Los Protocolos TCP/IP

Tabla de Contenidos

3. Los Protocolos TCP/IP

3.1 Arquitectura Del TCP/IP

El 1968 la **Agencia de investigación de Proyectos Avanzados** del Departamento de Defensa de EE.UU. (**DARPA**) comienza un programa de desarrollo que permitiese la transmisión de información entre redes de distintos tipos y características. Se implemento una red punto a punto de lineas telefónicas denominada **ARPANET**, usando un conjunto de protocolos que posteriormente se denominarían **TCP/IP**. Esta red formada por organizaciones educativas, militares y de investigación se convirtió en el núcleo de Internet hacia 1980, y en 1983, todos los hosts de ARPANET utilizaban dicho conjunto de protocolos.

Como hemos visto en el capitulo anterior, las funciones de una red de ordenadores pueden basarse en los siete niveles del modelo OSI, aunque la implantación real de una red puede diferir a nivel practico de dicho modelo. No existe un acuerdo general en como presentar el conjunto de protocolos **TCP/IP** con un modelo de capas. Generalmente se presentan como validos entre tres y cinco niveles funcionales en la arquitectura del protocolo.

4 – Nivel de aplicación
3 – Nivel de transporte
2 – Nivel Internet
1 – Nivel de acceso a la red

Nivel de acceso a la red

Este este es el nivel inferior de la jerarquía de protocolos de TCP/IP. Los protocolos de esta capa proporcionan los medios para que el sistema entregue los datos a otros dispositivos directamente conectados a la red. Define cómo utilizar la red para transmitir un *datagrama IP*.

En este nivel se encapsulan los datagramas IP formando frames que se transmiten a la red, y transforman las direcciones IP a las direcciones físicas usadas en la red. Un ejemplo de protocolo de este nivel seria **ARP** *(Address Resolution Protocol)* en redes ***LAN*** y ***SLIP*** (Ip de Linea Serie) o PPP (Protocolo de Punto a Punto) en redes **WAN**. Dicho protocolo proporciona .

Nivel Internet

Este nivel controla la comunicación entre equipos,eligiendo la ruta mas adecuada que deben seguir los paquetes de datos para llegar a su destino. Crea el servicio basico de entrega de paquetes sobre el que se construye una red TCP/IP.

El protocolo mas importante de este nivel es **IP** (Internet Protocol).

Nivel de transporte

Facilita comunicación punto a punto desde un programa de aplicación a otro,asegurándose en caso de que sea necesario de que los datos llegan sin errores y en la secuencia correcta. Realiza un **checksum** para verificar también que la información no ha sido modificada durante la transmisión.

TCP (Transmission Control Protocol) y **UDP** (User Datagram Protocol) serian los protocolos de ente nivel.

Nivel de aplicación

Encontramos en este nivel todos los procesos que hacen uso de los protocolos del nivel de transporte.

Entre todos los protocolos existentes en este nivel , podemos indicar **FTP** (File transfer Protocol), **HTTP** (Hipertext Transfer Protocol), **SMTP** (Simple Mail Transfer Protocol), **DNS** (Domain Name Server), **NFS** (Network File System), **telnet**, etc...

3.2 Protocolos TCP/IP

3.2.1 Protocolo SLIP Y PPP

Las redes WAN tienen como diferencia principal el hecho de que no utilizan estructuras de paquetes determinadas, unicamente envían un flujo de bytes, por lo que para poder enviar paquetes de información es necesario el uso de técnicas de encapsulamiento

SLIP (*Serial Line Internet Protocol*) :

Mas antiguo que **PPP** , no implementa ninguna de las ventajas de este. El protocolo **SLIP** unicamente encapsula los paquetes IP para que puedan ser enviados a traves de una conexión de flujo de bytes. Tiene varias limitaciones:

- Unicamente encapsula paquetes IP, por lo que no es posible utilizar otros, tales como IPX/SPX o NetBEUI.
- Las contraseñas de autentificacion se envían sin encriptacion de ningún tipo, comprometiendo seriamente la seguridad de la información.
- No integra detección ni corrección de errores.
- No integra compresión.
- La configuración del enlace se ha de realizar manualmente, lo que obliga a conocer tanto nuestra IP como la del host destino (imposibilitando por tanto la asignación dinámica), y valores como la unidad maxima de transmisión y de recepción (**MTU** y **MRU**),entre otros.

PPP (*Point to Point Protocol*)

Creado en 1993 por el **IETF** (*Internet Engineering Task Force*) para paliar algunas deficiencias de SLIP, y crear un estándar internacional que permitiese, además encapsular multiples protocolos. Sus ventajas respecto a SLIP serian, principalmente, la posibilidad de encapsular multiples protocolos, no exclusivamente IP, la mayor capacidad para autenticar, y la posibilidad de negociar y configurar la conexión.

Este protocolo se compone de tres componentes:

- Un metodo de encapsulamiento de paquetes sobre conexiones serie.
- El protocolo **LCP** (Link Control Protocol) para establecer, configurar y comprobar la conexión.
- La familia de protocolos **NCP** (Network Control Protocol) para configurar los protocolos del nivel de red.

PPP funcionaria , de manera general de esta forma:

El host origen **(1)** realiza una llamada telefonica al host destino **(2)** mediante un modem conectado a la linea telefonica. Tras realizar la conexión fisica, el host 1 envía paquetes **LCP** para determinar la configuración de red a utilizar en la conexión. Posteriormente se configura el nivel de red mediante el envío de paquetes **NCP** , incluyendo el uso de dirección IP dinámica en caso de ser necesario. NCP se utilizará también para liberar la IP al finalizar la conexión (operación que gestiona El protocolo LCP).

3.2.2 Protocolo ARP (Protocolo De Resolucion De Direcciones).

Habitualmente, en una red **LAN**, los paquetes enviados a un ordenador, son recibidos por todos los demás que comparten medio físico. Para poder diferenciar entre los diferentes sistemas, se decidió asignar de fabrica una dirección exclusiva, habitualmente en formato hexadecimal, a cada adaptador de red, denominada **MAC**. De esta forma, en cada paquete que se envía en una red local, incluye la dirección MAC del emisor , y del receptor, permitiendo así que las demás máquinas de la red ignoren dichos paquetes al recibirlos. El protocolo **ARP** se encarga de obtener la MAC del ordenador receptor.

Su funcionamiento seria:

Cuando se quiere enviar un paquete de información a una maquina, el protocolo ARP consulta si la dirección MAC del receptor se encuentra en la cache de ARP. En caso de que exista una entrada coincidente, se enviara el paquete a dicha MAC. En caso contrario, se envía un paquete especial (petición de ARP) a la dirección de difusión, que contiene la dirección IP y la MAC del emisor, y la IP del receptor que se busca. Cada maquina recibe entonces la petición ARP, y compara la IP solicitada con la suya propia. En caso de no coincidir, se desecha el paquete ARP, pero si la dirección IP es la requerida, el receptor envía una respuesta ARP con su dirección MAC, que sera convenientemente guardada en la cache ARP para consultas posteriores. Una vez identificadas ambas máquinas, se envían los paquetes de información directamente a la MAC del receptor.

3.2.3 Protocolo IP

Este es el protocolo principal en el nivel de Internet. Su función principal es identificar cada paquete que pasa por el nivel y seleccionar la mejor ruta para su envío al host destino.

Sus características principales son :

- El envío de los datos se realiza en datagramas (paquetes IP).
- No esta orientado a la conexión. Es decir, un paquete puede seguir una ruta totalmente diferente a otro, debido a que cada uno es tratado de forma independiente.
- No implementa corrección de errores, ni mecanismos de verificación de entrega de los paquetes IP. Estos controles los lleva el nivel de transporte, con el protocolo TCP.
- Tiene la capacidad para fragmentar los paquetes en caso de que sean demasiado grandes para la

arquitectura por la que se envían. Posteriormente, en el host destino, los paquetes vuelven a reensamblar.

Cada paquete **IP** contiene en su encabezado la dirección IP del host destino. Esta dirección **IP** es un valor exclusivo por cada host, que identifica tanto al host, como a la red a la que pertenece. La notación habitual de una dirección IP es de cuatro números con valores entre 0 y 255 separados por puntos (172.26.0.1), aunque realmente la red maneja dichas direcciones en valores binarios (11111111.00000000.11111111.00000000).

> *En el momento de la creación y diseño de la red que posteriormente daría lugar a Internet, se considero adecuado un sistema de asignación de 32 bits (4 grupos de 8 bits separados por puntos), creando un total de 4.294.967.296 direcciones únicas. El auge de Internet ha dejado claro que dicho numero es insuficiente, abriendo paso a Ipv6, version que maneja valores de 128 bits, permitiendo 340.282.366.920.938.463.463.374.607.431.768.211.456* ***direcciones simultaneas****.*

Cada IP contiene una parte de información de la red a la que pertenece, y otra parte a la del host a la que corresponde. El numero de bits utilizados en la identificación de cada uno es variable dependiendo del tipo de red que se trate. A nivel practico existen 3 clases de redes (y de direcciones IP) :

- *Clase A*: Actualmente asignadas a organizaciones gubernamentales, aunque en el pasado se reservaron para grandes empresas, como IBM o HP. En esta clase de red el primer octeto de la dirección IP define la red, y los tres octetos restantes se dedican a asignar direcciones a los hosts.

  El rango de esta clase seria:
  desde 00000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (0.xxx.xxx.xxx)
  hasta 01111111.xxxxxxxx.xxxxxxxx.xxxxxxxx (127.xxx.xxx.xxx)

Debido a que las direcciones 127.xxx.xxx.xxx se utilizan para auto diagnostico, el primer byte de esta clase estaría comprendido entre 1 y 126, y el numero total de direcciones que se pueden asignar a hosts seria de 16.777.214.

- *Clase B*: Utilizada por grandes empresas y organizaciones de tamaño medio .Los dos primeros octetos definen el rango de IP, y los dos restantes se asignan a los hosts de dicha red.

  El rango que correspondería a la clase B seria:
  desde 10000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (128.xxx.xxx.xxx)
  hasta 10111111.xxxxxxxx.xxxxxxxx.xxxxxxxx (191.xxx.xxx.xxx)
  En este caso el numero de IP asignables es de 65534.

- *Clase C*: Esta clase se asigna a todos los demás solicitantes. Los tres primeros octetos definen el tipo de red, y el ultimo las direcciones IP disponibles para asignación a hosts.

  El rango de la clase C seria:
  desde 11000000.xxxxxxxx.xxxxxxxx.xxxxxxxx (192.xxx.xxx.xxx)
  hasta 11011111.xxxxxxxx.xxxxxxxx.xxxxxxxx (223.xxx.xxx.xxx)
  El numero de direcciones IP disponibles en esta clase seria de 254.

Existen , además dos clases especiales para usos concretos. La *clase D* (con rango desde 224.xxx.xxx.xxx hasta 239.xxx.xxx.xxx), utilizada para multicast y otros usos específicos, y la *clase E*, aun sin especificar.

Debemos notar, también, que existen rangos de direcciones reservadas para la utilización en redes privadas, y por tanto, no utilizables en Internet. Estos tres rangos serian :

-10.xxx.xxx.xxx
-172.16.xxx.xxx a 172.31.xxx.xxx
-192.168.0.xxx a 192.169.255.xxx

Los valores 0 y 255 no son asignables en el ultimo octeto de la dirección IP, ya que se destinan a funciones especiales , siendo el 0 la dirección de red (172.26.0.0), y el 255 la dirección de broadcast (172.26.0.255).

A cada una de estas clases de IP le corresponde una **mascara de red** (dirección de 32 bits) por defecto, que discriminaría que parte de la IP pertenece a la red, y que parte al host. Esta mascara forma parte del proceso del protocolo IP para enviar paquetes y permite determinar cuando la IP pertenece a una red local o externa.

En la mascara de red todos los bits correspondientes al octeto de red se encuentran a 1, y todos los bits correspondientes al octeto de host, en 0:

-Clase A : 11111111.00000000.00000000.00000000 255.0.0.0
-Clase B : 11111111.11111111.00000000.00000000 255.255.0.0
-Clase C : 11111111.11111111.11111111.00000000 255.255.255.0

3.2.4 El Protocolo ICMP

El protocolo **ICMP** (Protocolo de control de Mensajes de Internet) es un protocolo sencillo, encargado de generar mensajes de error en el caso de producirse fallos en el transporte de paquetes IP entre los diferentes gateways que comunican los host origen y destino.

El propósito de ICMP no es hacer la comunicación fiable, y no evita la perdida de paquetes IP entre diferentes hosts. únicamente informa de problemas en la comunicación entre las máquinas. La labor de establecer un envío fiable de datos corresponde a protocolos de nivel superior.

Los mensajes ICMP se encapsulan en paquetes IP, como si fuese un protocolo de nivel superior. Sin embargo, ICMP es parte integrante de IP. Estos paquetes se estructuran iniciándose con un campo de cabecera (con valor 1), un campo indicando el tipo de mensaje, un campo de código, incluyendo el mensaje de error, y para finalizar una suma de control. Posteriormente , el cuerpo del mensaje. Los tipos de mensajes que genera ICMP son:

0- Echo Reply
1- Destination Unreachable
2- Source Quench
5- Redirect
8- Echo
11- Time exceeded
12- Parameter problem
13- Timestamp
14- Timestamp reply
15- Information request
16- Information reply
17- Addressmask
18- Addressmask reply

Entre estos mensajes podríamos destacar **echo** y **echo reply**, utilizados para comprobar si existe enlace a nivel de red entre los dos dispositivos. El comando **ping** haria uso de estos dos tipos para comprobar la existencia de comunicación y su calidad (calculando el tiempo que pasa entre la petición de eco y la respuesta de eco, y contando el numero de peticiones frente al numero de respuestas).

En caso de recibirse un mensaje tipo **3**, el error vendrá indicado por el campo código :

0- Network unreachable
1- Host unreachable
2- Protocol unreachable
3- Port unreachable
4- Fragmentation needed but the do not fragment bit was set.
5- Source route failed
6- Destination network unknown
7- Destination host unknown
8- source host isolated
9- Destination network administratively prohibited
10- Destination host administratively prohibited
11- network unreachable for this type of service
12- Host unreachable for this type of service
13- Communication administratively prohibited by filtering
14- Host precedence violation
15- Precedence cutoff in effect

Traceroute es otro comando que hace uso de ICMP, enviando paquetes IP con tiempos validos de respuesta muy bajos. Utilizando los mensajes **Time exceeded** de respuesta, genera un mapa del camino que siguen los paquetes IP hasta el host destino.

3.2.5 El Protocolo UDP

Pertenece al nivel de transporte, y se caracteriza por no estar orientado a la conexión, por lo que aunque incorpora mecanismos de detección de errores, no facilita ningún tipo de control sobre ellos. Es un protocolo sencillo basado en que el protocolo IP del nivel inferior tampoco esta basado en la conexión. Sus características son :

- No es **fiable.** Al no incorporar control de errores, no garantiza la recepción de los paquetes.
- No se encarga de que los paquetes se reciban en el orden correcto o no duplicados.
- Permite el envío de paquetes sin conexión previa.

Todos los servicios que requieran un mayor control sobre el envío de datos tendrán que utilizar el mas seguro protocolo TCP.

La información incluida en la cabecera de un paquete UDP consta de **puerto de origen** , **puerto de destino**, **longitud** (que indica la longitud del paquete, incluida su cabecera), y **la suma de comprobación.** Al no incluir control de errores, esta cabecera es mucho mas simple, y su utilización en determinado tipo de envíos, genera una mayor eficiencia.

Una de sus principales utilizaciones es el envío **multicast** o el envío **broadcast**. En estas circunstancias, en las que se envía información muchos hosts al mismo tiempo, no es deseable manejar la complejidad de cada sistema informando sobre la recepción de paquetes, teniendo que reenviar los perdidos, y provocando un mas que probable colapso en el host origen.

Otra utilización es la transmisión de información en tiempo real, como seria una video conferencia, en el que si se utilizase un control sobre la recepción y el orden de paquetes, se tendría que detener la transmisión únicamente para reenviar los paquetes perdidos, y poder retomarla después. Esto generaría una conexión lenta y con mucho retardo. Es preferible la perdida de una parte de la información para poder garantizar su emisión en tiempo real.

3.2.6 Protocolo TCP

TCP es el otro protocolo que pertenece , junto a UDP, al nivel de transporte de la pila de protocolos TCP/IP. Proporciona una conexión segura, incorporando control de errores, y garantizando así tanto la recepción de todos los paquetes, como su llegada en el orden correcto.

Sus principales características son:

- Es un protocolo orientado a la **conexión**.
- Es **full-duplex.**
- El envío se realiza mediante **stream de bytes** (segmentos),no a traves de paquetes.
- Puede establecer opciones de **prioridad** y **urgencia** en el envío y recepción de la información.

Una cabecera TCP es mucho mas compleja que una UDP, y consta de:

- Puerto de origen.
- Puerto de destino.
- Numero de secuencia.
- Numero de aviso de recibo.
- Offset de datos.

- Reservado(no implementado).
- Flags de control.
- Ventana.
- Suma de control.
- Puntero de urgencia.
- Relleno de 32 bits.

El procedimiento de TCP es el siguiente:

- El **host** origen establece una conexión con el host destino, en el que se especifica tanto el puerto origen como el puerto destino se utilizaran para el envío de la información.

- Se procede a la transmisión, realizando un control sobre la llegada de la totalidad de los datos (se solicita de la maquina destino el **aviso de recibo**, que en caso de no llegar en un tiempo limite, provoca el reenvío), así como de que la recepción sea en el orden correcto, mediante el **numero de secuencia**. Tambien se verifica mediante la **suma de control** que los datos no sean modificados durante la transmisión.
  En caso de que no sea así, TCP se encarga de realizar todos los pasos necesarios para que la maquina destino reciba la información en el orden correcto.
  Opcionalmente, y mediante el **puntero de urgencia** se podrán establecer prioridades sobre que segmentos deben procesarse primero. En caso de no necesitarse, el puntero de urgencia incorpora valores por defecto.

- Finalmente, y tras verificar que todos los datos han sido entregados de forma adecuada, tanto el host origen , como el destino, envían una **señal de cierre**. Se produce la desconexión, cerrando los **puertos** que se abrieron para la transmisión.

3.2.7 DNS Y DHCP

DNS

Las máquinas de una red (tanto una intranet ,como Internet)se comunican entre ellas a traves de su dirección IP. Esta dirección consta de cuatro bloques de tres números comprendidos ente 0 y 255, tal como anteriormente hemos indicado. Pero esta nomenclatura es difícil de manejar para los seres humanos, por lo que habitualmente se convierten esas direcciones ip en nombres de host,naciendo así el concepto de **DNS**.

El sistema y protocolo DNS es una base de datos encargada de asociar las direcciones IP con su correspondiente

nombre de host. Así una dirección IP 172.26.0.42 de una red local pasa a llamarse servernfs1, mucho mas fácil de recordar.

En una intranet pequeña, es posible llevar esta equivalencia a traves de un fichero plano de texto, en el que se indican tanto la IP como el nombre de host. La gestión de dicho fichero y su distribución pueden realizarse de forma manual, o bien mediante un servidor **NIS**. Pero en el caso de Internet, en el que hay estimadas mas de 500 millones de máquinas conectadas, es virtualmente imposible seguir este procedimiento. Si además tenemos en cuenta el numero de peticiones diarias que se generan hacia un servidor DNS, llegamos a la idea de este como una base de datos distribuida y jerárquica a nivel mundial, tanto para evitar el colapso de dicho servidor, como para evitar que todo el sistema de Internet dependa de una sola maquina. Cada uno de los servidores del sistema DNS solo almacenara una parte de la base de datos.

Tomemos como ejemplo la pagina web de **Google**, en su formato completo **FQDN** (fully qualified domain name): www.google.com. (terminado en punto y perteneciente al servidor raíz).

El esquema tiene forma de ramas de árbol, que terminan confluyendo en el DNS raíz (**.**).

Cuando un usuario quiere acceder a esta pagina desde su navegador, se realiza una petición DNS al servidor de su proveedor de Internet (**ISP**).En caso de que la información no se encuentre en su cache,la petición se traslada al servidor raíz. El servidor de nombres raíz únicamente tiene información sobre como acceder al nivel inmediatamente inferior, en este caso perteneciente al dominio .com (que forma parte de los **Top Level Domain** tales como . com,.org, .es, .net, .edu, etc...).

Esta información vuelve al ISP , que contacta con el DNS que gestiona **.com,** y tiene conocimiento de la dirección IP del nivel inferior de la rama. En este caso, **google**.

Este dato llega al ISP, que lo traslada entonces al servidor encargado de localizar la maquina **www**, que gestiona el servidor web que permitirá mostrar la pagina al usuario.

En este caso, el servidor DNS que incluiría la información de la IP de www se encontraría dentro de la misma empresa Google, al ser esta privada y tener un dominio **.com**. La información referente a la IP se pasaría en ese momento al DNS del ISP, que a su vez, se enviaría al ordenador del usuario que quería entrar en la pagina para realizar una búsqueda, siendo todo este proceso totalmente transparente para el.

Un servidor DNS que contiene información relevante de su zona de influencia, o de su dominio, se le considera **autoritario** (authoritative).Cada uno de estos servidores deberá estar duplicado al menos dos veces (uno **primario** o maestro y uno **secundario** o esclavo) para evitar la anteriormente mencionada dependencia del sistema.

La base de datos se creara en el DNS primario de zona, y el servidor secundario actualizara la suya tomándola del servidor primario, según un periodo de tiempo especificado, mediante una **transferencia de zona**.

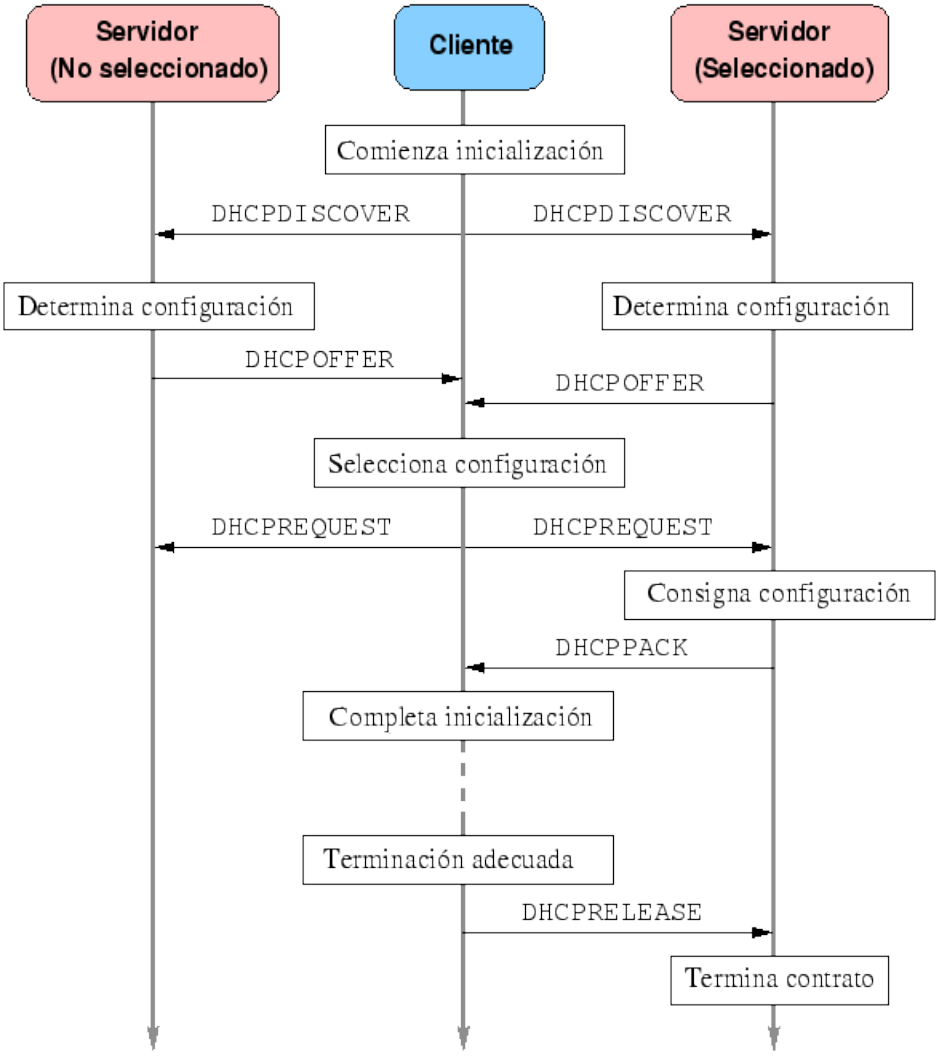
DHCP

DHCP (Dynamic Host Configuration Protocol) nació como una forma de mejorar **BOOTP**. Este protocolo permitía la configuración estática de los parámetros de los diferentes hosts de una red en función de una base de datos almacenada en el servidor. Esta configuración era única para cada maquina, y no podía ser reutilizada, por lo que no podían existir en la red mas máquinas que direcciones IP.

El protocolo DHCP permite una configuración automática y dinámica de los parámetros de TCP/IP (IP, mascara de red, DNS, gateway por defecto,nombre de host y dominio, etc..) a traves de un servidor.

En primera instancia un host que quiera conectar a una red, envía una señal broadcast a la red (**DHCPDISCOVER**). Esta señal es recibida por el servidor o servidores DHCP de la red, que consultaran en su tabla si queda alguna dirección IP libre para asignar ,devolviendo los valores que podrá utilizar el host (**DHCPOFFER**), así como el tiempo máximo de cesión para esa IP. En este punto, el host, en caso de aceptar la IP, envía un mensaje al servidor indicando que la acepta (**DHCPREQUEST**).

El servidor DHCP envía entonces un mensaje de confirmación (**DHCPACK**),almacenando en una tabla la dirección MAC del host y los detalles de la configuración del cliente.



Es importante indicar que estos datos no se guardan hasta que el host envía el mensaje DHCPREQUEST, ya que la misma IP se puede ofrecer a diferentes host, pero solo se asignara a aquel que primero envíe esta confirmación, recibiendo los demás un mensaje indicando que la IP ofrecida ya no esta libre (**DHCPNACK**).

Al finalizar el host el uso de la IP, se envía un mensaje indicándole al servidor que queda esta libre (**DHCPRELEASE**).

Esquema de utilización del protocolo DHCP.

Transcurrida la mitad del periodo de cesión, el host cliente envía un mensaje DHCPREQUEST solicitando la renovación de la cesión. Si el servidor continua activo devolverá un DHCPACK confirmando dicha renovación, iniciándose de nuevo el contador del tiempo de cesión. En caso de no contestar, al 87,5% del tiempo se reenviara la solicitud de renovación. Si el servidor continua sin confirmarla, próximo a finalizar el tiempo, se iniciara de nuevo todo el proceso de adquisición de IP mediante un mensaje DHCPDISCOVER. Tambien se enviara un DHCPRELEASE al anterior DHCP indicando la liberación de la IP.

3.2.8 GATEWAY Y ENRUTAMIENTO

Un **router** o un **gateway** e un dispositivo que opera en el **nivel 3** del **modelo de referencia OSI**, y conecta distintos segmentos de una red. Habitualmente se utilizan los dos términos de manera indistinta, aunque técnicamente hablando, un router enlaza redes del mismo tipo, mientras que un gateway realiza la misma función entre diferentes tipos de red.

Sus funciones principales son :

- La creación y mantenimiento de **tablas de enrutamiento** para los diferentes niveles de protocolos de red. El router realiza una decision de envío sobre el contenido de dicha tabla, y en función del protocolo de envío.
- -Elegir el mejor camino para el envío de los datos, tomando en cuenta factores como el numero de saltos, la velocidad del medio, el trafico, etc.
- Notificar al host origen mediante un mensaje **ICMP** cualquier problema que le impida enviar el paquete al host destino.
- Funciones opcionales como **Quality of Service** (**QoS**), balanceo de carga, firewalls,....

Las tablas de rutas pueden constar de tres tipos de rutas:implícitas, dinámicas, o estáticas.

Implicita: aquella que que se crea de manera automática al configurar una interfaz de red. S denomina también ruta implícita.

Estatica: se especifica de manera explicita mediante la introducción manual de una entrada en la tabla de enrutamiento

Dinamica: estas rutas se crean mediante la ejecución de daemons de direccionamiento en cada uno de los routers. Estos daemons se comunican entre si , intercambiando su información de las rutas disponibles, y creando de esta forma un mapa completo de la red. De esta forma calculan mejor el camino al host destino considerando el estado y estructura de la red en cada momento.

Los daemons que generan tablas dinámicas implementan unos protocolos específicos, como **RIP**, **RIPv2**, **BGP** y **OSPF**, que utilizan algoritmos para la elección de la mejor ruta en cada momento. Los dos algoritmos fundamentales son:

Distancia de vector: es el mas sencillo. Cada router actualiza su tabla con la información del router vecino, y la envía actualizada al siguiente router. En el caso de que se produzca un cambio en la red, la información se transfiere de un router a otro hasta que el mapa esta completo, lo cual puede llegar a durar varios minutos. Su desventaja principal es que el único método que utiliza para la elección de rutas es el numero de saltos, ignorando factores como la velocidad del enlace.

Estado del enlace: Cada router envía únicamente su tabla de rutas implícita a los demás de la red. Como cada uno de ellos recibe todas las rutas implícitas de la red, es capaz de generar un mapa de ella , pudiendo elegir el camino mas adecuado en base a muchos mas factores:

-Numero de saltos
-Rendimiento, aprovechando un ancho de banda mayor.
-Retardo, aprovechando el periodo de espera mas bajo.
-Perdida de paquetes, aumentando la fiabilidad del envío.
-El coste monetario.

3.2.9 Telnet, FTP, SMTP Y POP

Telnet (Telecommunicating Networks) es un protocolo estándar perteneciente al nivel de aplicación dentro del modelo de referencia OSI, que permite establecer una conexión remota entre un host cliente y un host servidor multiusuario (habitualmente UNIX-Linux), y facilita una interfaz estándar similar a la de una sesión local.

Se basa en tres ideas fundamentales:

- El concepto de **NVT** (Network Virtual Terminal): encargada de emular la estructura básica de una terminal real , representada en caracteres **ASCII**.
- Una perspectiva básica de las terminales y los procesos.
- La negociación de opciones de la terminal, lo que permite a muchos host servidores ofrecer servicios adicionales en sus conexiones Telnet.

La sesión se establece indicando la dirección del host y el numero del puerto por el que se establecerá la conexión (habitualmente el **23**). Una vez que el cliente y el servidor han realizado la conexión, se solicitara un usuario y contraseña al cliente. Tras la verificación, el usuario podrá trabajar en la sesión como si estuviese en una terminal local del servidor.

Es importante indicar que la conexión que se realiza con Telnet es del tipo no segura, al no utilizar ningún tipo de encriptacion para el envío de los datos (incluido el usuario y la contraseña de inicio de sesión), por lo que es relativamente sencillo interceptar la información. Por este motivo, se crearon diferentes protocolos de sesiones remotas seguras, como **SSH** (Secure Shell), cuyo funcionamiento es idéntico a Telnet, salvo por el hecho de que la información viaja fuertemente encriptada (su puerto de utilización por defecto es el **22**).

FTP (File Transfer Protocol) , es, al igual que los demás de este apartado, un protocolo perteneciente al nivel de aplicación. Su función es la de realizar transferencias de ficheros (en ambos sentidos) entre un cliente y un servidor. Se realizan dos conexiones realmente entre ambos: una sesión Telnet para la validación de usuario y la introducción de comandos, y la otra para la transferencia de ficheros.

Implementa comandos pertenecientes a telnet (ls, cd, ..), aunque como su funcionalidad principal es distinta, incluye solo aquellos destinados al tratamiento de ficheros, aportando otros específicos destinados a la transferencia por red (put, get,.....).

El procedimiento seria parecido al utilizado por telnet: el cliente solicita una conexión FTP al servidor mediante la aplicación necesaria, indicando la dirección y el puerto de conexión. Para una vez realizada la conexión, introducir el usuario y la contraseña. Posteriormente ya se podrá realizar la transferencia de ficheros entre los dos hosts.

Existen clientes y servidores FTP para la practica totalidad de las plataformas, siendo uno de los métodos de transferencia de archivos mas antiguos y extendidos de Internet.

SMTP (Simple Mail Transfer Protocol) es el protocolo que se utiliza para enviar correo electrónico de un sistema a otro. El envío se puede realizar desde un UA (programa cliente de correo) a un MTA, o entre dos MTA.EL MTA (Mail Transfer Agent) es el programa servidor de correo. Basicamente recibe correo de los UA y los Mta, y :

- Lo reenvía a otros MTA, habitualmente a traves del protocolo SMTP, aunque no necesariamente, hasta que el correo alcance su destino.
- En caso de ser el ultimo de la cadena, almacena el correo localmente, pudiendo ser recuperado a traves de los protocolos POP e IMAP.

SMTP utiliza código ASCII en la conexión al MTA, por lo que es posible realizar el mismo proceso manualmente conectando mediante telnet al puerto 25 del servidor. Tras establecer la conexión se recibe un mensaje de bienvenida del servidor (220 servidor.correo.com).A continuación, suele ser habitual el comando HELO o EHLO, para identificar a nuestra maquina (**HELO mi.maquina.com**). En caso de no requerirlo, se podrían enviar correos anónimos.

El siguiente paso es indicar el remitente de correo (**MAIL from**: prueba@mi.maquina.com), aunque puede dejarse en blanco .

A continuación indicamos la dirección de correo del destinatario

(**RCPT to**: correo@tu.maquina.com), seguido del comando **DATA**, para indicar que vamos a empezar con el mensaje en si. A partir de ese momento , todo lo que escribamos ira como parte de el. En caso de que queramos terminar, deberemos hacerlo con una linea con un solo punto.

Las direccion de de correo electrónico habitualmente tienen el formato correo@dominio.com, por lo que los MTA tienen que saber a que maquina hay que entregarle el correo dentro de este dominio.

Esto se hace indicando los registros **MX** dentro de las tablas del servidor **DNS** del dominio :

dominio.com IN MX 10 correo.dominio.com

Siendo el valor siguiente a MX la prioridad de recepción en caso de que el dominio tenga mas de un servidor de correo.

POP (Post Office Protocol) , en su version 3, es el protocolo que permite a los usuarios acceder al correo electrónico ubicado en el servidor de correo.

Debido a que la comunicación, al igual que con SMTP, se realiza en ASCII, podemos realizarla manualmente mediante telnet, a la dirección del servidor, indicando el puerto 110.

Tras recibir la confirmación de la conexión por parte del servidor, nos identificamos mediante los comandos **USER** y **PASS**.

Para saber el estado del correo utilizaremos **STAT**, y para listar los mensajes , **LIST**.

En caso de que queramos descargarlos, lo podremos hacer con **RETR** y el numero del mensaje, para posteriormente borrarlos con **DELE**.

Finalmente desconectamos la conexión con el servidor POP3 mediante **QUIT**.

El protocolo POP data de una epoca anterior a la popularización de Internet, por lo que se creo el protocolo **IMAP**, bastante mas avanzado, y que, entre otras cosas, permite dejar el correo en el servidor tras descargarlo, o crear carpetas en el. Si no se esta extendiendo mas, es debido a que el coste de mantenimiento de un buzón IMAP es mayor que el de un POP, al necesitar mas capacidad de almacenamiento.