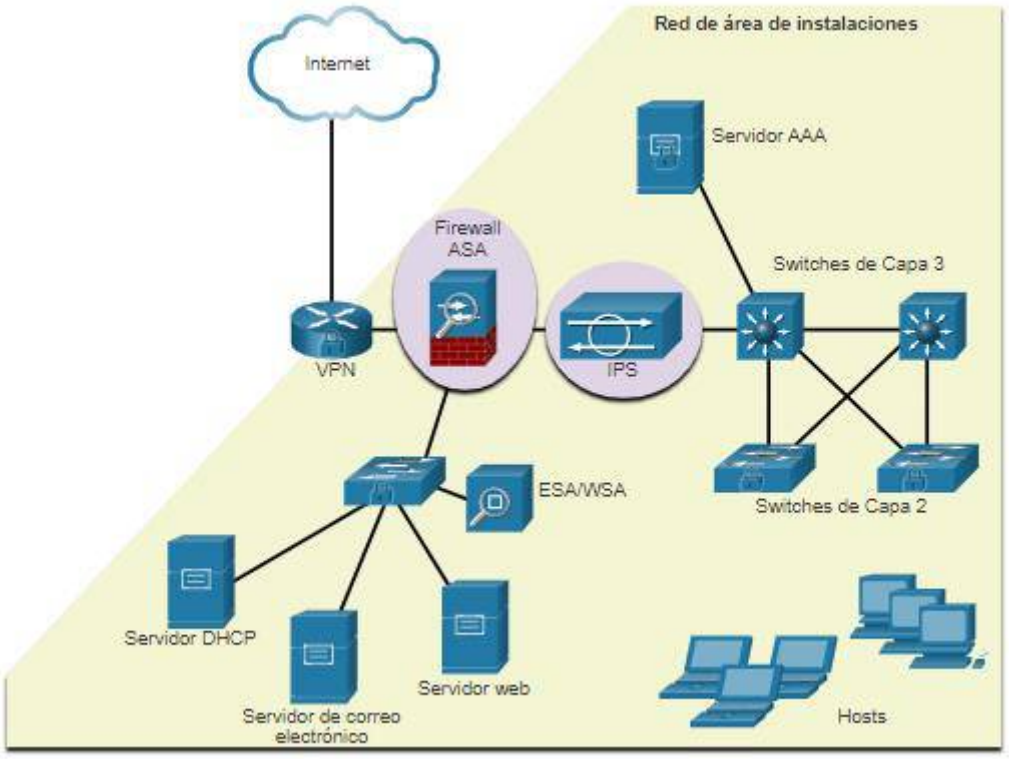
Ahora que sabe más acerca de cómo los actores de amenazas pueden entrar en las redes, debe comprender qué hacer para evitar este acceso no autorizado. En este tema se detallan varias acciones que puede realizar para que su red sea más segura.

Para mitigar los ataques de red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad (también conocido como enfoque en capas) para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que funcionen en conjunto.

Mire la red de la figura. Se han implementado varios dispositivos y servicios de seguridad para proteger a sus usuarios y activos contra las amenazas de TCP / IP.

Todos los dispositivos de red, incluidos el router y los switches, también están protegidos, como indican los candados de combinación de sus respectivos iconos. Esto indica que se han protegido para evitar que los actores de amenazas obtengan acceso y manipulen los dispositivos.

La figura representa una red de área del campus. Una nube que representa Internet está conectada a un enrutador, etiquetado VPN. El router VPN está conectado a un ASA firewall. El firewall tiene dos conexiones adicionales; una a un IPS y otro a un interruptor. El conmutador está conectado a un servidor DHCP, servidor de correo electrónico, servidor web y ESA/WSA. El IPS está conectado a un conmutador multicapa. La tiene una conexión a un servidor AAA, así como a dos capas 2 conmutadores y un a otro conmutador multicapa. El segundo interruptor multicapa también tiene conexiones a los mismos switches de capa 2, creando redundancia. Debajo de la sección Los switches de capa 2 son tres portátiles y tres PC que están etiquetados como hosts.



Se han implementado varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de las amenazas de TCP/IP.

- **VPN** - Se utiliza un enrutador para proporcionar servicios VPN seguros con sitios corporativos y soporte de acceso remoto para usuarios remotos que usan túneles cifrados seguros.
- **ASA Firewall** - Este dispositivo dedicado proporciona servicios de firewall con estado. Garantiza que el tráfico interno pueda salir y regresar, pero el tráfico externo no puede iniciar conexiones a hosts internos.
- **IPS** - Un sistema de prevención de intrusiones (IPS) monitorea el tráfico entrante y saliente en busca de malware, firmas de ataques a la red y más. Si el sistema reconoce una amenaza, puede detenerla inmediatamente.
- **ESA/WSA** - El dispositivo de seguridad de correo electrónico (ESA) filtra el correo no deseado y los correos electrónicos sospechosos. El dispositivo de seguridad web (WSA) filtra sitios de malware de Internet conocidos y sospechosos.
- **AAA Server** - Este servidor contiene una base de datos segura de quién está autorizado para acceder y administrar dispositivos de red. Los dispositivos de red autentican a los usuarios administrativos mediante esta base de datos.

16.3.2

Mantener copias de seguridad

Hacer una copia de seguridad de las configuraciones y los datos del dispositivo es una de las formas más efectivas de protección contra la pérdida de datos. Una copia de seguridad de

datos almacena una copia de la información de una PC en medios de copia de seguridad extraíbles que pueden conservarse en lugares seguros. Los dispositivos de infraestructura deben tener copias de seguridad de archivos de configuración e imágenes de IOS en un servidor FTP o de archivos similar. Si falla el equipo o el hardware del router, los datos o la configuración se pueden restaurar mediante la copia de seguridad.

Las copias de seguridad se deben realizar de forma regular tal como se identifica en la política de seguridad. Las copias de respaldo de datos suelen almacenarse externamente para proteger los medios de copia de respaldo en caso de que ocurra algo en la instalación principal. Los hosts de Windows tienen una utilidad de copia de respaldo y restauración. Es importante que los usuarios realicen una copia de seguridad de sus datos en otra unidad o en un proveedor de almacenamiento basado en la nube.

La tabla muestra las consideraciones de copia de seguridad y sus descripciones.

Consideración	Descripción
Frecuencia	Realice copias de seguridad de forma regular como se identifica en la seguridad de TI de la empresa. Los backups completos pueden llevar mucho tiempo, por lo tanto, realizar mensualmente o copias de seguridad semanales con copias de seguridad parciales frecuentes de archivos modificados.
Almacenamiento	Valide siempre las copias de seguridad para garantizar la integridad de los datos y validar los procedimientos de restauración de archivos.
Seguridad	Las copias de seguridad deben transportarse a un almacenamiento fuera del sitio aprobado en una rotación diaria, semanal o mensual, según lo requiera la política de seguridad.
Validación	Las copias deben protegerse con contraseñas seguras. La contraseña es requerido para restaurar los datos.

16.3.3

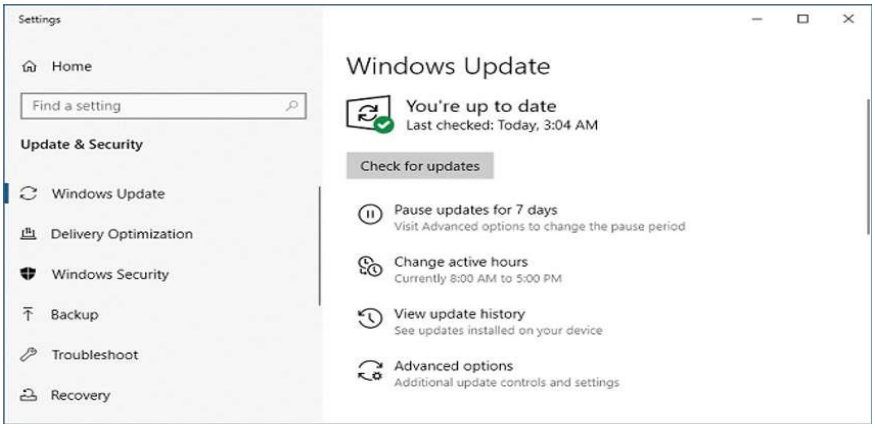
Actualización, actualización y revisión

Mantenerse al día con los últimos desarrollos puede conducir a una defensa más efectiva contra los ataques a la red. A medida que se publica nuevo malware, las empresas deben mantenerse al día con las versiones más recientes del software antivirus.

La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos

los sistemas vulnerables. La administración de numerosos sistemas implica la creación de una imagen de software estándar (sistema operativo y aplicaciones acreditadas cuyo uso esté autorizado en los sistemas cliente) que se implementa en los sistemas nuevos o actualizados. Sin embargo, los requisitos de seguridad cambian y los sistemas ya implementados pueden necesitar tener parches de seguridad actualizados instalados.

Una solución para la administración de parches de seguridad críticos es asegurarse de que todos los sistemas finales descarguen automáticamente actualizaciones, como se muestra para Windows 10 en la figura. Los parches de seguridad se descargan e instalan automáticamente sin la intervención del usuario.



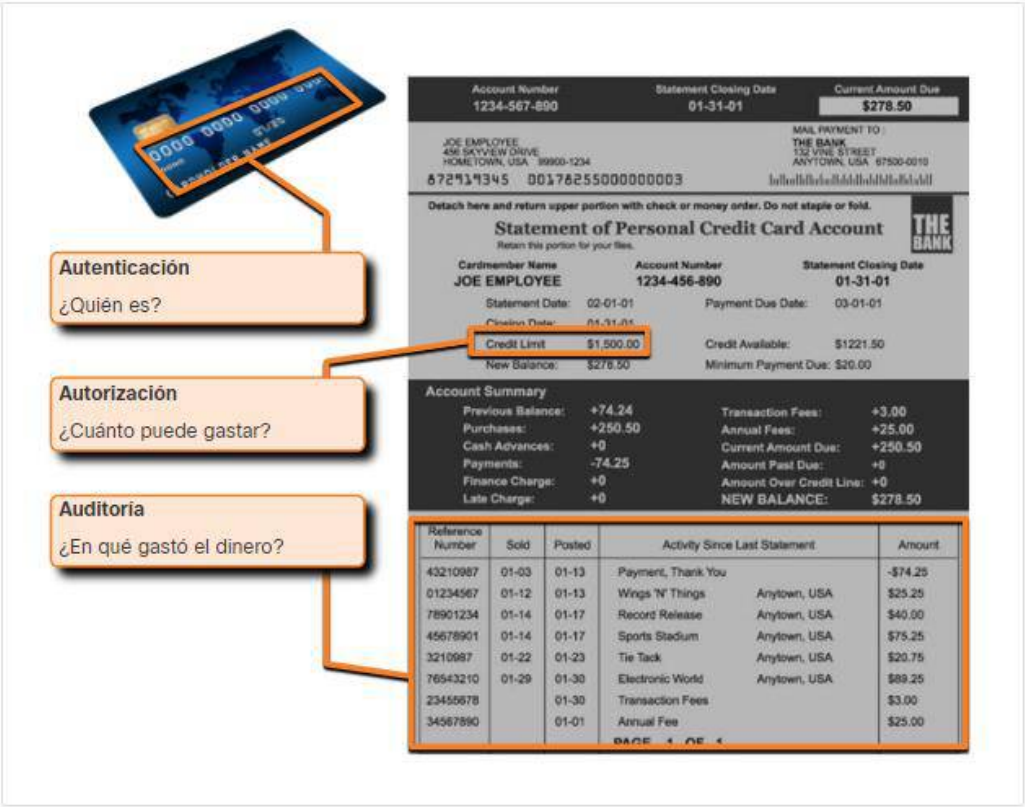
16.3.4

Autenticación, autorización y contabilidad AAA

Todos los dispositivos de red deben estar configurados de forma segura para proporcionar acceso solo a personas autorizadas. Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o "triple A") proporcionan el marco principal para configurar el control de acceso en dispositivos de red.

AAA es una forma de controlar quién tiene permiso para acceder a una red (autenticar), qué acciones realizan mientras acceden a la red (autorizar) y hacer un registro de lo que se hizo mientras están allí (contabilidad).

El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién la puede utilizar y cuánto puede gastar ese usuario, y lleva un registro de los elementos en los que el usuario gastó dinero, como se muestra en la ilustración.



La figura, muestra el estado de cuenta junto a una tarjeta de crédito. Hay un rectángulo alrededor de los números en la tarjeta de crédito superior con el texto, Autenticación ¿Quién eres? Un segundo rectángulo está alrededor del crédito límite en el estado de cuenta de la tarjeta de crédito con texto, Autorización ¿Cuánto puede gastar? Un tercer rectángulo está alrededor de la parte de transacción de la tarjeta de crédito resumen con el texto Auditoría ¿En qué gastaste el dinero?

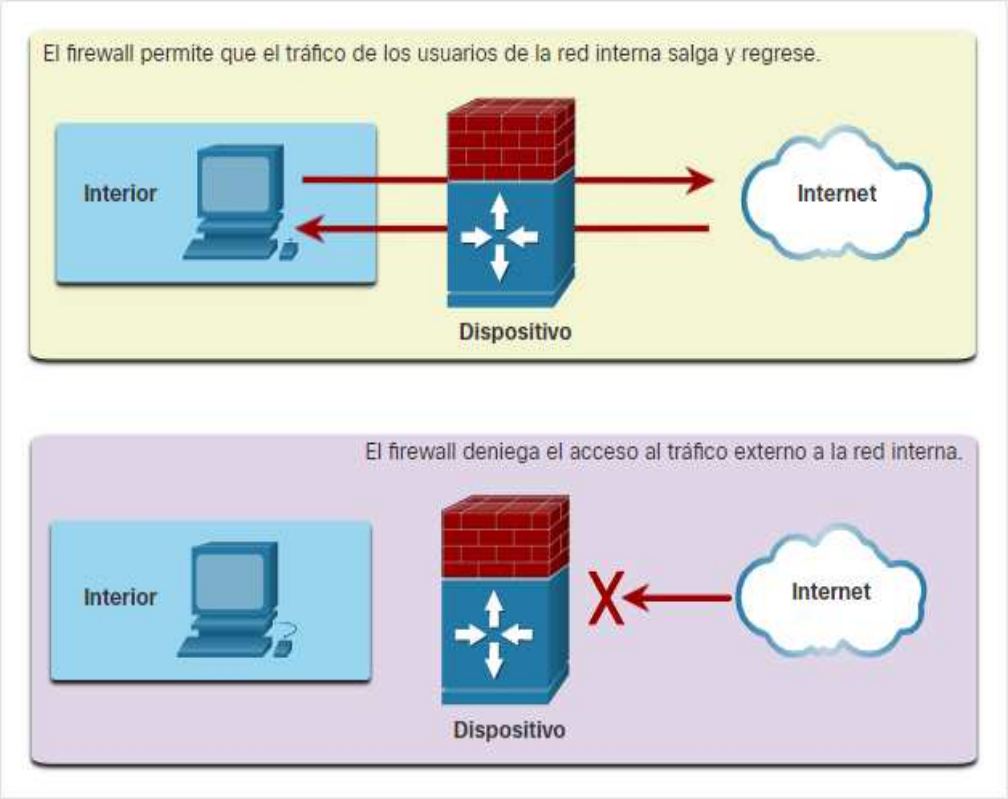
16.3.5

Firewalls

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios contra amenazas externas. Un firewall protege las computadoras y las redes evitando que el tráfico no deseado ingrese a las redes internas.

Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado. Por ejemplo, la topología superior en la figura ilustra cómo el firewall permite que el tráfico de un host de red interno salga de la red y regrese a la red interna. La topología inferior muestra cómo se niega el acceso a la red interna al tráfico iniciado por la red externa (es decir, Internet).

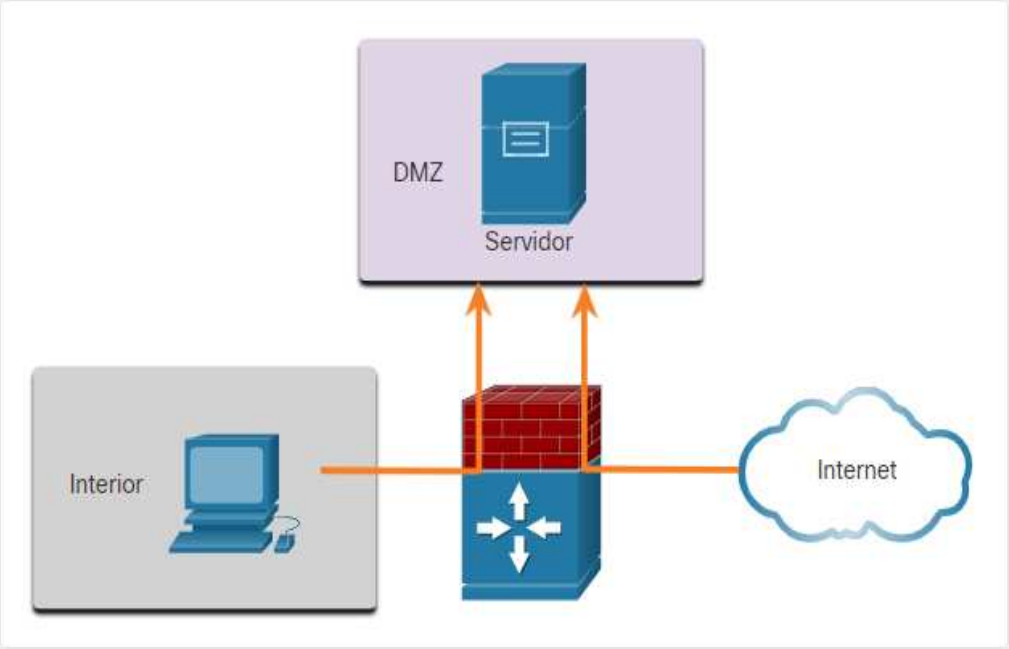
Funcionamiento del firewall



La figura muestra un rectángulo, etiquetado Inside. Dentro del rectángulo hay una (1) nube. Fuera y a la derecha del rectángulo, hay un firewall. A la derecha del firewall, hay una nube etiquetada, Internet. Hay dos flechas, uno que significa tráfico dejando el PC pasando por el firewall y fuera a la Internet. La segunda flecha indica el firewall que permite el tráfico desde el Internet a la PC. La figura muestra otro rectángulo, etiquetado Dentro. Dentro del rectángulo hay una (1) unidad. Fuera y a la derecha del rectángulo, hay un firewall. A la derecha del firewall, hay una nube etiquetada, Internet. Hay una flecha apuntando desde Internet al firewall con una X que indica que el tráfico es siendo denegado desde Internet a la red interna.

Un firewall podría brindar a usuarios externos acceso controlado a servicios específicos. Por ejemplo, los servidores accesibles para usuarios externos generalmente se encuentran en una red especial denominada zona desmilitarizada (DMZ), como se muestra en la figura. La DMZ permite a un administrador de red aplicar políticas específicas para los hosts conectados a esa red.

Topología de firewall con DMZ



La figura muestra un rectángulo, etiquetado Inside. Dentro del rectángulo hay una (1) nube. Fuera y a la derecha del rectángulo, hay un firewall. A la derecha del firewall, hay una nube etiquetada Internet. Por encima del cortafuegos. hay un servidor DMZ dentro de un rectángulo. Hay dos flechas, una va desde el PC a través del firewall al servidor DMZ y otro que va desde el Internet a través del firewall al servidor DMZ.

16.3.6

Tipos de firewalls

Los productos de firewall vienen empaquetados en varias formas. Estos productos utilizan diferentes técnicas para determinar qué se permitirá o negará el acceso a una red. Entre otros, se incluyen:

- **Filtrado de paquetes**: evita o permite el acceso en función de direcciones IP o MAC
- **Filtrado de aplicaciones**: evita o permite el acceso a tipos de aplicaciones específicos en función de los números de puerto
- **Filtrado de URL**: evita o permite el acceso a sitios web basados en URL o palabras clave específicas
- **Stateful packet inspection (SPI)**: los paquetes entrantes deben ser respuestas legítimas a las solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

16.3.7

Seguridad de terminales

Una terminal, o un host, es un sistema de computación o un dispositivo individual que actúa como cliente de red. Las terminales comunes son PC portátiles, computadoras de escritorio, servidores, teléfono inteligentes y tabletas. La seguridad de los dispositivos terminales es uno de los trabajos más desafiantes para un administrador de red, ya que incluye a la naturaleza humana. Las empresas deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas. Se debe capacitar a los empleados sobre el uso correcto de la red. En general, estas políticas incluyen el uso de software antivirus y la prevención de intrusión de hosts. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.

16.3.8

Verifique su comprensión - Mitigación de ataques de red

Verifique su comprensión de la mitigación de ataques de red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

1. Un firewall es un dispositivo dedicado que ayuda a evitar el acceso no autorizado al no permitir que el tráfico externo inicie conexiones a hosts internos.
2. Los servidores AAA realizan servicios de autenticación, autorización y contabilidad en nombre de otros dispositivos para administrar el acceso a los recursos.
3. La validación de copias de seguridad se refiere al uso de contraseñas seguras para proteger las copias de seguridad y restaurar los datos.
4. La zona desmilitarizada, o zona desmilitarizada, se utiliza para servidores que necesitan ser accesibles para usuarios externos.
5. El software antivirus que se ejecuta en un endpoint o host forma parte de una solución de seguridad integral para endpoint.

Has tenido 5 respuestas correctas de 5.

1. ¿Qué dispositivo controla el tráfico entre dos o más redes para evitar el acceso no autorizado?

¡Lo tienes!

- ○ Servidor AAA
- ◉ Firewall
- ○ ESA/WSA
- ○ Dispositivo

2. ¿Qué dispositivo utilizan otros dispositivos de red para autenticar y autorizar el acceso de administración?

¡Lo tienes!

- ◉ Servidor AAA
- ○ Firewall
- ○ ESA/WSA
- ○ Dispositivo

3. ¿Qué consideración de política de backup se refiere al uso de contraseñas seguras para proteger las copias de seguridad y restaurar los datos?

¡Lo tienes!

- ○ frecuencia
- ○ Almacenamiento
- ○ Seguridad
- ◉ validación

4. Esta zona se utiliza para alojar servidores que deben ser accesibles para usuarios externos.

¡Lo tienes!

- ○ interna
- ○ externa
- ○ Internet
- ◉ DMZ

5. ¿Qué es apropiado para proporcionar seguridad de endpoint?

¡Lo tienes!

- ○ un servidor AAA
- ◉ Software antivirus
- ○ un server-based firewall
- ○ un ESA/WSA

Correct

1. A firewall is a dedicated device that helps prevent unauthorized access by not allowing external traffic to initiate connections to internal hosts.
2. AAA servers perform authentication, authorization and accounting services on behalf of other devices to manage access to resources.
3. Backup validation is concerned with using strong passwords to protect backups and for restoring data.
4. The DMZ, or demilitarized zone, is used for servers that need to be accessible to external users.
5. Antivirus software running on an endpoint or host is part of a comprehensive endpoint security solution.

You got 5 out of 5 questions correct.

1. Which device controls traffic between two or more networks to help prevent unauthorized access?

You got it!

- AAA Server
- (•) firewall
- ESA/WSA
- IPS

2. Which device is used by other network devices to authenticate and authorize management access?

You got it!

- (•) AAA Server
- firewall
- ESA/WSA
- IPS

3. Which backup policy consideration is concerned with using strong passwords to protect the backups and for restoring data?

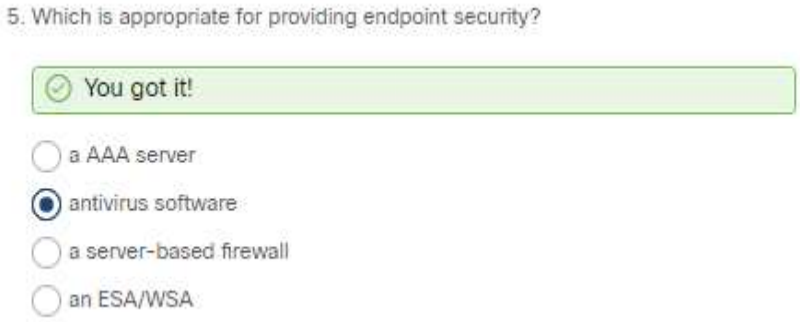
You got it!

- frequency
- storage
- security
- (•) validation

4. This zone is used to house servers that should be accessible to outside users.

You got it!

- inside
- outside
- internet
- (•) DMZ



Fundamentos de seguridad de la red / Seguridad de los dispositivos

Seguridad de los dispositivos

16.4.1

Cisco AutoSecure

Un área de redes que requiere especial atención para mantener la seguridad son los dispositivos. Probablemente ya tenga una contraseña para su computadora, teléfono inteligente o tableta. ¿Es tan fuerte como podría ser? ¿Está utilizando otras herramientas para mejorar la seguridad de sus dispositivos? En este tema se explica cómo hacerlo.

La configuración de seguridad se establece en los valores predeterminados cuando se instala un nuevo sistema operativo en un dispositivo. En la mayoría de los casos, ese nivel de seguridad es insuficiente. Para los enrutadores Cisco, la función Cisco AutoSecure se puede utilizar para ayudar a asegurar el sistema, como se muestra en el ejemplo.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

Además, existen algunos pasos simples que se deben seguir y que se aplican a la mayoría de los sistemas operativos:

- Se deben cambiar de inmediato los nombres de usuario y las contraseñas predeterminados.
- Se debe restringir el acceso a los recursos del sistema solamente a las personas que están autorizadas a utilizar dichos recursos.
- Siempre que sea posible, se deben desactivar y desinstalar todos los servicios y las aplicaciones innecesarios.

A menudo, los dispositivos enviados por el fabricante pasaron cierto tiempo en un depósito y no tienen los parches más actualizados instalados. Es importante actualizar todo el software e instalar todos los parches de seguridad antes de la implementación.

16.4.2

Contraseñas

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Las pautas estándar que se deben seguir son las siguientes:

- Use una contraseña de al menos ocho caracteres, preferiblemente 10 o más caracteres. Una contraseña más larga es una contraseña más segura.
- Cree contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si están permitidos.
- Evite las contraseñas basadas en la repetición, las palabras comunes de diccionario, las secuencias de letras o números, los nombres de usuario, los nombres de parientes o mascotas, información biográfica (como fechas de nacimiento), números de identificación, nombres de antepasados u otra información fácilmente identificable.
- Escriba una contraseña con errores de ortografía a propósito. Por ejemplo, Smith = Smyth = 5mYth, o Seguridad = 5egur1dad.
- Cambie las contraseñas con frecuencia. Si una contraseña se ve comprometida sin saberlo, la oportunidad para que el actor de la amenaza use la contraseña es limitada.
- No anote las contraseñas ni las deje en lugares obvios, por ejemplo, en el escritorio o el monitor.

Las tablas muestran ejemplos de contraseñas seguras y débiles.

Contraseñas Débiles

Contraseña débil	Por qué es débil
secreto	Contraseña de diccionario simple
perez	Nombre de soltera de la madre
toyota	Marca de un auto
bob1967	Nombre y cumpleaños del usuario.
Blueleaf23	Palabras y números simples

Contraseñas seguras

Contraseña segura	Por qué es segura
b67n42d39c	Combinación de caracteres alfanuméricos
12^h u4@1p7	Combina caracteres alfanuméricos, símbolos e incluye un espacio.

En los routers Cisco, se ignoran los espacios iniciales para las contraseñas, pero no ocurre lo mismo con los espacios que le siguen al primer carácter. Por lo tanto, un método para crear una contraseña segura es utilizar la barra espaciadora y crear una frase compuesta de muchas palabras. Esto se conoce como frase de contraseña. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar.

16.4.3

Seguridad adicional de contraseñas

Las contraseñas seguras solo son útiles si son secretas. Hay varios pasos que se pueden tomar para ayudar a garantizar que las contraseñas permanezcan secretas en un enrutador y conmutador Cisco, incluidas estas:

- Cifrar todas las contraseñas de texto sin formato
- Establecer una longitud mínima de contraseña aceptable
- Disuasión de ataques de adivinación de contraseñas de fuerza bruta
- Deshabilitar un acceso en modo EXEC privilegiado inactivo después de un período de tiempo especificado.

Como se muestra en la configuración de muestra en la figura, el comando de configuración global **service password-encryption,** evita que personas no autorizadas vean contraseñas de texto sin formato en el archivo de configuración. Este comando encripta todas las contraseñas de texto sin formato. Observe en el ejemplo que la contraseña «cisco» se ha cifrado como «03095A0F034F».

Para asegurarse de que todas las contraseñas configuradas tengan un mínimo de una longitud especificada, use el comando **security passwords min-length** *length* en el modo de configuración global. En la figura, cualquier nueva contraseña configurada tendría que tener una longitud mínima de ocho caracteres.

Los actores de amenazas pueden usar software de descifrado de contraseñas para llevar a cabo un ataque de fuerza bruta en un dispositivo de red. Este ataque intenta continuamente adivinar las contraseñas válidas hasta que uno funcione. Utilice el comando de configuración **login block-for # attempts # within #** global para disuadir este tipo de ataque. En la figura, por ejemplo, el comando **login block-for 120 attempts 3 within 60** bloqueará los intentos de inicio de sesión vty durante 120 segundos si hay tres intentos fallidos de inicio de sesión en 60 segundos.

Los administradores de red pueden distraerse y dejar accidentalmente abierta una sesión de modo EXEC privilegiado en un terminal. Esto podría permitir que un actor de amenazas internas acceda a cambiar o borrar la configuración del dispositivo.

De forma predeterminada, los routers Cisco desconectarán una sesión EXEC después de 10 minutos de inactividad. Sin embargo, puede reducir esta configuración mediante el comando de configuración de línea **exec-timeout** *minutes seconds*. Este comando se puede aplicar en línea consola, auxiliares y vty líneas. En la figura, le estamos diciendo al dispositivo Cisco que desconecte automáticamente a un usuario inactivo en una línea vty después de que el usuario haya estado inactivo durante 5 minutos y 30 segundos.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
 transport input ssh
Router#
```

16.4.4

Habilitación de SSH

Telnet simplifica el acceso remoto a dispositivos, pero no es seguro. Los datos contenidos en un paquete Telnet se transmiten sin cifrar. Por esta razón, se recomienda encarecidamente habilitar Secure Shell (SSH) en dispositivos para acceso remoto seguro.

Es posible configurar un dispositivo Cisco para admitir SSH mediante los siguientes seis pasos:

Paso 1. Configure un único nombre de dispositivo. Un dispositivo debe tener un nombre de host único distinto del predeterminado.

Paso 2. Configure la IP de nombre de dominio. Configure el nombre de dominio IP de la red mediante el comando de modo de configuración global **ip-domain name**.

Paso 3. Generar una llave para encriptar tráfico SSH. SSH cifra el tráfico entre el origen y el destino. Sin embargo, para ello, se debe generar una clave de autenticación única mediante el comando de configuración global **crypto key generate rsa general-keys modulus** *bits*. El módulo *bits* determina el tamaño de la clave y se puede configurar de 360 bits a 2048 bits. Cuanto mayor sea el valor de bit, más segura será la clave. Sin embargo, los valores de bits

más grandes también tardan más en cifrar y descifrar la información. La longitud mínima de módulo recomendada es de 1024 bits.

Paso 4. Verificar o crear una entrada a la base de datos local. Cree una entrada de nombre de usuario de la base de datos local utilizando el comando de configuración global **username**. En el ejemplo, el parámetro **secret** se usa para que la contraseña se encripte con MD5.

Paso 5. Autenticar contra la base de datos local. Utilice el comando de configuración de línea **login local** para autenticar la línea vty en la base de datos local.

Paso 6. Habilitar sesiones de entrada SSH. De forma predeterminada, no se permite ninguna sesión de entrada en las líneas vty. Puede especificar varios protocolos de entrada, incluidos Telnet y SSH mediante el comando **transport input [ssh | telnet]**.

Como se muestra en el ejemplo, el router R1 está configurado en el dominio span.com. Esta información se utiliza junto con el valor de bit especificado en el comando **crypto key generate rsa general-keys modulus**, para crear una clave de cifrado.

A continuación, se crea una entrada de base de datos local para un usuario llamado Bob. Finalmente, las líneas vty están configuradas para autenticarse en la base de datos local y para aceptar solo sesiones SSH entrantes.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
El nombre de las claves será: r1.span.com% El tamaño del módulo clave es 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
•Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

16.4.5

Inhabilitación de servicios no utilizados

Los routers y switches de Cisco comienzan con una lista de servicios activos que pueden o no ser necesarios en su red. Deshabilite los servicios no utilizados para preservar los recursos del sistema, como los ciclos de CPU y la RAM, e impida que los actores de amenazas exploten estos servicios. El tipo de servicios que están activados de forma predeterminada variará dependiendo de la versión de IOS. Por ejemplo, IOS-XE normalmente sólo tendrá puertos HTTPS y DHCP abiertos. Puede verificarlo con el comando **show ip ports all**, como se muestra en el ejemplo:

```
Router# show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp: ::443:::* ESCUCHAR 309/ [IOS] HTTP CORE
tcp *:443 *:* ESCUCHE 309/ [IOS] HTTP CORE
udp *:67 0.0.0.0:0 387/[IOS]DHCPD Receive
Router#
```

Las versiones de IOS anteriores a IOS-XE utilizan el comando **show control-plane host open-ports**. Mencionamos este comando porque es posible que lo vea en dispositivos antiguos. La salida es similar. Sin embargo, observe que este router anterior tiene un servidor HTTP inseguro y Telnet en ejecución. Ambos servicios deben estar deshabilitados. Como se muestra en el ejemplo, deshabilite HTTP con el comando de configuración global **no ip http server**. Deshabilite Telnet especificando sólo SSH en el comando de configuración de línea, **transport input ssh**.

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot Local Address Foreign Address Service State
 tcp *:23 *:0 Telnet LISTEN
 tcp *:80 *:0 HTTP CORE LISTEN
 udp *:67 *:0 DHCPD Receive LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

16.4.6

Packet Tracer - Configure contraseñas seguras y SSH

El administrador de red le ha pedido que prepare RTA y SW1 para la implementación. Antes de que puedan conectarse a la red, se deben habilitar las medidas de seguridad.

Configure contraseñas seguras y SSH

Configure contraseñas seguras y SSH

16.4.7

Laboratorio: configurar dispositivos de red con SSH

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Configurar los parámetros básicos de dispositivos
- Parte 2: Configurar el router para el acceso por SSH
- Parte 3: Configurar el switch para el acceso por SSH
- Parte 4: SSH desde la CLI en el Switch

Configurar dispositivos de red con SSH

Fundamentos de seguridad de la red / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

16.5.1

Packet Tracer - Dispositivos de red seguros

En esta actividad, configurará un enrutador y un conmutador según una lista de requisitos.

Dispositivos de red seguros

Dispositivos de red seguros

16.5.2

Laboratorio: dispositivos de red seguros

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Configurar los parámetros básicos de dispositivos
- Parte 2: Configurar medidas de seguridad básicas en el router
- Parte 3: Configurar medidas de seguridad básicas en el switch

Dispositivos de red seguros

16.5.3

¿Qué aprenderé en este módulo?

Vulnerabilidades y Amenazas de Seguridad

Los ataques en una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes. Los intrusos que obtienen acceso modificando software o explotando vulnerabilidades de software son actores de amenazas. Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas: robo de información, pérdida y manipulación de datos, robo de identidad e interrupción del servicio. Existen tres vulnerabilidades o debilidades principales: política tecnológica, de configuración y de seguridad. Las cuatro clases de amenazas físicas son: hardware, ambiental, eléctrico y mantenimiento.

Ataques de Seguridad

Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones "malas" o ilegítimas en los datos, hosts o redes. Los virus, gusanos y caballos de Troya son tipos de malware. Los ataques a la red se pueden clasificar en tres categorías principales: reconocimiento, acceso y denegación de servicio. Las cuatro clases de amenazas físicas son: hardware, ambiental, eléctrico y mantenimiento. Los tres tipos de ataques de reconocimiento son: consultas de Internet, barridos de ping y exploraciones de puertos. Los cuatro tipos de ataques de acceso son: contraseña (fuerza bruta, caballo de Troya, rastreadores de paquetes), explotación de confianza, redirección de puertos y Man-in-the-Middle. Los dos tipos de interrupción de los ataques de servicio son: DoS y DDoS.

Mitigación de ataques a la red

Para mitigar los ataques a la red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que trabajen juntos. Se implementan varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de una organización contra las amenazas TCP / IP: VPN, firewall ASA, IPS, ESA / WSA y servidor AAA. Los dispositivos de infraestructura deben tener copias de seguridad de archivos de configuración e imágenes de IOS en un servidor FTP o de archivos similar. Si falla el equipo o el hardware del router, los datos o la configuración se pueden restaurar mediante la copia de seguridad. La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables. Para administrar parches de seguridad críticos, para asegurarse de que todos los sistemas finales descargan actualizaciones automáticamente. AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la

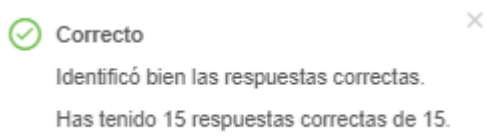
red (contabilizar). Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado. Los servidores accesibles para usuarios externos generalmente se encuentran en una red especial denominada DMZ. Los firewalls utilizan varias técnicas para determinar qué es el acceso permitido o denegado a una red, incluyendo: filtrado de paquetes, filtrado de aplicaciones, filtrado de URL y SPI. Proteger los dispositivos de punto final es fundamental para la seguridad de la red. Una empresa debe tener políticas bien documentadas, que pueden incluir el uso de software antivirus y la prevención de intrusiones en el host. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.

Seguridad del Dispositivo

La configuración de seguridad se establece en los valores predeterminados cuando se instala un nuevo sistema operativo en un dispositivo. Este nivel de seguridad es inadecuado. Para los routers Cisco, la función Cisco AutoSecure se puede utilizar para ayudar a proteger el sistema. Para la mayoría de los sistemas operativos, los nombres de usuario y las contraseñas predeterminados deben cambiarse inmediatamente, el acceso a los recursos del sistema debe restringirse únicamente a las personas autorizadas a utilizar esos recursos, y los servicios y aplicaciones innecesarios deben desactivarse y desinstalarse cuando sea posible. Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar. Para enrutadores y conmutadores, cifre todas las contraseñas de texto sin formato, establezca una longitud mínima aceptable de contraseña, desactive los ataques de adivinación de contraseñas de fuerza bruta y deshabilite un acceso en modo EXEC privilegiado inactivo después de un período de tiempo especificado. Configure los dispositivos apropiados para admitir SSH y deshabilite los servicios no utilizados.

16.5.4

Prueba del módulo - Fundamentos de seguridad de red



1. ¿Qué componente está diseñado para proteger contra comunicaciones no autorizadas hacia y desde una computadora?

Tema 16.3.0 - El software antivirus y antimalware se utiliza para prevenir la infección de software malintencionado. Un escáner de puertos se utiliza para probar una conexión de red de PC para determinar qué puertos está escuchando el PC. El centro de seguridad es un área de Windows que realiza un seguimiento del software de seguridad y la configuración de la PC. Un firewall está diseñado para bloquear los intentos de conexión no solicitados con un PC a menos que estén específicamente permitidos.

- ○ centro de seguridad
- ○ Escáner de puerto
- ○ Antimalware
- ○ Antivirus
- ◉ Firewall

2. ¿Qué comando bloqueará los intentos de inicio de sesión en el RouterA por un periodo de 30 segundos si hay 2 intentos fallidos de inicio de sesión en 10 segundos?

Tema 16.4.0 - La sintaxis correcta es RouterA(config)# **login block-for** (*number of seconds*) **attempts** (*number of attempts*) **within** (*number of seconds*).

- ○ RouterA (config) bloque de# **inicio de sesión para 10 intentos 2 dentro de 30**
- ◉ RouterA (config) bloque de# **inicio de sesión para 30 intentos 2 dentro de 10**
- ○ routera (config) bloque de# **inicio de sesión para 2 intentos 30 dentro de 10**
- ○ RouterA (config) bloque de# **inicio de sesión para 30 intentos 10 dentro de 2**

3. ¿Cuál es el propósito de la función de contabilidad de seguridad de red?

Tema 16.3.0: la autenticación, la autorización y la contabilidad son servicios de red conocidos colectivamente como AAA. La autenticación requiere que los usuarios prueben quiénes son. La autorización determina a qué recursos puede acceder un usuario. La contabilidad hace un seguimiento de las acciones del usuario.

- ○ Requerir que los usuarios prueben quiénes son.
- ○ Determinar a qué recursos puede acceder un usuario.
- ◉ No perder de vista las acciones de los usuarios.
- ○ Proporcionar preguntas de desafío y respuesta.

4. ¿Qué tipo de ataque puede implicar el uso de herramientas como nslookup y fping??

Tema 16.2.0: para los ataques de reconocimiento, los atacantes externos pueden usar herramientas de Internet, como el aspecto y las utilidades, para determinar fácilmente el espacio de direcciones IP asignado a una determinada empresa o entidad. Una vez que se determina el espacio de direcciones IP, un atacante puede hacer ping a las direcciones IP públicamente disponibles para identificar las direcciones que están activas.Fping es una herramienta de barrido de ping que puede ayudar a automatizar este proceso.

- ○ Ataque de acceso
- ◉ Ataque de reconocimiento
- ○ Ataque por denegación de servicio
- ○ ataque de gusano

5. ¿Qué beneficio ofrece SSH a través de Telnet para administrar remotamente un router?

Tema 16.4.0 - SSH proporciona acceso seguro a un dispositivo de red para la administración remota. Utiliza una autorización de contraseña más segura que Telnet y cifra los datos que se transportan durante la sesión.

- ◉ varios
- ○ Uso de TCP
- ○ autorización
- ○ conexiones a través de varias líneas VTY

6. ¿Cuál de las siguientes es una de las herramientas de seguridad más eficaces disponibles para proteger a los usuarios contra amenazas externas?

Tema 16.3.0: un firewall es una de las herramientas de seguridad más eficaces para proteger a los usuarios de la red interna de amenazas externas. Un firewall reside entre dos o más redes, controla el tráfico entre ellas y ayuda a evitar el acceso no autorizado.Un sistema host de prevención de intrusiones puede ayudar a prevenir intrusos externos y debe usarse en todos los sistemas.

- ◉ Firewalls
- ○ Routers que ejecutan servicios AAA
- ○ Servidores de parches
- ○ Técnicas de cifrado de contraseñas

7. ¿Qué tipo de amenaza de red tiene el objetivo de impedir que los usuarios autorizados accedan a los recursos?

Tema 16.2.0: los ataques de reconocimiento de red implican el descubrimiento y el mapeo no autorizados de la red y los sistemas de red. Los ataques de acceso y de explotación de confianza implican la manipulación de datos y el acceso a sistemas o a privilegios de usuario no autorizados. Los ataques de denegación de servicio (DoS) tienen el objetivo de impedir que los usuarios y dispositivos legítimos accedan a los recursos de red.

- (●) Ataques DoS
- ( ) Ataques de acceso
- ( ) Ataques de reconocimiento
- ( ) Explotación de confianza

8. ¿Cuáles son los tres servicios proporcionados por el marco de AAA? (Elija tres opciones).

Tema 16.3.0 - El marco de autenticación, autorización y registro (AAA) presta servicios de protección de acceso a dispositivos de red.

- [x] Registro
- [ ] Automatización
- [x] Autorización
- [x] Autenticación
- [ ] Equilibrio automático
- [ ] Configuración automática

9. ¿Qué ataque de código malicioso es autónomo e intenta aprovechar una vulnerabilidad específica en un sistema que se está atacando?

Tema 16.2.0 - Un gusano es un programa informático que se replica con la intención de atacar un sistema e intentar explotar una vulnerabilidad específica en el objetivo. Tanto el virus como el caballo de Troya dependen de un mecanismo de entrega para transportarlos de un host a otro. La ingeniería social no es un tipo de ataque de código malicioso.

- ( ) Virus
- (●) Gusano
- ( ) Caballo de Troya
- ( ) ingeniería social

10. En un armario de cableado, algunos routers y switches fallaron después de la falla de una unidad de aire acondicionado. ¿Qué tipo de amenaza describe esta situación?

Tema 16.1.0: las cuatro clases de amenazas son las siguientes:
- Amenazas de hardware: daño físico a servidores, enrutadores, conmutadores, planta de cableado y estaciones de trabajo
- Amenazas medioambientales: temperaturas extremas (demasiado calor o demasiado frío) o humedad extrema (demasiado húmedo o demasiado seco)
- Amenazas eléctricas: picos de voltaje, voltaje de suministro insuficiente (caídas de voltaje), energía no condicionada (ruido) y pérdida total de energía
- Amenazas de mantenimiento: manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado deficiente y etiquetado deficiente

- ( ) Configuración
- (•) Ambiental
- ( ) Eléctrica
- ( ) Mantenimiento

11. ¿Qué significa el término vulnerabilidad?

Tema 16.1.0: una vulnerabilidad no es una amenaza, pero es una debilidad que convierte a la PC o al software en blanco de ataques.

- (•) es una debilidad que hace que un objetivo sea susceptible a un ataque
- ( ) es una computadora que contiene información confidencial
- ( ) es un método de ataque para aprovechar un objetivo
- ( ) es una máquina conocida del objetivo o de la víctima
- ( ) es una posible amenaza que crea un hacker

12. ¿Qué tres pasos de configuración se deben realizar para implementar el acceso SSH a un enrutador? (Escoja tres opciones).

Tema 16.4.0 - Para implementar SSH en un router es necesario realizar los siguientes pasos:
- Configure un nombre de host único.
- Configurar el nombre de dominio de la red.
- Configurar una cuenta de usuario para utilizar la base de datos AAA o local para la autenticación.
- Generar claves RSA.
- Habilitar sesiones SSH VTY.

- [ ] una contraseña en la línea de consola
- [x] un nombre de dominio IP
- [x] una cuenta de usuario
- [ ] una contraseña de modo de activación
- [x] un nombre de host único
- [ ] una contraseña cifrada

13. ¿Cuál es el objetivo de un ataque de reconocimiento de red?

Tema 16.2.0: el objetivo de un ataque de reconocimiento de red es descubrir información sobre una red, sistemas de red y servicios de red.

- (•) Detección y esquematización de sistemas
- ( ) Manipulación de datos no autorizada
- ( ) Deshabilitación de sistemas o servicios de red
- ( ) Denegación de acceso de los usuarios legítimos a los recursos

14. Por razones de seguridad, un administrador de red debe asegurarse de que los equipos locales no pueden hacer ping entre sí. ¿Qué configuración puede realizar esta tarea?

Tema 16.3.0 - La configuración de la tarjeta inteligente y del sistema de archivos no afecta al funcionamiento de la red. La configuración de direcciones MAC y el filtrado se pueden utilizar para controlar el acceso a la red del dispositivo, pero no se puede utilizar para filtrar diferentes tipos de tráfico de datos.

- ○ configuración de tarjeta inteligente
- ◉ configuración de firewall
- ○ Configuración de la dirección MAC
- ○ configuración del sistema de archivos

15. Un administrador de red establece una conexión a un switch a través de SSH. ¿Qué característica describe de forma única la conexión SSH?

Tema 16.4.0 - SSH proporciona un inicio de sesión remoto seguro a través de una interfaz virtual. SSH proporciona una autenticación de contraseña más segura que Telnet. SSH también cifra los datos durante la sesión.

- ○ acceso fuera de banda a un switch mediante el uso de un terminal virtual con autenticación de contraseña
- ○ acceso remoto al conmutador mediante el uso de una conexión telefónica
- ○ acceso in situ a un conmutador mediante el uso de un PC conectado directamente y un cable de consola
- ◉ acceso remoto a un switch donde los datos se cifran durante la sesión
- ○ acceso directo al conmutador mediante el uso de un programa de emulación de terminal

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. Which component is designed to protect against unauthorized communications to and from a computer?

Topic 16.3.0 - Antivirus and antimalware software are used to prevent infection from malicious software. A port scanner is used to test a PC network connection to determine which ports the PC is listening to. The security center is an area of Windows that keeps track of the security software and settings on the PC. A firewall is designed to block unsolicited connection attempts to a PC unless they are specifically permitted.

- ○ security center
- ○ port scanner
- ○ antimalware
- ○ antivirus
- ◉ firewall

2. Which command will block login attempts on RouterA for a period of 30 seconds if there are 2 failed login attempts within 10 seconds?

Topic 16.4.0 - The correct syntax is RouterA(config)# **login block-for** (*number of seconds*) **attempts** (*number of attempts*) **within** (*number of seconds*).

- ○ RouterA(config)# **login block-for 10 attempts 2 within 30**
- ◉ RouterA(config)# **login block-for 30 attempts 2 within 10**
- ○ RouterA(config)# **login block-for 2 attempts 30 within 10**
- ○ RouterA(config)# **login block-for 30 attempts 10 within 2**

3. What is the purpose of the network security accounting function?

Topic 16.3.0 - Authentication, authorization, and accounting are network services collectively known as AAA. Authentication requires users to prove who they are. Authorization determines which resources the user can access. Accounting keeps track of the actions of the user.

- ○ to require users to prove who they are
- ○ to determine which resources a user can access
- ◉ to keep track of the actions of a user
- ○ to provide challenge and response questions

4. What type of attack may involve the use of tools such as nslookup and fping?

Topic 16.2.0 - For reconnaissance attacks, external attackers can use Internet tools, such as the nslookup and whois utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, an attacker can then ping the publicly available IP addresses to identify the addresses that are active. Fping is a ping sweep tool that can help automate this process.

- ○ access attack
- ◉ reconnaissance attack
- ○ denial of service attack
- ○ worm attack

5. Which benefit does SSH offer over Telnet for remotely managing a router?

Topic 16.4.0 - SSH provides secure access to a network device for remote management. It uses a stronger password authorization than Telnet does and encrypts any data that is transported during the session.

- ◉ encryption
- ○ TCP usage
- ○ authorization
- ○ connections via multiple VTY lines

6. What is one of the most effective security tools available for protecting users from external threats?

Topic 16.3.0 - A firewall is one of the most effective security tools for protecting internal network users from external threats. A firewall resides between two or more networks, controls the traffic between them, and helps prevent unauthorized access. A host intrusion prevention system can help prevent outside intruders and should be used on all systems.

- ◉ firewalls
- ○ router that run AAA services
- ○ patch servers
- ○ password encryption techniques

7. Which type of network threat is intended to prevent authorized users from accessing resources?

Topic 16.2.0 - Network reconnaissance attacks involve the unauthorized discovery and mapping of the network and network systems. Access attacks and trust exploitation involve unauthorized manipulation of data and access to systems or user privileges. DoS, or Denial of Service attacks, are intended to prevent legitimate users and devices from accessing network resources.

- (●) DoS attacks
- ( ) access attacks
- ( ) reconnaissance attacks
- ( ) trust exploitation

8. Which three services are provided by the AAA framework? (Choose three.)

Topic 16.3.0 - The authentication, authorization, and accounting (AAA) framework provides services to help secure access to network devices.

- [x] accounting
- [ ] automation
- [x] authorization
- [x] authentication
- [ ] autobalancing
- [ ] autoconfiguration

9. Which malicious code attack is self-contained and tries to exploit a specific vulnerability in a system being attacked?

Topic 16.2.0 - A worm is a computer program that is self replicated with the intention of attacking a system and trying to exploit a specific vulnerability in the target. Both virus and Trojan horse rely on a delivery mechanism to carry them from one host to another. Social engineering is not a type of malicious code attack.

- ( ) virus
- (●) worm
- ( ) Trojan horse
- ( ) social engineering

10. Some routers and switches in a wiring closet malfunctioned after an air conditioning unit failed. What type of threat does this situation describe?

Topic 16.1.0 - The four classes of threats are as follows:
- Hardware threats - physical damage to servers, routers, switches, cabling plant, and workstations
- Environmental threats - temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
- Electrical threats - voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
- Maintenance threats - poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling

- ○ configuration
- ◉ environmental
- ○ electrical
- ○ maintenance

11. What does the term vulnerability mean?

Topic 16.1.0 - A vulnerability is not a threat, but it is a weakness that makes the PC or the software a target for attacks.

- ◉ a weakness that makes a target susceptible to an attack
- ○ a computer that contains sensitive information
- ○ a method of attack to exploit a target
- ○ a known target or victim machine
- ○ a potential threat that a hacker creates

12. What three configuration steps must be performed to implement SSH access to a router? (Choose three.)

Topic 16.4.0 - To implement SSH on a router the following steps need to be performed:
- Configure a unique hostname.
- Configure the domain name of the network.
- Configure a user account to use AAA or local database for authentication.
- Generate RSA keys.
- Enable VTY SSH sessions.

- ☐ a password on the console line
- ☑ an IP domain name
- ☑ a user account
- ☐ an enable mode password
- ☑ a unique hostname
- ☐ an encrypted password

13. What is the objective of a network reconnaissance attack?

Topic 16.2.0 - The objective of a network reconnaissance attack is to discover information about a network, network systems, and network services.

- (●) discovery and mapping of systems
- ( ) unauthorized manipulation of data
- ( ) disabling network systems or services
- ( ) denying access to resources by legitimate users

14. For security reasons a network administrator needs to ensure that local computers cannot ping each other. Which settings can accomplish this task?

Topic 16.3.0 - Smartcard and file system settings do not affect network operation. MAC address settings and filtering may be used to control device network access but cannot be used to filter different data traffic types.

- ( ) smartcard settings
- (●) firewall settings
- ( ) MAC address settings
- ( ) file system settings

15. A network administrator establishes a connection to a switch via SSH. What characteristic uniquely describes the SSH connection?

Topic 16.4.0 - SSH provides a secure remote login through a virtual interface. SSH provides a stronger password authentication than Telnet. SSH also encrypts the data during the session.

- ( ) out-of-band access to a switch through the use of a virtual terminal with password authentication
- ( ) remote access to the switch through the use of a telephone dialup connection
- ( ) on-site access to a switch through the use of a directly connected PC and a console cable
- (●) remote access to a switch where data is encrypted during the session
- ( ) direct access to the switch through the use of a terminal emulation program

Capítulo 17_Crear una red pequeña

Introducción

17.0.1

¿Por qué debería tomar este módulo?

Bienvenido a Armado de una red pequeña!

¡Hurra! Ha llegado al módulo final en el curso Introducción a las redes v7.0. Usted tiene la mayor parte del conocimiento fundamental necesario para establecer su propia red. ¿Qué sigue a partir de ahora? Construyes una red, por supuesto. Y no solo crear una, sino verificar que funciona e incluso solucionar algunos problemas comunes de red. Este módulo cuenta con laboratorios y actividades de Packet Tracer para ayudarle a practicar sus nuevas habilidades como administrador de red. Pongámonos en marcha.

17.0.2

¿Qué aprenderé en este módulo?

Título del módulo: Crear una red pequeña

Objetivos del módulo: Implementar un diseño de red para que una red pequeña incluya un router, un switch y terminales.

Título del tema	Objetivo del tema
Dispositivos de una red pequeña	Identificar los dispositivos utilizados en una red pequeña.
Protocolos y aplicaciones de redes pequeñas	Identificar las aplicaciones y los protocolos utilizados en una red pequeña.
Escalar hacia redes más grandes	Explicar la forma en que una red pequeña sirve como base de redes más grandes.
Verificar la conectividad	Utilice el resultado de los comandos ping y tracert para verificar la conectividad y establecer el rendimiento relativo de la red.
Comandos de host y de IOS	Utilizar los comandos del host y del IOS para obtener información sobre los dispositivos en una red.

Título del tema	Objetivo del tema
Metodologías para la resolución de problemas	Describir las metodologías comunes para la resolución de problemas.
Escenarios de resolución de problemas	Solucionar problemas de los dispositivos de la red.

Crear una red pequeña / Dispositivos de una red pequeña

Dispositivos de una red pequeña

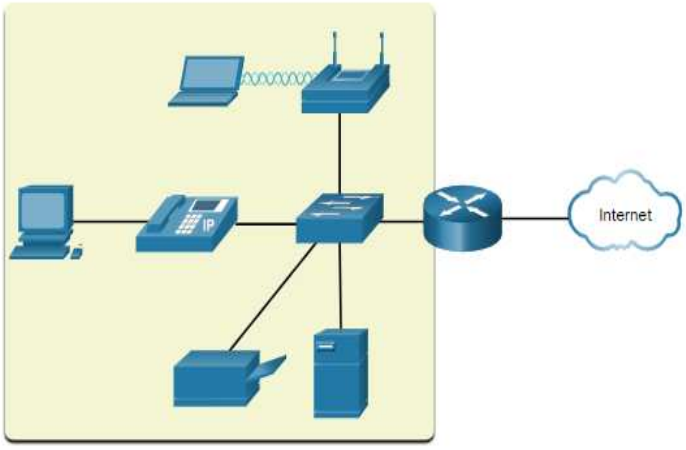
17.1.1

Topologías de redes pequeñas

La mayoría de las empresas son pequeñas; por lo tanto, no es sorprendente que la mayoría de las redes empresariales también sean pequeñas.

Un diseño de red pequeño suele ser simple. La cantidad y el tipo de dispositivos incluidos se reducen considerablemente en comparación con una red más grande.

Por ejemplo, consulte la red de ejemplo para pequeñas empresas que se muestra en la figura.



Topología de red pequeña con impresora, servidor, teléfono IP y host conectado, punto de acceso y portátil conectado, todo conectado a un switch conectado a un router conectado a la nube de Internet.

Esta pequeña red requiere un enrutador, un conmutador y un punto de acceso inalámbrico para conectar a usuarios cableados e inalámbricos, un teléfono IP, una impresora y un servidor. En cuanto a la conexión a Internet, las redes pequeñas normalmente tienen una única conexión WAN proporcionada por una conexión DSL, por cable o Ethernet.

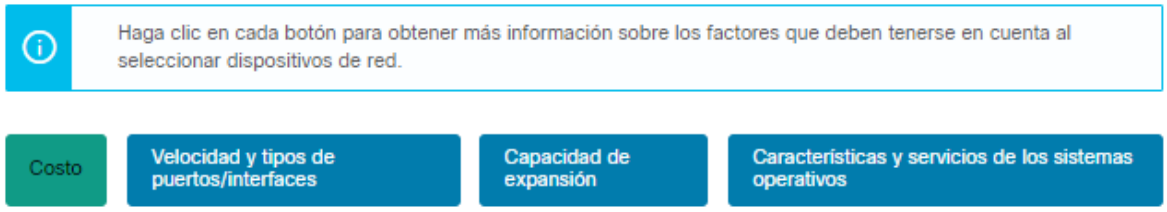
Las redes grandes requieren un departamento de TI para mantener, proteger y solucionar problemas de dispositivos de red y proteger los datos de la organización. La administración de una red pequeña requiere muchas de las mismas habilidades necesarias para administrar redes más grandes. Las redes pequeñas son administradas por un técnico local de TI o por un profesional contratado.

17.1.2

Selección de dispositivos para redes pequeñas.

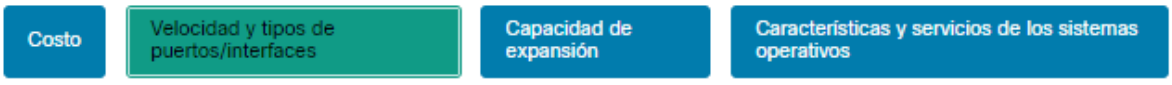
Al igual que las redes grandes, las redes pequeñas requieren planificación y diseño para cumplir con los requisitos del usuario. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación.

Una de las primeras consideraciones de diseño es el tipo de dispositivos intermediarios que se utilizarán para dar soporte a la red.



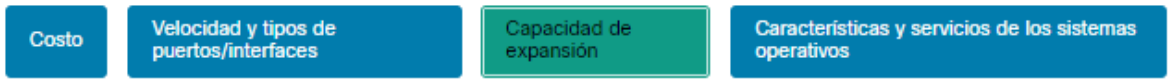
Costo (Cost)

El costo de un switch o un router se determina sobre la base de sus capacidades y características. Esto incluye la cantidad y los tipos de puertos disponibles, además de la velocidad de backplane. Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y tecnologías opcionales de switching avanzadas. También se debe tener en cuenta el costo del tendido de cable necesario para conectar cada dispositivo de la red. Otro elemento clave que afecta las consideraciones de costos es la redundancia que se debe incorporar en la red.



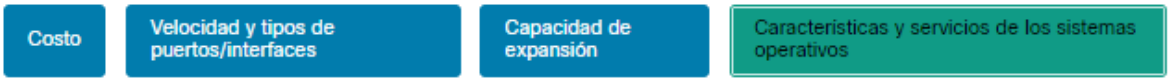
Velocidad y tipos de puertos/interfaces (Speed and types of Ports/interfaces)

Elegir la cantidad y el tipo de puertos en un router o un switch es una decisión fundamental. Las PC más modernas tienen NIC de 1Gbps incorporadas. Algunos servidores pueden incluso tener puertos de 10 Gbps. Si bien es más costoso, elegir dispositivos de capa 2 que puedan admitir velocidades mayores, estos permiten que la red evolucione sin reemplazar los dispositivos centrales.



Capacidad de expansión (Expandability)

Los dispositivos de red incluyen configuraciones físicas modulares y fijas. Las configuraciones fijas tienen un tipo y una cantidad específica de puertos o interfaces, que no puede aumentar. Los dispositivos modulares tienen ranuras de expansión para agregar nuevos módulos a medida que aumentan los requisitos. Existen switches con puertos adicionales para uplinks de alta velocidad. Se pueden utilizar routers para conectar diferentes tipos de redes. Se debe tener precaución al seleccionar las interfaces y los módulos adecuados para los medios específicos.



Características y servicios de los sistemas operativos (Operating System Features and Services)

Los dispositivos de red deben tener sistemas operativos que puedan admitir los requisitos de las organizaciones, como los siguientes:

- Switching de Capa 3
- Traducción de direcciones de red (NAT)
- Protocolo de configuración dinámica de host (DHCP)
- Seguridad
- Calidad de servicio (QoS)
- Voz sobre IP (VoIP)

17.1.3

Asignación de direcciones IP para redes pequeñas.

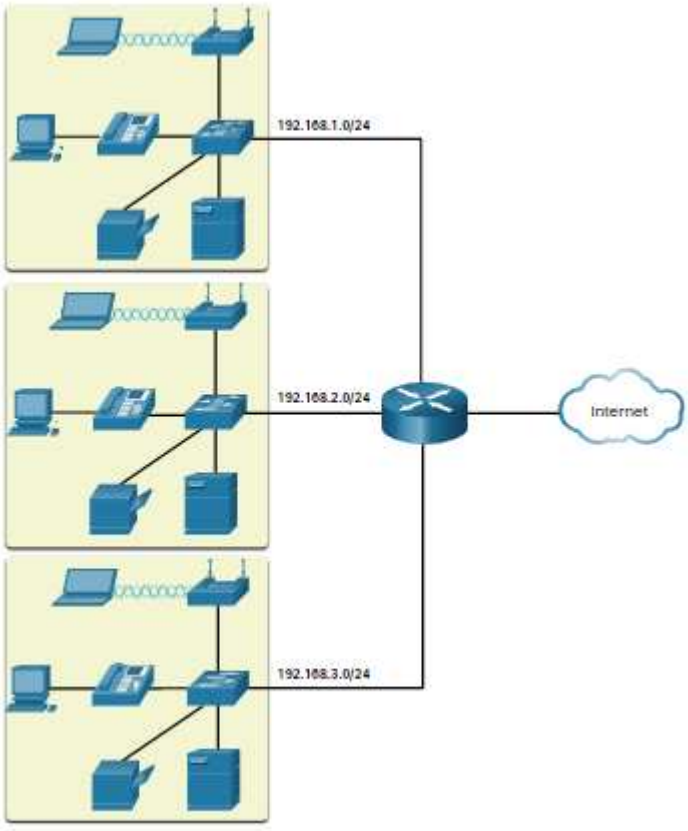
Al implementar una red, cree un esquema de direccionamiento IP y úselo. Todos los hosts dentro de una red interna deben tener una dirección exclusiva.

Entre los dispositivos que se incluirán en el esquema de direccionamiento IP se incluyen los siguientes:

- Dispositivos de usuario final: número y tipo de conexión (es decir, por cable, inalámbrico, acceso remoto)
- Servidores y dispositivos periféricos (por ejemplo, impresoras y cámaras de seguridad)
- Dispositivos intermedios, incluidos switches y puntos de acceso.

Se recomienda planificar, documentar y mantener un esquema de direccionamiento IP basado en el tipo de dispositivo. El uso de un esquema de direccionamiento IP planificado facilita la identificación de un tipo de dispositivo y la solución de problemas, como, por ejemplo, al solucionar problemas de tráfico de red con un analizador de protocolos.

Por ejemplo, consulte la topología de una organización de tamaño pequeño a mediano en la figura.

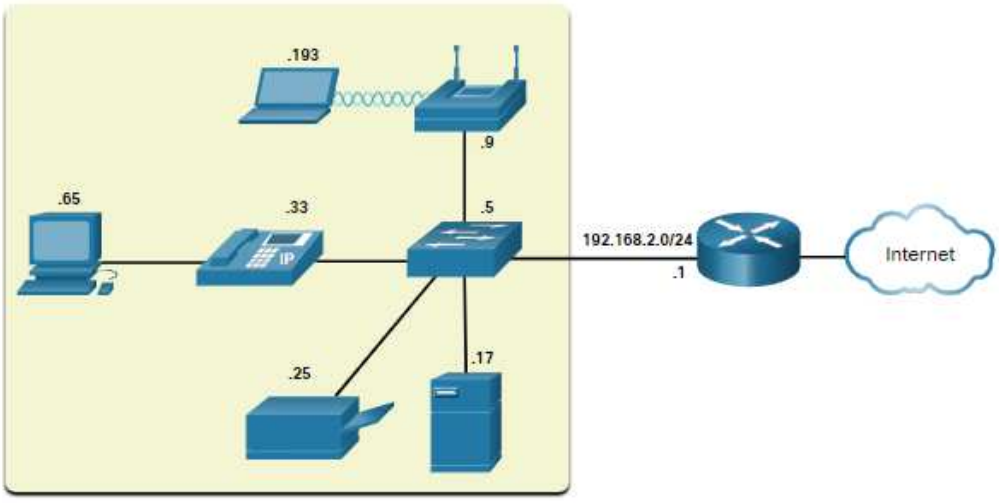


Topología de red que consta de tres LAN - 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24 - con varios dispositivos finales, conectados a un router conectado a la nube de Internet

La organización requiere tres LAN de usuario (es decir, 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24). La organización ha decidido implementar un esquema de direccionamiento IP coherente para cada LAN 192.168.x.0/24 utilizando el siguiente plan:

Tipo de dispositivo	Rango de direcciones IP Asignables	Resumido como ...
Puerta de Enlace Predeterminado (Router)	192.168.x**1** - 192.168.x.**2**	192.168.x**0/30**
Switches (max. 2)	192.168.x**5** - 192.168.x.**6**	192.168.x**4/30**
Puntos de acceso (máx. 6)	192.168.x**9** - 192.168.x.**14**	192.168.x**8/29**
Servidores (max. 6)	192.168.x**17** - 192.168.x.**22**	192.168.x**16/29**
Impresoras (max. 6)	192.168.x**25** - 192.168.x.**30**	192.168.x**24/29**
Teléfonos IP (max. 6)	192.168.x**33** - 192.168.x.**38**	192.168.x**32/29**
Dispositivos con cable (máx. 62)	192.168.x**65** - 192.168.x.**126**	192.168.x**64/26**
Dispositivos inalámbricos (max. 62)	192.168.x**193** - 192.168.x.**254**	192.168.x**192/26**

La figura muestra un ejemplo de los dispositivos de red 192.168.2.0/24 con direcciones IP asignadas utilizando el esquema de direcciones IP predefinido.



El diagrama es una topología LAN pequeña con una dirección de red 192.168.2.0/24. Muestra varios dispositivos finales todos conectados a un switch, con dirección .5, conectados a un router, en la dirección .1, conectados a la nube de Internet. A todos los dispositivos se les ha asignado una dirección IP. Una impresora tiene una dirección de .25; el servidor tiene una dirección de .17; un PC tiene una dirección de .65 conectada a un teléfono IP con una dirección de .3; y un portátil tiene una dirección de .193 conectada a un punto de acceso con una dirección de .9.

Por ejemplo, la dirección IP de la puerta de enlace predeterminada es 192.168.2.1/24, el switch es 192.168.2.5/24, el servidor es 192.168.2.17/24, etc.

Observe que los intervalos de direcciones IP asignables se asignaron deliberadamente en los límites de subred para simplificar el resumen del tipo de grupo. Por ejemplo, supongamos que otro switch con dirección IP 192.168.2.6 se agrega a la red. Para identificar todos los swicthes en una directiva de red, el administrador podría especificar la dirección de red resumida 192.168.x.4/30.

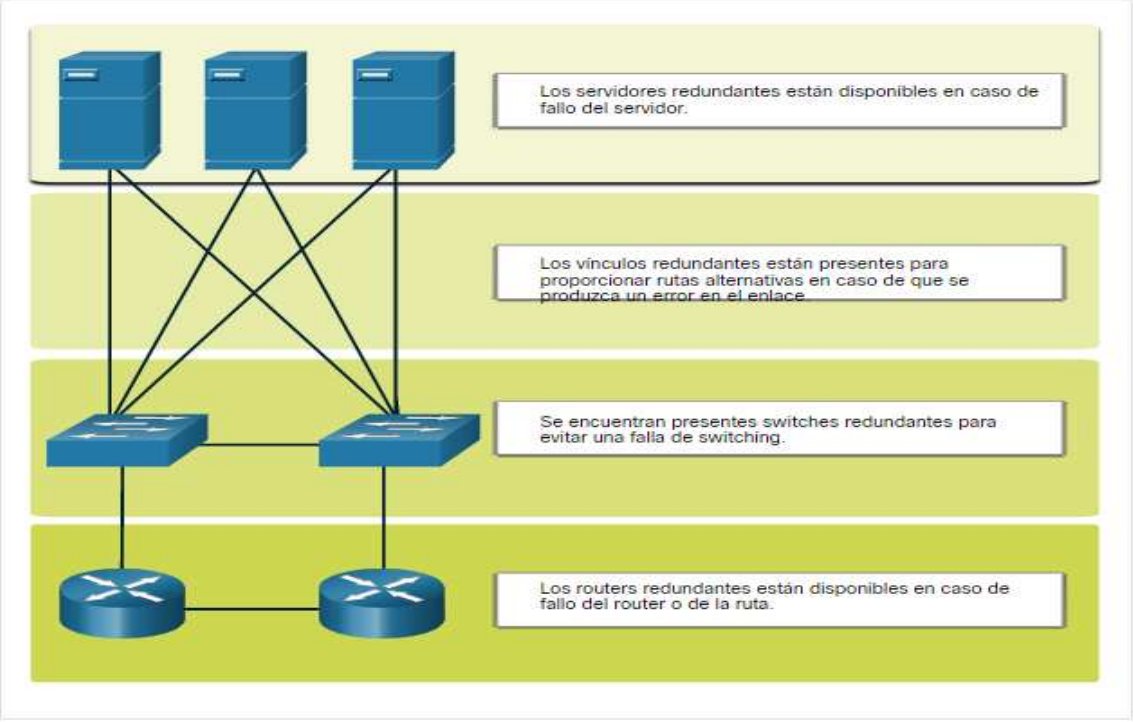
17.1.4

Redundancia en redes pequeñas

Otra parte importante del diseño de red es la confiabilidad. Incluso las pequeñas empresas, con frecuencia, dependen en gran medida de la red para su operación comercial. Una falla en la red puede tener consecuencias muy costosas.

Para mantener un alto grado de confiabilidad, se requiere *redundancia* en el diseño de red. La redundancia ayuda a eliminar puntos de error únicos.

Existen muchas formas de obtener redundancia en una red. La redundancia se puede obtener mediante la instalación de equipos duplicados, pero también se puede obtener al suministrar enlaces de red duplicados en áreas fundamentales, como se muestra en la ilustración.



Los servidores redundantes están disponibles en caso de fallo del servidor.

Los vínculos redundantes están presentes para proporcionar rutas alternativas en caso de que se produzca un error en el enlace.

Se encuentran presentes switches redundantes para evitar una falla de switching..

Los routers redundantes están disponibles en caso de fallo del router o de la ruta.

El diagrama ilustra el uso de servidores redundantes, enlaces, switches y routers en una red. Se muestran cuatro capas con una explicación de la redundancia lograda en cada una. La capa superior tiene tres servidores y una leyenda: los servidores redundantes están disponibles en caso de fallo del servidor. La siguiente capa muestra que cada servidor tiene dos conexiones que conducen a dos swicthes y la leyenda: los vínculos redundantes están presentes para proporcionar rutas alternativas en caso de un fallo de enlace. La siguiente capa muestra dos switches conectados entre sí, cada uno conectado a los tres servidores anteriores y la leyenda: Los switches redundantes están presentes en caso de fallo del switches. La capa inferior muestra dos routers conectados entre sí, cada uno conectado a uno de los switches y la leyenda: Los routers redundantes están disponibles en caso de fallo del router o de la ruta.

Por lo general, las redes pequeñas proporcionan un único punto de salida a Internet a través de uno o más gateways predeterminados. Si el router falla, toda la red pierde la conectividad a Internet. Por este motivo, puede ser recomendable para las pequeñas empresas contratar a un segundo proveedor de servicios a modo de respaldo.

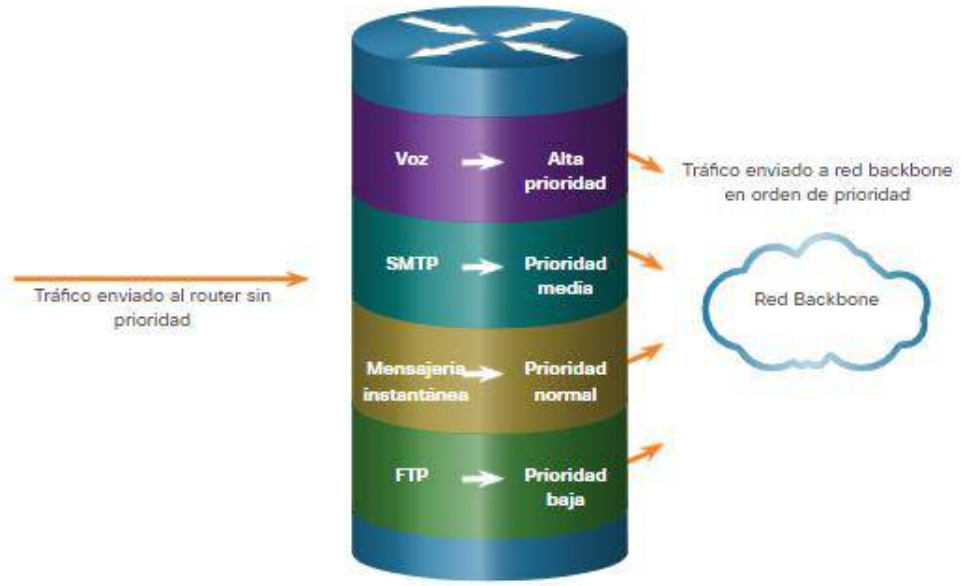
17.1.5

Administración del tráfico

El objetivo de un buen diseño de red, incluso para una red pequeña, es aumentar la productividad de los empleados y reducir el tiempo de inactividad de la red. El administrador de red debe tener en cuenta los diversos tipos de tráfico y su tratamiento en el diseño de la red.

Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, como voz y vídeo, de forma independiente del tráfico de otros datos. De hecho, un buen diseño de red clasifica el tráfico cuidadosamente según la prioridad, como se muestra en la ilustración.

El diagrama muestra cómo un router prioriza el tráfico de red. Una flecha muestra que el tráfico se envía a un router sin ninguna prioridad. A continuación, el router envía tráfico a la red troncal en orden de prioridad. El router tiene capas de tráfico diferente con diferentes niveles de prioridad, la prioridad más alta en la parte superior. La voz aparece primero con prioridad alta, luego SMTP con prioridad media, luego mensajería instantánea con prioridad normal y, por último, FTP con prioridad baja.



Hay cuatro colas de prioridad. La cola de alta prioridad alta siempre se vacía primero.

17.1.6

Compruebe su comprensión — Dispositivos en una red pequeña

Compruebe su comprensión de los dispositivos en una pequeña red eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. La mayoría de las empresas son pequeñas.
2. Los factores que deben tenerse en cuenta incluyen el costo, la velocidad y los tipos de puertos/interfaces, la capacidad de ampliación y las características y servicios del sistema operativo.
3. Al implementar una red, es necesario planificar y usar un esquema de direccionamiento IP.
4. La redundancia es necesaria para mantener un alto grado de fiabilidad y eliminar puntos únicos de falla.
5. Se requiere QoS para clasificar el tráfico de acuerdo con la prioridad.

Has tenido 5 respuestas correctas de 5.

1. ¿Qué declaración se relaciona correctamente con una red pequeña?

¡Lo tienes!

- ○ Las redes pequeñas son complejas.
- ○ Las redes pequeñas requieren un departamento de TI para mantenimiento.
- ◉ La mayoría de las empresas son pequeñas.

2. ¿Qué factor debe tenerse en cuenta al seleccionar dispositivos de red?

¡Lo tienes!

- ○ color
- ○ Conexiónes de la consola
- ◉ costo
- ○ elasticidad

3. ¿Qué es necesario planificar y utilizar al implementar una red?

¡Lo tienes!

- ○ Nombres de los dispositivos
- ◉ Esquema de direcciones IP
- ○ Esquema de direcciones MAC
- ○ ubicación de la impresora

4. ¿Qué se requiere para mantener un alto grado de confiabilidad y eliminar puntos únicos de falla?

¡Lo tienes!

- ○ Accesibilidad
- ○ Capacidad de expansión
- ○ Integridad
- ◉ redundancia

5. ¿Qué se requiere para clasificar el tráfico según la prioridad?

¡Lo tienes!

- ○ Esquema de direcciones IP
- ◉ calidad de servicio (QoS)
- ○ enrutamiento
- ○ Switching

Correct

You have successfully identified the correct answers.

1. The majority of businesses are small.
2. Factors to be considered include cost, speed and types of ports/interfaces, expandability, and operating system features and services.
3. When implementing a network, planning and using an IP addressing scheme is necessary.
4. Redundancy is required to maintain a high degree of reliability and eliminate single points of failure.
5. QoS is required to classify traffic according to priority.

You got 5 out of 5 questions correct.

1. Which statement correctly relates to a small network?

You got it!

- Small networks are complex.
- Small networks require an IT department to maintain.
- (•) The majority of businesses are small.

2. Which factor must be considered when selecting network devices?

You got it!

- color
- console connections
- (•) cost
- elasticity

3. What is necessary to plan and use when implementing a network?

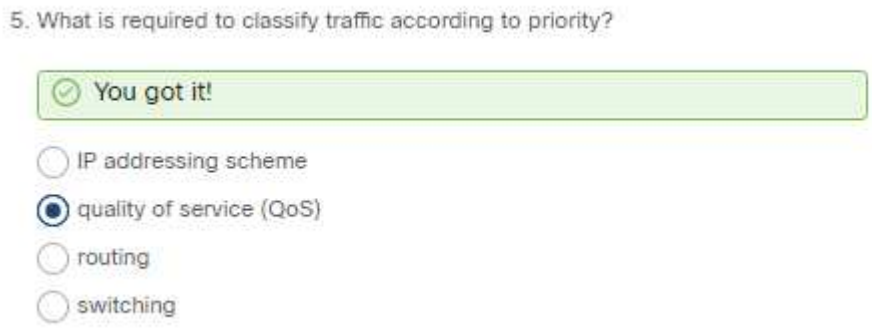
You got it!

- device names
- (•) IP addressing scheme
- MAC addressing scheme
- printer location

4. What is required to maintain a high degree of reliability and eliminate single points of failure?

You got it!

- accessibility
- expandability
- integrity
- (•) redundancy



Crear una red pequeña / Protocolos y aplicaciones de redes pequeñas

Protocolos y aplicaciones de redes pequeñas

17.2.1

Aplicaciones comunes

El tema anterior discutió los componentes de una red pequeña, así como algunas de las consideraciones de diseño. Estas consideraciones son necesarias cuando se acaba de configurar una red. Después de configurar, la red aún necesita ciertos tipos de aplicaciones y protocolos para funcionar.

La utilidad de las redes depende de las aplicaciones que se encuentren en ellas. Hay dos tipos de programas o procesos que proporcionan acceso a la red: las aplicaciones de red y los servicios de la capa de aplicación.

Aplicaciones de Red

Las aplicaciones son los programas de software que se utilizan para comunicarse a través de la red. Algunas aplicaciones de usuario final reconocen la red, lo que significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los navegadores web son ejemplos de este tipo de aplicaciones.

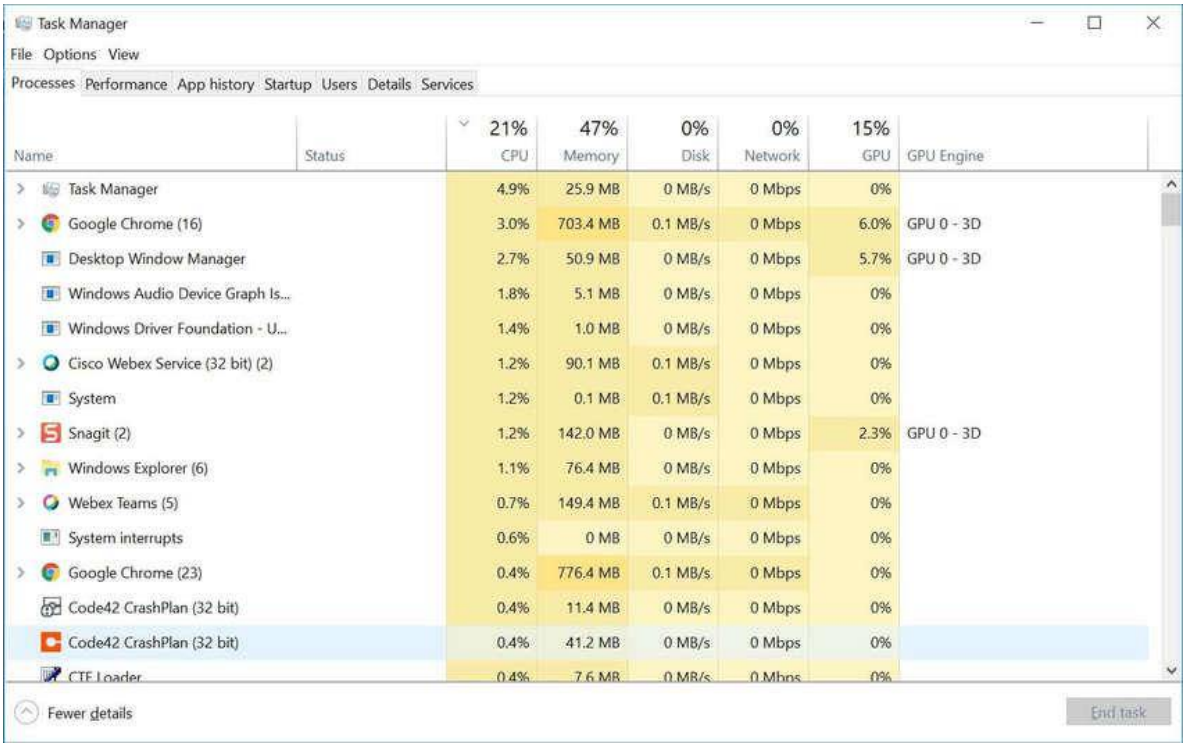
Servicios de Capa de Aplicación

Otros programas pueden necesitar la asistencia de los servicios de la capa de aplicación para utilizar recursos de red, como la transferencia de archivos o la administración de las colas de

impresión en la red. Si bien el empleado no se da cuenta, estos servicios son los programas que interactúan con la red y preparan los datos para la transferencia. Los distintos tipos de datos, ya sean de texto, gráficos o vídeo, requieren distintos servicios de red para asegurar que estén correctamente preparados para que los procesen las funciones que se encuentran en las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y los formatos de datos que se deben utilizar. Sin protocolos, la red de datos no tendría una manera común de dar formato y direccionar los datos. Es necesario familiarizarse con los protocolos subyacentes que rigen la operación de los diferentes servicios de red para entender su función.

Utilice el Administrador de tareas para ver las aplicaciones, los procesos y los servicios en ejecución en una PC Windows, como se muestra en la figura.



17.2.2

Protocolos comunes

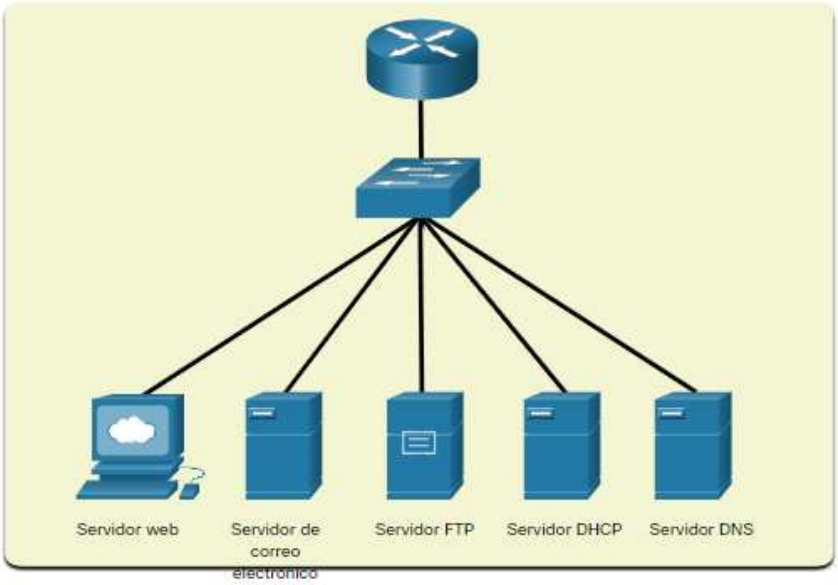
La mayor parte del trabajo de un técnico, ya sea en una red pequeña o una red grande, está relacionada de alguna manera con los protocolos de red. Los protocolos de red admiten los servicios y aplicaciones que usan los empleados en una red pequeña.

Los administradores de red suelen requerir acceso a los dispositivos y servidores de red. Las dos soluciones de acceso remoto más comunes son Telnet y Secure Shell (SSH). El servicio SSH es una alternativa segura a Telnet. Cuando están conectados, los administradores pueden acceder al dispositivo del servidor SSH como si hubieran iniciado sesión localmente.

SSH se utiliza para establecer una conexión de acceso remoto segura entre un cliente SSH y otros dispositivos habilitados para SSH:

- **Dispositivo de red** : el dispositivo de red (por ejemplo, router, switch, punto de acceso, etc.) debe admitir SSH para proporcionar acceso remoto a los servicios de servidor SSH a los clientes.
- **Servidor** - El servidor (por ejemplo, servidor web, servidor de correo electrónico, etc.) debe admitir servicios de servidor SSH de acceso remoto a los clientes.

Los administradores de red también deben admitir servidores de red comunes y sus protocolos de red relacionados, como se muestra en la figura.



Servidor web Servidor de correo electrónico Servidor FTP Servidor DHCP Servidor DNS

Haga clic en cada botón para obtener más información acerca de los servidores de red comunes y los protocolos de red relacionados a los mismos.

Servidor web | Servidor de correo electrónico | Servidor FTP | Servidor DHCP | Servidor DNS

Servidor Web

- Los clientes web y los servidores web intercambian tráfico web mediante el Protocolo de transferencia de Hipertexto (HTTP).
- El Protocolo de Transferencia de Hipertexto Seguro (HTTPS) se utiliza para la comunicación web segura.

Servidor de Correo Electrónico

- Los servidores y clientes de correo utilizan el Protocolo Simple de Transferencia de Correo (SMTP) para enviar correos.
- El Protocolo de Oficina de Correos (POP) y el Protocolo de Acceso a Mensajes de Internet (IMAP) se utilizan para recibir correos electrónicos.
- Los receptores están identificados con el formato usuario@xyz.

Servidor FTP

- El servicio de Protocolo de transferencia de archivos (FTP) permite descargar y cargar archivos entre un cliente y un servidor FTP.
- Secure FTP (SFTP) se utilizan para proteger el intercambio de archivos FTP.

Servidor DHCP

Los clientes utilizan el Protocolo de configuración dinámica de host (DHCP) para adquirir una configuración IP (es decir, dirección IP, máscara de subred, puerta de enlace predeterminada, etc.) de un servidor DHCP.

Servidor DNS

- El Servicio de nombres de dominio (DNS) resuelve un nombre de dominio en una dirección IP (por ejemplo, cisco.com = 72.163.4.185)
- DNS proporciona la dirección IP de un sitio web (es decir, nombre de dominio) a un host solicitante.

Nota: Un servidor podría proporcionar varios servicios de red. Por ejemplo, un servidor podría ser un servidor de correo electrónico, FTP y SSH.

Estos protocolos de red conforman el conjunto de herramientas fundamental de los profesionales de red. Cada uno de estos protocolos de red define lo siguiente:

- Procesos en cualquier extremo de una sesión de comunicación.
- Tipos de mensajes.
- La sintaxis de los mensajes

- Significado de los campos informativos.
- Cómo se envían los mensajes y la respuesta esperada.
- Interacción con la siguiente capa inferior

Muchas empresas establecieron una política de utilización de versiones seguras de estos protocolos (e.g., SSH, SFTP, and HTTPS), siempre que sea posible.

17.2.3

Aplicaciones de voz y vídeo

En la actualidad, las empresas utilizan cada vez más la telefonía IP y la transmisión de medios para comunicarse con sus clientes y partners comerciales. Muchas organizaciones están permitiendo a sus empleados trabajar de forma remota. Como muestra la figura, muchos de sus usuarios aún necesitan acceso a software y archivos corporativos, así como soporte para aplicaciones de voz y video.

El administrador de red debe asegurarse de que se instalen los equipos adecuados en la red y que se configuren los dispositivos de red para asegurar la entrega según las prioridades.

Haga clic en cada botón para obtener más información sobre los factores que un administrador de red debe tener en cuenta al admitir aplicaciones en tiempo real.

Infraestructura | VoIP | Telefonía IP | Aplicaciones en tiempo real

Infraestructura

- La infraestructura de red debe admitir las aplicaciones en tiempo real.
- Los dispositivos existentes y el cableado deben ser probados y validados.
- Es posible que se necesiten productos de red más recientes.

Infraestructura | VoIP | Telefonía IP | Aplicaciones en tiempo real

VoIP

- Los dispositivos VoIP convierten la señal analógica de los teléfonos en paquetes IP digitales.

- Generalmente, VoIP es mucho más económico que una solución de telefonía IP integrada, pero la calidad de las comunicaciones no cumple con los mismos estándares.
- En una red pequeña, el uso de voz y vídeo sobre IP se pueden resolver mediante Skype y versiones no empresariales de Cisco WebEx.

Telefonía IP

- Un teléfono IP realiza la conversión de voz a IP con el uso de un servidor dedicado para el control de llamadas y la señalización.
- Muchos proveedores ofrecen soluciones de telefonía IP para pequeñas empresas, como los productos Cisco Business Edition 4000 Series.

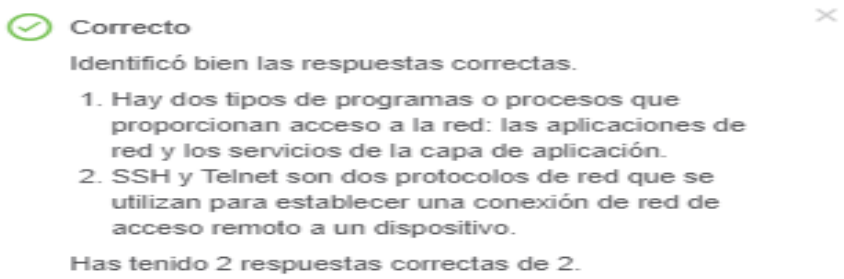
Aplicaciones en Tiempo Real

- La red debe admitir mecanismos de calidad de servicio (QoS) para minimizar los problemas de latencia de las aplicaciones de transmisión en tiempo real.
- El Protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol) y el Protocolo de control de transporte en tiempo real (RTCP, Real-Time Transport Control Protocol) admiten este requisito.

17.2.4

Compruebe su comprensión — Aplicaciones y protocolos en redes pequeñas

Compruebe su comprensión de las aplicaciones y protocolos de red pequeñas eligiendo la MEJOR respuesta para las siguientes preguntas.



1. ¿Cuales son los dos tipos de programas/procesos que proporcionan acceso a la red? (Escoja dos opciones).

¡Lo tienes!

- [ ] Software antivirus
- [x] Servicios de la capa de aplicación
- [ ] software de juegos
- [x] Aplicaciones de red
- [ ] software de productividad
- [ ] Programas de virtualización

2. ¿Qué dos protocolos de red se utilizan para establecer una conexión de red de acceso remoto a un dispositivo? (Escoja dos opciones).

¡Lo tienes!

- [ ] Protocolo de transferencia de archivos (FTP)
- [ ] Protocolo de transferencia de hipertexto (HTTP).
- [ ] Conexión remota (RC)
- [x] Secure Shell (SSH)
- [ ] Protocolo simple de transferencia de correo (SMTP)
- [x] Telnet

Correct

You have successfully identified the correct answers.

1. Application layer services and network applications are two forms of software programs that provide access to the network.
2. SSH and Telnet are two network protocols that are used to establish a remote access network connection to a device.

You got 2 out of 2 questions correct.

1. What are two forms of software programs or processes that provide access to the network? (Choose two.)

You got it!

- [ ] antivirus software
- [x] application layer services
- [ ] gaming software
- [x] network applications
- [ ] productivity software
- [ ] virtual machine software

2. Which two network protocols are used to establish a remote access network connection to a device? (Choose two.)

You got it!

- [ ] File Transfer Protocol (FTP)
- [ ] Hypertext Transfer Protocol (HTTP).
- [ ] Remote Connect (RC)
- [x] Secure Shell (SSH)
- [ ] Simple Mail Transfer Protocol (SMTP)
- [x] Telnet

Crear una red pequeña / Escalar hacia redes más grandes

Escalar hacia redes más grandes

17.3.1

Crecimiento de las redes pequeñas

Si su red es para una pequeña empresa, presumiblemente, desea que ese negocio crezca y que su red crezca junto con ella. Esto se denomina escalar una red, y existen algunas prácticas recomendadas para hacerlo.

El crecimiento es un proceso natural para muchas pequeñas empresas, y sus redes deben crecer en consecuencia. Idealmente, el administrador de la red tiene suficiente tiempo de preparación para tomar decisiones inteligentes sobre el crecimiento de la red en línea con el crecimiento de la empresa.

Para extender una red, se requieren varios elementos:

- **Documentación de la red** - Topologías física y lógica
- **Inventario de dispositivos** - Lista de dispositivos que utilizan o conforman la red
- **Presupuesto** - Presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal
- **Análisis de tráfico** - se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico

Estos elementos se utilizan para fundamentar la toma de decisiones que acompaña el escalamiento de una red pequeña.

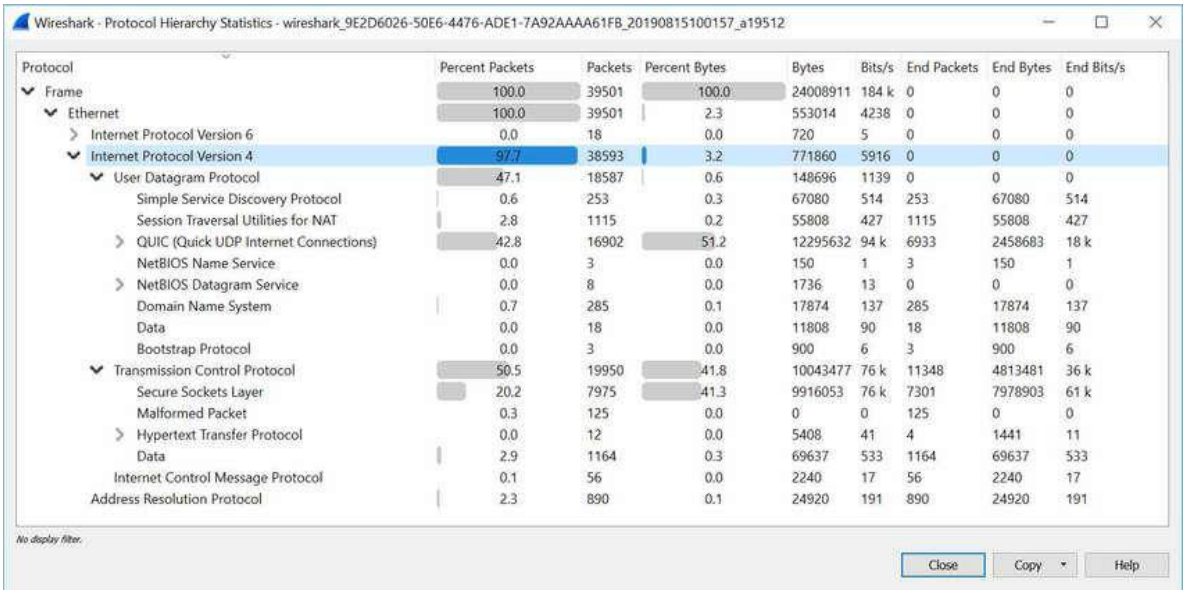
17.3.2

Análisis de protocolos

A medida que la red crece, es importante determinar cómo administrar el tráfico de red. Es muy importante entender el tipo de tráfico que atraviesa la red, así como el flujo de tráfico. Hay varias herramientas de administración de red que se pueden utilizar para este propósito. Sin embargo, también se puede utilizar un analizador de protocolos simple como Wireshark.

Por ejemplo, ejecutar Wireshark en varios hosts clave puede revelar los tipos de tráfico de red que fluye a través de la red. La siguiente figura muestra las estadísticas de jerarquía de protocolo en Wireshark para un host Windows en una red pequeña.

Captura de pantalla de estadísticas de jerarquía de protocolo en Wireshark para el tráfico capturado por un host



La captura de pantalla revela que el host está utilizando protocolos IPv6 e IPv4. La salida de IPv4 también revela que el host ha utilizado DNS, SSL, HTTP, ICMP y otros protocolos.

Para determinar los patrones de flujo de tráfico, es importante hacer lo siguiente:

- Capturar tráfico en horas de uso pico para obtener una buena representación de los diferentes tipos de tráfico.
- Realice la captura en diferentes segmentos de red y dispositivos, ya que parte del tráfico será local para un segmento en particular.

La información recopilada por el analizador de protocolos se evalúa de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía. Este análisis puede utilizarse para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Para hacerlo, se pueden reducir los flujos de tráfico innecesarios o modificar completamente los patrones de flujo mediante el traslado de un servidor, por ejemplo.

En ocasiones, simplemente reubicar un servidor o un servicio en otro segmento de red mejora el rendimiento de la red y permite adaptarse a las necesidades del tráfico creciente. Otras veces, la optimización del rendimiento de la red requiere el rediseño y la intervención de la red principal.

17.3.3

Utilización de la red por parte de los empleados

Además de comprender las tendencias cambiantes del tráfico, los administradores de red también deben ser conscientes de cómo cambia el uso de la red. Muchos sistemas operativos proporcionan herramientas integradas para mostrar dicha información. Por ejemplo, un host de Windows proporciona herramientas como el Administrador de tareas, el Visor de eventos y las herramientas Uso de datos.

Estas herramientas se pueden utilizar para capturar una «instantánea» de información como la siguiente:

- SO y versión del SO
- Utilización de CPU
- Utilización de RAM
- Utilización de unidades
- Aplicaciones que no utilizan la red
- Aplicaciones de red

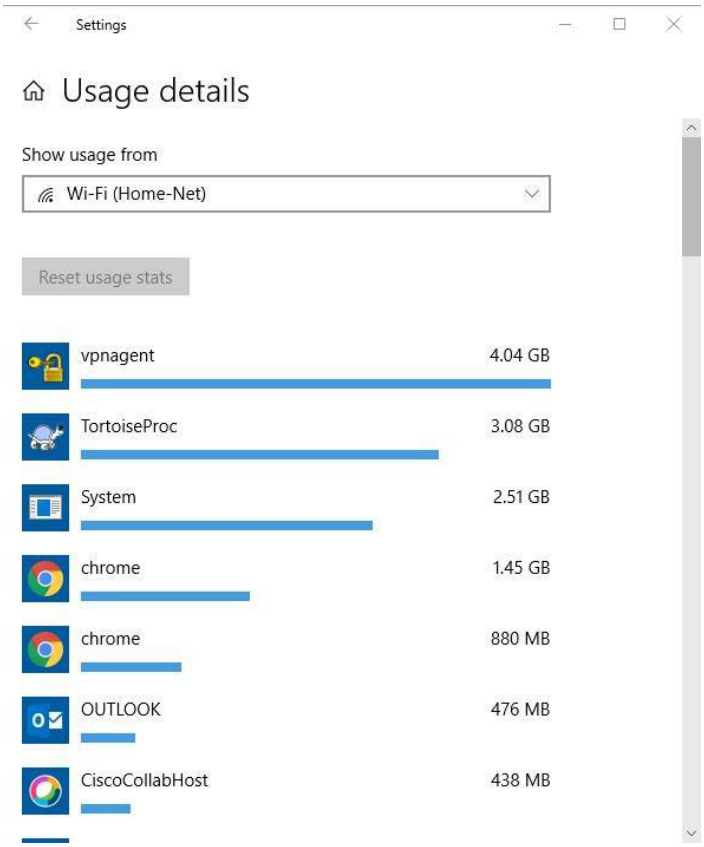
Documentar instantáneas para los empleados en una red pequeña, durante un período de tiempo, es muy útil para identificar los requisitos de crecimiento y los flujos de tráfico

asociados. Un cambio en la utilización de recursos puede requerir que el administrador de red ajuste la asignación de los recursos de red.

La herramienta Uso de datos de Windows 10 es especialmente útil para determinar qué aplicaciones utilizan servicios de red en un host. Se accede a la herramienta Uso de datos mediante **Settings > Network & Internet > Data usage > network interface** (desde los últimos 30 días).

El ejemplo de la figura muestra las aplicaciones que se ejecutan en un host Windows 10 de usuario remoto utilizando la conexión de red Wi-Fi local.

Captura de pantalla de la Herramienta de uso de datos de Windows 10 que muestra el uso de una conexión Wi-Fi local.



17.3.4

Verifique su comprensión — Crecimiento hacia redes más grandes

Compruebe su comprensión acerca de escalar a redes más grandes eligiendo la MEJOR respuesta a las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. Los elementos para escalar a una red más grande incluyen presupuesto, inventario de dispositivos, documentación de red y análisis de tráfico.
2. Wireshark puede revelar los tipos de tráfico de red que fluye a través de la red.
3. La herramienta Uso de datos de Windows 10 es útil para determinar qué aplicaciones utilizan servicios de red en un host.

Has tenido 3 respuestas correctas de 3.

Correct

You have successfully identified the correct answers.

1. Elements to scale to a larger network include budget, device inventory, network documentation, and traffic analysis.
2. Wireshark can reveal the types of network traffic flowing through the network.
3. The Windows 10 Data Usage tool is useful to determine which applications are using network services on a host.

You got 3 out of 3 questions correct.

1. ¿Qué elementos se requieren para escalar a una red más grande? (Escoja dos opciones).

¡Lo tienes!

- [x] Presupuesto
- [ ] configuraciones del dispositivo
- [ ] aumento de ancho de banda
- [x] documentación de red
- [ ] hosts de windows

2. ¿Qué software instalado en hosts importantes, puede revelar los tipos de tráfico de red que fluye a través de la red?

¡Lo tienes!

- ( ) Linux
- ( ) MacOS
- ( ) SSH
- ( ) Windows
- (•) Wireshark

3. ¿Qué herramienta de Windows 10 es útil para determinar qué aplicaciones utilizan servicios de red en un host?

¡Lo tienes!

- ◯ Panel de control
- ◉ Uso de datos
- ◯ administrador de archivos
- ◯ Firewall de Windows Defender
- ◯ Explorador de Windows

1. Which elements are required to scale to a larger network? (Choose two.)

You got it!

- ☑ budget
- ☐ device configurations
- ☐ increased bandwidth
- ☑ network documentation
- ☐ windows hosts

2. Which software installed on key hosts can reveal the types of network traffic flowing through the network?

You got it!

- ◯ Linux
- ◯ MacOS
- ◯ SSH
- ◯ Windows
- ◉ Wireshark

3. What Windows 10 tool is useful to determine which applications are using network services on a host?

You got it!

- ◯ Control panel
- ◉ Data Usage
- ◯ File Manager
- ◯ Windows Defender Firewall
- ◯ Windows Explorer

Crear una red pequeña / Verificar la conectividad

Verificar la conectividad

17.4.1

Verificar la conectividad con Ping

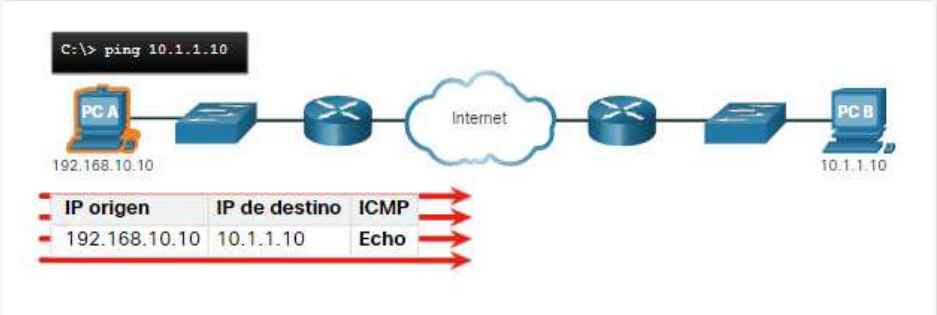
Si su red es pequeña y nueva, o si está escalando una red existente, siempre querrá poder verificar que sus componentes estén correctamente conectados entre sí y al Internet. En este tema se describen algunas utilidades que puede usar para asegurarse de que la red está conectada.

El comando **ping,** es la forma más eficaz de probar rápidamente la conectividad de Capa 3 entre una dirección IP de origen y destino. El comando también muestra varias estadísticas acerca del tiempo de ida y vuelta.

Específicamente, el comando **ping** utiliza los mensajes echo del Protocolo de Mensajes de Control de Internet (ICMP tipo 8) y respuesta de echo (ICMP tipo 0). El comando **ping** está disponible en la mayoría de los sistemas operativos, incluidos Windows, Linux, macOS y Cisco IOS.

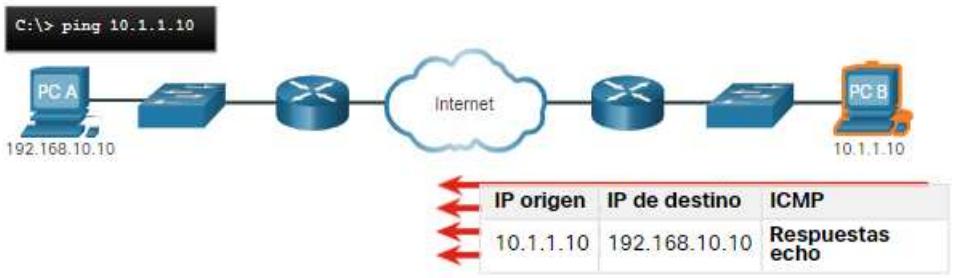
En un host de Windows 10, el comando **ping** envía cuatro mensajes de echo ICMP consecutivos y espera cuatro respuestas de echo ICMP consecutivas desde el destino.

Por ejemplo, supongamos que PC A hace ping a PC B. Como se muestra en la figura, el host PC A Windows envía cuatro mensajes de echo ICMP consecutivos al PC B (10.1.1.10).



El diagrama muestra el PC host A, en la dirección 192.168.10.10, utilizando el comando ping 10.1.1.10 del símbolo del sistema para enviar cuatro mensajes de echo ICMP con una IP de origen de 198.168.10.10 (debe leerse 192.168.10.10) y una IP de destino de 10.1.1.10, que es el PC host B en otra red.

El host de destino recibe y procesa los echos ICMP. Como se muestra en la figura, PC B responde enviando cuatro mensajes de respuesta de echo ICMP al PC A.



El diagrama muestra el PC host B, en la dirección 10.1.1.0, enviando cuatro respuestas de echo ICMP con IP de origen 10.1.1.10 e IP de destino 198.168.10.10 (debe ser 192.168.10.10) en respuesta a un ping desde el PC host A en la dirección 192.168.10.10.

Como se muestra en el resultado del comando, PC A ha recibido respuestas de echo de PC-B verificando la conexión de red de Capa 3.

```
C:\Users\PC -A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=47ms TTL=51
Reply from 10.1.1.10: bytes=32 time=60ms TTL=51
Reply from 10.1.1.10: bytes=32 time=53ms TTL=51
Reply from 10.1.1.10: bytes=32 time=50ms TTL=51
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 60ms, Average = 52ms
C:\Users\PC -A>
```

La salida confirma la conectividad de Capa 3 entre el PC A y el PC B.

La salida de un comando **ping** del IOS de Cisco varía de un host de Windows. Por ejemplo, el ping de IOS envía cinco mensajes de eco ICMP, como se muestra en la salida.

```
R1# ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

Observe los **!!!!!** caracteres en el resultado. El comando IOS **ping** muestra un indicador para cada respuesta de echo ICMP recibida. En la siguiente tabla se enumeran los posibles caracteres del comando **ping**:

Indicadores de ping IOS

Element	Description
!	• Exclamation mark indicates successful receipt of an echo reply message. • It validates a Layer 3 connection between source and destination.
.	• A period means that time expired waiting for an echo reply message. • This indicates a connectivity problem occurred somewhere along the path.
U	• Uppercase **U** indicates a router along the path responded with an ICMP Type 3 "destination unreachable" error message. • Possible reasons include the router does not know the direction to the destination network or it could not find the host on the destination network.

Nota: Otras posibles respuestas de ping incluyen Q, M, ? , o &. Sin embargo, el significado de estos, están fuera de alcance para este módulo.

17.4.2

Ping extendido

Un **ping** estándar utiliza la dirección IP de la interfaz más cercana a la red de destino como origen de **ping**. La dirección IP de origen del comando **ping 10.1.1.10** en R1 sería la de la interfaz G0/0/0 (209.165.200.225), como se ilustra en el ejemplo.

El diagrama muestra cómo un router utiliza un ping estándar para hacer ping a un host mediante el envío de cuatro mensajes de echo ICMP consecutivos procedentes de la interfaz más cercana al destino. El router R1 está conectado a dos redes: a la izquierda está 192.168.10.0/24 en la interfaz G0/0/1 con dirección .1 y a la derecha está la red 209.165.200.224/30 en la interfaz G0/0/0 con dirección .225. Esta última red está conectada a R2, que está conectada a la red 10.1.1.0/24 en la que la PC B está conectada con la dirección .10. R1 está enviando cuatro mensajes de echo ICMP PC B con una IP de origen de 209.165.200.225 y una IP de destino de 10.1.1.10.

Cisco IOS ofrece un modo "extendido" del comando **ping**. Este modo permite al usuario crear un tipo especial de pings ajustando los parámetros relacionados con la operación de comando.

El ping extendido se ingresa en modo EXEC privilegiado escribiendo **ping** sin una dirección IP de destino. A continuación, se le darán varias indicaciones para personalizar el **ping** extendido.

Nota: Al presionar **Enter,** se aceptan los valores predeterminados indicados.

Por ejemplo, suponga que desea probar la conectividad desde la LAN R1 (es decir, 192.168.10.0/24) a la LAN 10.1.1.0. Esto podría verificarse desde el PC A. Sin embargo, un **ping** extendido podría ser configurado en R1 para especificar una dirección de origen diferente.

Como se ilustra en el ejemplo, la dirección IP de origen del comando **ping** extendido en R1 podría configurarse para usar la dirección IP de interfaz G0/0/1 (es decir, 192.168.10.1).

El diagrama muestra cómo un router utiliza un ping extendido para hacer ping a un host mediante el envío de cuatro mensajes de eco ICMP consecutivos con una dirección IP de origen especificada. El router R1 está conectado a dos redes: a la izquierda está 192.168.10.0/24 en la interfaz G0/0/1 con dirección .1 y a la derecha está la red 209.165.200.224/30 en la interfaz G0/0/0 con dirección .225. Esta última red está conectada a R2, que está conectada a la red 10.1.1.0/24 en la que la PC B está conectada con la dirección .10. R1 está enviando al PC B cuatro mensajes de echo ICMP con una IP de origen de 192.168.10.1 y una IP de destino de 10.1.1.10.

El siguiente resultado del comando configura un **ping** extendido en R1 y especifica que la dirección IP de origen sea la de la interfaz G0/0/1 (es decir, 192.168.10.1).

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Nota: El comando **ping ipv6** se utiliza para pings IPv6 extendidos.

17.4.3

Verificar la conectividad con Traceroute

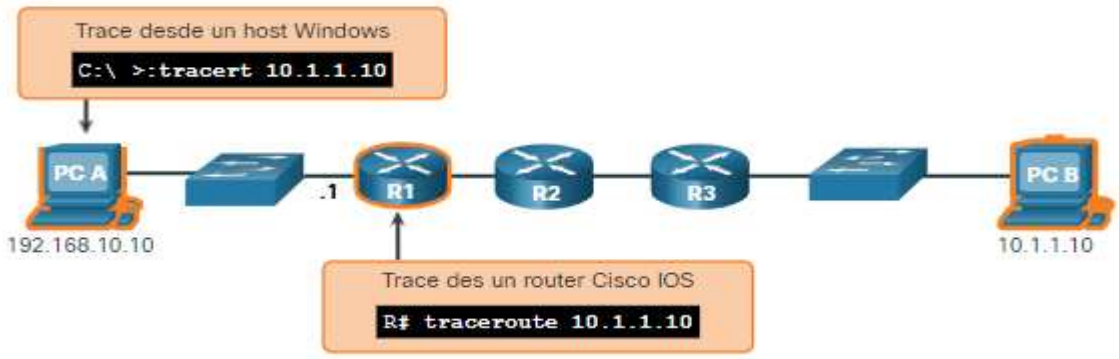
El comando **ping** es útil para determinar rápidamente si existe un problema de conectividad de Capa 3. Sin embargo, no identifica dónde se encuentra el problema a lo largo de la ruta.

Traceroute puede ayudar a localizar áreas con problemas de la Capa 3 en una red. Un trace proporciona una lista de saltos cuando un paquete se enruta a través de una red. Se podría utilizar para identificar el punto a lo largo de la ruta donde se puede encontrar el problema.

La sintaxis del comando trace varía según los sistemas operativos, como se ilustra en la figura.

El diagrama muestra la diferencia entre el comando trace emitido desde un host Windows frente a un router Cisco IOS. La topología de red consiste en un PC host A conectado a un switch conectado al router R1 conectado al router R2 conectado al router R3 conectado a un switch conectado al PC host B. El PC A, en la dirección IP 192.168.10.10, emite el siguiente comando desde un símbolo del sistema de Windows: C:\ >:tracert 10.1.1.10. R1 está emitiendo el siguiente comando desde la CLI del IOS de Cisco: R#traceroute 10.1.1.10.

Comando trace de Windows y Cisco IOS



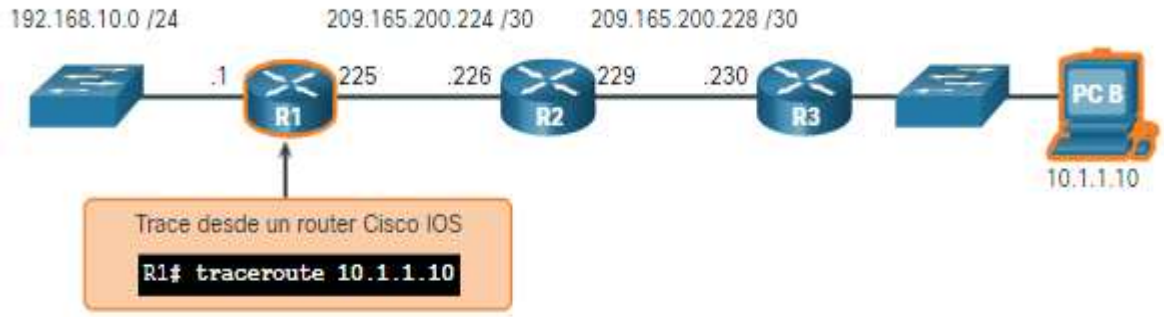
El siguiente es un ejemplo de salida de comando **tracert** en un host con Windows 10.

```
C:\Users\PC -A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1 2 ms 2 ms 2 ms 192.168.10.1
  2 * * * Request timed out.
  3 * * * Request timed out.
  4 * * * Request timed out.
^C
C:\Users\PC -A>
```

Nota: Use **Ctrl-C** para interrumpir **tracert** en Windows.

La única respuesta exitosa fue desde la puerta de enlace en R1. Las solicitudes de trace al siguiente salto se agotaron como indica el asterisco (\ *), lo que significa que el router de siguiente salto no respondió. Los resultados del trace indican que, o bien hay una falla en la interconexión de redes fuera de la LAN o que esos routers se configuraron para no responder a las solicitudes de echo que se utilizan en el trace. En este ejemplo parece haber un problema entre R1 y R2.

La salida de un comando **traceroute** del IOS de Cisco varía de la del comando **tracert** de Windows. Por ejemplo, consulte la topología en la figura.



El diagrama muestra una topología de red con el direccionamiento IP de las interfaces del router y un comando traceroute emitido desde un router Cisco IOS. La topología consiste en los siguientes dispositivos y redes, de izquierda a derecha. Un switch en la red 192.168.10.0/24 está conectado al router R1 en una interfaz con una dirección de .1. R1 está conectado al router R2 por la red 209.165.200.224/30. La interfaz en R1 tiene una dirección de .225 y la interfaz en R2 tiene una dirección de .226. R2 está conectado al router R3 por la red 209.165.200.228/30. La interfaz de R2 tiene una dirección de .229 y la interfaz de R3 tiene una dirección de .230. R3 está conectado a un switch que está conectado al PC host B con la dirección 10.1.1.10. R1 está emitiendo el siguiente comando trace desde la CLI: R1# traceroute 10.1.1.10.

El siguiente es el resultado de ejemplo del comando traceroute de R1:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 mseg 0 mseg 1 mseg
  2 209.165.200.230 1 mseg 0 mseg 1 mseg
  3 10.1.1.10 1 mseg 0 mseg
R1#
```

En este ejemplo, el trace validó que puede llegar a PC B sin problemas.

Los tiempos de espera indican un potencial problema. Por ejemplo, si el host 10.1.1.10 no estaba disponible, el comando **traceroute** mostraría el siguiente resultado:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 * * *
  4 * * *
  5*
```

Utilice **Ctrl-Shift-6** para interrumpir un **traceroute** en Cisco IOS.

Nota: La implementación de Windows de traceroute (tracert) envía solicitudes de echo ICMP. Cisco IOS y Linux utilizan UDP con un número de puerto no válido. El destino final devolverá un mensaje de puerto ICMP inalcanzable.

17.4.4

Traceroute extendido

Al igual que el comando **ping** extendido, también hay un comando **traceroute** extendido. Permite al administrador ajustar los parámetros relacionados con la operación del comando. Esto es útil para solucionar problemas de bucles de enrutamiento, determinando el router de siguiente salto, o ayudar a determinar dónde los paquetes son descartados por un router o denegados por un firewall.

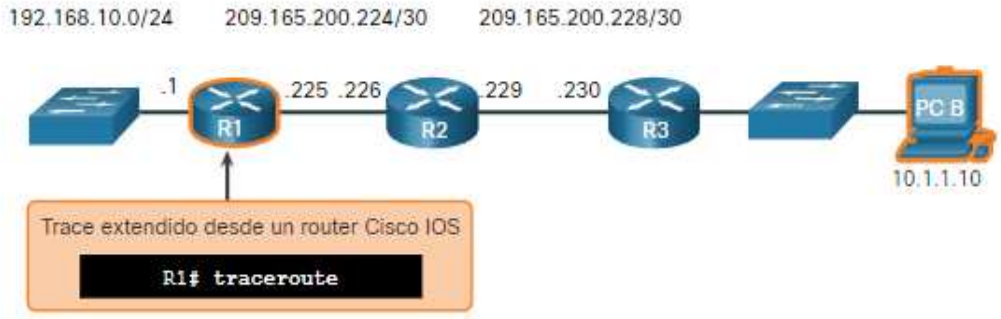
El comando **tracert** de Windows, permite la entrada de varios parámetros a través de opciones en la línea de comando. Sin embargo, no se guía como el comando extendido traceroute de IOS. El siguiente resultado muestra las opciones disponibles para el comando **tracert** de Windows.

```
C:\Users\PC -A> tracert/?
Uso: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [- R] [- srcaddr de S] [- 4] [- 6] target_name
Options:
    -d Do not resolve addresses to hostnames.
    -h maximum_hops Maximum number of hops to search for target.
    -j host-list Loose source route along host-list (IPv4-only).
    -w timeout Wait timeout milliseconds for each reply.
    -R Trace round-trip path (IPv6-only).
    -S srcaddr Source address to use (IPv6-only).
    -4 Force using IPv4.
    -6 Force using IPv6.
C:\Users\PC -A>
```

La opción **traceroute** extendida del IOS de Cisco permite al usuario crear un tipo especial de trace ajustando los parámetros relacionados con la operación del comando. El **traceroute** extendido se ingresa en privileged EXEC mode, escribiendo **traceroute** sin una IP address de destino. IOS lo guiará en las opciones de comando presentando varios indicadores relacionados con la configuración de todos los parámetros diferentes.

Al **Nota**: presiona **Enter** se aceptan los valores predeterminados indicados.

Por ejemplo, suponga que desea probar la conectividad al PC B desde la LAN R1. Esto podría verificarse desde el PC A. Sin embargo, un **traceroute** extedido podría ser configurado en R1 para especificar una dirección de origen diferente.



El diagrama muestra una topología de red con el direccionamiento IP de las interfaces del router y un comando traceroute extendido emitido desde un router Cisco IOS. La topología consiste en los siguientes dispositivos y redes, de izquierda a derecha. Un switch en la red 192.168.10.0/24 está conectado al router R1 en una interfaz con una dirección de .1. R1 está conectado al router R2 por la red 209.165.200.224/30. La interfaz en R1 tiene una dirección de .225 y la interfaz en R2 tiene una dirección de .226. R2 está conectado al router R3 por la red 209.165.200.228/30. La interfaz de R2 tiene una dirección de .229 y la interfaz de R3 tiene una dirección de .230. R3 está conectado a un switch que está conectado al PC host B con la dirección 10.1.1.10. R1 está emitiendo el siguiente comando trace desde la CLI: R1# traceroute.

Como se ilustra en el ejemplo, la dirección IP de origen del comando **traceroute** extendido en R1 podría configurarse para usar la dirección IP de interfaz LAN de R1 (es decir, 192.168.10.1).

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Tiempo de espera en segundos [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 mseg 1 mseg 1 mseg
  2 209.165.200.230 0 mseg 1 mseg 0 mseg
  3 *
    10.1.1.10 2 mseg 2 mseg
R1#
```

17.4.5

Línea base de red

Una de las herramientas más efectivas para controlar y resolver problemas relacionados con el rendimiento de la red es establecer una línea de base de red. La creación de una línea de base efectiva del rendimiento de la red se logra con el tiempo. La medición del rendimiento en distintos momentos y con distintas cargas ayuda a tener una idea más precisa del rendimiento general de la red.

El resultado derivado de los comandos de red aporta datos a la línea de base de red. Un método para iniciar una línea de base es copiar y pegar los resultados de **ping**, **trace**, u otros comandos relevantes en un archivo de texto. Estos archivos de texto pueden tener grabada la fecha y la hora y pueden guardarse en un archivo para su posterior recuperación y comparación.

Entre los elementos que se deben considerar se encuentran los mensajes de error y los tiempos de respuesta de host a host. Si se observa un aumento considerable de los tiempos de respuesta, es posible que exista un problema de latencia que debe considerar.

Por ejemplo, el siguiente **ping** de salida se capturó y pegó en un archivo de texto.

August 19, 2019 at 08:14:43

```
C:\Users\PC -A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC -A>
```

Observe que los tiempos de **ping** ida y vuelta son inferiores a 1 ms.

Un mes después, el ping se repite y captura.

September 19, 2019 at 10:18:21

```
C:\Users\PC -A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=50ms TTL=64
Reply from 10.1.1.10: bytes=32 time=49ms TTL=64
Reply from 10.1.1.10: bytes=32 time=46ms TTL=64
Reply from 10.1.1.10: bytes=32 time=47ms TTL=64
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 50ms, Average = 48ms
C:\Users\PC -A>
```

Observe esta vez que los tiempos de **ping** ida y vuelta son mucho más largos, lo que indica un problema potencial.

Las redes corporativas deben tener líneas de base extensas; más extensas de lo que podemos describir en este curso. Existen herramientas de software a nivel profesional para almacenar y mantener información de línea de base. En este curso, se cubren algunas técnicas básicas y se analiza el propósito de las líneas de base.

Las mejores prácticas de Cisco para los procesos de línea de base se pueden encontrar buscando en Internet "Mejores Prácticas de Proceso Baseline".

17.4.6

Práctica de laboratorio: Prueba de la latencia de red con los comandos ping y traceroute

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Utilizar el comando ping para registrar la latencia de la red
- Parte 2: Utilizar el comando traceroute para registrar la latencia de la red.

Pruebe la latencia de red con Ping y Traceroute

Crear una red pequeña / Comandos de host y de IOS

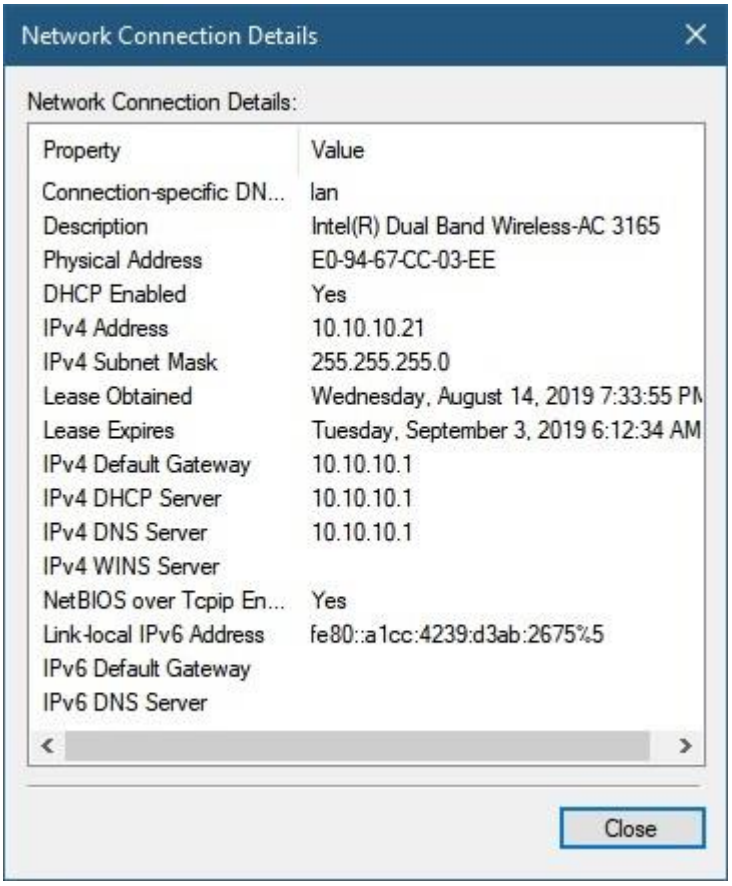
Comandos de host y de IOS

17.5.1

Configuración de IP en un host Windows

Si ha utilizado alguna de las herramientas del tema anterior para verificar la conectividad y ha descubierto que parte de la red no funciona como debería, ahora es el momento de utilizar algunos comandos para solucionar problemas de los dispositivos. Los comandos de host e IOS pueden ayudarle a determinar si el problema está relacionado con el direccionamiento IP de sus dispositivos, que es un problema común de red.

Comprobar el direccionamiento IP en dispositivos host es una práctica común en redes para verificar y solucionar problemas de conectividad extremo a extremo. En Windows 10, puede acceder a los detalles de la dirección IP desde **Network and Sharing Center**, como se muestra en la figura, para ver rápidamente las cuatro configuraciones importantes: dirección, máscara, router y DNS.



Sin embargo, los administradores de red suelen ver la información de direcciones IP en un host de Windows ejecutando el comando **ipconfig** en la línea de comandos de un equipo con Windows, como se muestra en el ejemplo.

```
C:\Users\PC -A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . .: fe80: :a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10 Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Utilice el comando **ipconfig /all** para ver la dirección MAC junto con varios detalles relacionados con la asignación de direcciones de capa 3 del dispositivo, Como se muestra en el ejemplo.

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : PC-A-00H20
   Primary Dns Suffix . . . . . . . : cisco.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cisco.com
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .: fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)  IPv4 Address. . . . . .
. . . . : 192.168.10.10(Preferred) Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   Servidor DHCP . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 IAID . . . . . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   Servidor DNSs . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Si un host está configurado como cliente DHCP, la configuración de la dirección IP se puede renovar utilizando los comandos **ipconfig /release ipconfig /renew** y, como se muestra en el resultado de ejemplo.

```
C:\Users\PC-A> ipconfig /release
(Output omitted)
Adaptador LAN inalámbrico Wi-Fi:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . .: fe80::a4aa:2dd1:ae2d:a75e%16
   Default Gateway . . . . . :
(Output omitted)
C:\Users\PC-A> ipconfig /renew
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . .: fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . : 192.168.1.124
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
(Output omitted)
C:\Users\PC -A>
```

El servicio del cliente DNS en PC con Windows también optimiza el rendimiento de la resolución de nombres DNS al almacenar en la memoria los nombres resueltos previamente. El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows., como se muestra en el ejemplo.

```
C:\Users\PC-A> ipconfig /displaydns
Configuración IP de Windows
(Output omitted)
    netacad.com
    -
    Record Name . . . . .: netacad.com
    Record Type . . . . . : 1
    Time To Live . . . . : 602
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 54.165.95.219
(Output omitted)
```

17.5.2

Configuración de IP en un host Linux

La verificación de la configuración IP usando la GUI en una máquina Linux variará dependiendo de la distribución Linux (distribución) y la interfaz de escritorio. La figura muestra el **Connection Information**, cuadro de diálogo en la distribución Ubuntu que ejecuta el escritorio Gnome.

En la línea de comandos, los administradores de red utilizan el comando **ifconfig** para mostrar el estado de las interfaces activas actualmente y su configuración IP, como se muestra en la salida.

```
[analyst@secOps ~]$ ifconfig
enp0s3 Encap:Ethernet HWADDR 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15 Bcast:10.0.2.255 Máscara: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          Bytes RX: 1855455014 (1,8 GB) bytes TX: 13140139 (13,1 MB)
lo: flags=73 mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10
        loop txqueuelen 1000 (Local Loopback)
        Paquetes RX 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

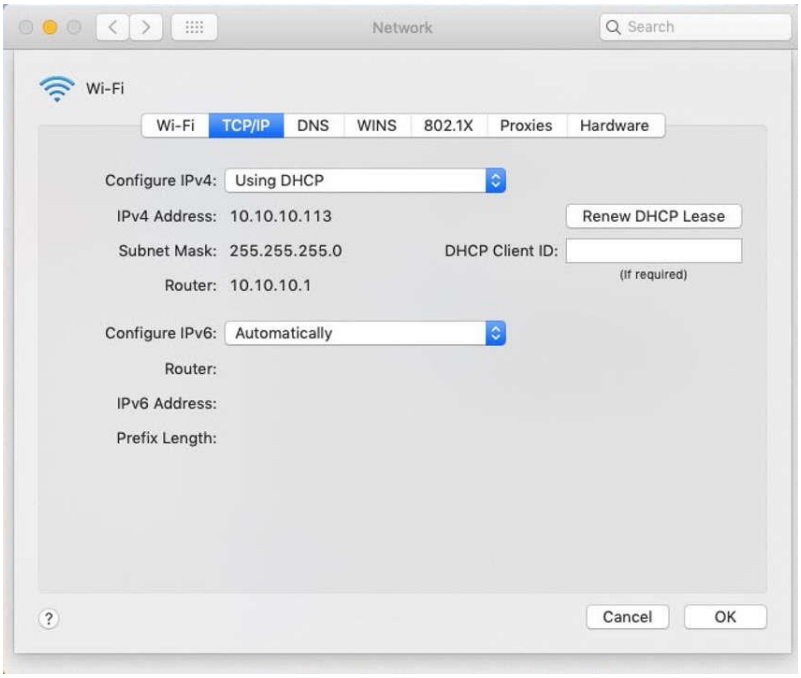
El comando **ip address** se utiliza para mostrar direcciones y sus propiedades. También se puede usar para agregar o eliminar direcciones IP.

Nota: La salida mostrada puede variar dependiendo de la distribución Linux.

17.5.3

Configuración de IP en un host macOS

En la GUI de un host Mac, abra **Network Preferences > Advanced** para obtener la información de direccionamiento IP, como se muestra en la figura.



Sin embargo, el comando **ifconfig** también se puede utilizar para verificar la configuración IP de la interfaz, como se muestra en el ejemplo.

```
MacBook-air: ~ Admin$ ifconfig es0
es0: flags=8863 mtu 1500
        éter c4:b 3:01:a 0:64:98
        inet6 fe80: :c0f:1bf 4:60 b 1:3 adb%es0 prefixlen 64 seguro scopeid 0x5
        inet 10.10.10.113 netmask 0xffffff00 broadcast 10.10.255
        nd6 options=201
        media: autoselect
        status: active
MacBook-Air: ~ Admin$
```

Otros comandos útiles de macOS para verificar la configuración IP del host incluyen **networksetup -listallnetworkservices** y el **networksetup -getinfo <***network service***>**, como se muestra en el siguiente resultado:

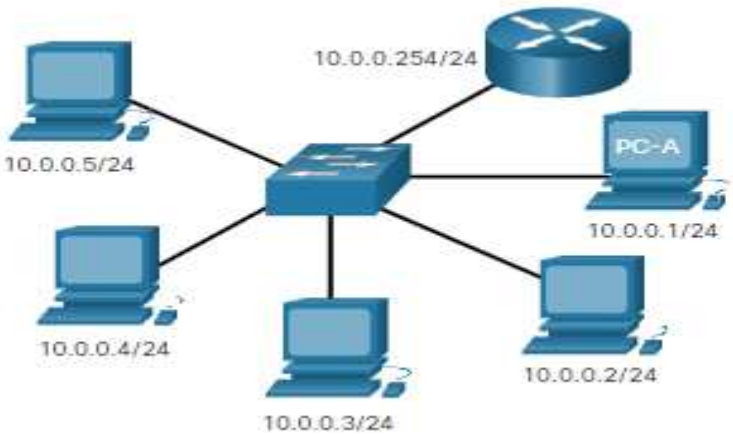
```
MacBook-air: ~ Admin$ networksetup -listallnetworkservices
Un asterisco (*) indica que un servicio de red está deshabilitado.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air: ~ Admin$
MacBook-Air: ~ Admin$ networksetup -getinfo Wi-Fi
Configuración DHCP
Dirección IP: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automático
IPv6 IP address: none
IPv6 Router: none
ID Wi-Fi: c4:b3:01:a0:64:98
MacBook-Air: ~ Admin$
```

17.5.4

El comando arp

El comando **arp,** se ejecuta desde el símbolo del sistema de Windows, Linux o Mac. El comando enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo

Por ejemplo, consulte la topología en la figura



Cinco hosts con direcciones IP 10.0.0.1/24, 10.0.0.0.2/24, 10.0.0.3/24, 10.0.0.4/24 y 10.0.0.5/24 están conectados a un switch conectado a un router con una dirección IP 10.0.0.254/24

Se muestra la salida del comando **arp -a** en el host PC-A de Windows.

```
C:\Users\PC -A> arp -a
Interface: 192.168.93.175 --- 0xc
  Internet Address Physical Address Type
  10.0.0.2 d0-67-e5-b6-56-4b dynamic
  10.0.0.3 78-48-59-e3-b4-01 dynamic
  10.0.0.4 00-21-b6-00-16-97 dynamic
  10.0.0.254 00-15-99-cd-38-d9 dynamic
```

El comando **arp -a** muestra los vínculos entre la dirección IP y la dirección MAC. Observe cómo la dirección IP 10.0.0.5 no está incluida en la lista. Esto se debe a que el caché ARP solo muestra información de dispositivos a los que se ha accedido recientemente.

Para asegurar que la caché ARP esté cargada, haga **ping** a un dispositivo de manera tal que tenga una entrada en la tabla ARP. Por ejemplo, si PC-A hizo ping 10.0.0.5, la memoria caché ARP contendrá una entrada para esa dirección IP.

Se puede borrar la caché mediante el comando **netsh interface ip delete arpcache** en caso de que el administrador de red desee volver a llenarla con información actualizada.

Nota: Es posible que necesite acceso de administrador en el host para poder usar el comando **netsh interface ip delete arpcache**.

17.5.5

Repaso de comandos show comunes

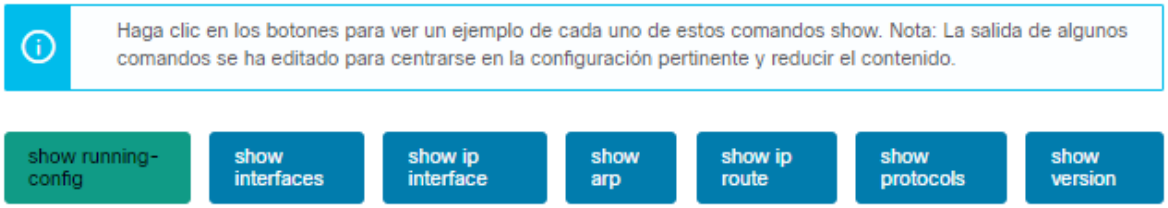
De la misma manera que los comandos y las utilidades se utilizan para verificar la configuración de un host, los comandos se pueden utilizar para verificar las interfaces de los dispositivos intermediarios. Cisco IOS proporciona comandos para verificar el funcionamiento de interfaces de router y switch.

Los comandos **show** de la CLI de Cisco IOS muestran información importante sobre la configuración y el funcionamiento del dispositivo. Los técnicos de red utilizan los comandos **show** con frecuencia para ver los archivos de configuración, revisar el estado de los procesos y las interfaces del dispositivo, y verificar el estado de funcionamiento del dispositivo.

Se puede mostrar el estado de casi todos los procesos o funciones del router mediante un comando **show**.

Los comandos **show** de uso común y cuándo usarlos se enumeran en la tabla:

Command	Useful for ...
show running-config	To verify the current configuration and settings
show interfaces	To verify the interface status and see if there are any error messages
show ip interface	To verify the Layer 3 information of an interface
show arp	To verify the list of known hosts on the local Ethernet LANs
show ip route	To verify the Layer 3 routing information
show protocols	To verify which protocols are operational
show version	To verify the memory, interfaces, and licences of the device



show running-config

Verifica la configuración actual

```
R1# show running-config

(Output omitted)

!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0/0
 description Link to R2
 ip address 209.165.200.225 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 description Link to LAN
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
!
router ospf 10
 network 192.168.10.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.3 area 0
!
banner motd ^C Authorized access only! ^C
!
line con 0
 password 7 14141B180F0B
 login
line vty 0 4
 password 7 00071A150754
 login
 transport input telnet ssh
!
end
R1#
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

```
R1# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Description: Link to R2
  Internet address is 209.165.200.225/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:21, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5127 packets input, 590285 bytes, 0 no buffer
     Received 29 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 5043 multicast, 0 pause input
     1150 packets output, 153999 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up

(Output omitted)
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

show ip interface

Verifica la información de la capa 3 de una interfaz

```
R1# show ip interface
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  Associated unicast routing topologies:
        Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  IPv4 WCCP Redirect outbound is disabled
  IPv4 WCCP Redirect inbound is disabled
  IPv4 WCCP Redirect exclude is disabled
GigabitEthernet0/0/1 is up, line protocol is up

(Output omitted)
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

show arp

Verifica la lista de hosts conocidos en las LAN Ethernet locales

```
R1# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.10.1 - a0e0.af0d.e141 ARPA GigabitEthernet0/0/1
Internet 192.168.10.10 95 c07b.bcc4.a9c0 ARPA GigabitEthernet0/0/1
Internet 209.165.200.225 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0
Internet 209.165.200.226 138 a03d.6fe1.9d90 ARPA GigabitEthernet0/0/0
R1#
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

show ip route

Verifica la informacion de enrutamiento de la Capa 3

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O 10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabiteThernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O 209.165.200.228/30
          [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

show protocols

Verifica qué protocolos están operativos

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
Serial0/1/0 is down, line protocol is down
Serial0/1/1 is down, line protocol is down
GigabitEthernet0 is administratively down, line protocol is down
R1#
```

show running-config | show interfaces | show ip interface | show arp | show ip route | show protocols | show version

show version

Verifica la memoria, las interfaces y las licencias del dispositivo

```
R1# show version
Cisco IOS XE Software, Version 03.16.08.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(3)S8, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 08-Aug-18 10:48 by mcpre

(Output omitted)

ROM: IOS-XE ROMMON
R1 uptime is 2 hours, 25 minutes
Uptime for this control processor is 2 hours, 27 minutes
System returned to ROM by reload
System image file is "bootflash:/isr4300-universalk9.03.16.08.S.155-3.S8-ext.SPA.bin"
Last reload reason: LocalSoft

(Output omitted)

Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
appxk9        appxk9        RightToUse    appxk9
uck9          None          None          None
securityk9    securityk9    Permanent     securityk9
ipbase        ipbasek9      Permanent     ipbasek9
cisco ISR4321/K9 (1RU) processor with 1647778K/6147K bytes of memory.
Processor board ID FLM2044W0LT
2 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
978928K bytes of USB flash at usb0:.
Configuration register is 0x2102
R1#
```

17.5.6

El comando show cdp neighbors

Existen otros comandos IOS que son útiles. Cisco Discovery Protocol (CDP) es un protocolo exclusivo de Cisco que se ejecuta en la capa de enlace de datos. Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco (como routers que admiten distintos protocolos de la capa de red) obtengan información de los demás incluso si no hay conectividad de Capa 3.

Cuando inicia un dispositivo Cisco, CDP se inicia de manera predeterminada. CDP descubre automáticamente los dispositivos Cisco vecinos que ejecutan ese protocolo, independientemente de los protocolos o los conjuntos de aplicaciones de Capa 3 en ejecución. CDP intercambia información del hardware y software del dispositivo con sus vecinos CDP conectados directamente.

CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:

- **Identificadores de dispositivo**:nombre de host configurado de un switch, router u otro dispositivo
- **Lista de direcciones:** hasta una dirección de capa de red para cada protocolo admitido.
- **Identificador de puerto:** el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, FastEthernet 0/0.
- **Lista de capacidades:** por ejemplo, si un dispositivo específico es un switch de capa 2 o un switch de capa 3
- **Plataforma:** plataforma de hardware del dispositivo; por ejemplo, un router Cisco serie 1841.

Consulte la topología y la salida del comando **show cdp neighbor**.

El router R3 está conectado a través de la interfaz G0/0/1 al switch S3 en el puerto F0/5 que está conectado al switch S4.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
S3 Gig 0/0/1 122 S I WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

La salida muestra que la interfaz R3 GigabitEthernet 0/0/1 está conectada a la interfaz FastEthernet 0/5 de S3, que es un switch Cisco Catalyst 2960+. Observe que R3 no ha

recopilado información sobre S4. Esto porque CDP solo puede descubrir dispositivos directamente conectados. S4 no está conectado directamente a R3 y, por lo tanto, no aparece istado.

El comando **show cdp neighbors detail,** revela la dirección IP de un dispositivo vecino, como se muestra en la salida. CDP revelará la dirección IP del vecino, independientemente de que se pueda hacer ping en ese vecino o no. Este comando es muy útil cuando dos routers Cisco no pueden enrutar a través de su enlace de datos compartido. El comando **show cdp neighbors detail,** contribuye a determinar si uno de los vecinos CDP tiene un error de configuración IP.

Pese a que CDP es útil, también puede ser un riesgo de seguridad, ya que puede proporcionar a los atacantes información útil sobre la infraestructura de la red. Por ejemplo, de manera predeterminada muchas versiones de IOS envían anuncios de CDP por todos los puertos habilitados. Sin embargo, las prácticas recomendadas sugieren que CDP debe habilitarse solamente en las interfaces que se conectan a otros dispositivos Cisco de infraestructura. Los anuncios de CDP se deben deshabilitar en los puertos para el usuario.

Debido a que algunas versiones de IOS envían publicaciones CDP de manera predeterminada, es importante que sepa cómo deshabilitar el CDP. Para deshabilitar CDP globalmente, utilice el comando de configuración global **no cdp run**. Para deshabilitar CDP en una interfaz, utilice el comando de interfaz **no cdp enable**.

17.5.7

El comando show ip interface brief

Uno de los comandos más utilizados es el comando **show ip interface brief**. Este comando proporciona un resultado más abreviado que el comando **show ip interface**. Proporciona un resumen de la información clave para todas las interfaces de red de un router.

Por ejemplo, l resultado de **show ip interface brief** muestra todas las interfaces del router, la dirección IP asignada a cada interfaz (si las hubiera) y el estado de funcionamiento de la interfaz.

```
R1# show ip interface brief
¿Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 209.165.200.225 YES manual up up
GigabitEthernet0/0/1 192.168.10.1 YES manual up up
Serial0/1/0 unassigned NO unset down down
Serial0/1/1 unassigned NO unset down down
GigabitEthernet0 unassigned YES unset administratively down down
R1#
```

Verify Switch Interfaces

El comando **show ip interface brief,** también se puede utilizar para verificar el estado de las interfaces del switch, como se muestra en el ejemplo.

```
S1# show ip interface brief
¿Interface IP-Address OK? Method Status Protocol
Vlan1 192.168.254.250 YES manual up up
FastEthernet0/1 unassigned YES unset down down
FastEthernet0/2 unassigned YES unset up up
FastEthernet0/3 unassigned YES unset up up
```

La interfaz VLAN1 recibió la dirección IPv4 192.168.254.250 y está habilitada y en funcionamiento.

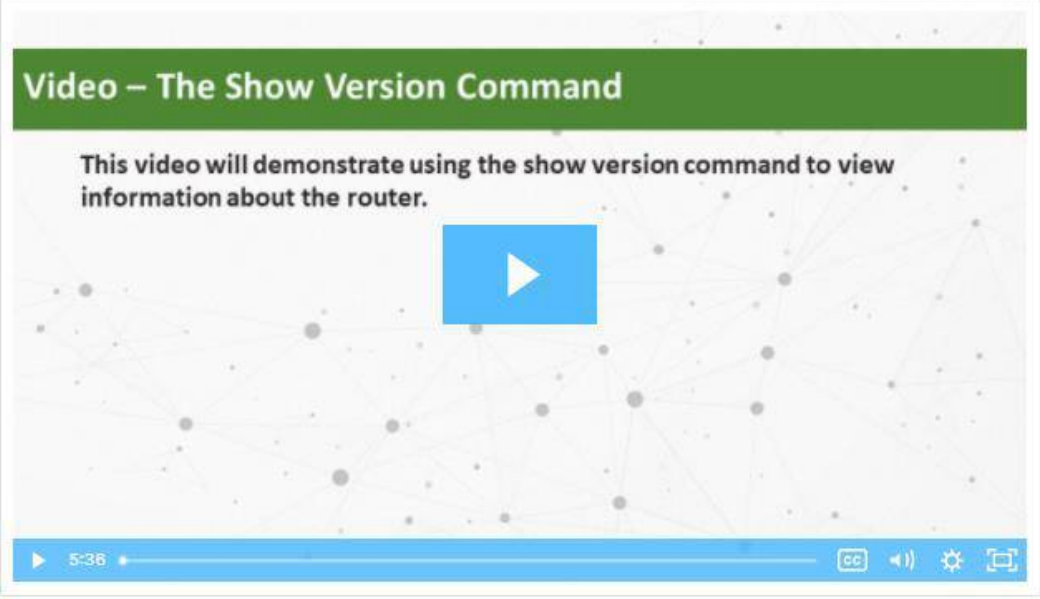
El resultado también muestra que la interfaz FastEthernet0/1 está inactiva. Esto indica que no hay ningún dispositivo conectado a la interfaz o que el dispositivo que está conectado tiene una interfaz de red que no funciona.

Por otro lado, el resultado muestra que las interfaces FastEthernet0/2 y FastEthernet0/3 funcionan. Esto lo indica el valor up en las columnas Status y Protocol.

17.5.8

Video: El comando show version

El comando **show version** se puede utilizar el comando show version para comprobar y solucionar problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque. Haga clic en Reproducir para ver un vídeo anterior del curso y repasar la explicación del comando **show versión**.



17.5.9

Packet Tracer - Interpretar la salida del comando show

Esta actividad está diseñada para reforzar el uso de los comandos **show** del router. No debe realizar configuraciones, sino examinar el resultado de diversos comandos show.

Interpretar la salida del comando show

Interpretar la salida del comando show

Crear una red pequeña / Metodologías para la solución de problemas

Metodologías para la solución de problemas

17.6.1

Enfoques básicos para la solución de problemas

En los dos temas anteriores, ha aprendido acerca de algunas utilidades y comandos que puede utilizar para ayudar a identificar las áreas problemáticas de la red. Esta es una parte importante de la solución de problemas. Hay muchas maneras de solucionar un problema de red. En este tema se detalla un proceso estructurado de solución de problemas que puede ayudarle a convertirse en un mejor administrador de red. También proporciona algunos comandos más para ayudarle a resolver problemas. Los problemas de red pueden ser simples o complejos, y pueden ser el resultado de una combinación de problemas de hardware, software y conectividad. Los técnicos informáticos deben ser capaces de analizar el problema y determinar la causa del error para poder reparar el problema de red. Este proceso se denomina “solución de problemas”.

Una metodología de resolución de problemas común y eficiente se basa en el método científico.

La tabla muestra los seis pasos principales del proceso de resolución de problemas.

Paso	Descripción
Paso 1. Identificar del problema	Este es el primer paso en el proceso de solución de problemas. Aunque se pueden usar herramientas en este paso, una conversación con el usuario suele ser muy útil.
Paso 2. Establecer una teoría de causas probables	Después de identificar el problema, intente establecer una teoría de causas probables. Este paso generalmente permite ver más causas probables del problema.
Paso 3. Poner a prueba la teoría para determinar la causa	Según las causas probables, pruebe sus teorías para determinar cuál es la causa del problema. El técnico aplica a menudo un procedimiento rápido para probar y ver si resuelve el problema.. Si un procedimiento rápido no corrige el problema, es posible que tenga que investigar el problema mas a fondo, para establece la causa.
Paso 4. Establecer un plan de acción e implementar la solución	Una vez que haya determinado la causa raíz del problema, establezca un plan de acción para solucionar el problema e implementar la solución.
Paso 5. Verificar la solución e implementar medidas preventivas.	Una vez que haya corregido el problema, verifique la funcionalidad total. Si es necesario, implemente medidas preventivas.
Paso 6. Registrar hallazgos, acciones y resultados	El último paso del proceso de solución de problemas consiste en registrar los hallazgos, acciones y resultados. Esto es muy importante para referencia futura.

Para evaluar el problema, determine cuántos dispositivos de la red lo tienen. Si existe un problema con un dispositivo de la red, inicie el proceso de solución de problemas en ese dispositivo. Si existe un problema con todos los dispositivos de la red, inicie el proceso de solución de problemas en el dispositivo donde se conectan todos los otros dispositivos. Debe desarrollar un método lógico y coherente para diagnosticar problemas de red mediante la eliminación de un problema a la vez.

17.6.2

¿Solucionar o escalar?

En algunas situaciones, quizás no sea posible solucionar el problema de inmediato. Un problema debería escalarse cuando requiere la decisión del gerente, cierta experiencia específica, o el nivel de acceso a la red no está disponible para el técnico que debe solucionar el problema.

Por ejemplo, después de diagnosticar el problema, el técnico decide que un módulo de router debe reemplazarse. Este problema se debe escalar para obtener la aprobación del gerente. Es probable que el gerente tenga que escalar el problema nuevamente, ya que podría necesitar la aprobación del departamento de finanzas antes de comprar un nuevo módulo.

La política de la empresa debe indicar claramente cuándo y cómo un técnico debe escalar un problema.

17.6.3

Comando debug

Los procesos, protocolos, mecanismos y eventos del sistema operativo generan mensajes para comunicar su estado. Estos mensajes pueden proporcionar información valiosa cuando hay que solucionar problemas o verificar las operaciones del sistema. El comando **debug** de IOS, permite que el administrador muestre estos mensajes en tiempo real para su análisis. Es una herramienta muy importante para supervisar eventos en un dispositivo Cisco IOS.

Todos los comandos **debug** se introducen en el modo EXEC privilegiado. Cisco IOS permite limitar el resultado de **debug** para incluir solo la característica o la subcaracterística relevante. Esto es importante porque se le asigna alta prioridad al resultado de depuración en el proceso de CPU y puede hacer que el sistema no se pueda utilizar. Por este motivo, use los comandos **debug** sólo para trabajar en problemas específicos.

Para supervisar el estado de mensajes de ICMP en un router Cisco, utilice **debug ip icmp**, como se muestra en el ejemplo.

```
R1# debug ip icmp
ICMP packet debugging is on
R1#
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1#
```

Para acceder a una breve descripción de todas las opciones del comando debug, utilice el comando **debug ?** en modo EXEC con privilegios, en la línea de comandos.

Para desactivar una característica de depuración específica, agregue la palabra clave **no** delante del comando **debug**:

```
Router# no debug ip icmp
```

Alternativamente, puede ingresar la forma **undebug** del comando en modo EXEC privilegiado:

```
Router# undebug ip icmp
```

Para desactivar todos los comandos debug activos de inmediato, utilice el comando **undebug all**:

```
Router# undebug all
```

Tenga cuidado usando algún comando **debug**. Algunos comandos debug, como **debug all** y **debug ip packet**, generan una importante cantidad de resultados y usan una gran porción de recursos del sistema. El router podría estar tan ocupado mostrando mensajes de **debug** que no tendría suficiente potencia de procesamiento para realizar sus funciones de red, o incluso escuchar comandos para desactivar la depuración. Por este motivo, no se recomienda y se debe evitar utilizar estas opciones de comando.

17.6.4

El monitor terminal de comandos

Las conexiones para otorgar acceso a la interfaz de línea de comandos de IOS se pueden de las 2 maneras siguientes:

- **Localmente** - Las conexiones locales requieren acceso físico al router o switch a través de un cable.
- **Remotamente** -- Las conexiones remotas requieren el uso de Telnet o SSH para establecer una conexión a un dispositivo configurado por IP.

Algunos mensajes IOS se muestran automáticamente en una conexión de consola, pero no en una conexión remota. Por ejemplo, el **debug** resultado se muestra de forma predeterminada en las conexiones de la consola. Sin embargo, el resultado **debug** no se muestra automáticamente en las conexiones remotas. Esto se debe, a que **debug** los mensajes son mensajes de registro, que se muestran en líneas vty.

En el siguiente resultado, por ejemplo, el usuario estableció una conexión remota usando Telnet desde R2 a R1. A continuación, el usuario emitió el comando **debug ip icmp**. Sin embargo, el comando no pudo mostrar el resultado de **debug**.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

Para mostrar mensajes de registro en un terminal (virtual console), use el comando EXEC privilegiado **terminal monitor**. Para detener el registro de mensajes en un terminal, use el comando EXEC privilegiado **terminal no monitor**.

Por ejemplo, observe cómo se ha introducido el comando **terminal monitor** y el comando **ping** muestra el resultado de **debug**.

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0 **Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE,
dscp 0 topoid 0 **Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0 **Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst
209.165.200.225,topology BASE, dscp 0 topoid 0 **Aug 20 16:03:49.741: ICMP: echo reply rcvd, src
10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

Nota: La intención del comando **debug** es capturar la salida en directo durante un corto período de tiempo (es decir, unos pocos segundos a un minuto más o menos). Siempre desactive **debug** cuando no sea necesario.

17.6.5

Verifique su comprensión: Metodologías de solución de problemas

Verifique su entendimiento acerca de las metodologías de resolución de problemas, seleccionando la mejor respuesta para las siguientes preguntas.

Correcto

Identificó bien las respuestas correctas.

1. El siguiente paso después de «Establecer una teoría de causas probables» es «probar la teoría para determinar la causa».
2. El técnico debe remitir el problema a su gerente.
3. Para deshabilitar el comando **debug ip icmp** puede usar **no debug ip icmp**, **undebug ip icmp**, o **undebug all**.
4. El comando **terminal monitor** muestra mensajes de registro en una conexión remota.

Has tenido 4 respuestas correctas de 4.

1. Un técnico está solucionando un problema de red y acaba de establecer una teoría de causas probables. ¿Cuál es el siguiente paso en el proceso de solución de problemas?

¡Lo tienes!

- ○ Registrar hallazgos, acciones y resultados
- ○ Establecer un plan de acción e implementar la solución
- ○ Identificar el problema.
- ◉ Poner a prueba la teoría para determinar la causa.
- ○ Verificar la solución e implementar medidas preventivas.

2. Un técnico está solucionando un problema de red. después de diagnosticar el problema, el técnico decide que un switch debe reemplazarse. ¿Qué debe hacer el técnico a continuación?

¡Lo tienes!

- ○ Envía un correo electrónico a todos los usuarios para que sepan que están reemplazando un switch.
- ◉ Escala el ticket de problemas al administrador para aprobar el cambio.
- ○ Compra un switch nuevo y reemplaza el defectuoso.
- ○ Resuelve el problema.

3. Un técnico está utilizando el comando EXEC privilegiado **debug ip icmp** para capturar la salida del router en vivo. ¿Qué comandos detendrían este **debug** comando en un router Cisco? (Escoja dos opciones).

¡Lo tienes!

- ☐ **debug ip icmp off**
- ☐ **no debug debug ip icmp**
- ☑ **no debug ip icmp**
- ☑ **undebug all**
- ☐ **undebug debug ip icmp**

4. Un técnico ha establecido una conexión remota al router R1 para observar la **debug** salida. El técnico ingresa el **debug ip icmp** comando y luego hace ping a un destino remoto. Sin embargo, no se muestra ninguna salida. ¿Qué comando tendría que introducir el técnico para mostrar los mensajes de registro en una conexión remota?

¡Lo tienes!

- ○ **salidade depuración del monitor**
- ○ **terminalde monitor**
- ◉ **terminal monitor**
- ○ **depuracióndel monitor de terminal**

Correct

You have successfully identified the correct answers.

1. The next step after "Establish a Theory of Probable Causes" is to "Test the Theory to Determine Cause".
2. The technician should escalate the problem to their manager.
3. To disable the **debug ip icmp** command you can use **no debug ip icmp, undebug ip icmp,** or **undebug all**.
4. The **terminal monitor** command displays log messages on a remote connection.

You got 4 out of 4 questions correct.

1. A technician is troubleshooting a network problem and has just established a theory of probable causes. What would be the next step in the troubleshooting process?

You got it!

- ○ Document findings, actions, and outcomes.
- ○ Establish a plan of action and implement the solution.
- ○ Identify the problem.
- ◉ Test the theory to determine cause.
- ○ Verify solution and implement preventive measures.

2. A technician is troubleshooting a network problem. After troubleshooting, the technician concludes that a switch should be replaced. What should the technician do next?

You got it!

- ○ Email all users to let them know they are replacing a switch.
- ◉ Escalate the trouble ticket to the manager to approve the change.
- ○ Purchase a new switch and replace the defective one.
- ○ Resolve the problem.

3. A technician is using the **debug ip icmp** privileged EXEC command to capture live router output. Which commands would stop this **debug** command on a Cisco router? (Choose two.)

You got it!

- ☐ **debug ip icmp off**
- ☐ **no debug debug ip icmp**
- ☑ **no debug ip icmp**
- ☑ **undebug all**
- ☐ **undebug debug ip icmp**

4. A technician has established a remote connection to router R1 to observe **debug** output. The technician enters the **debug ip icmp** command then pings a remote destination. However, no output is displayed. Which command would the technician have to enter to display log messages on a remote connection?

You got it!

- monitor debug output
- monitor terminal
- terminal monitor
- terminal monitor debug

Crear una red pequeña / Escenarios de resolución de problemas

Escenarios de resolución de problemas

17.7.1

Problemas de funcionamiento dúplex y discordancia

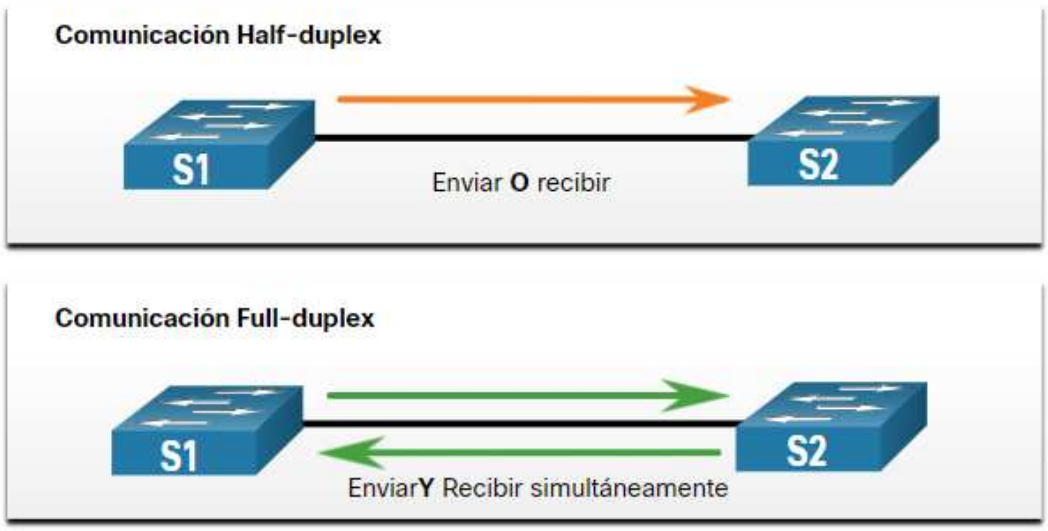
Muchos problemas comunes de red se pueden identificar y resolver con poco esfuerzo. Ahora que dispone de las herramientas y el proceso para solucionar problemas de una red, este tema revisa algunos problemas comunes de red que es probable que encuentre como administrador de red.

Cuando se trata de comunicación de datos, *duplex* se refiere a la dirección de la transmisión de datos entre dos dispositivos.

Hay dos modos de comunicación dúplex:

- **Half-duplex** - Se restringen el intercambio de datos a una dirección a la vez.
- **Full-duplex** - Se permite enviar y recibir simultáneamente.

La figura ilustra cómo funciona cada método dúplex.



La imagen es una comparación de las comunicaciones Half-duplex frente a Full-duplex. El diagrama de arriba muestra la comunicación Half-duplex. El switch S1 está conectado al switch S2 con una flecha que fluye de S1 a S2 indicando que un dispositivo puede enviar o recibir. El diagrama inferior muestra la comunicación Full-duplex. El switch S1 está conectado al switch S2 con flechas apuntando en ambas direcciones indicando que un dispositivo puede enviar Y recibir simultáneamente.

Las interfaces de interconexión de Ethernet deben funcionar en el mismo modo dúplex para un mejor rendimiento de comunicación y para evitar la ineficiencia y la latencia en el enlace.

La función de negociación automática Ethernet facilita la configuración, minimiza los problemas y maximiza el rendimiento de los enlaces Ethernet. Los dispositivos conectados primero anuncian sus capacidades utilizadas y luego eligen el modo de mayor rendimiento soportado por ambos extremos. Por ejemplo, el switch y el router en la ilustración negociaron de manera automática y correcta el modo full-duplex.

Surge una incongruencia si uno de los dos dispositivos conectados funciona en modo Full-Duplex y el otro funciona en modo Half-Duplex. Si bien la comunicación de datos se realizará a través de un enlace con una incongruencia de dúplex, el rendimiento del enlace será muy deficiente.

La incongruencia de dúplex suele deberse a una interfaz mal configurada o, en raras ocasiones, a una negociación automática fallida. Las incongruencias de dúplex pueden ser difíciles de resolver mientras los dispositivos se comunican entre sí.

17.7.2

Problemas de asignación de direcciones IP en dispositivos IOS

Los problemas relacionados con la dirección IP probablemente no permitirán la comunicación de los dispositivos de redes remotas. Debido a que las direcciones IP son jerárquicas, cualquier dirección IP asignada a un dispositivo de red debe adaptarse al rango de direcciones de esa red. Las direcciones IP asignadas incorrectamente crean una variedad de problemas, incluso conflictos de direcciones IP y problemas de enrutamiento.

Dos causas comunes de asignación incorrecta de IPv4 son los errores de asignación manuales o los problemas relacionados con DHCP.

Los administradores de redes tienen que asignar a menudo las direcciones IP manualmente a los dispositivos como servidores y routers. Si se genera un error durante la asignación, es muy probable que ocurran problemas de comunicación con el dispositivo.

En un dispositivo IOS, utilice los comandos **show ip interface** o **show ip interface brief** para comprobar qué direcciones IPv4 se asignan a las interfaces de red. Por ejemplo, emitir el comando **show ip interface brief** como se muestra validaría el estado de la interfaz en R1.

```
R1# show ip interface brief
¿Interface IP-Address OK? Method Status Protocol
GigabiteThernet0/0/0 209.165.200.225 SÍ manual arriba
GigabitEthernet0/0/1 192.168.10.1 YES manual up up
Serial0/1/0 unassigned NO unset down down
Serial0/1/1 unassigned NO unset down down
GigabitEthernet0 unassigned YES unset administratively down down
R1#
```

17.7.3

Problemas de asignación de direcciones IP en terminales

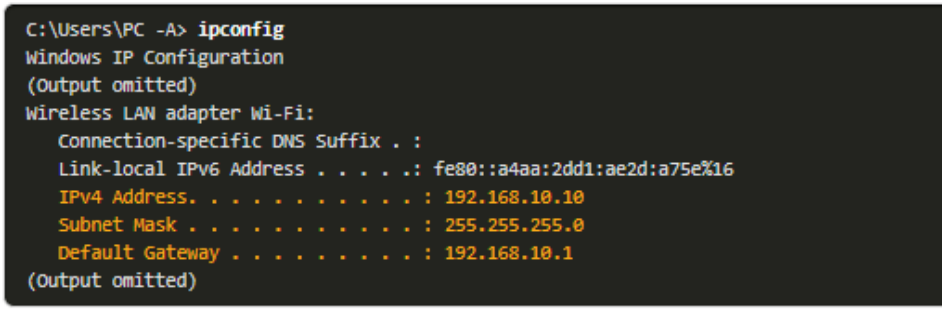
En las máquinas con Windows, cuando el dispositivo no puede comunicarse con un servidor DHCP, Windows asigna automáticamente una dirección que pertenezca al rango 169.254.0.0/16. Esta función se denomina Dirección IP Privada Automática (APIPA) y está diseñada para facilitar la comunicación dentro de la red local. Piense que Windows dice: “Utilizaré esta dirección del rango 169.254.0.0/16 porque no pude obtener ninguna otra dirección”.

Una computadora con una dirección APIPA no podrá comunicarse con otros dispositivos en la red porque esos dispositivos probablemente no pertenecerán a la red 169.254.0.0/16. Esta situación indica un problema de asignación automática de direcciones IPv4 que debe solucionarse.

Nota: Otros sistemas operativos, como Linux y OS X, no asignarán una dirección IPv4 a la interfaz de red si falla la comunicación con un servidor DHCP.

La mayoría de los terminales se configuran para confiar en un servidor DHCP para la asignación automática de direcciones IPv4. Si el dispositivo no puede comunicarse con el servidor DHCP, el servidor no puede asignar una dirección IPv4 para la red específica y el dispositivo no podrá comunicarse.

Para comprobar las direcciones IP asignadas a una computadora con Windows, utilice el comando **ipconfig** , como se muestra en la ilustración.



17.7.4

Problemas con la puerta de enlace predeterminada

La puerta de enlace predeterminada para un terminal es el dispositivo de red más cercano que puede reenviar tráfico a otras redes. Si un dispositivo tiene una dirección de puerta de enlace predeterminada incorrecta o inexistente, no podrá comunicarse con los dispositivos de las redes remotas. Dado que la puerta de enlace predeterminada es la ruta a las redes remotas, su dirección debe pertenecer a la misma red que el terminal.

La dirección de la puerta de enlace predeterminada se puede configurar u obtener manualmente de un servidor DHCP. Como sucede con los problemas de asignación de direcciones IPv4, los problemas de la puerta de enlace predeterminada pueden estar relacionados con la

configuración incorrecta (en el caso de la asignación manual) o problemas de DHCP (si está en uso la asignación automática).

Para resolver los problemas de una puerta de enlace predeterminada mal configurada, asegúrese de que el dispositivo tenga configurado la puerta de enlace predeterminada correcta. Si la dirección predeterminada fue configurada manualmente, pero es incorrecta, simplemente reemplácela por la dirección apropiada. Si la dirección de la puerta de enlace predeterminada fue configurada automáticamente, asegúrese de que el dispositivo pueda comunicarse correctamente con el servidor DHCP. También es importante verificar que se configuraron la dirección IPv4 y la máscara de subred correspondientes en la interfaz del router y que la interfaz esté activa.

Para verificar el gateway predeterminado en las computadoras con Windows, utilice el comando **ipconfig**, como se muestra.

```
C:\Users\PC -A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . .: fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Gateway predeterminado. . . . . . . . . : 192.168.10.1
(Output omitted)
```

En un router, utilice el comando **show ip route** para mostrar la tabla de enrutamiento y verificar que se ha establecido el gateway predeterminado, conocido como ruta predeterminada. Se usa esta ruta cuando la dirección de destino del paquete no coincide con ninguna otra ruta en la tabla de routing.

Por ejemplo, la salida verifica que R1 tenga una puerta de enlace predeterminada (es decir, Puerta de enlace de último recurso) configurada apuntando a la dirección IP 209.168.200.226.

```
R1# show ip route | begin Gateway Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O 10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O 209.165.200.228/30
          [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

La primera línea resaltada básicamente establece que la puerta de enlace a cualquiera (es decir, 0.0.0.0) debe enviarse a la dirección IP 209.165.200.226. El segundo resaltado muestra cómo

R1 aprendió acerca de la puerta de enlace predeterminada. En este caso, R1 recibió la información de otro router habilitado para OSPF.

17.7.5

Solución de problemas de DNS

El Servicio de Nombres de Dominio (DNS) es un servicio automatizado que hace coincidir los nombres, como www.cisco.com, con la dirección IP. Aunque la resolución de DNS no es fundamental para la comunicación del dispositivo, es muy importante para el usuario final.

Es común que los usuarios relacionen erróneamente el funcionamiento de un enlace de Internet con la disponibilidad del servicio DNS. Las quejas de los usuarios como “la red está inactiva” o “Internet está inactiva” se deben a menudo a un servidor DNS al que no se puede acceder. Aunque los servicios de routing de paquetes y cualquier otro tipo de servicios de red estén todavía operativos, los errores de DNS generalmente llevan al usuario a la conclusión incorrecta. Si un usuario escribe un nombre de dominio como www.cisco.com en un navegador web y no se puede acceder al servidor DNS, el nombre no será traducido a una dirección IP y la página web no se mostrará.

Las direcciones del servidor DNS pueden asignarse de manera manual o automática. Los administradores de redes a menudo son responsables de asignar manualmente las direcciones del servidor DNS en servidores y otros dispositivos, mientras que el DHCP se usa para asignar automáticamente las direcciones del servidor DNS a los clientes.

Si bien es común que las empresas y las organizaciones administren sus propios servidores DNS, cualquier servidor DNS accesible puede utilizarse para resolver nombres. Los usuarios de oficinas pequeñas y oficinas en el hogar con frecuencia dependen del servidor DNS que mantiene su ISP para la resolución de nombres. Los servidores DNS mantenidos por un ISP son asignados a los clientes de SOHO mediante DHCP. Adicionalmente, Google mantiene un servidor DNS público que puede ser utilizado por cualquier persona y es muy útil para realizar pruebas. La dirección IPv4 del servidor DNS público de Google es 8.8.8.8 y 2001:4860:4860::8888 para su dirección IPv6 DNS.

Cisco ofrece OpenDNS que proporciona un servicio DNS seguro mediante el filtrado de phishing y algunos sitios de malware. Puede cambiar la dirección DNS a 208.67.222.222 y 208.67.220.220 en los campos Servidor DNS preferido y Servidor DNS alternativo. Las funciones avanzadas, como el filtrado y la seguridad de contenido web, están disponibles para familias y empresas.

Use **ipconfig /all** como se muestra para verificar qué servidor DNS está usando la computadora con Windows.

```
C:\Users\PC-A> ipconfig /all
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   Servidor DHCP . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 IAID . . . . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   Servidor DNSs . . . . . . . . . . . : 208.67.222.222
   NetBIOS over Tcpip. . . . . . . . : Enabled
(Output omitted)
```

El comando **nslookup** es otra herramienta útil para la solución de problemas de DNS para PC. Con **nslookup** un usuario puede configurar manualmente las consultas de DNS y analizar la respuesta de DNS. El comando **nslookup** muestra el resultado de una consulta para www.cisco.com. Tenga en cuenta que también puede simplemente introducir una dirección IP y **nslookup** resolverá el nombre.

```
C:\Users\bvachon > nslookup
Default Server: Home-Net
Address: 192.168.1.1
> cisco.com
Servidor: Home-Net
Address: 192.168.1.1
Non-authoritative answer:
Name: cisco.com
Direcciones: 2001:420:1101:1::185
          72.163.4.185
> 8.8.8.8
Server: Home-Net
Address: 192.168.1.1
Nombre: dns.google
Dirección: 8.8.8.8
>
> 208.67.222.222
Server: Home-Net
Address: 192.168.1.1
Nombre: resolver1.opendns.com
Dirección: 208.67.222.222
>
```

17.7.6

Lab - Solucione problemas de conectividad

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Identificar del problema
- Implementar de cambios de la red
- Verificar de la funcionalidad total.
- Documentar hallazgos y cambios de configuración

Solucione problemas de conectividad

17.7.7

Packet Tracer - Solucionar problemas de conectividad

El objetivo de esta actividad de Packet Tracer es solucionar problemas de conectividad, si es posible. De lo contrario, los problemas se deben documentar claramente para que puedan escalarse.

Solucione problemas de conectividad

Solucione problemas de conectividad

Crear una red pequeña / Práctica del Módulo y Cuestionario

Práctica del Módulo y Cuestionario

17.8.1

Lab – Diseñar y construir una red de empresa pequeña

En este laboratorio, diseñará y construirá una red.

Diseñe y construya una red pequeña

17.8.2

Packet Tracer: Desafío de integración de habilidades

En esta actividad Packet Tracer, usarás todas las habilidades que hayas adquirido a lo largo de este curso.

Desafío de integración de habilidades

Desafío de integración de habilidades

17.8.3

Packet Tracer: Desafío de resolución de problemas

En esta actividad Packet Tracer, solucionará y resolverá una serie de problemas en una red existente.

Troubleshooting Challenge

Troubleshooting Challenge

17.8.4

¿Qué aprendí en este módulo?

Dispositivos en una Red Pequeña

En cuanto a la conexión a Internet, las redes pequeñas normalmente tienen una única conexión WAN proporcionada por una conexión DSL, por cable o Ethernet. Las redes pequeñas son administradas por un técnico local de TI o por un profesional contratado. Los factores que se deben tener en cuenta al seleccionar dispositivos de red para una red pequeña son el costo, la velocidad y los tipos de puertos/interfaces, la capacidad de ampliación y las características y servicios del sistema operativo. Al implementar una red, cree un esquema

de direccionamiento IP y úselo en dispositivos finales, servidores y periféricos, y dispositivos intermediarios. La redundancia se puede lograr mediante la instalación de equipos duplicados, pero también se puede lograr mediante el suministro de enlaces de red duplicados para áreas críticas. Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, como voz y vídeo, de forma independiente del tráfico de otros datos. De hecho, un buen diseño de red clasifica el tráfico cuidadosamente según la prioridad.

Small Aplicaciones de Red and Protocols

Hay dos tipos de programas o procesos que proporcionan acceso a la red: las aplicaciones de red y los servicios de la capa de aplicación. Some end-user applications implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack. Los clientes de correo electrónico y los navegadores web son ejemplos de este tipo de aplicaciones. Otros programas pueden necesitar la asistencia de los servicios de la capa de aplicación para utilizar recursos de red, como la transferencia de archivos o la administración de las colas de impresión en la red. Estos servicios son los programas que interactúan con la red y preparan los datos para la transferencia. Las dos soluciones de acceso remoto más comunes son Telnet y Secure Shell (SSH). El servicio SSH es una alternativa segura a Telnet. Los administradores de red también deben admitir servidores de red comunes y sus protocolos de red relacionados, como el servidor web, el servidor de correo electrónico, el servidor FTP, el servidor DHCP y el servidor DNS. En la actualidad, las empresas utilizan cada vez más la telefonía IP y la transmisión de medios para comunicarse con sus clientes y partners comerciales. Estas son aplicaciones en tiempo real La infraestructura de red debe admitir VoIP, telefonía IP y otras aplicaciones en tiempo real.

Escalar a una Red Grande

Para escalar una red, se requieren varios elementos: documentación de red, inventario de dispositivos, presupuesto y análisis de tráfico. Conocer el tipo de tráfico que atraviesa la red, así como el flujo de tráfico actual. Capture tráfico durante los tiempos de uso máximo para obtener una buena representación de los diferentes tipos de tráfico y realice la captura en diferentes segmentos de red y dispositivos, ya que parte del tráfico será local para un segmento determinado. Los administradores de red deben saber cómo está cambiando el uso de la red. Los detalles de uso de los equipos empleados se pueden capturar en una 'instantánea' con herramientas como el Administrador de tareas de Windows, el Visor de eventos y el Uso de datos.

Verificar Conectividad

El comando **ping** es la forma más eficaz de probar rápidamente la conectividad de Capa 3 entre una dirección IP de origen y destino. El comando también muestra varias estadísticas acerca del tiempo de ida y vuelta. El IOS de Cisco ofrece un modo «extendido» del comando ping que permite al usuario crear tipos especiales de pings ajustando parámetros relacionados con la operación del comando. El ping extendido se ingresa en modo EXEC privilegiado escribiendo ping sin una dirección IP de destino. Traceroute puede ayudar a localizar áreas

con problemas de la Capa 3 en una red. Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red. Se utiliza para identificar el punto a lo largo de la ruta donde se puede encontrar el problema. En Windows, el comando es **tracert**. En Cisco IOS el comando es **traceroute**. También hay un comando**traceroute** extendido. Permite al administrador ajustar los parámetros relacionados con la operación del comando. El resultado derivado de los comandos network aporta datos a la línea de base de red. Un método para iniciar una línea de base es copiar y pegar en un archivo de texto los resultados de los comandos ping, trace u otros comandos relevantes. Estos archivos de texto se pueden marcar con la fecha y guardarse en un archivo para su posterior recuperación y comparación.

Comandos de Host y de IOS

Los administradores de red ven la información de direcciones IP (dirección, máscara, router y DNS) en un host de Windows ejecutando el comando**ipconfig** . Otros comandos necesarios son **ipconfig /all**, **ipconfig /release**, **ipconfig /renew**, e **ipconfig /displaydns**. La verificación de la configuración IP mediante el uso de la GUI en una máquina Linux variará dependiendo de la distribución Linux (distribución) y de la interfaz de escritorio. Los comandos necesarios son **ifconfig**, y **ip address**. En la GUI de un host Mac, abra Preferencias de red > Avanzadas para obtener la información de direcciones IP. Otros comandos de direccionamiento IP para Mac son **ifconfig**, **networksetup -listallnetworkservices** y **networksetup -getinfo** <*network service*\ >. El comando**arp** se ejecuta desde el símbolo del sistema de Windows, Linux o Mac. El comando enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo El comando**arp -a** muestra los vínculos entre la dirección IP y la dirección MAC. **show** Comandos comunes son **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, y **show version**. El comando **show cdp neighbor** proporciona la siguiente información sobre cada dispositivo vecino CDP: identificadores, lista de direcciones, identificador de puerto, lista de capacidades y plataforma. El comando **show cdp neighbors detail** contribuye a determinar si uno de los vecinos CDP tiene un error de configuración IP. El resultado del comando **show ip interface brief** muestra todas las interfaces del router, la dirección IP asignada a cada interfaz (si las hubiera) y el estado de funcionamiento de la interfaz.

Metodologías de Resolución de Problemas

Paso 1. Identificar el problema

Paso 2. Establecer una teoría de causas probables.

Paso 3. Poner a prueba la teoría para determinar la causa

Paso 4. Establecer un plan de acción e implementar la solución

Paso 5. Verificar la solución e implementar medidas preventivas.

Paso 6. Registrar hallazgos, acciones y resultados

Un problema debería escalarse cuando requiere la decisión del gerente, cierta experiencia específica, o el nivel de acceso a la red no está disponible para el técnico que debe solucionar el problema. Los procesos, protocolos, mecanismos y eventos del sistema operativo generan mensajes para comunicar su estado. El comando **debug** de IOS permite que el administrador muestre estos mensajes en tiempo real para su análisis. Para mostrar los mensajes de registro en una terminal (consola virtual), utilice el comando modo EXEC privilegiado **terminal monitor** .

Troubleshooting Scenarios

Hay dos modos de comunicación dúplex: Half-duplex y Full-duplex. Surge una discordancia si uno de los dos dispositivos conectados funciona en modo dúplex completo y el otro funciona en modo semidúplex. Si bien la comunicación de datos se realizará a través de un enlace con una discordancia de dúplex, el rendimiento del enlace será muy deficiente.

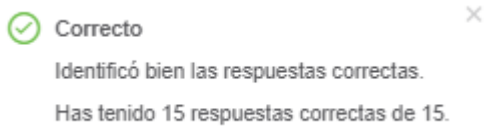
Las direcciones IP asignadas incorrectamente crean una variedad de problemas, incluso conflictos de direcciones IP y problemas de routing. Dos causas comunes de asignación incorrecta de IPv4 son los errores manuales de asignación o los problemas relacionados con DHCP. La mayoría de los terminales se configuran para confiar en un servidor DHCP para la asignación automática de direcciones IPv4. Si el dispositivo no puede comunicarse con el servidor DHCP, el servidor no puede asignar una dirección IPv4 para la red específica y el dispositivo no podrá comunicarse.

El gateway predeterminado para un terminal es el dispositivo de red más cercano que puede reenviar tráfico a otras redes. Si un dispositivo tiene una dirección de gateway predeterminado incorrecta o inexistente, no podrá comunicarse con los dispositivos de las redes remotas. Dado que el gateway predeterminado es la ruta a las redes remotas, su dirección debe pertenecer a la misma red que el terminal.

Las fallas de DNS a menudo llevan al usuario a concluir que la red está desconectada. Si un usuario escribe un nombre de dominio como www.cisco.com en un navegador web y no se puede acceder al servidor DNS, el nombre no será traducido a una dirección IP y la página web no se mostrará.

17.8.5

Módulo Quiz — Construir una red pequeña



1. ¿Qué consideración de diseño de red sería más importante para una gran empresa que para una pequeña empresa?

Tema 17.1.0 - Las pequeñas empresas hoy en día necesitan acceso a Internet y utilizan un router de Internet para atender esta necesidad. Se requiere un switch para conectar los dos dispositivos host y cualquier teléfono IP o dispositivo de red, como una impresora o un escáner. El switch puede estar integrado en el router. Se necesita un firewall para proteger los activos informáticos empresariales. La redundancia no se encuentra normalmente en empresas muy pequeñas, pero las pequeñas empresas ligeramente más grandes pueden utilizar redundancia de densidad de puertos o tener proveedores o enlaces redundantes de Internet.

- ○ Router de Internet
- ○ Firewall
- ○ Un switch de baja densidad de puertos
- ◉ redundancia

2. Un técnico de red contratado recientemente recibe la tarea de pedir hardware nuevo para una empresa pequeña con un gran pronóstico de crecimiento. ¿Cuál es el factor principal que debe tener en cuenta el técnico al elegir los nuevos dispositivos?

Tema 17.1.0 - En una empresa pequeña con un gran pronóstico de crecimiento, el factor influyente principal sería la capacidad de los dispositivos de admitir la modularidad.Los dispositivos que tienen una cantidad o un tipo de interfaces fijos no admitirían el crecimiento. La redundancia es un factor importante, pero se suele encontrar en las empresas grandes. La supervisión de red también es una consideración importante, pero no tanto como la modularidad.

- ○ Dispositivos con una cantidad y un tipo de interfaces fijos
- ○ Dispositivos compatibles con la supervisión de red
- ○ Dispositivos redundantes
- ◉ Dispositivos compatibles con la modularidad

3. ¿Qué tipo de tráfico probablemente tendría la prioridad más alta a través de la red?

Tema 17.1.0 - No todo el tráfico debe recibir el mismo tratamiento o prioridad en una red. Algunos tipos de tráfico, como el de voz y video, requieren la mayor prioridad porque son muy sensibles a la latencia y a las demoras de la red. Otros tipos de tráfico, como el de FTP, que no son sensibles a la latencia ni a las demoras, deben recibir el nivel más bajo de prioridad para que el tráfico de mayor prioridad pueda pasar.

- ○ FTP
- ○ Mensajería instantánea
- ◉ Voz
- ○ SNMP

4. Un técnico de red investiga la conectividad de red de una PC a un módulo remoto de E/S con la dirección 10.1.1.5. ¿Qué comando, cuando se emite en una PC con Windows, muestra la ruta al módulo remoto de E/S?

Tema 17.4.0 - El comando tracert se usa para iniciar un trace desde el símbolo del sistema en una PC con Windows. El comando traceroute se usa para iniciar un rastreo desde un switch o un router Cisco. Algunos otros sistemas operativos de PC, como Linux y Mac OS, también utilizan el comando traceroute. El comando ping no muestra la ruta de la red hacia el host remoto.

- ○ **trace 10.1.1.5**
- ○ **traceroute 10.1.1.5**
- ◉ **tracert 10.1.1.5**
- ○ **ping 10.1.1.5**

5. Un usuario no puede acceder al sitio web cuando escribe **http://www.cisco.com** en un navegador web, pero puede acceder al mismo sitio si escribe **http://72.163.4.161**. ¿Cuál es el problema?

Tema 17.7.0 - El servicio de nombre de dominio (DNS) se utiliza para traducir una dirección web a una dirección IP. La dirección del servidor DNS se proporciona a los servidores por medio de DHCP.

- ○ Puerta de enlace predeterminada
- ○ DHCP
- ◉ DNS
- ○ Modelo TCP/IP

6. ¿Dónde se envían de manera predeterminada los mensajes de resultado de depuraciónde Cisco IOS?

Tema 17.6.0 - Los mensajes debug, como otros mensajes de registro del IOS, se envían a la línea de consola de manera predeterminada. El envío de estos mensajes a las líneas terminales requiere del comando **terminal monitor** .

- ○ búferes de memoria
- ○ líneas vty
- ○ Servidor de syslog
- ◉ La línea de consola

7. ¿Qué elemento del escalamiento de red involucra la identificación de las topologías física y lógica?

Tema 17.3.0 - Para extender una red, se requieren varios elementos:

- Documentación de la red - Topologías física y lógica
  Inventario de dispositivos - Lista de dispositivos que utilizan o conforman la red
  Presupuesto- Presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal
  Análisis de tráfico- se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico

- ○ Análisis de tráfico
- ◉ Registro de red
- ○ Inventario de dispositivos
- ○ Análisis de costos

8. ¿Qué mecanismo se puede implementar en una red pequeña para ayudar a minimizar la latencia de red para aplicaciones de streaming en tiempo real?

Tema 17.1.0 - Calidad de servicio (QoS) es un mecanismo que se utiliza para clasificar y priorizar el tráfico a través de la red. Esto permite a los dispositivos de red minimizar la latencia para aplicaciones en tiempo real como voz y video.

- (●) QoS
- ( ) PoE
- ( ) AAA
- ( ) ICMP

9. ¿Qué proceso falló si una computadora no puede tener acceso a Internet y recibió una dirección IP de 169.254.142.5?

Topic 17.7.0 - Cuando una computadora Windows no puede comunicarse con un servidor DHCP IPv4, la computadora automáticamente se asigna una dirección IP en el rango de 169.254.0.0/16. Las computadoras Linux y Apple no asignan automáticamente una dirección IP.

- ( ) IP
- ( ) DNS
- (●) DHCP
- ( ) HTTP

10. Una pequeña empresa tiene solo un router como punto de salida a su ISP. ¿Qué solución se podría adoptar para mantener la conectividad si el router mismo, o su conexión al ISP, falla?

Tema 17.1.0 - Las redes pequeñas generalmente tienen un solo enlace a un ISP para establecer una conexión a Internet. Pueden ocurrir problemas en la red, lo que puede causar la interrupción de este servicio. Para mantener la conectividad, debe proporcionarse redundancia. Si el problema está en la interfaz del router que está conectada al ISP, se puede activar otra interfaz en el router, por lo que si una interfaz falla, el tráfico se puede redirigir hacia la otra interfaz. Sin embargo, si el router falla, se puede usar un segundo router conectado a otro ISP como copia de seguridad.

- ( ) Active otra interfaz de enrutador que esté conectada al ISP, para que el tráfico pueda fluir a través de ella.
- (●) Tener un segundo router que esté conectado a otro ISP.
- ( ) Adquiera un segundo enlace de menor costo de otro ISP para conectarse a este router.
- ( ) Agregue más interfaces al enrutador que está conectado a la red interna.

11. ¿Cuándo debe un administrador establecer una línea de base de red?

Tema 17.4.0 - Se puede establecer una línea de base de red efectiva supervisando el tráfico a intervalos regulares. Esto permite al administrador tomar nota cuando ocurre cualquier desviación de la norma establecida en la red.

- ( ) cuando el tráfico está en el pico de la red
- ( ) cuando hay una caída repentina en el tráfico
- ( ) en el punto más bajo de tráfico de la red
- (●) a intervalos regulares durante un período de tiempo

12. ¿Cuáles son los dos tipos de tráfico que requieren distribución sensible a las demoras? Elija dos opciones.

Tema 17.1.0 - El tráfico de voz y video tiene características sensibles a las demoras, y se les debe dar prioridad sobre otros tipos de tráfico, como el tráfico web, de correo electrónico y de transferencia de archivos.

- [ ] correo electrónico
- [ ] Web
- [ ] FTP
- [x] Voz
- [x] Video

13. Un técnico en redes sospecha que una conexión de red particular entre dos switches de Cisco tiene una diferencia entre dúplex. ¿Qué comando usaría el técnico para ver los detalles de capa 1 y capa 2 de un puerto de switch?

Topic 17.5.0 - El comando **show interfaces** se puede utilizar tanto en routers como switches para ver velocidad, dúplex, tipo de medio, dirección MAC, tipo de puerto y otra información relacionada con la capa 1 y 2.

- (•) **show interfaces**
- ( ) **show running-config**
- ( ) **show ip interface brief**
- ( ) **show mac-address-table**

14. ¿Qué declaración es verdadera acerca de CDP en un dispositivo Cisco?

Tema 17.5.0 - CDP es un protocolo propietario de Cisco que puede deshabilitarse globalmente mediante el comando de configuración global **no cdp run** , o deshabilitarse en una interfaz específica mediante el comando de configuración de interfaz **no cdp enable** . Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco obtengan información de los demás incluso si no hay conectividad de capa 3. El comando **show cdp neighbors detail** revelará la dirección IP del vecino, independientemente de que se pueda hacer ping en ese vecino o no.

- ( ) El comando **show cdp neighbor detail** revelará la dirección IP de un vecino solo si hay conectividad de Capa 3.
- ( ) Para deshabilitar CDP, utilice el comando **no cdp enable** en el modo de configuración de interfaz
- (•) CDP se puede desactivar globalmente o en una interfaz específica.
- ( ) Dado que se ejecuta en la capa de enlace de datos, el protocolo CDP sólo se puede implementar en conmutadores.

15. ¿Qué factor debe tenerse en cuenta en el diseño de una red pequeña cuando se eligen dispositivos?

Tema 17.1.0 - Los factores a tener en cuenta al diseñar una red incluyen el costo de los dispositivos, la velocidad, la modularidad y la escalabilidad, y la facilidad de administración de la red.

- (•) costo de los dispositivos
- ( ) redundancia
- ( ) análisis de tráfico
- ( ) ISP

Correct

You have successfully identified the correct answers.

You got 15 out of 15 questions correct.

1. Which network design consideration would be more important to a large corporation than to a small business?

Topic 17.1.0 - Small businesses today do need Internet access and use an Internet router to provide this need. A switch is required to connect the two host devices and any IP phones or network devices such as a printer or a scanner. The switch may be integrated into the router. A firewall is needed to protect the business computing assets. Redundancy is not normally found in very small companies, but slightly larger small companies might use port density redundancy or have redundant Internet providers/links.

- Internet router
- firewall
- low port density switch
- (•) redundancy

2. A newly hired network technician is given the task of ordering new hardware for a small business with a large growth forecast. Which primary factor should the technician be concerned with when choosing the new devices?

Topic 17.1.0 - In a small business with a large growth forecast, the primary influencing factor would be the ability of devices to support modularity. Devices with a fixed type/number of interfaces would not support growth. Redundancy is an important factor, but typically found in large enterprises. Network monitoring is also an important consideration, but not as important as modularity.

- devices with a fixed number and type of interfaces
- devices that have support for network monitoring
- redundant devices
- (•) devices with support for modularity

3. What type of traffic would most likely have the highest priority through the network?

Topic 17.1.0 – Not all traffic should receive the same treatment or priority through a network. Some types of traffic, such as voice and video, require the highest priority because they are very sensitive to network latency and delay. Other types of traffic, such as FTP, which is not sensitive to latency and delay, should be given the lowest level of priority so that the higher priority traffic can get through.

- FTP
- instant messaging
- (•) voice
- SNMP

4. A network technician is investigating network connectivity from a PC to a remote host with the address 10.1.1.5. Which command, when issued on a Windows PC, will display the path to the remote host?

Topic 17.4.0 - The tracert command is used to initiate a trace from the command prompt on a Windows PC. The traceroute command is used to initiate a trace from a Cisco router or switch. Some other PC operating systems, such as Linux and Mac OS also use the traceroute command. The ping command does not display the network path to the remote host.

- ○ **trace 10.1.1.5**
- ○ **traceroute 10.1.1.5**
- ◉ **tracert 10.1.1.5**
- ○ **ping 10.1.1.5**

5. A user is unable to reach the website when typing **http://www.cisco.com** in a web browser, but can reach the same site by typing **http://72.163.4.161**. What is the issue?

Topic 17.7.0 - Domain Name Service (DNS) is used to translate a web address to an IP address. The address of the DNS server is provided via DHCP to host computers.

- ○ default gateway
- ○ DHCP
- ◉ DNS
- ○ TCP/IP protocol stack

6. Where are Cisco IOS debug output messages sent by default?

Topic 17.6.0 - Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the terminal lines requires the **terminal monitor** command.

- ○ memory buffers
- ○ vty lines
- ○ Syslog server
- ◉ console line

7. Which element of scaling a network involves identifying the physical and logical topologies?

Topic 17.3.0 - To scale a network, several elements are required:
- Network documentation - physical and logical topology
- Device Inventory - list of devices that use or make up the network
- Budget - itemized IT budget, including fiscal year equipment purchasing budget
- Traffic analysis - protocols, applications, and services and their respective traffic requirements should be documented

- ○ traffic analysis
- ◉ network documentation
- ○ device inventory
- ○ cost analysis

8. What mechanism can be implemented in a small network to help minimize network latency for real-time streaming applications?

Topic 17.1.0 - Quality of service (QoS) is a mechanism which is used to classify and prioritize traffic through the network. This enables network devices to minimize the latency for real-time applications such as voice and video.

- (●) QoS
- ( ) PoE
- ( ) AAA
- ( ) ICMP

9. Which process failed if a computer cannot access the internet and received an IP address of 169.254.142.5?

Topic 17.7.0 - When a Windows computer cannot communicate with an IPv4 DHCP server, the computer automatically assigns itself an IP address in the169.254.0.0/16 range. Linux and Apple computers do not automatically assign an IP address.

- ( ) IP
- ( ) DNS
- (●) DHCP
- ( ) HTTP

10. A small company has only one router as the exit point to its ISP. Which solution could be adopted to maintain connectivity if the router itself, or its connection to the ISP, fails?

Topic 17.1.0 - Small networks generally have only one link to an ISP to establish a connection to the Internet. Problems can occur in the network, which can cause the disruption of this service. In order to keep connectivity, redundancy has to be provided. If the problem is in the router interface that is connected to the ISP, another interface can be activated on the router, so if one interface fails, traffic may be redirected toward the other interface. However, if the router itself fails, a second router that is connected to another ISP can be used as a backup.

- ( ) Activate another router interface that is connected to the ISP, so the traffic can flow through it.
- (●) Have a second router that is connected to another ISP.
- ( ) Purchase a second least-cost link from another ISP to connect to this router.
- ( ) Add more interfaces to the router that is connected to the internal network.

11. When should an administrator establish a network baseline?

Topic 17.4.0 - An effective network baseline can be established by monitoring the traffic at regular intervals. This allows the administrator to take note when any deviance from the established norm occurs in the network.

- ◯ when the traffic is at peak in the network
- ◯ when there is a sudden drop in traffic
- ◯ at the lowest point of traffic in the network
- ◉ at regular intervals over a period of time

12. Which two traffic types require delay sensitive delivery? (Choose two.)

Topic 17.1.0 - Voice and video traffic have delay sensitive characteristics and must be given priority over other traffic types such as web, email, and file transfer traffic.

- ☐ email
- ☐ web
- ☐ FTP
- ☑ voice
- ☑ video

13. A network technician suspects that a particular network connection between two Cisco switches is having a duplex mismatch. Which command would the technician use to see the Layer 1 and Layer 2 details of a switch port?

Topic 17.5.0 - The **show interfaces** command can be used on both routers and switches to see speed, duplex, media type, MAC address, port type, and other Layer 1/Layer 2-related information.

- ◉ **show interfaces**
- ◯ **show running-config**
- ◯ **show ip interface brief**
- ◯ **show mac-address-table**

14. Which statement is true about CDP on a Cisco device?

Topic 17.5.0 - CDP is a Cisco-proprietary protocol that can be disabled globally by using the **no cdp run** global configuration command, or disabled on a specific interface, by using the **no cdp enable** interface configuration command. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers can learn about each other even if Layer 3 connectivity does not exist. The **show cdp neighbors detail** command reveals the IP address of a neighboring device regardless of whether you can ping the neighbor.

- ◯ The **show cdp neighbor detail** command will reveal the IP address of a neighbor only if there is Layer 3 connectivity.
- ◯ To disable CDP globally, the **no cdp enable** command in interface configuration mode must be used.
- ◉ CDP can be disabled globally or on a specific interface.
- ◯ Because it runs at the data link layer, the CDP protocol can only be implemented in switches.

15. What factor should be considered in the design of a small network when devices are being chosen?

Topic 17.1.0 - Factors to consider when designing a network include the cost of devices, speed, modularity and scalability, and ease of managing the network.

- ◉ cost of devices
- ◯ redundancy
- ◯ traffic analysis
- ◯ ISP

17.8.5

Anexo Gráfico

Se muestran todos los archivos utilizados en este curso y descargados en su totalidad.

Nombre

1.1.1.1 Video Transcripción - Introduction to Packet Tracer
1.1.2.1 Video Transcripción - Download and Install Packet Tracer
1.1.2.-Video - La experiencia de aprendizaje en Cisco Networking Academy
1.2.3.-animación del flujo de datos por una red
1.5.5.-proceso de descarga e instalación de Packet Tracer.
1.5.6.- aprender a utilizar los menús y a crear su primera red Packet Tracer
1.5.7-packet-tracer---network-representation_es-XL
1.5.7-packet-tracer---network-representation_es-XL
1.7.5.-Vídeo - Cisco Webex para Huddles
1.9.3-lab---research-it-and-networking-job-opportunities_es-XL
2.1.1.1 Video - Getting Started with Packet Tracer
2.2.3.-IOS CLI modos de comando principal
2.2.4.-Navegación entre los modos de IOS
2.3.4.-Ayuda sensible al contexto y verificación de sintaxis de comandos
2.3.5.-Teclas de acceso rápido y métodos abreviados
2.3.7-packet-tracer---navigate-the-ios_es-XL
2.3.7-packet-tracer---navigate-the-ios_es-XL
2.3.8-lab---navigate-the-ios-by-using-tera-term-for-console-connectivity_es-XL
2.5.5-packet-tracer---configure-initial-switch-settings_es-XL
2.5.5-packet-tracer---configure-initial-switch-settings_es-XL
2.7.6-packet-tracer---implement-basic-connectivity
2.7.6-packet-tracer---implement-basic-connectivity
2.8.1-video-activity---test-the-interface-assignment
2.8.2-video-activity---test-end-to-end-connectivity_es-XL
2.9.1-packet-tracer---basic-switch-and-end-device-configuration
2.9.1-packet-tracer---basic-switch-and-end-device-configuration
2.9.2-lab---basic-switch-and-end-device-configuration
3.0.3-class-activity---design-a-communications-system_es-XL
3.1.1.-Vídeo - Dispositivos en una burbuja
3.1.3.-Protocolos de comunicación
3.1.6.-Codificación de los mensajes
3.1.7.-Formato y encapsulamiento del mensaje
3.1.8a.-Tamaño del mensaje - Analogía
3.1.8b.-Tamaño del mensaje - Red
3.1.9.-Sincronización del mensaje
3.3.5.-desencapsular la página Web para mostrarla en el explorador Web
3.3.5.-encapsulamiento cuando un servidor web envía una página web a un cliente web
3.4.4-lab---research-networking-standards_es-XL
3.5.5-packet-tracer---investigate-the-tcp-ip-and-osi-models-in-action_es-XL
3.5.5-packet-tracer---investigate-the-tcp-ip-and-osi-models-in-action_es-XL

Nombre

4.1.2.-ejemplo del proceso de encapsulación. La última parte de este proceso muestra los bits que se envían a través del medio físico
4.6.5-packet-tracer---connect-a-wired-and-wireless-lan_es-XL
4.6.5-packet-tracer---connect-a-wired-and-wireless-lan_es-XL
4.6.6-lab---view-wired-and-wireless-nic-information_es-XL
4.7.1-packet-tracer---connect-the-physical-layer_es-XL
4.7.1-packet-tracer---connect-the-physical-layer_es-XL
5.1.2.-Conversión entre sistemas de numeración binarios y decimales
5.2.2.-ver cómo convertir entre sistemas de numeración hexadecimal y decimal.
6.1.3.-provisión de acceso a los medios
7.1.6-lab---use-wireshark-to-examine-ethernet-frames_es-XL (1)
7.1.6-lab---use-wireshark-to-examine-ethernet-frames_es-XL
7.2.3.- Proceso de reenvío de tramas
7.2.4.-cómo se procesa una trama de unicast
7.2.5.-cómo se procesa un trama de broadcast
7.2.6.-cómo se procesa un trama de multicast
7.3.4.-demostración de cómo dos switches conectados crean tablas de direcciones MAC.
7.3.5.-demostración de cómo la PC-A se comunica con el gateway predeterminado
7.3.7-lab---view-the-switch-mac-address-table_es-XL
7.4.1.-demostración del proceso de store-and-forward
7.4.2.-demostración del proceso cut-through switching
8.1.1.-animación sobre el intercambio de datos
8.2.3.-demostración de una revisión de encabezados IPv4 en una captura de Wireshark
8.3.5.-demostración de una revisión de encabezados IPv6 en una captura de Wireshark
8.5.5.-introducción a la tabla de enrutamiento IPv4
9.1.3-packet-tracer---identify-mac-and-ip-addresses_es-XL
9.1.3-packet-tracer---identify-mac-and-ip-addresses_es-XL
9.2.2.-animación de la función ARP
9.2.3.-demostración de una solicitud de ARP para una dirección IPv4 de destino que está en la red local
9.2.4.-demostración de una respuesta de ARP
9.2.5.-demostración de una solicitud de ARP y una respuesta de ARP asociadas con el gateway predeterminado
9.2.9-packet-tracer---examine-the-arp-table_es-XL
9.2.9-packet-tracer---examine-the-arp-table_es-XL
9.3.1.-demostración de Descubrimiento de vecinos IPv6
10.1.4-packet-tracer---configure-initial-router-settings
10.1.4-packet-tracer---configure-initial-router-settings
10.3.4-packet-tracer---connect-a-router-to-a-lan
10.3.4-packet-tracer---connect-a-router-to-a-lan
10.3.5-packet-tracer---troubleshoot-default-gateway-issues
10.3.5-packet-tracer---troubleshoot-default-gateway-issues
10.4.1.-Diferencias de dispositivos de red - Parte 1

Nombre

10.4.2.-Diferencias de dispositivos de red - Parte 2
10.-Video - Proteger el acceso administrativo a un switch
11.1.5.-demostración de cómo se determinan las direcciones de red, de host y de difusión para una dirección IPv4 y una máscara de subred dadas
11.2.1.-ejemplo de transmisión de unidifusión
11.2.2.-ejemplo de transmisión de difusión limitada
11.2.3.-En la animación, se muestran clientes que aceptan paquetes de multidifusión
11.5.3.-explicación de la máscara de subred
11.5.4.-explicación del número mágico
11.5.5-packet-tracer---subnet-an-ipv4-network_es-XL
11.5.5-packet-tracer---subnet-an-ipv4-network_es-XL
11.6.4.-explicación de cómo usar el número mágico a través de los límites de los octetos
11.6.6-lab---calculate-ipv4-subnets_es-XL
11.8.1.-demostración de las técnicas de VLSM básicas
11.8.2.-demostración de la división en subredes VLSM
11.9.3-packet-tracer---vlsm-design-and-implementation-practice_es-XL
11.9.3-packet-tracer---vlsm-design-and-implementation-practice_es-XL
11.10.1-packet-tracer---design-and-implement-a-vlsm-addressing-scheme_es-XL
11.10.1-packet-tracer---design-and-implement-a-vlsm-addressing-scheme_es-XL
11.10.2-lab---design-and-implement-a-vlsm-addressing-scheme_es-XL
11.-Video - Modificación de la configuración en ejecución
12.6.6-packet-tracer---configure-ipv6-addressing
12.6.6-packet-tracer---configure-ipv6-addressing
12.7.4-lab---identify-ipv6-addresses_es-XL
12.9.1-packet-tracer---implement-a-subnetted-ipv6-addressing-scheme_es-XL
12.9.1-packet-tracer---implement-a-subnetted-ipv6-addressing-scheme_es-XL
12.9.2-lab---configure-ipv6-addresses-on-network-devices_es-XL
12.-Video Activity - Test the Interface Assignment
13.1.2.-Animación del host 1 enviando una solicitud de eco ICMP ping al host 2 y la respuesta de eco ICMP del host 2 al host 1
13.2.4.-Solicitud de eco de ping a una red remota que se enruta a través de un enrutador y la respuesta de eco que se enruta desde la red remota.
13.2.5.-animación - cómo traceroute aprovecha el TTL
13.2.6-packet-tracer---verify-ipv4-and-ipv6-addressing_es-XL
13.2.6-packet-tracer---verify-ipv4-and-ipv6-addressing_es-XL
13.2.7-packet-tracer---use-ping-and-traceroute-to-test-network-connectivity_es-XL
13.2.7-packet-tracer---use-ping-and-traceroute-to-test-network-connectivity_es-XL
13.Video Activity - Test End-to-End Connectivity
14.1.4.-ver cómo los segmentos de TCP y los reconocimientos se transmiten entre el emisor y el receptor.
14.1.5.-animación de los datagramas UDP que se transmiten del remitente al receptor
14.5.5.-demostración en video del protocolo de enlace TCP de 3 vías, utilizando Wireshark
14.6.2.-lección acerca de los reconocimientos y los números de secuencia TCP
14.6.4.-lección acerca de la retransmisión TCP

Nombre

14.8.1-packet-tracer---tcp-and-udp-communications_es-XL (1)
14.8.1-packet-tracer---tcp-and-udp-communications_es-XL (1)
14.8.1-packet-tracer---tcp-and-udp-communications_es-XL
14.8.1-packet-tracer---tcp-and-udp-communications_es-XL
15.4.8-lab---observe-dns-resolution_es-XL
16.2.1.-explicación animada de los tres tipos de malware
16.2.2.-Barridos de Ping
16.2.2.-Consultas a través de Internet
16.2.2.-Escaneo de puertos
16.2.3.-Explotación de confianza
16.2.4.-Ataque DDoS
16.2.4.-Ataque DoS
16.4.6-packet-tracer---configure-secure-passwords-and-ssh_es-XL
16.4.6-packet-tracer---configure-secure-passwords-and-ssh_es-XL
16.4.7-lab---configure-network-devices-with-ssh_es-XL
16.5.1-packet-tracer---secure-network-devices_es-XL
16.5.1-packet-tracer---secure-network-devices_es-XL
16.5.2-lab---secure-network-devices_es-XL
17.5.8.-explicación del comando show version
17.5.9-packet-tracer---interpret-show-command-output_es-XL
17.5.9-packet-tracer---interpret-show-command-output_es-XL
17.8.1-lab---design-and-build-a-small-network_es-XL
17.8.2-packet-tracer---skills-integration-challenge_es-XL
17.8.2-packet-tracer---skills-integration-challenge_es-XL
17.8.3-packet-tracer---troubleshooting-challenge_es-XL
17.8.3-packet-tracer---troubleshooting-challenge_es-XL