TEORÍA DE LAS REDES INFORMÁTICAS

(redesafull.com.ar)

por ***Mariano López Figuerola***
mlopezf@softhome.net

Descargar **PDF**

Índice

---

1 - GENERALIDADES

La teoría de las redes informáticas no es algo reciente.
La necesidad de compartir recursos e intercambiar información fue una inquietud permanente desde los primeros tiempos de la informática. Los comienzos de las redes de datos se remontan a los años '60 , en los cuales perseguían exclusivamente fines militares o de defensa.
Paulatinamente se fueron adoptando para fines comerciales.
Obviamente en esa época no existían las PCs , por lo cual los entornos de trabajo resultaban centralizados y lo común para cualquier red era que el procesamiento quedara delegado a una única computadora central o mainframe. Los usuarios accedían a la misma mediante terminales "bobas" consistentes en sólo un monitor y un teclado.
Los tiempos han cambiado y hoy prácticamente todos los usuarios acceden a los recursos de las redes desde PCs. Sin embargo, la teoría, los principios básicos, los protocolos han mantenido vigencia y si bien es cierto, se va produciendo obsolecencia de parte de ellos, resulta muy conveniente comenzar el estudio partiendo de los principios y de la teoría básica. Resulta dificultoso comprender las redes actuales si no se conocen los fundamentos de la teoría de redes.
En nuestro análisis partiremos de **X.25**; un tradicional sistema que trabaja sobre redes analógicas, es decir líneas telefónicas dedicadas. Actualmenteconserva unas pocas aplicaciones, como ser cajeros automáticos, validación de tarjetas de crédito, etc; pero su robustez, seguridad y confiabilidad han hecho mantenerlo como un estándar para las redes públicas y privadas durante una gran cantidad de años. Además sus principios, su teoría de funcionamiento aporta conceptos sumamente importantes que nos ayudarán a comprender los

siguientes.
Frame Relay es una mejora de **X.25** . Se trata de un sistema mucho más simple y eficiente, el cual tiene plena vigencia hoy en día en redes de área amplia. Trabaja sobre enlaces digitales generalmente punto a punto.
Posteriormente veremos las tecnologías **LAN** y por último culminaremos con el de mayor auge en nuestros días, base indispensable del funcionamiento de Internet: **TCP/IP**.

1.1 - CONCEPTOS BÁSICOS ASOCIADOS A REDES

1.1.1 - Primeras definiciones

- **RED :** Una RED es un conjunto de computadoras o terminales conectados mediante una o más vías de transmisión y con determinadas reglas para comunicarse.
- **HOST :** Aunque en general este término suele relacionarse con Servidores, en un sentido amplio llamaremos HOST a cualquier equipo que se conecta a una red.
- **PROTOCOLO:** Conjunto de comandos establecido por convención que deben conocer tanto emisor como receptor para poder establecer una comunicación en un red de datos. Constituyen el **software** de la red.
- **DTE:** Data Terminal Equipement es el equipo terminal de datos, la computadora o terminal que es el extremo final de la red.
- **DCE:** Data Communication Equipement es el equipo de comunicación. Generalmente un modem u algún otro dispositivo que establece el enlace físico y lógico con la red.
- **INTERNET:** aunque todos sabemos lo que es Internet, aquí lo utilizaremos también en otro sentido. Una Internet es un conjunto de dos o más redes diferentes que se interconectan mediante los medios adecuados.

1.1.2 - Redes orientadas a la conexión vs. no orientadas a la conexión

Se dice que una red es **Orientada a la Conexión** cuando se establece un único camino para la transferencia de la información. Los datos viajarán uno tras otro por dicho camino. No hay más de un camino simultáneamente.
Requieren obligatoriamente de 3 fases:

- **Establecimiento**
- **Transferencia**
- **Desconexión**

Son el caso de X.25 , Frame Relay, ATM y TCP.
Las redes **No Orientadas a la Conexión** (connectionless) no utilizan un único camino, sino que los datos se fraccionan y toman por distintas vías simultáneamente para llegar a destino. Se la conoce también como **Servicio de Datagramas** y los casos típicos son IP y UDP.

1.1.3 - Circuitos Virtuales Conmutados vs. Circuitos Virtuales Permanentes

Las redes **Orientadas a la Conexión** pueden constituir 2 tipos de circuitos o caminos para establecer la comunicación:

- **Circuitos Virtuales Conmutados (SVC´s)** establecen un camino de comunicación a través de la red que no es siempre el mismo. La conexión se establece por un camino al necesitar intercambiar datos y se libera al finalizar. Al establecerse una nueva conexión el camino a través de la red puede ser diferente. X.25 trabaja de esta forma.
- **Circuitos Virtuales Permanentes (PVC´s)** son similares a una línea punto a punto , están siempre fijos y no alternan entre caminos diferentes. La conexión se establece por única vez por un único medio físico al contratar el servicio y se mantiene inalterable hasta la baja del mismo. Frame Relay suele trabajar de esta forma aunque soporta también conmutados.

1.1.4 - Conmutación de Circuitos vs Conmutación de paquetes

Las redes pueden conmutar circuitos , como es el caso de la red telefónica o conmutar paquetes, que son una subdivisión lógica de la información.
Casi todas las tecnologías actuales : X.25 , Frame Relay , ATM , TCP/IP son de conmutación de paquetes.

1.2 - CLASIFICACIÓN DE LAS REDES

1.2.1 - Clasificación por área de cobertura

El universo de las redes , puede clasificarse según la extensión que abarcan.
Cada uno de los tipos requiere de tecnologías y topologías específicas.
Se distinguen en general 3 categorías:

- **REDES LAN o Local Area Networks**: Son las que **no exceden 1 km** de extensión. Lo más habitual es que abarquen un edificio o varios dentro de una manzana o un área limitada
- **REDES MAN o Metropolitan Area Network**: **Hasta 10 Km**, es decir , distintos puntos dentro de una misma ciudad.
- **REDES WAN o Wide Area Networks**: **Más de 10 Km**. Distintas ciudades dentro de un mismo país o distintos países.

1.2.2 - Clasificación por método de comunicación

Las redes pueden utilizar dos métodos de comunicación que las diferencia en:

- **REDES DE BROADCAST:** todas las máquinas comparten un único medio de transmisión . Es decir que cuando un de ellas transmita , todas recibirán la información y solamente aquella a ala cual va dirijida la utilizará.
- **REDES PUNTO A PUNTO:** existen conexiones individuales entre pares de máquinas.

1.3 - EL MODELO DE REFERENCIA OSI

El modelo **OSI (Open System Interconnection)** es el comienzo de cualquier estudio de redes
Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema.
A cada capa se le asigna una función bien específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento.
Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo - y de hecho, normalmente no lo hacen- pero de todas formas se recomienda siempre tener en cuenta el modelo OSI como referencia , ya que conocimiento del mismo posibilita la correcta comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.
Las 7 capas son las siguientes:

- **CAPA 1 : Physical (Física):** Define las reglas para transmitir el flujo de bits por el medio físico
- **CAPA 2 : Data Link (Enlace) :** Organiza los bits en grupos lógicos denominado tramas o **frames .** Proporciona además control de flujo y control de errores.
- **CAPA 3 : Network (Red) :** Proporciona la posibilidad de rutear la info agrupada en **paquetes.**
- **CAPA 4 : Transport (Transporte):** Realiza el control de extremo a extremo de la comunicación, proporcionando control de flujo y control de errores. Esta capa es asociada frecuentemente con el concepto de **confiabilidad**.
- **CAPA 5 : Session (Sesión):** conexión y mantenimiento del enlace
- **CAPA 6 : Presentation (Presentación):** frecuentemente forma parte del sistema operativo y se encarga de dar formato los datos.
- **CAPA 7 : Aplication (Aplicación) :** Servicios para el usuario como ser e-mail, servicios de archivos e impresión, emulación de terminal, loguin , etc.

Es importante aclarar con respecto a esta última que no cualquier aplicación que corra dentro de una PC encuadra en la capa Aplicación del modelo OSI, sino solamente las aplicaciones a los efectos del trabajo en red.

1.4 - TOPOLOGÍAS DE REDES

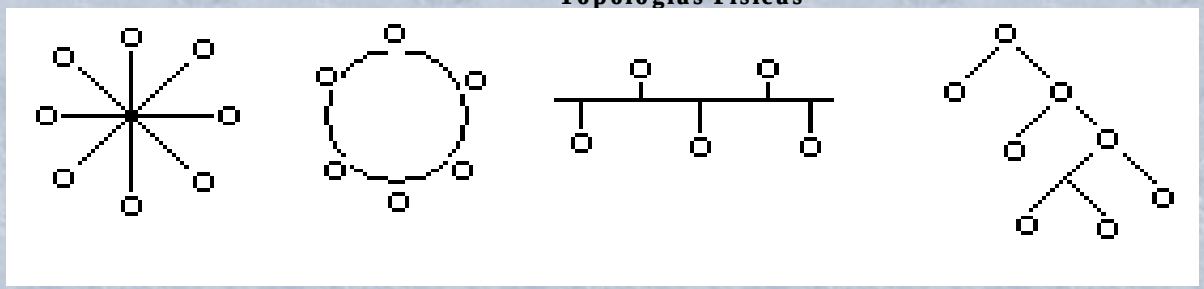
Es necesario, en principio, diferenciar entre topologías **físicas** y **lógicas**.
Este es un tema que generalmente se presta a confusión.

1.4.1 - Topologías físicas

La **topología física** es la conexión real del cableado entre los dispositivos .
Hay una gran variedad, nosotros enumeraremos las 4 principales.

- **ESTRELLA:** Las terminales se conectan todas directamente a un dispositivo central
- **ANILLO:** El cable de interconección recorre uno a uno las terminales cerrándose en un lazo
- **BUS:** Un único cable recorre todas las terminales desde un extremo a otro. También se la conoce como "**topología horizontal**"
- **ÁRBOL:** Partiendo de un dispositivo central los equipos se van ramificando. También se la conoce como "**estructura jerárquica**".

Topologías Físicas



(1) Estrella (2) Anillo (3) Bus (4) Árbol

1.4.2 - Topologías lógicas

La **topología lógica** se refiere comportamiento de los datos en la red independientemente del conexionado físico.
Topologías **lógicas** sólo hay 2:

- **BUS**
- **ANILLO**

Todas las anteriores físicas encuadran en alguna de las 2 topologías lógicas.
Por ejemplo : una red Ethernet que utiliza cable UTP y se conecta en estrella a un hub en realidad se comporta lógicamente como un bus .

1.5 - COMPONENTES DE HARDWARE DE UNA RED

Una red en general puede constar de algunos o todos de los siguientes elementos básicos:

- **PLACAS DE RED o NIC´s (Network interface Connector):** proporcionan la interfaz entre las PCs o terminales y el medio físico.
- **REPETIDORES:** son elementos activos que se utilizan como "refuerzo" de la señal. Permiten incorporar nuevos segmentos de cableado.
- **CONCENTRADORES O HUBS:** se utilizan como punto de partida del cableado **UTP** (léase tipo telefónico) . De allí salen los cables a cada una de los terminales. Su funcionamiento se basa en "repetir" la señal que llega por una boca en las demás. Pueden conectarse en cascada constituyendo una entructura tipo **"árbol".**
- **SWITCHES:** cumplen la misma función que los **hubs** pero poseen una cierta inteligencia que losa hace más eficientes. En vez de repetir la señal a todas las bocas sólo la envía a la salida correspondiente. esto permite reducie el tráfico en la red.
- **BRIDGES:** interconectan 2 redes iguales.
- **ROUTERS:** encaminan la información hacia otras redes. Son la piedra fundamental de **Internet**.
- **GATEWAYS:** igual que los **routers** pero permiten conectar redes de diferentes tipos.

1.5.1 - Los diferentes componentes de hardware en el modelo OSI

Acorde a la clasificación hecha en base al modelo **OSI**, podremos decir que cada uno de los componentes de una red encuadran en una o varias capas del mismo.
Corresponden a **Capa 1** los **Hubs** y **Repetidores** además de los **cables y dispositivos de interconexión.**
Haré una aclaración antes de proseguir. Hay una diferencia de criterios en este sentido: algunos autores definen a la **Capa 1**, no como el medio físico en sí mismo, sino como los medios eléctricos y técnicas para transmitir la información a través del mismo, consideran que estos elementos formarían una capa aún inferior - llamada a veces **Capa 0** - , sobre la cual se montan las superiores. En nuestro caso, para simplificar, nos referiremos a estos elementos como integrantes de la **Capa 1**.
Las **NIC´s** (Network Interface Connectors) o simplemente **placas de red,** aunque puedan creerse exclusividad del medio físico, trabajan en **Capa 2** (enlace). **Switches** y **Bridges** son también dispositivos de **enlace**, es decir trabajan en **Capa 2.**
Los **Routers**, en cambio, trabajan en **Capa 3** ya que necesitan interpretar el contenido de los paquetes para poder encaminar los datos.
Los **Gateways** son dispositivos de las capas superiores.

1.6 - SOFTWARE DE UNA RED

El **Software** de una red lo constituyen los **protocolos** de comunicaciones.
Es el conjunto de instrucciones que deben conocer ambos extremos de un enlace para poder establecer una comunicación.
Ejemplos de protocolos son :

- **X.25**
- **Frame Relay**
- **ATM**
- **IP**
- **Apple Talk**

Los mismos pueden también estratificarse en las distintas capas del modelo **OSI.**
Existen por lo tanto protocolos de **capa 2**, **capa 3, capa 4** y así sucesivamente.
Pero los mismos no actúan en forma independiente. La relación entre los mismos es lo que le da la verdadera dinámica al modelo OSI.
Los protocolos de distintas capas se suelen agrupar para su estudio en los llamados **"stacks"** (pilas) de protocolos. La idea sería que cualquier stack cumpla con todas las funciones definidas por el modelo OSI, aunque la correspondencia no deba ser necesariamente capa a capa. Por ejemplo un conjunto o "suite" de protocolos que forma un stack es **TCP/IP**.
El mismo cumple todas las funciones del modelo OSI pero su distribución no es la misma. **TCP/IP** está formado sólo por cuatro capas y algunas de ellas equivalen a más de una del modelo OSI.
Del mismo modo se pueden hacer otras agrupaciones siempre respetando la estructura del modelo OSI.
Existen multitud de recomendaciones que nos posibilitan armar conjuntos de protocolos que contituyan esquemas armónicamente funcionales.
Por ejemplo la recomendación del **ITU-T** (ex CCITT) para el protocolo de nivel de **Red X.25**, es que esté montado sobre **LAPB** a nivel de **Enlace** y **EIA-232** ó **V.24** a nivel **Físico.**

2 - REDES X.25

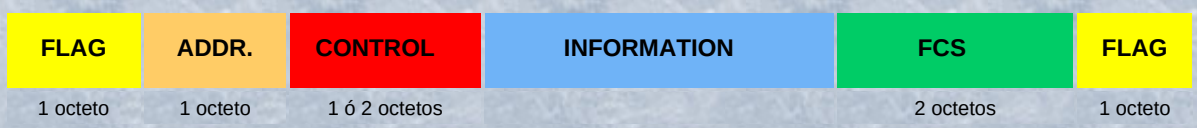
X.25 es la especificación para redes públicas de conmutación de paquetes que trabajan sobre **SVC's Switched Virtual Circuits** (Circuitos Virtuales Conmutados).
El stack es de tres capas que corresponden a las 3 primeras del modelo OSI.
Los protocolos recomendados en la especificación son : **RS-232** ó **V.24** para la capa física y **LAPB** (un subconjunto del estándard **HDLC**) para la de enlace.
X.25 propiamente dicho corresponde a la capa 3 y se la denomina **PLP (Packet Layer Protocol).**
Define las especificaciones para la comunicación de los equipos terminales de datos: **DTE** (Data Terminal Equipement) y los equipos de comunicaciones: **DCE** (Data Communication Equipement).
Es muy importante tener claro estos conceptos.
El **DTE** generalmente es una PC, una terminal de usuario o cualquier equipo donde se hará el procesamiento final de la información. El **DCE** es el equipo de comunicaciones, generalmente un modem u otro dispositivo de conexión a una red de datos.
La norma **X.25** y sus protocolos de soporte definen sólo la comunicación entre estos 2 dispositivos, no interesa cómo es la red en su interior. La red puede ser Frame Relay , ATM, TCP/IP u otra.
Vermos en primer lugar el funcionamiento de **LAPB**.

2.1 - LAPB

LAPB es la especificación que define la comunicación a nivel enlace entre el **DTE** y el **DCE**. Es un subconjunto de comandos de la especificación **HDLC**.
Sus funciones son **entramado , control de flujo** y **control de errores.**
Las tramas toman los datos de la capa superior , los encapsulan dicha info en el campo **INFORMATION.** agregándole los flags, encabezado y control de errores . Luego se transfieren al nivel físico para ser transmitidos.
Es un protocolo full duplex, es decir ambos extremos pueden transmitir simultáneamente.
El entramado proporciona tramas o "frames" que contienen la dirección destino, el comando que representan y un chequeo de errores sin corrección.
Además proporciona control de flujo mediante los números de secuencia que estudiaremos a continuación.
LAPB es un protocolo de "ventana deslizante" . Para explicarlo debemos introdicir primero el concepto de ventana.
Ventana es el número de tramas recibidas pendientes de confirmación. Es importante para determinar la velocidad de transferencia en función del ancho de banda del enlace y la capacidad del receptor.
La trama puede setearse para módulo 8 o módulo 128. En cualquiera de ambos casos :

Ventana = módulo – 1

Por ejemplo . módulo 8 implica ventana igual a 7.
El concepto de ventana deslizante va asociado al hecho de que las mismas se numeran de 0 a 7 y esos números se repiten cíclicamente. Volveremos sobre este punto.
El la figura se muestra la trama **LAPB**:



2.1.1 - Los Flags

Son una secuencia de 8 bits de los cuales los 6 centrales son unos y los extremos son ceros (01111110). Su única función es delimitar la trama indicando principio y final.
Pero: ¿Qué ocurriría si eventualmente en los datos apareciera una secuencia similar?
Respuesta: para evitar que dicha secuencia pueda ser confundida con una prematura finalización de la trama se introduce una técnica conocida como "bit stuffing".
El transmisor al armar la trama chequea previamente los datos y si encuentra seis unos seguidos intercala un

cero antes del último. Por ejemplo, la siguiente secuencia:

0111111 quedaría así : **011111 0 1**

El receptor entonces al recibir la trama , descarta los flags y si encuentra cinco unos seguidos sabe que tiene que haber habido un "bit stuffing" , por lo tanto simplemente retira el cero adicional. Este método garantiza la "transparencia" del código.

2.1.2 - El campo Address

Como LAPB se define sólo entre un **DTE** y un **DCE** solamente hay 2 posibilidades. Se utilizan: 00000011 para el **DTE** y 00000001 para el **DCE.**
Luego veremos que cuando una trama lleva un comando que es una orden lleva la dirección del destino, y si es una rta lelva la propia.

2.1.3 - El campo FCS

Hace un chequeo de redundacia cíclica de los campos de Address , Control e Information para detectar errores en los mismos.

2.1.4 - El Campo de Control y los formatos de trama

El campo de control es el que representa el tipo de trama, y en caso de llevar un comando éste es el campo que lo lleva codificado.
En base a esto, el campo puede tener 3 formatos diferentes que representan los 3 tipos de trama disponibles.
Los 3 tipos de trama son:

- **Information :** transmite datos y nro de secuencia
- **Supervision :** emite comandos y nros de secuencia
- **Unnumbered :** (no numerada) sólo emite comandos de control, no transmite nros de secuencia (de allí su nombre).

Los 3 formatos del campo de **CONTROL** son los que se muestran:
Los campos CTRL codifican el comando en particular.
Como **LAPB** es un subconjunto de **HDLC** sólo se utilizan 9 comandos.
De los 9 comandos, 3 son de **Supervisión** y 6 son **No Numerados.**
Los mismos se detallan a continuación:

Supervisión *(pueden ser comandos o rtas)*:
- **RR Receive Ready :** indica listo para recibir
- **REJ Reject :** indica que se ha recibido una trama con error de FCS.
- **RNR Receive Not ready :** indica no listo para recibir

No numerados:
Comandos:
- **SABM Set Asyncronious Balanced Mode:** inicializa modo balanceado sincrónico
- **SABME Set Extended Asyncronious Balanced Mode:** ídem sincrónico extendidio
- **DISC Disconnect:** solicitud de desconexión

Respuestas:
- **UA Unnumbered Acknow :** comando no numerado reconocido
- **DM Disconnect Mode:** indica que el equipo está en estado de no conexión
- **FRMR Frame Reject:** rechazo de trama con formato no válido

El 1er bit en 0 del campo de control indica que la trama es de Información.
Si el 1er bit es 1 y el 2do es 0 indica **Supervisión** y si el 2do es 1 indica **No Numerada.**
Los campos de **CTRL** son los que identifican según una determinada codificación el tipo de comando. La trama de Información no lleva transporta ningún comando ya que sólo contiene datos.
Los campos **N(S)** y **N(R)** son los números de secuencia de envío y recepción respectivamente. Nótese que sólo la trama de información los posee a ambos y la de supervisión sólo posee **N(R)**.
Las tramas de supervisión sólo poseen rtas y las no numeradas, como su nombre lo indica, no poseen número de secuencia
Debemos destacar que el nro de secuencia **N(S)** es el orden lógico que posee la trama en una cadena de datos enviada y el **N(S)** es la próxima que se espera recibir. Normalmente, en una comunicación full-duplex (que es lo más habitual) ambos extremos envían y reciben datos simultáneamente. Por eso lo común es que una trama de información tenga ambos nros de secuencia válidos, uno por lo transmitido y otro por lo recibido. A este proceso de simultaneidad se lo conoce como **"piggybacking".**
Los campos de **N(S)** y **N(R)** poserán 3 bits cuando se inicializó con **SABM** y 7 bits cuando se inicializó con **SABME**, esta es precisamente la diferenciea entre ambos. Para el 1er caso por lo tanto habrá 8 combinaciones posibles (se dice que está en módulo 8) y la ventana entonces será 7. En el 2do caso son 128 (módulo 128) combinaciones lo que implica ventana 127.
El bit **P/F** : Poll /Final indica si la terminal está enviando un comando de encuesta (Poll), es decir que requiera respuesta, o bien un comando de respuesta (Final). Si es cero indica que no es ninguna de ambas.

Cualquier comando de Supervisión puede ser o bien comando o bien respuesta dependiendo del bit P/F y de las dirección. Para los comandos No Numerados hay 3 que son comando exclusivamente y 3 que son respuesta exclusivamente. Entonces el bit **P/F** activo indica **Poll (P)** en el 1er caso y **Final (F)** en el 2do. Aquí no hay confusión, pero en los de supervisión esto no está discriminado.
¿ Entonces cómo diferenciamos si se trata de Poll o Final ?.
Respuesta : Por la dirección.
Como dijimos con anterioridad una trama siempre llevará la dirección del destino cuando emite un comando y la propia si es respuesta.
Por ejemplo: si el **DTE** desea enviar un **RR** pidiendo respuesta (Poll) llevará como dirección la del **DCE** (00000001), pero si está respondiendo deberá emitir la propia (00000011). Lo mismo vale para el **DCE**. En todos estos casos el bit **P/F** estará en 1.

2.2 - NIVEL DE PAQUETES X.25

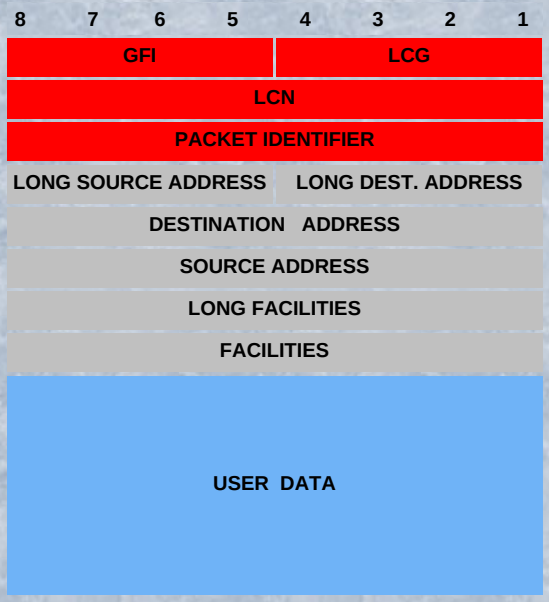
La **Capa 3** de **X.25** la constituye el **Packet Layer Protocol (PLP).**
Esta capa es la primera que permite ver del otro lado de la red.
Si bien la norma define, igual que LAPB la comunicación entre DTE y DCE, permite enviar y recibir paquetes del otro lado del enlace sin importar qué hay en medio.
Aclaremos este concepto : X.25 es la especificación para la comunicación entre los equipos DTE y DCE .
Significa que estudia sólo éstas interfaces y como dijimos, no interesa qué protocolos ni medio utiliza la red.
X.25 es sólo el enlace entre el terminal y el punto de acceso a la red. A pesar de eso , la comunicación se establece **de extremo a extremo** , es decir **de DTE a DTE**.
Como es un protocolo **orientado a la conexión**, que trabaja sobre **circuitos virtuales conmutados (SVC´s)** utiliza estas 3 fases :

- **Establecimiento**
- **Transferencia**
- **Desconexión**

Por lo tanto existen distintos tipos de paquetes:

- **Paquetes de llamada (Call)**
- **Paquetes de liberación (Clear)**
- **Paquetes de interrupción**
- **Paquetes de supervisión**
- **Paquetes de RR , RNR , REJ**

El de **Llamada** y el de **Interrupción** también pueden contener datos.
Como ejemplo se muestra un paquete de llamada.



A continuación se describen los campos:

- **GENERAL FORMAT IDENTIFIER (GFI):** formato del paquete
- **LOGICAL CHANNEL GROUP (LCG):** grupo de canales lógicos

- **LOGICAL CHANNEL NUMBER (LCN):** número de canal lógico
- **PACKET IDENTIFIER:** identificador del tipo de paquete
- **LONG SOURCE ADDRESS:** longitud, en nibbles, de la dirección de origen (calling)
- **LONG DESTINATION ADDRESS:** longitud, en nibbles, de la dirección de destino (called)
- **DESTINATION ADDRESS:** dirección del DTE de destino (called)
- **SOURCE ADDRESS:** dirección del DTE de origen (calling)
- **FACILITIES LONG:** longitud del campo de facilidades
- **FACILITIES:** opciones varias
- **USER DATA:** datos de usuario

Como vemos, define **Canales Lógicos o Logical Channels (LCN)**, los cuales tienen únicamente significado local. Esto significa que están definidos entre cada **DTE** y su correspondiente **DCE.** El número de **LCN** no tiene por qué ser el mismo en ambos extremos, y de hecho es muy poco probable que lo sea: como el **GFI** es de cuatro bits y el **LCN** es de ocho, entonces habrá en total 2^{12} posibilidades, es decir **4096** canales lógicos posibles.

---

3 - FRAME RELAY

Es una técnica de Fast Packet Switching, es decir es de **conmutación de paquetes**, **orientada a la conexión**, diseñada especialmente para trabajar sobre enlaces digitales de alta confiabilidad y con baja tasa de errores.
Puede trabajar sobre SVC´s o PVC´ pero se recomiendan los últimos. Se pretende que, con el tiempo , tiendan a reemplazar a los enlaces punto a punto.
Las velocides de trabajo van de *64kbps* a *2Mbps* y por su modo de transmisión en forma de ráfagas es ideal para la interconexión entre redes LAN.

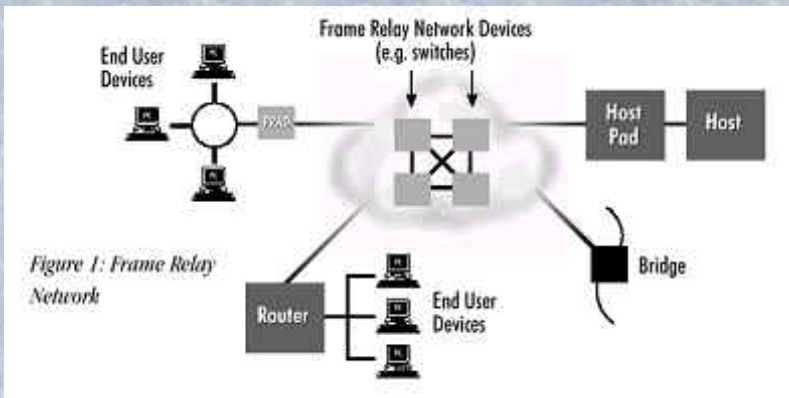
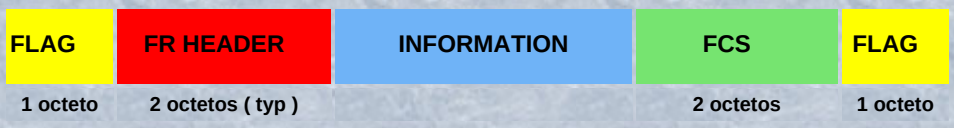


Figure 1: Frame Relay Network

Frame Relay (FR) es un protocolo de solamente **capas 1 y 2**.
Posee una importante diferencia de funcionamiento con respecto a **X.25** que lo simplifica notablemente.
Frame Relay no realiza control de flujo ni de secuencia y no hace un manejo de los errores: si se recibe una trama con error de checksum simplemente la descarta y no envía ninguna notificación al respecto. ¿Qué ocurre entonces con los errores? : **FR** delega esta tarea, al igual que el control de flujo a las capas de nivel superior.
Esto reduce notablemente el tráfico en la red aumentando significativamente su rendimiento.
Es por eso que se dice que **FR** pose bajo overhead, lo que lo hace mucho más eficiente que **X.25.**
Lo que sí posee **FR** es control de congestión.

3.1 - LA TRAMA FRAME RELAY



- **FLAGS :** Octetos 01111110 . Igual que en X.25, delimitan la trama.
- **FR HEADER :** Encabezado con las opciones de control (2 bytes por default)
- **INFORMATION :** Datos de usuario
- **FCS :** Chequeo de redundancia cíclica CRC para comprobación de errores (ídem X.25)

3.2 - EL FR HEADER

El campo **FR Header** de **Frame Relay** es el encabezado de la trama. es el que contiene toda la información de control. El Header típico está formado por 2 octetos pero puede ser mayor.
El primer octeto estáformado por el **DLCI** de 6 bits más **C/R** y **EA**. El segundo posee la continuación del **DLCI** de 4 bits más el **EA** y tres bits : **DE**, **FECN** (FN), **BECN** (BN).

FR HEADER (2 octetos):

- **DIGITAL LOGICAL CHANNEL IDENTIFIER (DLCI):** Número identificatorio del canal lógico
- **COMMAND/RESPONSE (C/R):** Indica si es comando o respuesta . Generalmente no se utiliza.
- **EXTENDED ADDRESS (EA):** Indica extensión del Header, es decir si hay algún octeto más. Cuando es 1 no hay más octetos.
- **FORWAED EXPLICIT CONGESTION NOTIFICATION (FECN):** es una indicación al siguiente switch que hubo congestión y que tramas fueron descartadas.
- **BACKWARD EXPLICIT CONGESTION NOTIFIER (BECN):** es una indicación al switch anterior que hubo congestión y que tramas fueron descartadas.
- **DISCARD ELEGIBILITY (DE):** es una marca que se hace en el DTE para indicar que en caso de congestión esta trama puede descartarse en primer término.

Como vemos, **FR** es muy simple y no tiene elementos para realizar control de flujo. Sí realiza control de congestión gracias a los bits **FECN**, **BECN** y **DE** pero el mismo, igual que el de errores sólo consiste en eliminar tramas y enviar una notificación.

---

4 - REDES LAN

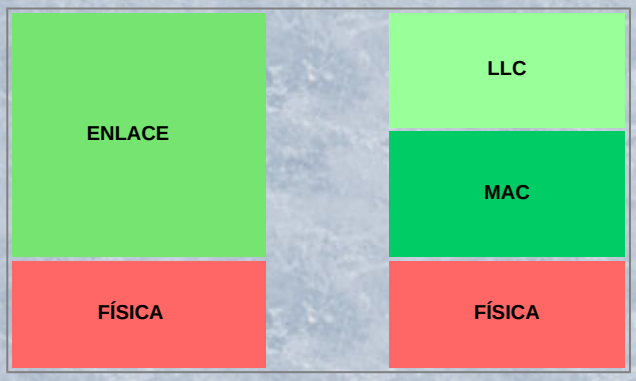
Las **REDES DE ÁREA LOCAL (LAN)** corresponden a un área limitada, típicamente de un máximo de entre 500 y 1000 metros según la topología física.
La denominación se refiere a configuraciones que normalmente no exceden de un edificio o varios contiguos.
Para más distancias se requiere de tecnologías **WAN**.
La Norma **IEEE 802** es la especificación para redes **LAN**. Su nombre se debe aque fue definida en febrero de 1980.
Se distinguen básicamente 2 tipos de redes **LAN**, cada una responde a una de las topologías lógicas vistas con anterioridad.

- **Ethernet**
- **Token Ring**

La primera corresponde a la topología de **bus lógico** y la segunda a **anillo lógico.**
Sus principios de funcionamiento son esencialmente bien diferentes por lo que las veremos en detalle.
Previamente necesitamos definir a las redes LAN en el modelo OSI.

4.1 - REDES LAN EN EL MODELO OSI

El modelo de redes LAN es de 3 capas pero abarca solamente las 2 primeras capas del modelo OSI :
La inferior el la capa física que coincide con el OSI. La capa de Enlace se encuentra dividida en 2 subcapas. La inferior se llama **Subcapa MAC (Medium Access Control)**. La superior es la **Subcapa LLC (Logical Link Control)**.



OSI **LAN**

4.1.1 - Subcapa LLC

Es la encargada de mantener el enlace.
Es igual para una red Ethernet que una Token Ring.
Cumple esencialmente 3 funciones:

- **Sincronización de tramas:** arma las tramas y delimita comienzo y final de cada una
- **Servicios de conexión :** establece una comunicación del tipo sin conexión y no confiable entre las terminales
- **Control de errores:** mediante chequeo de redundancia cíclica (CRC)

4.1.2 - Subcapa MAC

Se encarga de controlar cómo los dispositivos de la red acceden al medio.
Es lo que diferencia, por ejemplo, a una red Ethernet de una Token Ring o Token Bus.
Sus funciones son:

- **Establecimiento del control de acceso al medio y la topología lógica:** es decir arbitrar la forma en que las distintas terminales transmiten y reciben los datos. esto constituye lo que habíamos llmado topología lógica.
- **Direccionamiento (addressing):** posibilitan la identificación de cada elemento conectado a la red.Hay 3 niveles de direccionamiento.

4.1.3 - Direcciones MAC

Este es un concepto muy importante.
Cada dispositivo físico conectado a la red debe tener una dirección única, la cual se conoce como **Dirección MAC (MAC Address)**, **Dirección de hardware (HW Address)** o simplemente **Dirección Fisica**.
Es un código hexadecimal de **6 bytes**, es decir 12 nibbles que va grabada en el Firmware (memoria no volátil incorporada) de cada unidad, de modo que no pueda ser modificada.
El siguiente es un ejemplo:

00 60 3F 93 E0 37

Existe una convención en la asignación de las mismas de modo que en todo el mundo no pueda haber dos dispositivos con la misma **Dirección de HW.**
La convención consiste en lo siguiente:

- Los 3 primeros bytes identifican al **fabricante**. Y un organismo internacional se encarga de asignar un código de 3 bytes único a cada fabricante.
- Los 3 últimos bytes identifican a la **unidad.** Y cada fabricante se ocupa de, en su producción, no lanzar 2 unidades con el mismo número de MAC Address.

4.1.4 - La Norma IEEE 802

Dijimos que la **802** de la **IEEE** es lo especificación para redes LAN.
En realidad es un conjunto de normas que van de la 802.1 a la 802.12.
Enunciaremos solamente las que nos interesan para nuestro estudio.

- **IEEE 802.1:** define el estandard **Físico** y de **Enlace** para la comunicación dentro de una misma LAN o una LAN o WAN diferente.
- **IEEE 802.2:** define la subcapa **LLC**
- **IEEE 802.3:** define una serie de opciones de la capa física, señalización, tipos de medios, topologías, etc; siendo el elemento más característico el mecanismo **CSMA/CD**. Se basa en la especificación **Ethernet** de *Xerox*, aunque impone unas mínimas diferencias.
- **IEEE 802.5:** se basa en la especificación **Token Ring** de *IBM* aunque, a diferencia de ésta no impone un determinado medio de transmisión ni una determinada topología física.

4.2 - REDES ETHERNET

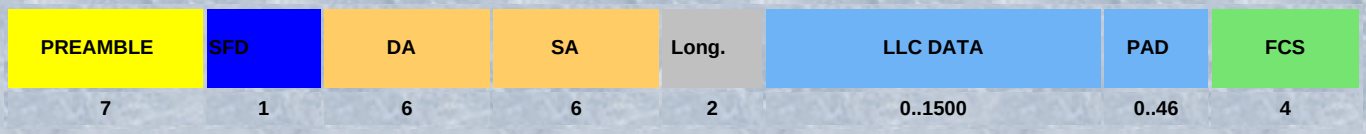
Desarrollada inicialmente por *Xerox* , fue luego normalizada posteriormente por la **IEEE** en la **norma 802.3** , la cual introduce algunas diferencias. Pero se siguen denominando genéricamente de la misma forma.
Ethernet se basa en **CSMA/CD** : **Carrier Sense Multiple Access with Collision Detect** (Acceso múltiple por sensado de portadora con detección de colisiones).
Es básicamente un método de contienda que trabaja por broadcast.
Cuando una estación desea transmitir lo hace a todas las estaciones y sólo la estación destino recibe los datos. El resto los descartan.
Es un método de contienda porque cada estación primero “sensa” el medio físico (escucha) para determinar si otra estación está transmitiendo y en caso de que lo esté espera a que el mismo se libere. Cuando esto ocurre , comienza la transmisión.
Esto pretende evitar las colisiones aunque no siempre lo consigue.
En un medio congestionado éstas suelen ser frecuentes.
Ocurre que la señal tiene un tiempo de propagación . Si otra estación comienza a transmitir habiendo señal en camino , indefectiblemente se producirá una colisión.
El proceso de allí en adelante consiste en anular las tramas invalidadas por la colisión, y esperar un tiempo aleatorio tras lo cual se reintenta volver a transmitir.
Como se deduce fácilmente , el método **CSMA/CD** resulta muy efectivo en medios de poco tráfico, pero por el contrario, en medios con mucha congestión la cantidad de colisiones que se produce reduce notablemente la eficiencia.

4.2.1 - Topologías físicas para Ethernet

Se encuentran definidas en la **802.3**.

- **10Base2 : Tipo bus con coaxil fino (Thin coaxil).** Soporta segmentos de hasta 185 metros y un máximo de 30 nodos por segmento. Es económico pero posee una gran desventaja una apertura o cortocircuito en el cable hace "caer" a toda la red. Su aplicación está cayendo en desuso.
- **10Base5 : Tipo bus con coaxil grueso (Thick coaxil).** Soporta segmentos de hasta 500 metros y un máximo de 100 nodos por segmento. Requiere de duispositivos de interconexión especiales. Es muy robusto confiable pero su alto costo lo delegan exclusivamente a backbones.
- **10BaseT : Tipo estrella con cable UTP (Unshielded Twisted Pair).** Su configuración estrella, con cable telefónico no blindado, partiendo de un hub o switch central lo hace muy versátil y económico. Tiende a reemplazar al coaxil dado que la apertura de un cable no perjudica a toda la red sino solamente a la estación en cuestión.
- **10 BaseF** : **Tipo estrella con Fibra óptica.** Distancias de hasta 2000 metros y 1024 nodos por segmento lo hacen ideal para unir, por ejemplo, distintos.

4.2.2 - Trama IEEE 802.3



- **PREAMBLE:** Su única función es de sincronización . Es una secuencia se 0´s y 1´s
- **START OF FRAME DELIMITER (SFD):** marca el comienzo de la trama . Es el siguente octeto **10101011**.
- **DESTINATION ADDRESS (DA):** Destination Address : MAC Address del destino
- **SOURCE ADDRESS (SA)**: Source Address : MAC Address del origen
- **Long LLC** : Longitud en bytes del campo de datos.
- **LLC data :** El mínimo es de 46 bytes y si no rellena con 0´s (PAD)
- **FCS**: Chequeo de Redundancia Cíclica , comprueba errores en los datos

4.3 - REDES TOKEN RING

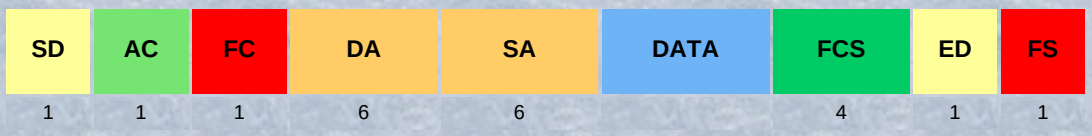
Las redes **Token Ring** fueron desarrolladas por *IBM* y hoy en día están quedando relegadas a algunas pocas redes que por sus caracteríasticas requieren de sus ventajas.
Token Ring no es un método de contienda basado en CSMA/CD sino que se basa en el principio de **"paso de testigo"** (token passing) con prioridad y su funcionamiento es el que encuentra normalizado en la **IEEE 802.5.**
El **Token** es una trama especial que circula de terminal en terminal cíclicamente. Para eso necesita que todos los equipos se conecten mediante una interfaz llmada RIU (Ring Interface Unit) a un dispositivo central denominado **Medium Access Unit (MAU)**. Nuevamente : se trata de una topología tipo **estrella** que se comporta lógicamente como un **anillo**.
Cada terminal posee una unidad de interfaz que es la que se conecta físicamente con el **MAU** . El mismo trabaja a nivel enlace y se encarga de recibir el Token y retransmitirlo.
La estación que pose datos para transmitir , al recibir el token le adosa los datos y lo retrasmite. La estación destino tomará los datos sin eliminarlos y el mismo entonces dará toda la vuelta hasta volver a la estación de origen, la cual será la encargada de retirarlos y reestablecer el token.

4.3.1 - Trama IEEE 802.5

El **Token** es una trama de 3 bytes:

- **START DELIMITER (SD) :** demarca el comienzo del token
- **ACCESS CONTROL (AC) :** establece la prioridad y otras opciones
- **END DELIMITER (ED) :** delimita el fin del token

Cuando alguna estación le agrega datos se incorporan todos los campos siguientes.



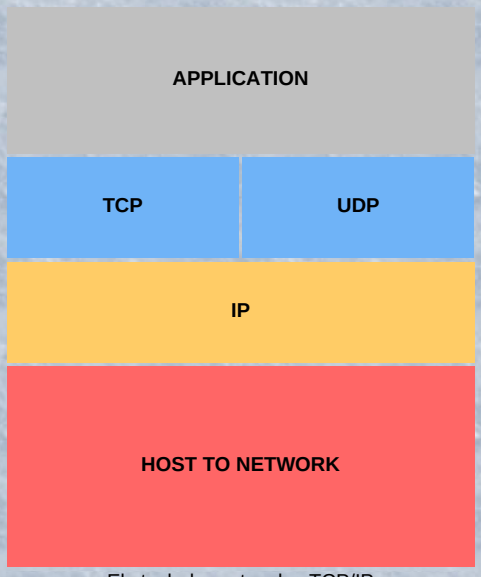
- **FRAME CONTROL (FC).** distingue el tipo de trama
- **DESTINATION ADDRESS (DA) Y SOURCE ADDRESS (SA):** direcciones destino y origen
- **DATA:** campo de informacion
- **FRAME CHECK SEQUENCY:** verificación de Checksum
- **FRAME STATUS (FS):** se utiliza a indicar que la estación receptora ha reconocido la dirección y ha copiado los datos en el campo correspondiente

5 - TCP/IP

Es el conjunto de protocolos utilizado por **Internet.**
Puede trabajar sobre una multitud de protocolos como ser PPP , Frame Relay , X.25 o ATM.

5.1 - EL STACK DE PROTOCOLOS TCP/IP

TCP / IP no es un único par de protocolos. Es un conjunto de ellos estratificado en distintas capas que conforman el denominado **STACK** de protocolos **TCP / IP**.
TCP / IP posee sólo **4** niveles, aunque en relación al Modelo **OSI** cubre la totalidad de capas del mismo.



El stack de protocolos TCP/IP

- **HOST TO NETWORK :** abarca las capas **FÍSICA** y **EENLACE** de **OSI**
- **INTERNET PROTOCOL (IP):** equivale a la capa de **RED** de **OSI**
- **TRANSPORT CONTROL PROTOCOL (TCP):** corresponde a la capa de **Transporte**
- **USER DATAGRAM PROTOCOL (UDP) :** también corresponde a la capa de **Transporte**
- **APPLICATION:** abarca las capas de **SESIÓN** , **PRESENTACIÓN** y **APLICACIÓN.**

5.2 - INTERNET PROTOCOL (IP)

5.2.1 - Direccionamiento IP

Cada elemento conectado a una red **TCP / IP** debe tener una **"dirección IP"** única a fin de ser identificado en la misma en forma unívoca y además una **máscara de subred o "subnet mask"** que identifica la red o subred a la que pertenece el equipo.
Tanto la **dirección IP** como la **subnet mask** son conjuntos de 4 bytes denominados **"octetos"** , separados por puntos.

Las direcciones IP de los equipos se agrupan de forma de poder identificar la **red** a la cual pertenece un determinado **Host** o equipo. Si no se utilizan subredes (caso más simple) la máscara de subred adopta valores fijos para cada uno de esos tipos de red. La máscara de subred cobra mayor importancia en el caso de **"subnetting"**, lo cual veremos más adelante.
Generalmente estos parámetros se expresan en forma decimal, o sea que cada octeto puede adoptar 256 valores ($2^8 = 256$) y van desde 0 a 255.
Ejemplo de dirección IP:

192.234.15.122

y de máscara de subred:

255.255.0.0

A fin de poder efectuar la agrupación antedicha, cada dirección IP se subdivide en 2 partes : la primera parte identifica a la **RED** y se denomina ***NetID*** **.** La 2da es la dirección del **HOST** o ***HostID***.
Con respecto a la extensión de cada parte, como son 4 octetos hay 4 posibilidades para determinar el tipo de red.
Por lo tanto clasificamos las redes en 4 clases de acuerdo a la extensión de cada una de estas partes de la dirección IP. Se distinguen además sus bits de comienzo.

	1er octeto	2do octeto	3er octeto	4to octeto
CLASE A	0 *Net ID*	*Host ID*		
CLASE B	1 0 *Net ID*		*Host ID*	
CLASE C	1 1 0 *Net ID*			*Host ID*
CLASE D	1 1 1 0 *Multicast*			

Las Redes **Clase A** son las que comienzan el **1er octeto** con 0.
Definen sólo el 1er octeto como Identificador de Red. Los otros 3 identifican el **Host** en particular. Se deduce que el rango de **Clase A** va de las redes *0* a la *127* , aunque después veremos que esta última está reservada y no puede utilizarse. Si no hay subredes la **máscara de subred** es todos unos para el primer octeto y todos ceros para el resto, es decir: *255.0.0.0* .
Las Redes **Clase B** comienzan con *10* y utilizan 2 octetos para la identificación de red por lo tanto van desde la *128.0* a la *191.255*. Los 2 restantes identifican el host. Sin subredes la **máscara de subred** es *255.255.0.0*.
La Redes **Clase C** comienzan con *110* y utilizan los 3 primeros octetos para la ***NetID***. El rango por ende va de la *192.0.0* a la *223.255.255*. Sólo el último octeto identifica el **host**, o sea que este tipo de redes sólo permite hasta 256 direcciones de hosts o ***HostId´***s. Sin subredes la **máscara de subred** es *255.255.255.0*.
Las redes **Clase D** van desde la *224.0.0.0* hasta la *239.255.255.255* y son reservadas para multicast.

Consideraciones especiales:

1 - Las direcciones cuyo número de host es todos 0´s definen a la red en general, por lo tanto ningún host puede tener el HostID = 0 . Por ejemplo : *200.233.12.0* define en general a la red Clase C cuyo Net ID es : *200.223.12*
2 - Las direcciones cuyo número de host todos 1´s representa la dirección de broadcast. Por ejemplo *187.34.255.255* significa que se está haciendo un broadcast a la red clase B cuyo Net ID es *187.34* . La dirección *255.255.255.255* es broadcast generalizado.
3 - Las direcciones que comienzan con un Net ID todos 0´s indican un determinado Host de “esta red”. Por ejemplo: *0.0.150.34* significa el host *150.34* de esta red Clase B. Además : todos 0´s , *0.0.0.0* , indica “este host”
4 - La red *127.0.0.0* no se utiliza ya que puede usarla cualquier equipo para loopback. Ésta es una comunicación “a si mismo”, es decir se envían datos a la misma PC pero los mismos no salen al medio físico.

Las direcciones para redes conectadas a "**Internet**" no pueden ser asignadas en forma arbitraria. Existe una entidad única a nivel mundial, con sede en Estados Unidos y con filiales en todos los países llamada "**IANA**" **(*Internet Assigned Numbera Authority*)** que se encarga de aignar las direcciones **IP**. Es a quien se le debe solicitar una ***NetID*** o dirección de red única, para una red que se conecta a Internet. Los ***HostID*** o direcciones individuales de los dispositivos y equipos dentro de la red son asignados libremente por el administrador.
Para redes sin conexión a Internet, que son la mayoría, existen rangos reservados a redes privadas que es aconsejable utilizar.

No puede haber en una misma red y por lo tanto tampoco en "**Internet**" dos dispositivos conectados con una misma **dirección IP**, pero como hay equipos que se conectan a más de una red simultáneamente, un mismo equipo sí puede tener más de una IP. Este es el caso por ejemplo de los bridges y los routers, que poseen una dirección **IP** por cada adaptador, correspondiente al rango de la red a la cual se conecta.
Otro caso más cotidiano sería el de una PC que se conecta a una red **TCP/IP** privada y a su vez lo hace a **"Internet"** mediante un módem: entonces asigna una **IP** (privada) para el adapatdor LAN y otra (pública), del rango asignado por ***IANA*** para la región, para el módem que se conecta a "Internet".

5.2.2 -Subnetting

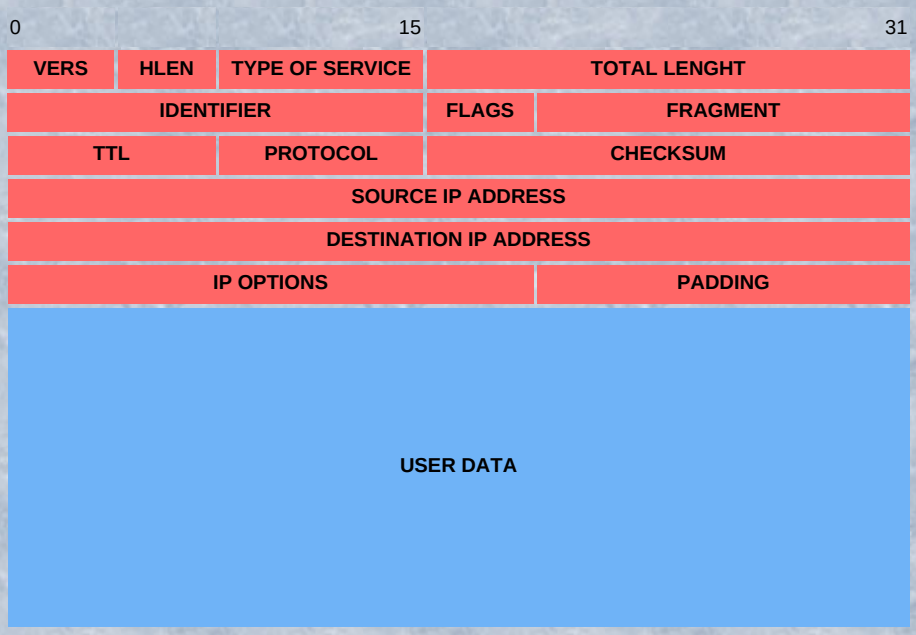
Dijimos que la **máscara de subred** o "**subnet mask**" era importante en el caso de subredes. En efecto, si no hay subredes la misma adopta valores fijos de acuerdo al tipo de red.
Dado que en ocasiones es necesario subdividir lógicamente una red dentro de una misma organización y no se

justifica solicitar a **IANA** nuevos rangos de direcciones, ya que los que se poseen no están completamente utilizados y quedan suficientes direcciones libres, puede utilizarse la técnica de **"subnetting".**
Entonces se particionan los rangos de direcciones IP asignados a la organización en tantas subredes como sea necesario y las mismas se interconectan por routers. Estos routers deben soportar **subnetting**.
Para diferenciar lógicamente las distintas subredes, se utiliza una máscara de subred diferente para cada una mediante una técnica precisa que no detallaremos en este momento *.

** NOTA: El detalle de subnetting será incorporado a esta página en una próxima actualización*

5.2.3 - Datagrama IP

Dijimos que **IP** es un protocolo **"no orientado a la conexión" (connectionless)** y a esto lo llamábamos **"servicio de datagramas".** El datagrama es la unidad de información que se transmite a través de la red a nivel **IP**.
En la figura se muestra el esquema de un datagrama IP.



- **VERSION:** Indica la versión IP. actualmente se utiliza siempre la 4 , por lo que este campo siempre será 0100.Cualquier datagrama que no contenga este valor será descartado. La versión 6 está actualmente en desarrollo.
- **HEADER LENGHT (HLEN):** es la longitud del header o encabezado medido en múltiplos de 32 bits. Lo normal es que este valor sea 5, ya que las opciones generalmente no se utilizan. En caso de que se utilicen, como son 4 bits, el valor puede llegar como máximo a 15. Este es el máximo encabezado posible
- **TYPE OF SERVICE:** está formado por 3 bits de **Priority** que pueden setearse desde 000 (mínima prioridad) a 111(máxima prioridad) y 3 bits individuales que son:: **D= Delay,T=Throughput, R=Reliability** solicitados.
- **TOTAL LENGHT:** longitud total del datagrama medido en octetos. Como son 16 bits , el máximo datagrama puede ser de 65532 bytes.
- **IDENTIFIER :** identifica al datagrama , es importante para la fragmentación.
- **FLAGS:** hay un bit no utilizado y otros que son **DF: Don´t Fragment** y **MF= More Fragments**
- **FRAGMENT:** numera los distintos fragmentos de un mismo grupo
- **TIME TO LIVE:** se decrementa al pasar por cada router. Cuando llega a cero se descarta . Es para evitar loops.
- **PROTOCOL:** identifica con una identificación numérica cuál es el protocolo de nivel superior
- **CHECKSUM :** chequeo de errores del Header solamente
- **SOURCE IP ADDRESS:** IP completa de origen
- **DESTINATION IP ADDRESS:** IP completa de destino
- **IP OPTIONS + PADDING:** no es obligatorio. El Padding es el relleno que completa los 32 bits.
- **USE DATA:** datos de la capa superior encapsulados

5.2.4 - Ruteo de datagramas IP

El tema **ruteo** es bastante complejo y requeriría un apartado independiente para su correcto desarrollo. Daremos aquí sólo una breve reseña.

Dijimos que un **Router** es un equipo de **Capa 3**, que se utiliza para interconectar distintas redes que deben ser del mismo tipo.
Utilizaremos **"red"** en el sentido estricto de la palabra, es decir en la definición que le da **TCP/IP**, que es el conjunto de equipos que tienen el mismo ***NetID.***
Podemos decir entonces que los **routers** interconectan distintas redes formando una **interred** o **Internet**, pero en sentido amplio, es decir, NO NECESARIAMENTE nos referimos a **"La Internet",** es decir la "red de redes" , por más que ésta sigue la misma filosofía.
Al estudio de la interconexión de distintas redes se lo denomina **"Internetworking".**

Volviendo al tema de los **Routers**, dijimos también que los mismos poseen distintas salidas o **puertos**, una para cada una de las redes a las que se conecta, con una **dirección IP** correspondiente a cada una de ellas.
Cada **Router** recibe datagramas por cualquiera de los puertos y lo redirecciona hacia otro. Éste corresponderá a otra red, que tendrá a su vez otro u otros **Routers** que realizan la misma operación. Ésta es la forma en que se arma la interred y los datagramas viajan a través de la misma.
Pero :¿cómo sábe un **Router** en qué dirección debe enviar los datagramas?
Bueno, obviamente no es en forma arbitraria, cada router sábe en qué dirección debe retransmitir la información. Esto es a que cada uno de estos equipos posee una tabla con información de las redes a las cuales se encuentra conectado directa o indirectamente cada puerto. Por lo tanto puede decidir por qué camino redirigir el datagrama.
Estas tablas se llaman **Tablas de Ruteo (Routing Tables)** y consan de 3 campos:

- Nro de **Puerto**
- **Red** (NetID y máscara de subred) a la que stá conectado
- Nro de routers o "**hops**" (saltos) que lo separan de dicha red

Existen 2 tipos de tablas de ruteo :

- **Estáticas:** poseen información que fue ingresada manualmente y permanece inalterable, es sólo útil en redes pequeñas.
- **Dinámicas:** se van actualizando automáticamente y "aprenden" las direcciones de las redes a las cuales se encuentran conectados. Obviamente los Routers que utilizan tablas dinámicas son más sofisticados ya que necesitan de cierta inteligencia y utilizan los llamados **"protocolos de ruteo"** para poder comunicarse con otros routers y "aprender" las direcciones de dichas redes.

Hay varios **protocolos de ruteo**, con características de funcionamiento bien diferenciadas.
Básicamente se pueden clasificar según su funcionamiento en 2 tipos:

- **Protocolos vectorizados por distancia:**
- **Protocolos por estado del enlace:**

Según la cobertura de las redes que interconectan los protocolos pueden ser **Internos** o **Externos**.

- **Protocolos de ruteo internos:** lo utilizan routers que interconectan redes dentro de una misma organización y bajo una misma administración, es decir dentro de sistemas autónomos.
Los más utilizados son:

- **RIP (Routing Information Protocol):** fue desarrolado por ***Xerox*** y fue pensado para interconectar LANs. Es vectorizado a distancia y no es apto para subredes. Se basa en buscar el mejor camino mediante la asignación de un "costo" a cada camino, en función del número de saltos (hops) que lo separan del destino.
- **IGRP (Interior Gateway Routing Protocol):** es también vectorizado a distancia. Lo introdujo ***Cisco*** pero actualmente lo incorporan también otros fabricantes.
- **OSPF (Open Shortest):** se ha popularizado últimamente para sitios Internet ya que es altamente eficiente e introduce bajo overhead lo que lo hace apto para redes de alta velocidad. Además soporta subredes y máscaras variables de subred. Posee un algoritmo que evita loops y es compatible con RIP y EGP.

- **Protocolos de ruteo externos:** o interdominio son para routers que unen redes distintas bajo distintas administraciones (por ejemplo **"Internet"**). Los más comunes son:

- **EGP (Exterior Gateway Protocol):** está pensado para solamente intercambiar información de accesibilidad de redes entre routers o gateways vecinos. No realiza cálculos de actualuización de ruta y no es apto para implementar topologías elaboradas.
- **BGP (Border Gateway Protocol):** mejora a EGP y permite encontrar la mejor ruta entre dos sistemas autónomos.

5.3 - TRANSMISSION CONTROL PROTOCOL (TCP)

El protocolo **TCP (Transmission Control Protocol)** , o **Servicio de Transporte de Flujo Confiable,** al igual que **UDP** es un protocolo de **Capa 4,** es decir de **Transporte**, pero, a diferencia de IP, es **Orientado a la**

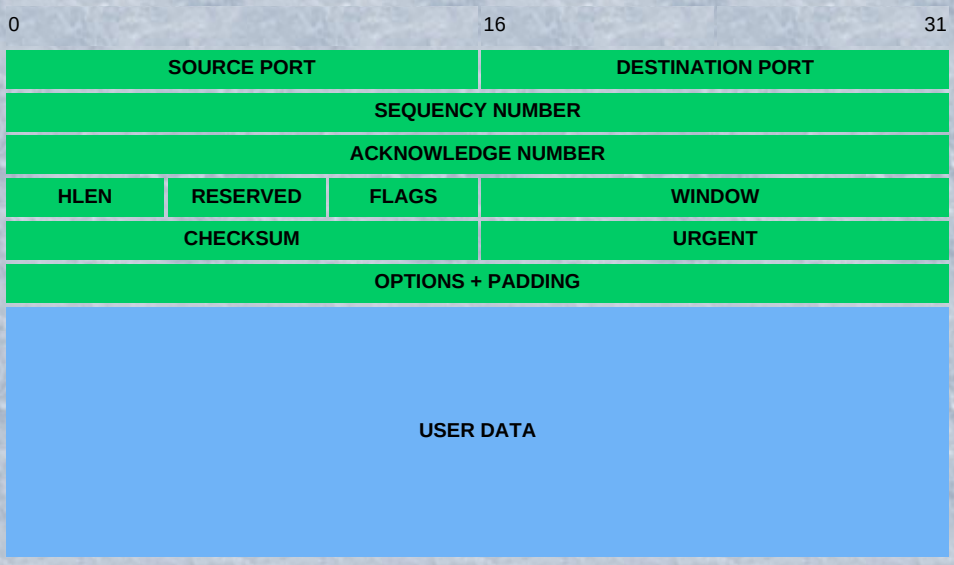
Conexión.
TCP es el encargado de asegurar un flujo de datos confiable entre los extremos de la red. Se encarga por lo tanto del control de flujo y del control de errores, tareas que no realiza IP.
Es uno de los protocolos más complejos de todo el stack TCP/IP.
Trabaja en modo *"string"* , es decir recibe cadenas de bits de las capas superiores y las arma en segmentos que luego son enviados a la capa IP.
Aparece el concepto de "**Port"** (Puerto), que es la entidad lógica que identifica los extremos de la comunicación.
Toda cominicación **TCP** se realiza entre puertos.
Una misma PC normalmente posee más de un puerto abierto simultáneamente.
Los números de puerto se asignan dinámicamente pero algunas aplicaciones poseen números predefinidos que se encuentran en el rango de 0 a 255. No se pueden crear puerto en este rango sino solamente para las aplicaciones predefinidas . Por ejemplo : FTP utiliza el puerto 21 , Telnet el 23 y SMTP el 25. Los puertos en este rango se llaman "**Well Known Ports".**
Cualquier aplicación que deba crear un puerto y no esté predefinida debe elegir un número fuera de este rango.

5.3.1 - Características de TCP

Las características del servicio de entrega confiable son las siguientes:

- **Orientación de flujo**
- **Conexión de circuito virtual**
- **Transferencia con memoria intermedia**
- **Flujo no estructurado**
- **Conexión Full Duplex**

5.3.2 - Segmento TCP



- **SOURCE PORT:** puerto de origen
- **DESTINATION PORT:** puerto de dertino
- **SEQUENCY NUMBER:** número de secuencia de la comunicación
- **ACKNOWLEDGE NUMBER:** número de acuse de recibo
- **HLEN:** longitud del header en múltiplos de 32 bits
- **FLAGS:** indicadores varios
- **WINDOW:** tamaño de la ventana
- **CHECKSUM:** chequeo de redundancia cíclica (CRC)
- **URGENT:** puntero al comienzo de los datos urgentes
- **OPTIONS + PADDING:** opciones varias y relleno
- **USER DATA:** datos de usuario

5.3.4 - Servicios que corren sobre TCP

A continuación se listan algunos de los protocolos de la capa **APPLICATION** que corren sobre **TCP** con sus correspondiente **números de puertos:**

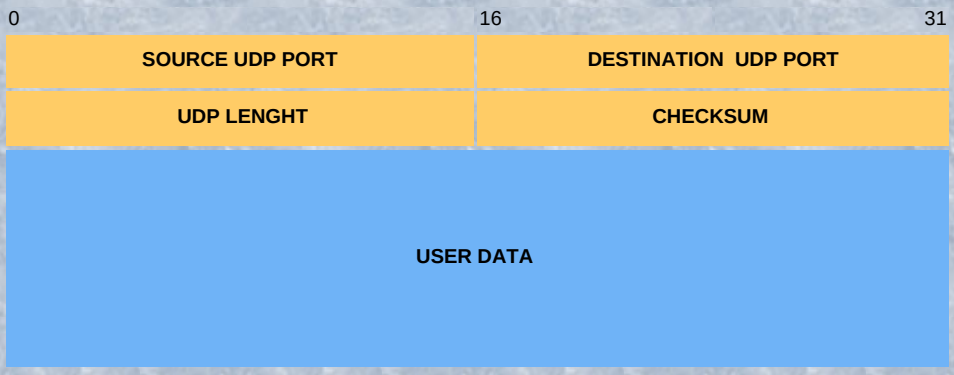
- **Port 21 : FTP**
- **Port 23 : TELNET**
- **Port 25: SMTP**

5.4 - USER DATAGRAM PROTOCOL (UDP)

El protocolo **UDP (User Datagram Protocol)** es, a diferencia de **TCP**, **no orientado a la conexión.** Es decir constituye la modalidad de entrega **no confiable**.
Emplea el **IP** para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos **(puertos)** dentro de un determinado host.
Es un servicio extremadamente simple y eso puede comprobarse viendo la sencillez de su Datagrama.

5.4.1 - El Datagrama UDP

UDP posee el siguente **Datagrama**, llamado **"Mensaje UDP".**



- **SOURCE UDP PORT:** Puerto de origen (opcional)
- **DESTINATION UDP PORT:** Puerto de destino
- **UDP LENGHT:** Longitud completa del Datagrama en octetos , contando el encabezado y los datos.
- **CHECKSUM:** Chequeo de redundancia cíclica (CRC)
- **USER DATA:** Datos de usuario

5.4.1 - Servicios que corren sobre UDP

A continuación se listan algunos de los protocolos de la capa **APPLICATION** que corren sobre **UDP** con sus correspondiente **números de puertos:**

- **Port 69 : TFTP**
- **Port 123 : NTP**
- **Port 161: SNMP**

* *Continuará*

Autor: ***Mariano López Figuerola***

Podés enviarme tus comentarios a: mlopezf@softhome.net
o ingresar a mi página: www.mlopezf.com.ar.

Bibliografía :

- **Redes de Computadores** . *Uyless Black* . Alfaomega . 1995
- **Frame Relay Networks** . *Uyless Black*. McGraw Hill . 1994
- **Computer Networks** . *Andrew Tanenbaum* . Prentice Hall . 1996
- **TCP/IP** . **Vol. 1** . *Douglas Comer* . Prentice Hall . 1996

Links recomendados:

- Frame Relay Forum
- Protocols .com

Otros trabajos del mismo autor :

- *Telefonía Móvil Satelital*
- *Osciloscopios Actuales*
- Página Personal: *Mariano López Figuerola*

Ud es el visitante Nro

Última actualización: 10 /08 /2003