# FUNDAMENTOS DE REDES Y ENRUTAMIENTO BÁSICO

**ALMANZA G, GUSTAVO E.**
**ARBELÁEZ A, LUIS F.**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**
**FACULTAD DE INGENIERÍA**
**PROGRAMA SISTEMAS**
**CARTAGENA**
**MAYO 2004**

# FUNDAMENTOS DE REDES Y ENRUTAMIENTO BÁSICO

**ALMANZA G, GUSTAVO E.**
**ARBELÁEZ A, LUIS F.**

**Monografía presentada para optar al**
**Título de Ingeniero de Sistemas**

**Director**
**ISAAC ZÚÑIGA SILGADO**
**Ingeniero de Sistemas**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**
**FACULTAD DE INGENIERÍA**
**PROGRAMA SISTEMAS**
**CARTAGENA**
**MAYO 2004**

## ARTICULO 107

La institución reserva el derecho de propiedad intelectual de todos los trabajos grupo aprobados, los cuales no pueden ser explotados comercialmente sin su autorización. Esta observación debe quedar impresa en parte visible del proyecto.

Cartagena, 28 de Mayo de 2004

Señores

**Universidad Tecnológica de Bolívar**

Comité de Evaluación de Proyectos

Ciudad

Apreciados Señores.

Cordialmente me permito informarles que he llevado a cabo la dirección del trabajo de grado de los estudiantes GUSTAVO ENRIQUE ALMANZA GÓMEZ y LUIS FERNANDO ARBELÁEZ AGUIRRE, titulado: “FUNDAMENTOS DE REDES Y ENRUTAMIENTO BÁSICO”.

Cordialmente,

_____

ISAAC ZÚÑIGA SILGADO

**AUTORIZACIÓN**

Cartagena de Indias, D. T. y C., Mayo 28 de 2004

Nosotros **GUSTAVO ENRIQUE ALMAZA GOMEZ** y **LUIS FERNANDO ARBELAEZ AGUIRRE**, identificados con números de cédula 73'185,766 de Cartagena y 80'103,111 de Bogotá, autorizamos a la **Universidad Tecnológica de Bolívar** para hacer uso de nuestro trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

_____ _____

GUSTAVO E. ALMANZA GOMEZ LUIS F. ARBELAEZ AGUIRRE

Cartagena, 28 de Mayo de 2004

Señores

**Universidad Tecnológica de Bolívar**

Comité de facultad de Ingeniería de Sistemas

Ciudad

Estimados Señores:

De la manera más atenta nos permitimos presentar a su consideración y aprobación el trabajo de grado titulado "FUNDAMENTOS DE REDES Y ENRUTAMIENTO BÁSICO". Elaborado por GUSTAVO ENRIQUE ALMANZA GÓMEZ y LUIS FERNANDO ARBELÁEZ AGUIRRE.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la universidad para los trabajos de grado.

Cordialmente,

_____ _____

GUSTAVO E. ALMANZA GÓMEZ LUIS F. ARBELÁEZ AGUIRRE

**Nota de Aceptación**

_____

_____

_____

_____

_____

_____

**Presidente del Jurado**

_____

**Jurado**

_____

**Jurado**

**CONTENIDO**

## LISTA DE TABLAS

**Pág.**

## LISTA DE FIGURAS

**Pág.**

# INTRODUCCIÓN

A medida que transcurre el tiempo podemos observar que las redes informáticas se hacen cada día más necesarias en todos los ámbitos de nuestra cotidianidad. Esta es una de las mayores razones por lo cual el estudio de las redes de comunicación ha obtenido una gran importancia en las ultimas décadas, hasta el punto de existir grandes areas de investigación acerca de este tema en reconocidas universidades y la creación de empresas dedicadas únicamente al estudio de redes. ¿Pero qué nos permite hacer una red de comunicación? Una red de comunicación nos brinda la posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas, cargar aplicaciones desde puntos de ultramar, enviar mensajes a otros países y compartir archivos, todo ello desde un computador personal.

Al realizar un estudio de las redes de comunicación hay que tener en cuenta que estas son un conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más computadoras. Los usuarios de una red

pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros computadores. [1]

Para conocer los objetivos de este trabajo, puede consultarlo en la carpeta PROPUESTA que aparece en el CD correspondiente a esta monografía.

---

[1] "Redes de comunicación," *Enciclopedia Microsoft® Encarta® 2000.* © 1993-1999 Microsoft Corporation. Reservados todos los derechos.

# CAPÍTULO UNO

## FUNDAMENTOS DE REDES DE COMUNICACIÓN

**1.1 GENERALIDADES Y CONCEPTOS BASICOS DE LAS LAN**

**1.2 TECNOLOGÍAS DE ENLACE DE DATOS DE LAS LAN**

**1.3 GENERALIDADES Y CONCEPTOS BASICOS DE LAS REDES MAN**

**1.4 GENERALIDADES REDES WAN Y ACCESO TELEFÓNICO**

**1.5 MEDIOS DE TRANSMISIÓN DE SERVICIOS DEDICADOS**

## 1.1 GENERALIDADES Y CONCEPTOS BÁSICOS DE LAS LAN

**Red de área local** (**LAN)**, conjunto de ordenadores que pueden compartir datos, aplicaciones y recursos (por ejemplo impresoras). Las computadoras de una red de área local (LAN, *Local Area Network*) están separadas por distancias de hasta unos pocos kilómetros, y suelen usarse en oficinas o campus universitarios. Una LAN permite la transferencia rápida y eficaz de información en el seno de un grupo de usuarios y reduce los costes de explotación. *Véase* Red (informática).

## 1.2 TECNOLOGÍAS DE ENLACE DE DATOS DE LAS LAN

La capa (2) de enlace de datos en el modelo OSI esta subdividida en dos subniveles:

**LLC** (Subcapa de Control del Enlace Lógico): ofrece al nivel de red un servicio de transmisión de datos entre máquinas adyacentes, encargándose de:

- Composición / Descomposición de tramas.
- Control de flujo (opcional).
- Gestión de los errores en la transmisión (opcional).

El protocolo LLC es derivado del protocolo de Alto nivel para Control de Enlaces de Datos (HDLC) y es similar en su operación, el LLC provee las direcciones de

Puntos de Acceso a Servicios (SAP's), mientras que la subcapa MAC provee la dirección física de red de un dispositivo. Las SAP's son específicamente las

direcciones de una o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

El LLC provee los siguientes servicios:

- Servicio orientado a la conexión, en el que una sesión es empezada con un Destino, y terminada cuando la transferencia de datos se completa. Cada nodo participa activamente en la transmisión, pero sesiones similares requieren un tiempo de configuración y monitoreo en ambas estaciones.
- Servicios de reconocimiento orientado a conexiones. Similares al anterior, del que son reconocidos los paquetes de transmisión.
- Servicio de conexión sin reconocimiento. En el cual no se define una sesión. Los paquetes son puramente enviados a su destino. Los protocolos de alto nivel son responsables de solicitar el reenvío de paquetes que se hayan perdido. Este es el servicio normal en redes de área local (LAN's), por su alta confiabilidad.

**MAC** (Subcapa de Control de Acceso al Medio): gobierna el acceso a un medio de transmisión compartido por varias máquinas.

### 1.2.1 IEEE 802.2. Control de Enlaces Lógicos

**IEEE Instituto de ingeniería eléctrica y electrónica (*Institute of Electrical and Electronic Engineers*) 802.2. Control de Enlaces Lógicos:** Define el protocolo de LAN que especifica una implementación del la subcapa de control de enlaces lógicos (LLC) de la capa de enlace de datos del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación,

manejando errores, entramados, control de flujo y la interfaz de servicio de la capa de red (capa 3). Este se utiliza en las LAN IEEE 802.3 e IEEE 802.5. [2]

### 1.2.2 IEEE 802.3 Tecnología Ethernet

**ETHERNET E IEEE 802.3:** Protocolo para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos, este protocolo es el más usado actualmente y define de la siguiente manera la operación del método de Acceso Múltiple con Detección de Colisiones (CSMA/CD) sobre varios medios.

El método CSMA/CD (*carrier sense multiple access with collision detect*) ejecuta tres funciones principales:

1. Transmitir y recibir paquetes de datos
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI
3. Detectar errores dentro de los paquetes de datos o en la red

En el método CSMA/CD, los dispositivos que tienen datos para transmitir a través de los medios funcionan según el modo "escuchar antes de transmitir". Esto significa que cuando un dispositivo desea enviar datos, primero debe verificar si los medios están ocupados. El dispositivo debe verificar si existen señales en los medios. Una vez que el dispositivo determina que los medios no están ocupados,

[2] http://www.eduangi.com

el dispositivo comienza a transmitir los datos. Mientras transmite los datos en forma de señales, el dispositivo también escucha. Esto lo hace para comprobar que no haya ninguna otra estación que esté transmitiendo datos a los medios al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escucha.[2]

Los dispositivos pueden detectar cuando se ha producido una colisión (daño en los datos de cada uno de los dispositivos que trato de enviar paquetes al mismo tiempo) porque aumenta la amplitud de la señal en el medio. Cuando se produce una colisión, cada dispositivo que está realizando una transmisión continúa transmitiendo datos durante un período breve. Esto se hace para garantizar que todos los dispositivos puedan detectar la colisión. Una vez que todos los dispositivos de una red detectan que se ha producido una colisión, cada dispositivo invoca algoritmos de *Backoff* que determinan cuándo podrán volver a transmitir las estaciones que entraron en colisión. Después de que todos los dispositivos de una red han sufrido una postergación durante un período determinado de tiempo (que es distinto para cada dispositivo), cualquier dispositivo puede intentar obtener acceso a los medios nuevamente. Cuando se reanuda la transmisión de datos en la red, los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

Ethernet es una tecnología de difusión o ***broadcast*** (Paquete de datos enviado a todos los nodos de una red, cuando se requiere información acerca de un

[2] http://www.eduangi.com

dispositivo específico) de medios compartidos, esto significa que todos los dispositivos de una red pueden ver todas las tramas en circulación en el medio sin importar el destino pretendido. Sin embargo, no todos los dispositivos de la red procesan los datos. Solamente el dispositivo cuya dirección MAC y cuya dirección IP concuerdan con la dirección MAC y la dirección IP destino que transportan los datos copiará los datos. Una vez que el dispositivo ha verificado las direcciones MAC e IP destino que transportan los datos, entonces verifica el paquete de datos para ver si hay errores y la trama se pasa hacia una capa de protocolo superior para continuar su procesamiento. Si el dispositivo detecta que hay errores, se descarta el paquete de datos. El dispositivo destino no enviará ninguna notificación al dispositivo origen, sin tener en cuenta si el paquete de datos ha llegado a su destino con éxito o no. Ethernet es una arquitectura de red no orientada a conexión considerada como un sistema de entrega de "máximo esfuerzo".

El estándar define la conexión de redes sobre cable coaxial, cable de par trenzado, y medios de fibra óptica. La tasa de transmisión original es de 10 Mbits/seg, pero existen implementaciones que transmiten arriba de los 100 Mbits/seg calidad de datos en cables de par trenzado, además, una nueva implementación de 1000 Mbits/seg en cable de par trenzado categoría 6.

Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT, y 10Broad36. Las variaciones físicas para Fast

Ethernet incluyen 100BaseTX y 100BaseFX. Variaciones para Gigaethernet 1000BaseT, 1000BaseTX. Las tecnologías se describen como 10Base2, 10BaseT, entre otros, donde el método de señalización es **Base** abreviación para **BandaBase,** aunque, también puede ser ***Broad*** que es una abreviación para **BandaAncha** y 10,100 entre otros es la capacidad de transmisión del medio, ya sea *Twisted Pair* (T) o fibra óptica (FX, FL) o cables coaxiales (2,5 longitud máxima del segmento en centenas de metros).

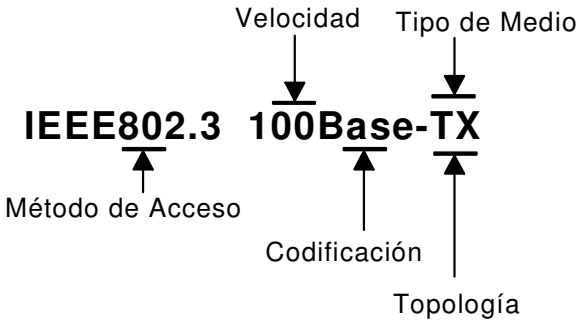



**Figura 1.** Significado de los estándares IEEE

Características más importantes de las tecnologías Ethernet

| Tecnologías | Velocidad de transmisión | Método señalización | Longitud máxima de segmento | Medio | Topología |
|---|---|---|---|---|---|
| **10BASE-2** | **10** | **BASE** | **185** | **coaxial 50 ohms** | **Bus** |
| **10BASE-5** | **10** | **BASE** | **500** | **coaxial 50 ohms** | **Bus** |
| **10BASE-T** | **10** | **BASE** | **100** | **UTP** | **Estrella** |
| **10BASE-FL** | **10** | **BASE** | **2000** | **FO Multimodo** | **Estrella** |
| **100BASE-TX** | **100** | **BASE** | **100** | **UTP Cat 5** | **Estrella** |
| **100BASE-LX** | **100** | **BASE** | **3000** | **FO Monomodo** | **Estrella** |
| **100BASE-FX** | **100** | **BASE** | **2000** | **FO Multimodo** | **Estrella** |
| **1000BASE-T** | **1000** | **BASE** | **100** | **UTP Cat 5** | **Estrella** |
| **1000BASE-TX** | **1000** | **BASE** | **100** | **UTP Cat 6** | **Estrella** |

**TABLA 1.** Características de la Ethernet

**Formato De Trama Ethernet**

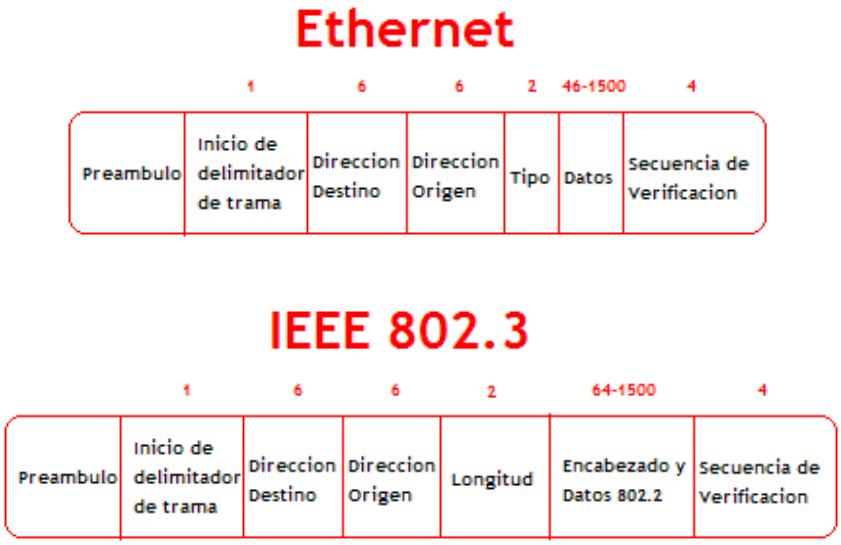



**Figura 2.** Formato de trama para Ethernet e IEEE 802.3

Los campos de trama Ethernet e IEEE 802.3 se describen en los siguientes resúmenes:

- *preámbulo*: El patrón de unos y ceros alternados les indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de trama (SOF) de la trama IEEE 802.3.

- *inicio de trama (SOF)*: El byte delimitador de IEEE 802.3 finaliza con dos bits 1 consecutivos, que sirven para sincronizar las porciones de recepción de trama de todas las estaciones de la LAN. SOF se especifica explícitamente en Ethernet.

- *direcciones destino y origen*: Los primeros 3 bytes de las direcciones son especificados por IEEE según el proveedor o fabricante. El proveedor de Ethernet o IEEE 802.3 especifica los últimos 3 bytes. La dirección origen siempre es una dirección *unicast* (de nodo único). La dirección destino puede ser *unicast*, *multicast* (grupo de nodos) o de *broadcast* (todos los nodos).

- *tipo (Ethernet)*: El tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

- *longitud (IEEE 802.3)*: La longitud indica la cantidad de bytes de datos que sigue este campo.

- *datos (Ethernet)*: Una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos contenidos en la trama se envían a un protocolo de capa superior, que se identifica en el campo tipo. Aunque la versión 2 de Ethernet no especifica ningún relleno, al contrario de lo que sucede con IEEE 802.3, Ethernet espera por lo menos 46 bytes de datos.

- *datos (IEEE 802.3)*: Una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos se envían a un protocolo de capa superior, que debe estar definido dentro de la porción de datos de la trama. Si los datos de la trama no son suficientes para llenar la trama hasta

una cantidad mínima de 64 bytes, se insertan bytes de relleno para asegurar que por lo menos haya una trama de 64 bytes.

- *secuencia de verificación de trama (FCS)*: Esta secuencia contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. [3]

### 1.2.3 IEEE 802.5 Tecnología Token Ring

**TOKEN RING E IEEE 802.5** También llamado ANSI 802.1-1985, Protocolo de LAN IEEE que especifica la implementación de la capa físicas y de la subcapa MAC de la capa de enlace de datos. Define los protocolos de acceso, cableado e *interface* para la LAN token ring. IBM *(Internacional Business Machines*) desarrollo e hizo popular este estándar. Usa un método de acceso de paso de tokens y es físicamente conectada en topología estrella, pero lógicamente forma un anillo. Token Ring usa un protocolo llamado *token capture* para conceder acceso al medio físico de la red. El protocolo Token Ring se ha implementado a dos velocidades: 4 Mbps y 16 Mbps en cableado STP O UTP y desde el punto de vista funcional y operacional es equivalente a token Ring de IBM.

Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens. Las redes de transmisión de tokens transportan una pequeña trama, denominada token, a través del anillo en sentido contrario a las manecillas del reloj. La posesión del token otorga el derecho a transmitir datos. Si un nodo que

[3] FORD, Merilee. Tecnologías de Interconectividad de Redes

captura el token no tiene información para enviar, transfiere el token a la siguiente estación terminal. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.

Cuando una estación que transfiere un token tiene información para transmitir, toma el token y le modifica 1 bit. El token se transforma en una secuencia de inicio de trama. A continuación, la estación agrega la información para transmitir al token y envía estos datos a la siguiente estación del anillo. No hay ningún token en la red mientras la trama de información gira alrededor del anillo, a menos que el anillo acepte envíos anticipados del token. En este momento, las otras estaciones del anillo no pueden realizar transmisiones. Deben esperar a que el token esté disponible. Las redes Token Ring no tienen colisiones. Si el anillo acepta el envío anticipado del token, se puede emitir un nuevo token cuando se haya completado la transmisión de la trama.[3]

La trama de información gira alrededor del anillo hasta que llega a la estación destino establecida, que copia la información para su procesamiento. La trama de información gira alrededor del anillo hasta que llega a la estación emisora y entonces se elimina. La estación emisora puede verificar si la trama se recibió y se copió en el destino.

[3] FORD, Merilee. Tecnologías de Interconectividad de Redes

En las redes Token Ring de 16 Mbps, el sistema fuente envía un *token* nuevo antes de recibir la trama de datos, usando una característica que se llama *early token release* (envío temprano de *token).*

Las redes de transmisión de tokens son determinísticas. Esto significa que se puede calcular el tiempo máximo que transcurrirá antes de que cualquier estación terminal pueda realizar una transmisión de una trama. Esta característica, y varias características de confiabilidad, hacen que las redes Token Ring sean ideales para las aplicaciones en las que cualquier demora deba ser predecible y en las que el funcionamiento sólido de la red sea importante. Los entornos de automatización de fábricas son ejemplos de operaciones de red que deben ser sólidas y predecibles. En algunas aplicaciones de redes, como las transacciones en tiempo real, este determinismo es un requisito importante para un protocolo de LAN.

Las redes Token Ring usan un sistema de prioridad sofisticado que permite que determinadas estaciones de alta prioridad designadas por el usuario usen la red con mayor frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad: el campo de *prioridad* y el campo de *reserva*.

Sólo las estaciones cuya prioridad es igual o superior al valor de prioridad que posee el token pueden tomar ese token. Una vez que se ha tomado el token y éste se ha convertido en una trama de información, sólo las estaciones cuyo valor de prioridad es superior al de la estación transmisora pueden reservar el token para el siguiente paso en la red. El siguiente token generado incluye la mayor prioridad de

la estación que realiza la reserva. Las estaciones que elevan el nivel de prioridad de un token deben restablecer la prioridad anterior una vez que se ha completado la transmisión.

Las redes Token Ring usan varios mecanismos para detectar y compensar las fallas de la red. Uno de los mecanismos consiste en seleccionar una estación de la red Token Ring como el monitor activo. Esta estación actúa como una fuente centralizada de información de temporización para otras estaciones del anillo y ejecuta varias funciones de mantenimiento del anillo. Potencialmente cualquier estación de la red puede ser la estación de monitor activo. Una de las funciones de esta estación es la de eliminar del anillo las tramas que circulan continuamente. Cuando un dispositivo transmisor falla, su trama puede seguir circulando en el anillo e impedir que otras estaciones transmitan sus propias tramas; esto puede bloquear la red. El monitor activo puede detectar estas tramas, eliminarlas del anillo y generar un nuevo token.

La topología en estrella de la red Token Ring de IBM también contribuye a la confiabilidad general de la red. Las *MSAU* (*unidades de acceso de estación múltiple*) activas pueden ver toda la información de una red Token Ring, lo que les permite verificar si existen problemas y, de ser necesario, eliminar estaciones del anillo de forma selectiva. *Beaconing*, una de las fórmulas Token Ring, detecta e intenta reparar las fallas de la red. Cuando una estación detecta la existencia de un problema grave en la red (por ejemplo, un cable roto), envía una *trama de beacon*. La trama de beacon define un *dominio de error*. Un dominio de error

incluye la estación que informa acerca del error, su *vecino corriente arriba activo más cercano (NAUN)* y todo lo que se encuentra entre ellos. El beaconing inicia un proceso denominado *autoreconfiguración*, en el que los nodos situados dentro del dominio de error automáticamente ejecutan diagnósticos. Este es un intento de reconfigurar la red alrededor de las áreas en las que hay errores. Físicamente, las MSAU pueden lograrlo a través de la reconfiguración eléctrica.

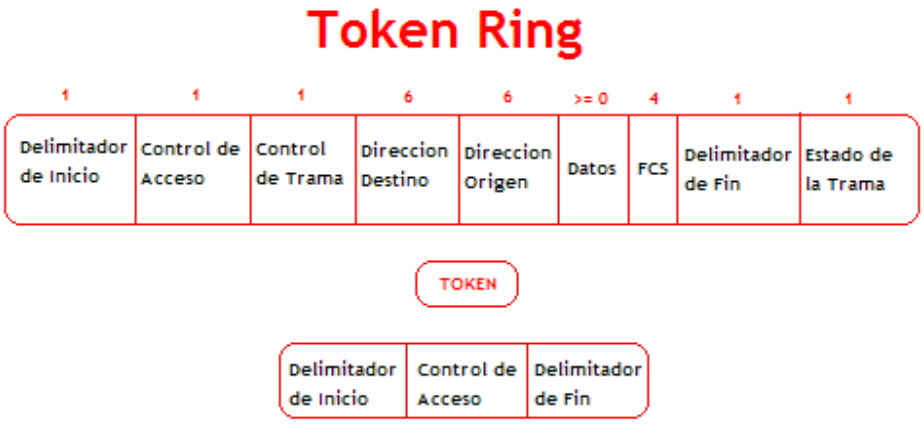



**Figura 3.** Formato de trama Token Ring

**Tokens** Los tokens tienen una longitud de 3 bytes y están formados por un *delimitador de inicio*, un *byte de control de acceso* y un *delimitador de fin*. El delimitador de inicio alerta a cada estación ante la llegada de un token o de una trama de datos/comandos. Este campo también incluye señales que distinguen al byte del resto de la trama al violar el esquema de codificación que se usa en otras partes de la trama.

**Byte de control de acceso** El byte de control de acceso contiene los campos de *prioridad* y de *reserva*, así como un bit de *token* y uno de *monitor*. El bit de token distingue un token de una trama de datos/comandos y un bit de monitor determina si una trama gira continuamente alrededor del anillo. El delimitador de fin señala el fin del token o de una trama de datos/comandos. Contiene bits que indican si hay una trama defectuosa y una trama que es la última de una secuencia lógica.

**Tramas datos/comandos** El tamaño de las tramas de datos/comandos varía según el tamaño del campo de información. Las tramas de datos transportan información para los protocolos de capa superior; las tramas de instrucciones contienen información de control y no poseen datos para los protocolos de capa superior.

En las tramas de datos o instrucciones hay un *byte de control de trama* a continuación del byte de control de acceso. El byte de control de trama indica si la trama contiene datos o información de control. En las tramas de control, este byte especifica el tipo de información de control.

A continuación del byte de control de trama hay dos campos de dirección que identifican las estaciones destino y origen. Como en el caso de IEEE 802.5, la longitud de las direcciones es de 6 bytes. El campo de datos está ubicado a continuación del campo de dirección. La longitud de este campo está limitada por el token de anillo que mantiene el tiempo, definiendo de este modo el tiempo máximo durante el cual una estación puede retener al token.

A continuación del campo de datos se ubica el campo de *secuencia de verificación de trama (FCS)*. La estación origen completa este campo con un valor calculado según el contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado mientras estaba en tránsito. Si la trama está dañada se descarta. Como en el caso del token, el delimitador de fin completa la trama de datos/comandos.

### 1.2.4 Estándar FDDI

**FDDI (Interfaz de datos distribuida por fibra - *fiber distributed data interface*)** la comisión normalizadora ANSI X3T9.5 creó el estándar **FDDI,** basado en el protocolo token ring 802.5, pero en vez de utilizar una arquitectura de un solo anillo, usa un anillo de fibra dual que transmite datos en direcciones opuestas. En la actualidad las implementaciones de la FDDI no son tan comunes como Token Ring o menos como Ethernet, la FDDI tiene muchos seguidores y continúa creciendo a medida que su costo disminuye. La FDDI se usa con frecuencia como una tecnología *backbone* y para conectar los computadores de alta velocidad en una LAN.[3]

FDDI tiene cuatro especificaciones:

1. *Control de acceso al medio (MAC)*: Define la forma en que se accede al medio, incluyendo:

[3] FORD, Merilee. Tecnologías de Interconectividad de Redes

- formato de trama
- tratamiento del token
- direccionamiento
- algoritmo para calcular una verificación por redundancia cíclica y mecanismos de recuperación de errores

2. *Protocolo de capa física (PHY)*: define los procedimientos de codificación o decodificación, incluyendo:

    - requisitos de reloj
    - entramado
    - otras funciones

3. *Medio de capa física (PMD)*: Define las características del medio de transmisión, incluyendo:

    - enlace de fibra óptica
    - niveles de potencia
    - tasas de error en bits
    - componentes ópticos
    - conectores

4. *Administración de estaciones(SMT)*: define la configuración de la estación FDDI, incluyendo:

- configuración del anillo
- características de control del anillo
- inserción y eliminación de una estación
- inicialización
- aislamiento y recuperación de fallas
- programación
- recopilación de estadísticas

FDDI utiliza una estrategia de transmisión de tokens similar a la de Token Ring. Las redes de transmisión de tokens transportan una pequeña trama, denominada token, a través de la red. La posesión del token otorga el derecho de transmitir datos. Si un nodo que recibe un token no tiene información para enviar, transfiere el token a la siguiente estación terminal. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.

Cuando una estación que retiene el token tiene información para transmitir, toma el token y modifica uno de sus bits. El token se transforma en una secuencia de inicio de trama. A continuación, la estación agrega la información para transmitir al token y envía estos datos a la siguiente estación del anillo.

No hay ningún token en la red mientras la trama de información gira alrededor del anillo, a menos que el anillo soporte el envío anticipado del token. Las demás estaciones del anillo deben esperar a que el token esté disponible. No se

producen colisiones en las redes FDDI. Si se soporta el envío anticipado del token, se puede emitir un nuevo token cuando se haya completado la transmisión de la trama.

La trama de información gira alrededor del anillo hasta que llega a la estación destino, que copia la información para su procesamiento. La trama de información gira alrededor del anillo hasta que llega a la estación emisora y entonces se elimina. La estación emisora puede verificar en la trama que retorna si la trama se recibió y se copió en el destino.

Las redes de transmisión de tokens son determinísticas. Esto significa que se puede calcular el tiempo máximo que transcurrirá antes de que cualquier estación terminal pueda realizar una transmisión. Los anillos dobles de la FDDI garantizan no sólo que cada estación tenga asegurado su turno para transmitir, sino también que, si alguna parte de uno de los anillos se daña o desactiva por algún motivo, se pueda recurrir al segundo anillo o anillo de respaldo. Esto hace que FDDI sea muy confiable.

La FDDI acepta la asignación en tiempo real del ancho de banda de la red, lo que la hace ideal para varios tipos de aplicación. La FDDI proporciona esta ayuda mediante la definición de dos tipos de tráfico: síncrono y asíncrono.

**Síncrono**

- El tráfico síncrono puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.
- El ancho de banda síncrono se asigna a las estaciones que requieren una capacidad de transmisión continua. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas.
- La especificación SMT de FDDI define un esquema de subasta distribuida para asignar el ancho de banda de FDDI.

**Asíncrono**

- El ancho de banda asíncrono se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.
- FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.
- El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda síncrono y que tienen una prioridad asíncrona demasiado baja.

**MEDIOS FDDI**

- FDDI especifica una LAN de anillo doble de 100 Mbps (al igual que fast ethernet) con transmisión de tokens, que usa un medio de transmisión de fibra óptica. Define la capa física y la porción de acceso al medio de la capa de enlace, que es semejante al IEEE 802.3 y al IEEE 802.5 en cuanto a su relación con el modelo OSI. Aunque funciona a velocidades más altas, la FDDI es similar al Token Ring. Ambas configuraciones de red comparten ciertas características, tales como su topología (anillo) y su método de acceso al medio (transferencia de tokens). Una de las características de FDDI es el uso de la fibra óptica como medio de transmisión.

FDDI especifica el uso de anillos dobles para las conexiones físicas. El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de la FDDI se conocen como primario y secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.

Las estaciones Clase B, o *estaciones de una conexión (SAS),* se conectan a un anillo, mientras que las de Clase A, o *estaciones de doble conexión(DAS),* se conectan a ambos anillos. Las SAS se conectan al anillo primario a través de un concentrador que suministra conexiones para varias SAS. El concentrador garantiza que si se produce una falla o interrupción en el suministro de

alimentación en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando se conectan al anillo PC o dispositivos similares que se encienden y se apagan con frecuencia. En la figura 2. se muestra una configuración FDDI típica que cuenta tanto con DAS como con SAS. Cada DAS de FDDI tiene dos puertos, designados como A y B. 3Estos puertos conectan las estación al anillo FDDI doble; por lo tanto, cada puerto proporciona una conexión tanto para el anillo primario como para el secundario

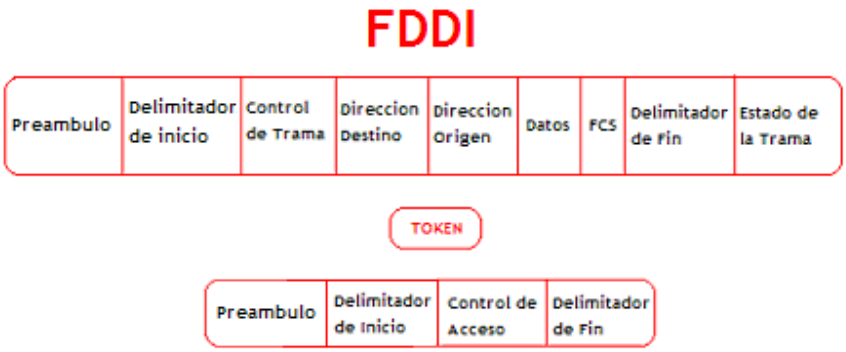



**Figura 4.** Formato de trama FDDI

Los campos de una trama FDDI son los siguientes:

- *preámbulo*: Prepara cada estación para recibir la trama entrante
- d*elimitador de inicio*: indica el comienzo de una trama, y está formado por patrones de señalización que lo distinguen del resto de la trama
- *control de trama*: indica el tamaño de los campos de dirección, si la trama contiene datos asíncronos o síncronos y otra información de control

- *dirección destino*: contiene una dirección *unicast* (singular), *multicast* (grupal) o *broadcast* (toda estación); las direcciones destino tienen 6 bytes (por ejemplo, Ethernet y Token Ring)
- *dirección origen*: identifica la estación individual que envió la trama. Las direcciones origen tienen 6 bytes (como Ethernet y Token Ring)
- *datos*: información de control, o información destinada a un protocolo de capa superior
- *secuencia de verificación de trama (FCS)*: la estación origen la completa con una verificación por redundancia cíclica (CRC) calculada, cuyo valor depende del contenido de la trama (como en el caso de Token Ring y Ethernet). La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado durante el tránsito. La trama se descarta si está dañada.
- *delimitador de fin*: contiene símbolos que no son datos que indican el fin de la trama

*estado de la trama*: permite que la estación origen determine si se ha producido un error y si la estación receptora reconoció y copió la trama.

## 1.3 GENERALIDADES Y CONCEPTOS BÁSICOS DE LAS REDES MAN

**1.3.1 IEEE 802.6 *Redes de Área Metropolitana (MAN).*** Define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuida (DQDB). El bus dual provee tolerancia de fallos para mantener las conexiones si el

bus se rompe. El estándar MAN esta diseñado para proveer servicios de datos, voz y vídeo en un área metropolitana de aproximadamente 50 kilómetros a tasas de 1.5, 45, y 155 Mbits/seg. DQDB es el protocolo de acceso subyacente para el SMDS (Servicio de Datos de Multimegabits Switcheados), en el que muchos de los portadores públicos son ofrecidos como una manera de construir redes privadas en áreas metropolitanas. El DQDB es una red repetidora que switchea celdas de longitud fija de 53 bytes; por consiguiente, es compatible con el Ancho de Banda ISDN y el Modo de Transferencia Asíncrona (ATM). Las celdas son switcheables en la capa de Control de Enlaces Lógicos.

Los servicios de las MAN son Sin Conexión, Orientados a Conexión, y/o isócronas (vídeo en tiempo real). El bus tiene una cantidad de slots de longitud fija en el que son situados los datos para transmitir sobre el bus. Cualquier estación que necesite transmitir simplemente sitúa los datos en uno o más slots. Sin embargo, para servir datos isócronos, los slots en intervalos regulares son reservados para garantizar que los datos llegan a tiempo y en orden.

## 1.4 GENERALIDADES REDES WAN Y ACCESO TELEFÓNICO

Una forma de ampliar una LAN es por medio de redes de mayor envergadura llamadas redes de área amplia (WAN) donde el servicio telefónico y de datos juega un papel fundamental en la estructura de la red. Casi todos los operadores de redes nacionales (como DBP en Alemania, British Telecom en Inglaterra o la Telefónica en España) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad

que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como *frame relay* y *SMDS-Synchronous Multimegabit Data Service*) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad se suelen denominar conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

### 1.4.1 Protocolo PPP

**Point To Point Protocol – Protocolo Punto A Punto:** protocolo abierto para trabajar con varios protocolos de la capa de red. Se puede considerar como la versión no patentada de HDLC (de propietario ***cisco systems***), aunque son diferentes. [4]

El protocolo Funciona en encapsulación sincrona y asíncrona, debido a que utiliza un indicador para indicar el inicio y final de una trama, en encapsulaciones asíncronas y se usa como una encapsulación sincrona orientada a bit.

PPP es el protocolo WAN más popular y más ampliamente utilizado porque ofrece todas estas funciones:

- Control de la configuración del enlace de datos
- Proporciona asignación dinámica de direcciones IP
- Multiplexión de protocolo de red

[4] http://www.cisco.com

- Configuración de enlace y verificación de la calidad del enlace
- Detección de errores
- Opciones de negociación para destrezas tales como negociación de la dirección de capa de red y negociaciones de compresión de datos

Los problemas de conectividad de Internet PPP busca resolverlos basándose en tres componentes:

- Un método para encapsular datagramas a través de enlaces seriales. PPP utiliza el Control de enlace de datos de alto nivel (HDLC) como base para encapsular datagramas a través de enlaces punto a punto.
- Un Protocolo de control de enlace (LCP) para establecer, configurar y probar la conexión de enlace de datos.
- Una familia de Protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de capa de red. En la actualidad, PPP soporta otros protocolos además de IP, incluyendo Intercambio de paquetes de internetworking (IPX) y Appletalk. Como se indica en la figura, PPP utiliza su componente de NCP para encapsular múltiples protocolos.

PPP utiliza una arquitectura dividida en capas. Con sus funciones de nivel inferior, PPP puede utilizar:

- Medios físicos síncronos, como los que conectan las redes de la Red digital de servicios integrados (RDSI).

- Medios físicos asíncronos, como los que utilizan el servicio telefónico básico para las conexiones de acceso telefónico del módem.

Mediante sus funciones de nivel superior, PPP soporta o encapsula varios protocolos de capa de red con los NCP. Estos protocolos de nivel superior incluyen los siguientes:

- BCP - Protocolo de control de puente
- IPCP - Protocolo de control de protocolo Internet
- IPXCP - Protocolo de control de intercambio de paquetes de internetworking
- ATALKCP - funciona a través de PPP para AppleTalk.

Estos son campos funcionales que contienen códigos estandarizados que indican el tipo de protocolo de capa de red que encapsula PPP.

Formato trama PPP:

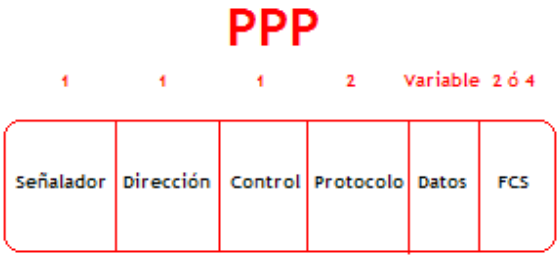



**Figura 5.** Formato de trama PPP

Como se indica en la figura, los campos de una trama PPP son los siguientes:

- Señalador: Indica el comienzo o el fin de una trama y está formado por la secuencia binaria 01111110.

- Dirección: Está formada por la dirección de broadcast estándar, que es la secuencia binaria 11111111. PPP no asigna direcciones de estaciones individuales.
- Control: 1 byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos del usuario en una trama no secuencial. Se suministra un servicio de enlace no orientado a conexión similar al del Control de enlace lógico (LLCC) de Tipo 1.
- Protocolo: 2 bytes que identifican el protocolo encapsulado en el campo de datos de la trama.
- Datos: 0 o más bytes que contienen el datagrama para el protocolo especificado en el campo de protocolo. El fin del campo de datos se detecta ubicando la secuencia de cierre del señalador y dejando 2 bytes para el campo de la secuencia de verificación de trama (FCS). La longitud máxima por defecto del campo de datos es 1.500 bytes.
- FCS: Por lo general, 16 bits (2 bytes). Se refiere a los caracteres adicionales que se agregan a una trama para fines de control de errores.

PPP suministra un método para establecer, configurar, mantener y terminar una conexión punto a punto. Para establecer comunicaciones a través de un enlace punto a punto, PPP atraviesa cuatro fases distintas:

- Establecimiento del enlace y negociación de la configuración: Un nodo PPP origen envía tramas LCP para configurar y establecer el enlace de datos.

- Determinación de la calidad del enlace: El enlace se prueba para determinar si la calidad del enlace es suficiente para establecer los protocolos de capa de red. Tenga en cuenta que esta es una fase opcional.
- Negociación de la configuración del protocolo de capa de red: El nodo PPP origen envía tramas NCP para seleccionar y configurar los protocolos de capa de red. Se configuran los protocolos de capa de red seleccionados (como IP, Novell IPX y AppleTalk) se configuran y se pueden enviar los paquetes desde cada protocolo de capa de red.
- Terminación del enlace: El enlace permanece configurado para la comunicación hasta que las tramas LCP o NCP cierran el enlace o hasta que se produzca algún hecho externo (por ejemplo, el vencimiento de un temporizador de inactividad o la intervención de un usuario).

Hay tres clases de tramas LCP:

- Tramas de establecimiento de enlace: Se utilizan para establecer y configurar un enlace.
- Tramas de terminación del enlace: Se utilizan para terminar un enlace.
- Tramas de mantenimiento del enlace: Se utilizan para administrar y depurar un enlace.

Las tramas LCP se utilizan para cumplir con el trabajo de cada una de las fases LCP: (1) Establecimiento del enlace; (2) Calidad del enlace; (3) Protocolo de capa de red; (4) Terminación del enlace. Estas fases se describen en las secciones siguientes.

**Fase 1, Establecimiento del enlace y negociación de la configuración:**

En esta fase, cada dispositivo PPP envía paquetes LCP para configurar y establecer el enlace de datos. Los paquetes LCP contienen un campo de opción de configuración que permite que los dispositivos negocien el uso de opciones, como la unidad máxima de transmisión (MTU), la compresión de determinados campos PPP y el protocolo de autenticación de enlace. Si no se incluye ninguna opción de configuración en un paquete LCP, se adopta el valor por defecto para esa configuración.

Antes de que se pueda intercambiar cualquier datagrama de capa de red (por ejemplo, IP), LCP primero debe abrir la conexión y negociar los parámetros de configuración. Esta fase se completa cuando se ha enviado y recibido una trama de acuse de recibo de configuración.

**Fase 2, Determinación de la calidad del enlace:**

LCP permite una fase opcional de determinación de la calidad del enlace a continuación de la fase de establecimiento del enlace y negociación de la configuración. En la fase de determinación de la calidad del enlace, el enlace se prueba para determinar si la calidad del enlace es lo suficientemente buena como para establecer los protocolos de capa de red.

Además, una vez que se ha establecido el enlace y que se ha elegido el protocolo de autenticación, se puede autenticar la estación de trabajo del cliente o usuario. La autenticación, en caso de que se utilice, se lleva a cabo antes de que comience

la fase de configuración del protocolo de la capa de red. LCP puede retardar la transmisión de la información del protocolo de la capa de red hasta que esta fase se haya completado.

PPP soporta dos protocolos de autenticación: Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación de saludo (CHAP). Ambos protocolos se describen en detalle en RFC 1334, "Protocolos de autenticación PPP". Estos protocolos se describen posteriormente en este capítulo en la sección "Autenticación PPP".

**Fase 3, Negociación de la configuración del protocolo de la capa de red:** Cuando LCP finaliza la fase de determinación de la calidad del enlace, los protocolos de capa de red pueden ser configurados individualmente por el NCP adecuado y se pueden activar y desactivar en cualquier momento.

En esta fase, los dispositivos PPP envían paquetes NCP para seleccionar y configurar uno o varios protocolos de capa de red (como IP). Cuando se ha configurado uno de los protocolos de capa de red elegidos, se pueden enviar datagramas desde cada uno de los protocolos de capa de red a través del enlace. Si LCP cierra el enlace, informa esto a los protocolos de la capa de red, de modo que puedan tomar las medidas adecuadas. Cuando PPP está configurado, puede verificar el estado de LCP y NCP utilizando el comando **show interfaces**.[5]

[5] CHAPPELL, Laura. Advanced Cisco Router Configuration.

**Descripción de la fase 4, Terminación del enlace:**

LCP puede terminar el enlace en cualquier momento. Esto generalmente se realiza a pedido del usuario, pero puede ocurrir debido a un suceso físico, como la pérdida de una portadora o la expiración de un límite de tiempo.

**Autenticación PPP**

**PAP**

La fase de autenticación de una sesión PPP es opcional. Una vez que se ha establecido el enlace, y que se ha seleccionado el protocolo de autenticación, se puede autenticar el igual. La autenticación, en caso de que se utilice, se lleva a cabo antes de que comience la fase de configuración del protocolo de la capa de red. Las opciones de autenticación requieren que la parte del enlace que realiza la llamada introduzca información de autenticación para ayudar a garantizar que el usuario cuenta con el permiso del administrador de red para realizar la llamada. Los routers iguales intercambian mensajes de autenticación.

Al configurar la autenticación PPP, puede seleccionar el protocolo de autenticación de contraseña (PAP) o el protocolo de autenticación de saludo de llamada (CHAP). En general, el protocolo preferido es CHAP.

PAP ofrece un método simple para que un nodo remoto establezca su identidad, utilizando el saludo de dos vías. Una vez que se completa la fase de establecimiento del enlace PPP, el nodo remoto envía un par de nombre de

usuario/contraseña de forma reiterada a través del enlace hasta que se acusa recibo de la autenticación o la conexión se termina.

PAP no es un protocolo de autenticación sólido. Las contraseñas se envían a través del enlace en texto no cifrado, y no hay protección contra la reproducción o los ataques reiterados de ensayo y error. El nodo remoto tiene control de la frecuencia y la temporización de los intentos de conexión.

CHAP se utiliza para verificar periódicamente la identidad del nodo remoto, utilizando un saludo de tres vías, tal como se indica en la figura. Esto se realiza durante el establecimiento inicial del enlace y se puede repetir en cualquier momento una vez que se ha establecido el enlace. CHAP ofrece funciones tales como verificación periódica para mejorar la seguridad. Esto hace que CHAP sea más efectivo que PAP. PAP realiza la verificación sólo una vez, lo que lo hace vulnerable a los "hackers" y a la reproducción por módem. Además, PAP permite que la persona que realiza la llamada intente realizar la autenticación a voluntad (sin antes recibir un pedido de verificación), lo que lo hace vulnerable a los ataques, mientras que CHAP no permite que la persona que realiza la llamada intente realizar la autenticación sin recibir un pedido de verificación.

Una vez que se ha completado la fase de establecimiento del enlace PPP, el host envía un mensaje de comprobación al nodo remoto. El nodo remoto responde con un valor. El host compara el valor de la respuesta con su propio valor. Si los valores concuerdan, se produce un acuse de recibo de la autenticación. De otro modo, la conexión se termina.

CHAP suministra protección contra los intentos de reproducción a través del uso de un valor de comprobación variable que es exclusivo e impredecible. El uso de comprobaciones reiteradas tiene como fin limitar el tiempo de exposición ante cualquier ataque único. El router local (o un servidor de autenticación de terceros, como Netscape Commerce Server) tiene el control de la frecuencia y la temporización de las señales.

### 1.4.2 Estándar FRAME RELAY

**Frame Relay,** es un estándar del Comité Consultivo Internacional Telegráfico y Telefónico (CCITT) y del Instituto Nacional Americano de Normalización (ANSI) que define un proceso para el envío de datos a través de una red de datos públicos (PDN). FR se desarrollo inicialmente para su uso en INTERFACES RDSI, las propuestas iniciales de este protocolo se presentaron en el comité CCITT en 1984. Aunque el estándar ya existía, había problemas con la interoperabilidad entre los fabricantes, porque la tecnología recibió poco apoyo por parte de la industria hasta finales de los ochenta.

FR es una tecnologia eficiente y elevado desempeño para enviar información a través de una WAN dividiendo los datos en paquetes. Cada paquete viaja a través de una serie de dispositivos en una red FR para alcanzar su destino. Esta opera en la capa física y de enlace de datos del modelo OSI, pero depende de los protocolos de capa superior como TCP para la corrección de errores.

Actualmente, FR es un protocolo de switching de paquetes de la capa de enlace de datos, de estándar industrial, que maneja circuitos virtuales PVC (circuito virtual permanente) y SVC (circuito virtual conmutado, aunque PVC es más usado) mediante el encapsulamiento de Control de Enlace de Datos de Alto Nivel (HDLC) entre los dispositivos conectados. FR utiliza circuitos virtuales para realizar conexiones a través de un servicio orientado a conexión.

FR utiliza la configuración de llamada, transferencia de datos y proceso de terminación de llamada. Los dispositivos finales, realizan las llamadas a través de la red FR, una vez establecida la llamada, el dispositivo traslada los datos y da por finalizada la llamada.

La red que proporciona la interfaz FR puede ser una red pública proporcionada por una portadora o una red de equipos privados, que sirven a una misma empresa. Una red FR puede componerse de computadores, servidores, etc. en el extremo del usuario y por dispositivos de red FR como switches, routers, CSU/DSU, o multiplexores. Como ha aprendido, con frecuencia se hace referencia a los dispositivos del usuario como Equipo Terminal de Datos (DTE), mientras que el equipo de red que hace interfaz con el DTE se conoce a menudo como Equipo de Transmisión de Datos (DCE),

Este protocolo utiliza identificadores de conexión de enlace de datos (DLCI), lo habitual es que estas direcciones tengan importancia local pero también pueden tener importancia global en toda la red. Un dispositivo puede usar la misma

dirección DLCI en cada lado de un circuito virtual, ya que FR asigna un numero DLCI local a un circuito virtual en cada Switch de la LAN.

FR se puede utilizar como interfaz para un servicio ofrecido por portadora disponible públicamente o para una red con equipo de propiedad privada. Se puede implementar un servicio FR público colocando el equipo de conmutación FR en la oficina central de una portadora de telecomunicaciones. En este caso, los usuarios obtienen beneficios económicos implícitos en tarifas sensibles al tráfico y no tienen que invertir tiempo y esfuerzo para administrar y mantener el equipo y el servicio de red.

No existe ningún estándar en la actualidad para la conexión cruzada de equipo dentro de una red FR. Por lo tanto, el soporte de las interfaces FR no necesariamente implica que se deba utilizar el protocolo FR entre los servicios de red. De esta manera, se puede utilizar la conmutación por circuito tradicional, la conmutación por paquetes o un enfoque híbrido que combine estas tecnologías.

Las líneas que conectan los dispositivos de usuario al equipo de red pueden operar a una velocidad seleccionada de una amplia gama de velocidades de transmisión de datos. Las velocidades entre 56 kbps y 2 Mbps son típicas, aunque FR puede soportar velocidades inferiores y superiores.

Como interfaz entre el equipo del usuario y de red, FR proporciona un medio para realizar la multiplexión de varias conversaciones de datos lógicas, denominadas circuitos virtuales, a través de un medio físico compartido asignando DLCI a cada par de dispositivos DTE/DCE.

La multiplexión FR permite un uso más flexible y eficiente del ancho de banda disponible. Por lo tanto, FR permite a los usuarios compartir el ancho de banda a un costo reducido. Por ejemplo, supongamos que tiene una WAN que utiliza FR y que FR es equivalente a un grupo de rutas. La compañía telefónica generalmente es propietaria de las rutas y está a cargo de su mantenimiento. Puede elegir arrendar la ruta exclusivamente para su empresa (dedicada), o bien puede pagar menos para arrendar una ruta compartiéndola con otras empresas. Por supuesto, FR también se puede ejecutar totalmente en redes privadas; sin embargo, rara vez se utiliza de esta manera.

Los estándares FR direccionan PVC que se encuentran administrativamente configurados y administrados en una red FR. Los PVC de FR son identificados por los DLCI. Es decir que los valores en sí no son únicos en la WAN FR. Dos dispositivos DTE conectados por un circuito virtual podrían utilizar un valor DLCI distinto para referirse a la misma conexión.

FR proporciona un medio para realizar la multiplexión de varias conversaciones de datos lógicas. El equipo de conmutación del proveedor de servicios genera una tabla asignando los valores DLCI a puertos salientes. Cuando se recibe la trama, el dispositivo de conmutación analiza el identificador de conexión y entrega la trama al puerto saliente asociado. La ruta completa al destino se establece antes de enviar la primera trama

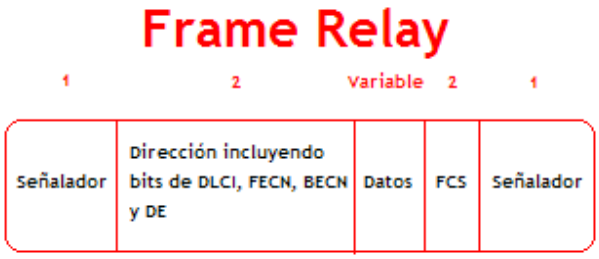



**Figura 6.** Formato de trama Frame Relay

Formato de trama FR:

- Indicador: Indica el principio y el final de la trama FR
- Dirección: Indica la longitud del campo de dirección Aunque las direcciones FR son actualmente todas de 2 bytes de largo, los bits de Dirección ofrecen la posibilidad de extender las longitudes de las direcciones en el futuro. El octavo bit de cada byte de campo Dirección se utiliza para indicar la dirección. La Dirección contiene la siguiente información:
    - Valor DLCI: Indica el valor de DLCI. Consiste en los 10 primeros bits del campo Dirección.
    - Control de congestión: Los últimos 3 bits del campo de dirección, que controlan los mecanismos de notificación de congestión FR. Estos son FECN, BECN y bits posibles para descarte (DE)
- Datos: Campo de longitud variable que contiene datos de la capa superior encapsulados.
- FCS: Secuencia de verificación de trama (FCS), utilizada para asegurar la integridad de los datos transmitidos.

**Interfaz de administración local (LMI)**

En 1990 se produjo un avance importante en la historia de FR, cuando Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation se reunieron para concentrarse en el desarrollo de la tecnología FR y acelerar la introducción de productos FR interoperables. Este grupo desarrolló una especificación conforme al protocolo FR básico, pero extendiéndolo con funciones que proporcionaban capacidades adicionales para entornos de internetworking complejos. Estas extensiones de FR se conocen como LMI La cual permite que los dispositivos DTE se comuniquen con los DCE e intercambien la información que se utiliza para pasar el tráfico de interconexión de red a través de una WAN de FR.

Las principales funciones del proceso LMI son las siguientes:

- Determinar el estado operacional de distintos PVC que el router conoce.
- Transmitir paquetes de mensaje de actividad para garantizar que el PVC permanezca activo y no se inhabilite por inactividad
- Comunicarle al router que los PVC están disponibles

El router puede invocar tres tipos de LMI: **ansi**, **cisco** y **q933a**.

**Extensiones LMI**

Además de las funciones básicas del protocolo FR para realizar la transferencia de datos, la especificación FR incluye extensiones LMI que permiten soportar más fácilmente internetworks grandes y complejas. Algunas extensiones LMI se

denominan comunes y se espera que todos los que adopten la especificación puedan implementarla. Otras funciones LMI se consideran opcionales A continuación, presentamos un resumen de las extensiones LMI:

- Mensajes de estado de circuito virtual (común): Proporcionan comunicación y sincronización entre la red y el dispositivo de usuario, informando periódicamente acerca de la existencia de nuevos PVC y la eliminación de PVC existentes, y brindando información general acerca de la integridad del PVC. Los mensajes de estado de circuito virtual evitan el envío de datos a través de PVC que ya no existen.
- Multicast (opcional): Permite al emisor transmitir una sola trama pero que sea entregada por la red a múltiples receptores. Así, el multicast soporta la distribución eficiente de mensajes de protocolo de enrutamiento y protocolos de resolución de direcciones que normalmente se deben enviar a varios destinos simultáneamente.
- Direccionamiento global (opcional): Otorga a los identificadores de conexión significación global más que local, permitiendo que se puedan usar para identificar una interfaz específica en relación con la red FR. El direccionamiento global hace que la red FR se parezca a una red de área local (LAN) en términos de direccionamiento. Los protocolos de resolución de direcciones, por lo tanto, ejecutan su función en FR exactamente de la misma manera que en una LAN.

- Control de flujo simple (opcional): Proporciona un mecanismo de control de flujo XON/XOFF (de conexión/desconexión) que se aplica a toda la interfaz FR. Está destinado a dispositivos cuyas capas superiores no pueden utilizar los bits de notificación de congestión y que necesitan algún nivel de control de flujo.

La especificación FR también incluye procedimientos de LMI. Los mensajes LMI se envían en tramas que se distinguen por un DLCI específico del LMI (definidas en la especificación de consorcio como DLCI = 1023).

Formato de trama LMI:

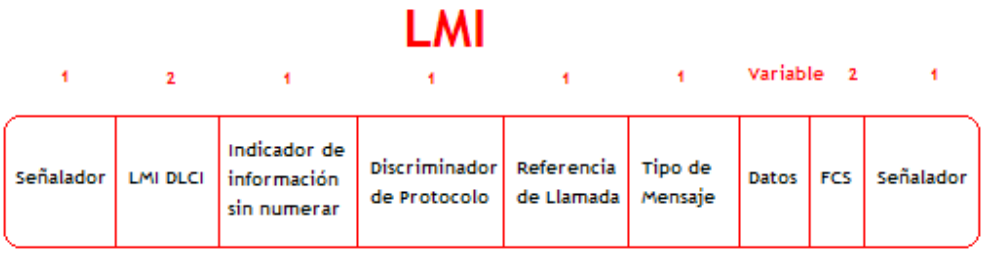



**Figura 7.** Formato de trama LMI

Después del indicador y de los campos DLCI de LMI, la trama LMI contiene 4 bytes obligatorios. El primero de los bytes obligatorios (indicador de información sin número) posee el mismo formato que el indicador de trama de información sin número (UI) de LAPB, con el bit de sondeo/final en cero. El siguiente byte se conoce como discriminador de protocolo, que se establece en un valor que indica LMI. El tercer byte obligatorio (referencia de llamada) siempre se rellena con ceros.

El ultimo byte obligatorio es el campo con el tipo de mensaje. Se han definido dos tipos de mensajes: mensajes de estado y mensajes de petición de estado Los

mensajes de estado responden a los mensajes de petición de estado Ejemplos de estos mensajes son (1) mensajes de actividad (mensajes enviados a través de una conexión para asegurar que ambos lados sigan considerando la conexión como activa) y (2) un mensaje de estado de un informe individual sobre cada DLCI definido para el enlace. Se espera que estas funciones LMI comunes puedan formar parte de todas las implementaciones de conformidad con la especificación FR.

Juntos, los mensajes de estado y de petición de estado, ayudan a verificar la integridad de los enlaces lógicos y físicos. Esta información resulta fundamental en un medio de enrutamiento, ya que los protocolos de enrutamiento toman decisiones según la integridad del enlace.

A continuación, presentamos un campo de elementos de información (IE) de un número variable de bytes. A continuación del campo de tipo de mensaje, hay una cantidad de IE. Cada IE se compone de un identificador IE de 1 byte, un campo de longitud IE y 1 o más bytes que contienen los datos en sí.

Caracteristicas LMI

El multicast es otra función LMI opcional importante. Los grupos de multicast son designados por una serie de cuatro valores DLCI reservados (de 1019 a 1022). Las tramas enviadas por un dispositivo que utiliza uno de estos DLCI reservados son replicados por la red y se envían a todos los puntos de salida en el conjunto designado. La extensión de multicast también define los mensajes LMI que notifican a los dispositivos del usuario acerca del agregado, eliminación y

presencia de los grupos de multicast. Para las redes que aprovechan el enrutamiento dinámico, la información de enrutamiento se debe intercambiar entre muchos routers. Los mensajes de enrutamiento se pueden enviar con eficiencia utilizando tramas con un DLCI de multicast. Esto permite que los mensajes se envíen a grupos determinados de routers.

El mecanismo ARP inverso permite al router generar la asignación de FR automáticamente, como aparece en la figura. El router detecta los DLCI que se están utilizando desde el switch durante el intercambio LMI inicial. El router envía entonces una petición ARP inversa a cada DLCI por cada protocolo configurado en la interfaz si el protocolo es soportado. La información de retorno desde del ARP inverso entonces se utiliza para generar la asignación FR.

Asignación FR: La dirección del router de salto siguiente determinada por la tabla de enrutamiento se debe resolver a un DLCI FR, como se ve en la figura. La resolución se realiza mediante una estructura de datos denominada asignación FR. La tabla de enrutamiento se utiliza entonces para suministrar la dirección de protocolo del salto siguiente o el DLCI para el tráfico saliente. Esta estructura de datos se puede configurar estáticamente en el router, o bien, la función ARP inverso se puede utilizar para configurar automáticamente la asignación.

Tabla de conmutación: La tabla de conmutación FR consta de cuatro entradas: dos para el puerto y DLCI entrante, y dos para el puerto y DLCI saliente, como aparece en la figura. El DLCI se puede, por lo tanto, reasignar a medida que pasa

a través de cada switch; el hecho de que se pueda cambiar la referencia de puerto explica por qué el DLCI no cambia aún cuando la referencia de puerto cambia.

Subinterfaces: Se puede contar con varios circuitos virtuales en una sola interfaz serie y tratar cada uno de ellos como una interfaz separada, llamada subinterfaz (interfaz de Hardware definida por IOS), Las subinterfaces son subdivisiones lógicas de una interfaz física. En una configuración de subinterfaz, cada VC se puede configurar como una conexión punto a punto, que permite a la subinterfaz actuar como línea dedicada. La ventaja de utilizarlas es que se puede asignar características de capa de red diferentes y circuito virtual a cada una. Es posible definir interfaces virtuales con el comando **interface serial slot/port.number.**

Las primeras implementaciones de FR requerían que un router (es decir, un dispositivo DTE) tuviera una interfaz serial WAN para cada VC, Dividiendo lógicamente una sola interfaz serial WAN física en varias subinterfaces virtuales, el costo total de la implementación de la red FR se puede reducir. Una sola interfaz de router puede prestar servicios a varias ubicaciones remotas a través de subinterfaces individuales únicas.

Split horizon (horizonte dividido): Reduce los loops de enrutamiento evitando que una actualización de enrutamiento recibida en una interfaz física se vuelva a enviar a la misma interfaz.. Como resultado, si un router remoto envía una actualización al router de la sede central que conecta múltiples PVC a través de una sola interfaz física, el router de la sede central no puede publicar esta ruta a través de la misma interfaz física a otros routers remotos

Puede configurar subinterfaces para soportar los siguientes tipos de conexión:

- Punto a punto: Se utiliza una sola subinterfaz para establecer un VC en relación con otra interfaz física o subinterfaz en un router remoto. En este caso, las interfaces estarían en la misma subred y cada interfaz tendría un solo DLCI Cada conexión punto a punto constituye su propia subred. En este entorno, los broadcasts no son un problema porque los routers son punto a punto y emulan un enlace dedicado.
- Multipunto: Se utiliza una sola subinterfaz para establecer múltiples VC a múltiples interfaces físicas o subinterfaces en routers remotos. En este caso, todas las interfaces participantes estarían en la misma subred y cada interfaz tendría su propio DLCI local. En este entorno, como la subinterfaz funciona como una red FR común, las actualizaciones de enrutamiento están sujetas a un split horzion (horizonte dividido). Es posible definir un numero ilimitado de subinterfaces en una interfaz física determinada (la unica excepción es la memoria del router)

### 1.4.3 Tecnología DSL

**DSL (Digital Subscriber Line - Línea de Abonados Digitales)** tecnología que suministra el ancho de banda suficiente para numerosas aplicaciones, incluyendo además un rápido acceso a Internet utilizando líneas telefónicas; acceso remoto a las diferentes Redes de área local (LAN), videoconferencia y Sistemas de Redes Privadas Virtuales (VPN).

**xDSL** esta formado por un conjunto de tecnologías que proveen un gran ancho de banda sobre circuitos locales de cable de cobre, sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo de la red, convierten las líneas analógicas convencionales en líneas digitales de alta velocidad, con las que es posible ofrecer servicios de banda ancha en el domicilio de los abonados, similares a los de las redes de cable o las inalámbricas, aprovechando los pares de cobre existentes, siempre que estos reúnan un mínimo de requisitos en cuanto a la calidad del circuito y distancia. Estas son tecnologías de acceso punto a punto a través de la red pública, que permiten un flujo de información tanto simétrico como asimétrico y de alta velocidad sobre el bucle de abonado.

La historia de DSL realmente empezó a tener éxito en 1999, tomó la convergencia de varios eventos antes de que DSL empezara a mostrarse. Las compañías del teléfono estaban en una posición ideal para ofrecer los servicios DSL porque ellos poseían el cable de cobre sobre el que DSL opera.

Funcionan sobre par trenzado y usan la modulación para alcanzar elevadas velocidades de transmisión, aunque cada una de ñlas tecnologías con sus propias características de distancia operativa y configuración. Las diferentes tecnologías se caracterizan por la relación entre la distancia alcanzada entre módems, velocidad y simetrías entre el tráfico de descendente (el que va desde la central hasta el usuario) y el ascendente (el que va del usuario hasta la central). Como

consecuencia de estas características, cada tipo de módem DSL se adapta preferentemente a un tipo de aplicaciones.

Las velocidades de datos de entrada dependen de diversos factores como:

- Longitud de la línea de Cobre.
- El calibre/diámetro del hilo (especificación AWG/mms).
- La presencia de derivaciones puenteadas.
- La interferencia de acoplamientos cruzados.
- La atenuación de la línea aumenta con la frecuencia y la longitud de la línea y disminuye cuando se incrementa el diámetro del hilo.

Muchas aplicaciones previstas para ADSL suponen vídeo digital comprimido. Como señal en tiempo real, el vídeo digital no puede utilizar los procedimientos de control de errores de nivel de red ó de enlace comúnmente encontrados en los Sistemas de Comunicaciones de Datos. Los módem ADSL por tanto incorporan mecanismos FEC (Forward Error Correction) de corrección de errores sin retransmisión (codificación Reed Soloman) que reducen de forma importante los errores causados por el ruido impulsivo. La corrección de errores símbolo a símbolo también reduce los errores causados por el ruido continuo acoplado en una línea.

**MODULACIÓN**

Las tres técnicas de modulación usadas actualmente para xDSL son 2B1Q (2 Bit, 1 Quaternary), "carrier-less amplitude phase modulation" (CAP) y "discrete multitone modulation" (DMT).

En general, el rango máximo para DSL sin los repetidores es 5.5 Km. El cable de medida 24 consigue llevar tasas de datos más lejos que de medida 26.

**Funcionamiento** Para trabajar con DSL, el modem digital o router debe estar accesible a la oficina central (CO) de telefonía local, donde la compañía telefónica tiene instalada un DSLAM que traduce las señales DSL. La señal es transmitida desde la línea telefónica de cobre por nuestra red backbone, y directamente al router del servidor DSL, donde se verifica el acceso a la red y da servicio para la conexión a Internet.

xDSL utiliza mas de un ancho de banda sobre las líneas de cobre, las cuales son actualmente usadas para los viejos servicios telefónicos planos (plain old telephone service, POTS). Utilizando frecuencias superiores al ancho de banda telefónico (300Hz to 3,200Hz), xDSL puede codificar mas datos y transmitir a más elevadas tasas de datos que por otro lado esta posibilidad estaría restringida por el rango de frecuencias de una red POTS. Para utilizar frecuencias superiores al espectro de audio de voz, equipos xDSL deben instalarse en ambos terminales y un cable de cobre entre ellos debe ser capaz de sostener las altas frecuencias

para completar la ruta. Esto quiere decir que las limitaciones del ancho de banda de estos aparatos deben ser suprimida o evitadas.

En general, en los servicios xDSL, el envío y recepción de datos se establece a través de un módem xDSL (que dependerá de la clase de xDSL utilizado). Estos datos pasan por un dispositivo, llamado "splitter", que permite la utilización simultánea del servicio telefónico básico y del servicio xDSL. El splitter se coloca delante de los módems del usuario y de la central; está formado por dos filtros, uno paso bajo y otro paso alto. La finalidad de estos dos filtros es la de separar las señales transmitidas por el canal en señales de alta frecuencia (datos) y señales de baja frecuencia (Telefonía).

Las transmisiones de voz, residen en la banda base (4 KHz e inferior), mientras que los canales de datos de salida y de entrada están en un espectro más alto (centenares de KHz). El resultado es que los proveedores de servicio pueden proporcionar velocidades de datos de múltiples megabits mientras dejan intactos los servicios de voz, todo en una sola línea.

La tecnología xDSL soporta formatos y tasas de transmisión especificados por los estándares, como lo son T1 (.1544 Mbps) y E1 (2.048 Mbps), y es lo suficientemente flexible para soportar tasas y formatos adicionales como sean especificados (ej. 6 Mbps asimétricos para transmisión de alta velocidad de datos y video). xDSL puede coexistir en el circuito con el servicio de voz. Como resultado, todos los tipos de servicios, incluyendo el de voz existente, video,

multimedia y servicios de datos pueden ser transportados sin el desarrollo de nuevas estrategias de infraestructura.

xDSL es una tecnología "Modem-Like", donde es requerido un dispositivo xDSL terminal en cada extremo del circuito de cobre. Estos dispositivos aceptan flujo de datos, generalmente en formato digital, y lo sobrepone a una señal análoga de alta velocidad

**TÉCNICAS XDSL**

Hay varias tecnologías xDSL, cada diseño especifica fines y necesidades de venta de mercado. Algunas formas de xDSL son propiedad, otras son simplemente modelos teóricos y otras son usadas como estándar.

**ADSL** - (Asymmetric Digital Subscriber Line - Línea de Abonado Digital Asimétrica) Es una tecnología de módem desarrollada en 1989, que transforma las líneas telefónicas o el par de cobre del abonado en líneas de alta velocidad permanentemente establecidas. ADSL facilita el acceso a Internet de alta velocidad así como el acceso a redes corporativas para aplicaciones como el teletrabajo y aplicaciones multimedia como juegos on-line, vídeo on demand, videoconferencia, voz sobre IP. La denominación asimétrica es debido a que las velocidades de transmisión y de recepción son distintas La velocidad con la que baja (llega) la información a nuestro ordenador, es mayor a la velocidad con la que suben (mandan) los datos desde nuestro equipo. La distancia máxima entre el

usuario y la central, permitida para implementar ADSL es 5847 mt. Y la distancia optima es 3658mt.

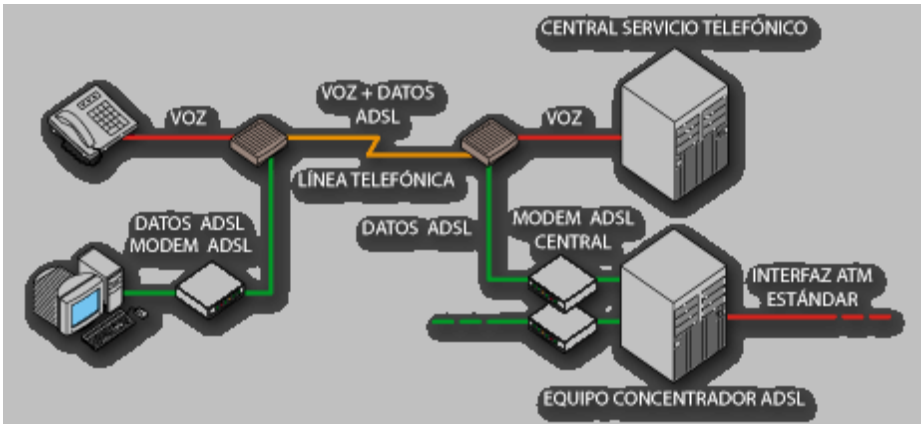



**Figura 8.** Conexión ADSL

**RADSL** (Rate Adative DSL - Línea de Abonados Digital de Tasa Adaptable) Se ajusta a la velocidad de acceso de acuerdo a las condiciones de la línea. Funciona en los mismos márgenes de velocidad que ADSL, pero tiene la ventaja de ajustarse de forma dinámica a las condiciones de la línea y su longitud. La velocidad final de conexión utilizando esta variante de ADSL puede seleccionarse cuando la línea se sincroniza, durante la conexión o como resultado de una señal procedente de la central telefónica. Soporta aplicaciones simetricas y asimetricas es espectralmente compatible con voz convencional y otras tecnologías DSL sin el bucle local.

Esta variante, utiliza la modulación CAP. El sistema de FlexCap2 de Westell usa RADSL para entregar de 640 Kbps a 2.2 Mbps downstream y de 272 Kbps a 1.088 Mbps upstream sobre una línea existente.

**ADSL G.LITE o UDSL** (Línea de Abonados Digital Pequeña) "Splitterless" ADSL sin el "truck roll" (sin filtro voz/datos) G.Lite es también conocido como DSL Lite y ADSL Universal. Hasta la llegada del estándar, el UAWG (Universal ADSL Work Group, Grupo de trabajo de ADSL) llamaba a la tecnología G.Lite o Universal ADSL. En Junio de 1999, G.992.2 fue adoptado por la ITU como el estándar que recogía esta tecnología.

Desgraciadamente para los consumidores, G.Lite es más lento que ADSL. Ofrece velocidades de 1.3Mbps (downstream) y de 512Kbps (upstream). El estandar ADSL; sacrifica velocidad para no tener que instalar un splitter en casa del usuario. Los consumidores de G.lite pueden vivir a más de 18,000 los pies de la oficina central, siendo disponible la tecnología a un muy mayor número de clientes.

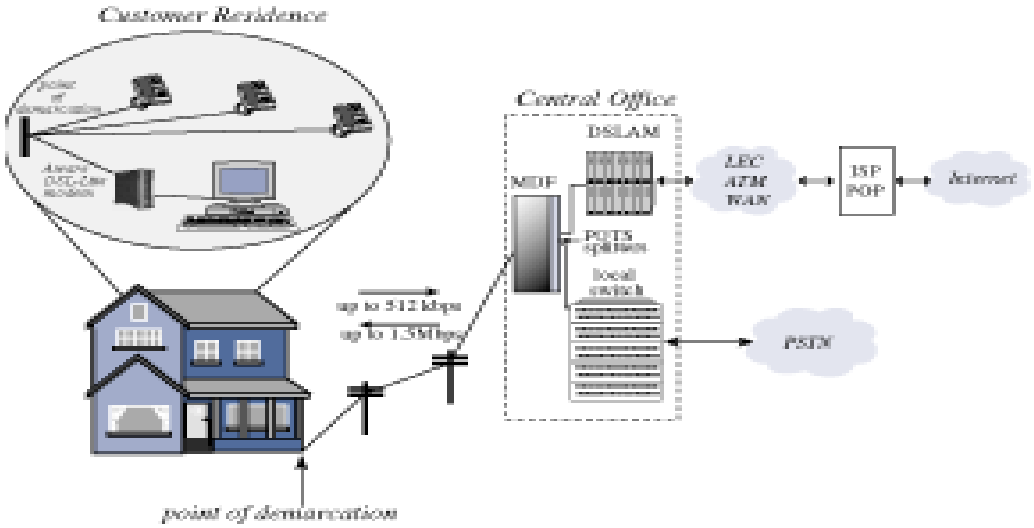



**Figura 9.** Conexión ADSL en residencias

**VDSL** (Línea de Abonados Digital de Tasa Muy Alta) La modalidad **VDSL** es la más rápida de las tecnologías xDSL, ya que puede llegar a alcanzar velocidades entre 13 y 52 Mbps desde la central hasta el abonado y de 1,5 a 2,3 Mbps en sentido contrario, por lo que se trata de un tipo de conexión también asimétrica.

La máxima distancia que puede haber entre los dos módems VDSL no puede superar los 1.371 metros. VDSL es la tecnología idónea para suministrar señales de TV de alta definición.

VDSL está destinado a proveer el enlace final entre una red de fibra óptica y las premisas. Es la tecnología que permite la transmisión de datos en un cierto estilo, sobre algún medio físico. El medio físico utilizado es independiente de VDSL. Una posibilidad es utilizar la infraestructura existente de cableado local.

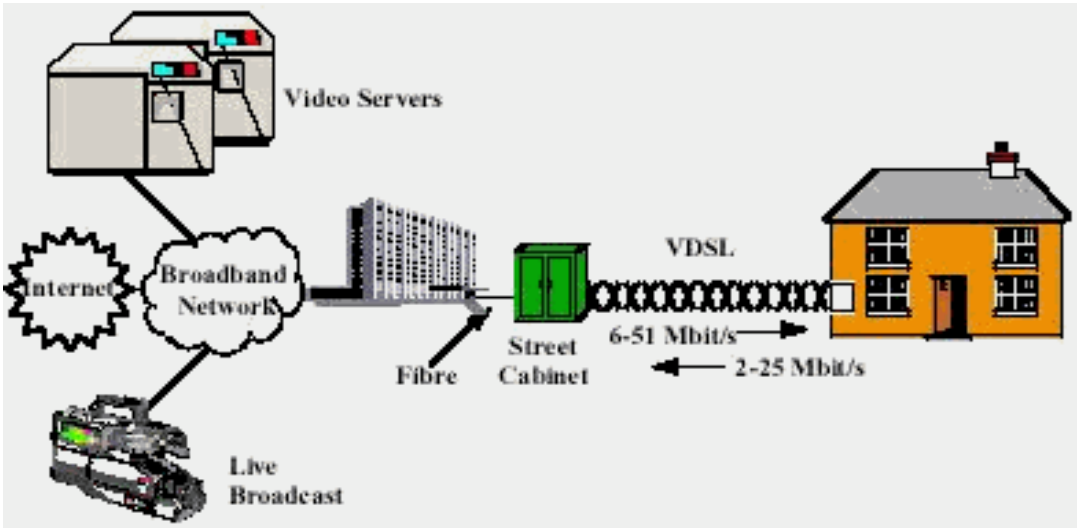



**Figura 10.** Conexión VDSL

**HDSL** (High Bit Rate DSL - Linea de Abonados Digital de Indice de Datos alto) La tecnología HDSL es simétrica y bidireccional, por lo que la velocidad desde la central al usuario y viceversa será la misma. Se implementa principalmente en las PBX. Esta es la tecnología más avanzada de todas, ya que se encuentra implementada en grandes fábricas donde existen grandes redes de datos y es necesario transportar información a muy alta velocidad de un punto a otro.

La velocidad que puede llegar a alcanzar es de 2,048 Mbps (full duplex) utilizando dos pares de cobre, aunque la distancia de 4.500 metros que necesita es algo menor a la de ADSL, utilizando la la modulación por amplitud de pulso 2B1Q.

Las compañías telefónicas han encontrado en esta modalidad una sustitución a las líneas T1/E1 (líneas de alta velocidad) sobre otro tipo de medio - fibra óptica, utilizadas en Norteamérica y en Europa y Latino America, respectivamente.

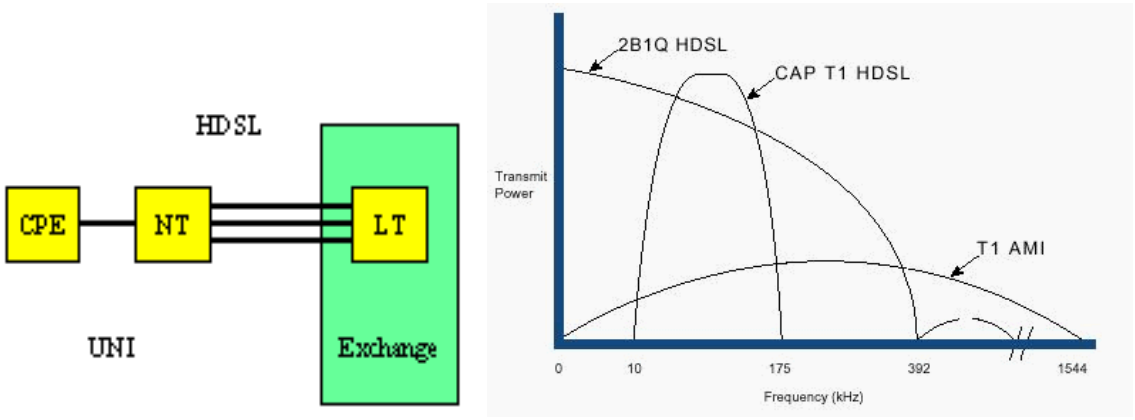



**Figura 11.** Nivel de frecuencia de HDSL

HDSL está enfocado principalmente hacia usos empresariales (interconexión de nodos proveedores de Internet, redes privadas de datos, enlaces entre centralitas, etc) más que hacia el usuario (cuyas necesidades se verán mejor cubiertas por las tecnologías ADSL y SDSL).

Una de las principales aplicaciones de HDSL es el acceso de última milla a costo razonable a redes de transporte digital para RDI, redes satelitales y del tipo FR.

La tecnología HDSL tiene cabida en las comunicaciones de redes públicas y privadas también. Cada empresa puede tener requerimientos diferentes, orientados al uso de líneas privadas de fácil acceso y obtención para que con productos de tecnología HDSL se puedan obtener soluciones de bajo costo y alta efectividad.

**HDSL2 o SHDSL** (High Bit Rate DSL 2 - Linea de Abonados Digital de Indice de Datos alto 2) Está diseñada para transportar señales T1 a 1.544 Mb/s sobre un

simple par de cobre. HDSL2 usa: overlapped phase Trellis-code interlocked spectrum (OPTIS). (espectro de interbloqueo de codigo Trellis de fases solapadas).

Ofrece los mismos 2.048 Mbps de ancho de banda como solución a los tradicionales 4 cables de HDSL, con la ventaja de requerir solamente un simple par de cobre.

HDSL2 espera aplicarse en Norte América solamente, ya que algunos vendedores han optado por construir una especificación universal de G.shdsl.

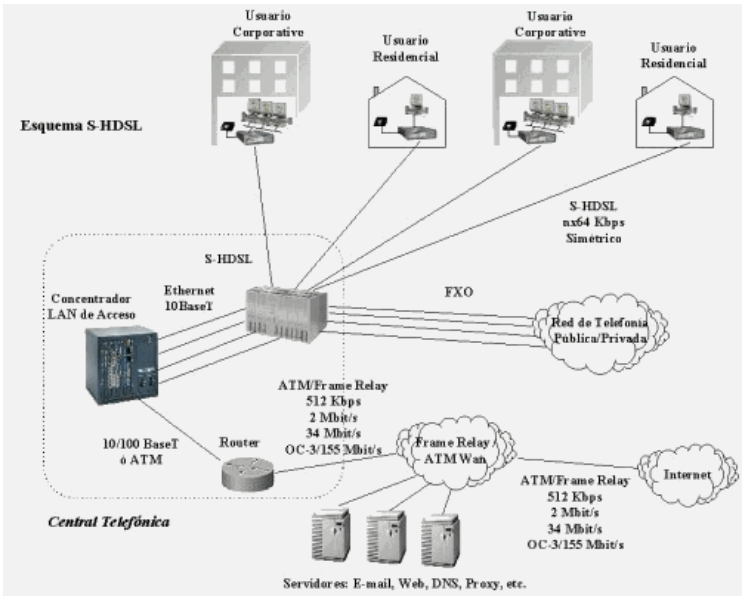



**Figura 12.** Esquema S.HDSL

**SDSL** (Symmetric DSL - Linea de Abonados Digital Simétrica) Es muy similar a la tecnología HDSL, ya que soporta transmisiones simétricas, pero con dos

particularidades: utiliza un solo par de cobre y tiene un alcance máximo de 3.048 metros. Dentro de esta distancia será posible mantener una velocidad similar a HDSL.

Esta tecnología provee el mismo ancho de banda en ambas direcciones, tanto para subir y bajar datos; es decir que independientemente de que estés cargando o descargando información de la Web, se tiene el mismo rendimiento de excelente calidad. SDSL brinda velocidades de transmisión entre un rango de T1/E1, de hasta 1,5 Mbps, y a una distancia máxima de 3.700 m a 5.500 desde la oficina central, a través de un único par de cables. Este tipo de conexión es ideal para las empresas pequeñas y medianas que necesitan un medio eficaz para subir y bajar archivos a la Web.

**M/SDSL** (MultiRate DSL - Línea de Abonados Digital Simétrica Multi Tasa propiedad de **NORTEL**) Mas allá de los 144 kbps de ancho de banda de IDSL, hay nuevas tecnologías que ofrecen rangos entre 128 Kbps y 2.048 Mbps.

Para una aplicación simétrica, M/SDSL ha surgido como una tecnología valorada en los servicios TDM (Multiplexación por División de Tiempo) sobre una base ubicua. Construida sobre un par simple de la tecnología SDSL, M/SDSL soporta cambios operacionales en la tasa del transceiver y distancias con respecto el mismo.

La version CAP soporta ocho tasas distintas de 64 Kbps/128 Kbps y da servicios a una distancia de 8.9 Km sobre cables de 24 AWG (0.5 mm) y 4.5 Km, para una

tasa completa de 2 Mbps. Con una habilidad de auto-tasa (similar a RADSL), las aplicaciones simetricas pueden ser universalmente desarrolladas.

**IDSL o ISDN-BA** (Línea de Abonados Digital ISDN) Esta tecnología es simétrica, similar a la SDSL, pero opera a velocidades más bajas y a distancias más cortas. ISDN se basa el desarrollo DSL de Ascend Communications.

IDSL se implementa sobre una línea de ISDN y actualmente se emplea como conexión al Internet para la transferencia de datos, no permite voz en la misma linea. El servicio de IDSL permite velocidades de 128Kbps o 144Kbps.

La linea de código de nivel 4 PAM (banda base) conocida como 2B1Q era iniciada por los Laboratorios BT. ETSI también adaptó esto para Europa y también desarrolló la linea de código 4B3T (aka MMS43) como un opción alternativa, primero para usarla en Alemania.

Los modems ISDN-BA emplean técnicas de cancelación de eco (EC) capaces de transmitir fullduplex a 160 kbit/s sobre un simple par de cables telefónicosr. Los transceivers ISDN-BA basados en cancelación de eco permiten utilizar anchos de banda de ~10 kHz hasta 100 kHz, y esto es instructivo para notar que la densidad espectral más alta de capacidad de los sistemas DSL basados en 2B1Q esta cerca de los 40 kHz con el primer espectro nulo a los 80 kHz.

Los estandares internacionales sobre ISDN-BA especifican los aspectos físicos de transmisionto en el ISDN ‘U’. En Europa es usual para el NT formar parte del

Telco y proveer de un bus S/T, el cual forma el estandar digital User Network Interface (UNI).

La carga útil de DSL está integrada usualmente por 2 canales B o canales Bearer de 64 kbit/s cada uno mas un 'D' (delta) o canal de de señalización de 16 kbit/s, el cual puede aveces ser utilizado para transmitir datos. Esto da al usuario un acceso de 128 kbit/s mas la señalización (144kbit/s). Un canal extra de 16 kbit/s esta preparado para un Embedded Operations Channel (EOC), intentando intercambiar información entre el LT (Line Terminal) y el NT . El EOC normalmente no es accesible para el usuario.

**G.shdsl** Es un estandar de la ITU el cual ofrece un conjunto de características muy ricas (por ejemplo, tasas adaptables) y ofrece mayores distancias que cualquier estandar actual.

Este método ofrece anchos de bandas simétricos comprendidos entre 192 Kbps y 2.3 Mbps, con un 30% más de longitud del cable que SDSL y presenta cierta compatibilidad con otras variantes DSL. Espera aplicarse en todo el mundo.

G.shdsl también puede negociar el numero de tramas del protocolo incluyendo ATM, T1, E1, ISDN e IP. Esta solicitado para empezar a reemplazar las tecnologías T1, E1, HDSL, SDSL HDSL2, ISDN y IDSL.

En el siguiente cuadro se muestran las velocidades que pueden alcanzar las diferentes tecnologías xDSL, dependiendo de la distancia del nodo a la oficina telefónica central, factor que influye en el funcionamiento de la tecnología.

| VELOCIDADES MÁXIMAS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Tipo de servicio** | **ADSL** | **CDSL** | **HDSL** | **ISDL** | **RADSL** | **S-HDSL** | **SDSL** | **VDSL** |
| **Downstream 18000 pies** | 1.5 Mbit/s | 1 Mbit/s | 1.544 Mbit/s | 128 kbit/s | 1.5 Mbit/s | No soportado | 1 Mbit/s | 51 Mbit/s |
| **Upstream 18000 pies** | 64 kbit/s | 128 kbit/s | 1.544 Mbit/s | 128 kbit/s | 64 kbit/s | No soportado | 1 Mbit/s | 2.3 Mbit/s |
| **Downstream 12000 pies** | 6 Mbit/s | 1 Mbit/s | 1.544 Mbit/s | 128 kbit/s | 6 Mbit/s | 768 kbit/s | 2 Mbit/s | 51 Mbit/s |
| **Upstream 12000 pies** | 640 kbit/s | 128 kbit/s | 1.544 Mbit/s | 128 kbit/s | 640 kbit/s | 768 kbit/s | 2 Mbit/s | 2.3 Mbit/s |

**TABLA 2.** Velocidades Máximas de DSL

**VENTAJAS xDSL**

- **Conexión Ininterrumpida y veloz:** Los usuarios podrán bajar gráficos, vídeo clips, y otros archivos, a alta velocidad.
- **Flexibilidad:** Al utilizar la tecnología DSL, los usuarios podrán utilizar la misma línea para recibir y hacer llamadas telefónicas mientras estén on-line.
- **Línea digital:** DSL convierte las líneas telefónicas analógicas en digitales adhiriendo un dispositivo de interconexión de línea en la oficina central, y un módem del tipo DSL en la casa del abonado. Para esto, los clientes deberán suscribirse al servicio DSL desde sus proveedores de servicio telefónico.

**DESVENTAJAS xSL**

Para poder utilizarlo, se debe estar aproximadamente a menos de 5.500 mts de la oficina central de la empresa telefónica, ya que a una distancia mayor no se obtiene la gran velocidad que provee el servicio. Después de los 2.400 mts la velocidad comienza a disminuir, pero aún así este tipo de tecnologías es más veloz que una conexión mediante un módem y una línea telefónica.

## 1.5 MEDIOS DE TRANSMISIÓN DE SERVICIOS DEDICADOS

Son aquellos en que se establece una conexión permanente entre dos lugares, manteniéndose permanentemente disponible para el intercambio de información entre los dos puntos. Entre algunos servicios se encuentran: Fibra Óptica, Microondas, Par de Cobre, Enlaces Ópticos, entre otras.

### 1.5.1 Par Trenzado

El par trenzado es el medio guiado más económico y a la vez más usado. Consiste en dos cables de cobre embutidos en u aislante, entrecruzados en forma espiral. Cada par de cables constituyen sólo un enlace de comunicación. Normalmente, se utilizan haces en los que se encapsulan varios pares mediante una envoltura protectora. En aplicaciones de larga distancia, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para enlaces de larga distancia, la longitud del trenzado varía entre 5 y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0.5 y 0.9 mm.

**Características de la transmisión**

Los cables de cobre se pueden usar para transmitir tanto señales analógicas como señales digitales. Para señales analógicas, se necesitan amplificadores cada 5 o 6 kms. Para transmisión digital (usando tanto señales analógicas y digitales) se requieren repetidores cada 2 o 3 kms.

Comparando con otros medios guiados (cable coaxial y fibra óptica), el par trenzado permite menores distancias, menor ancho de banda y menor velocidad de transmisión. Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido, debido a su fácil acoplamiento con campos electromagnéticos externos. El ruido impulso también afecta a los pares trenzados. Para reducir estos efectos negativos es posible tomar algunas medidas.

Para la señalización analógica punto a punto, un par trenzado puede ofrecer hasta 1MHz de ancho de banda, lo que permite transportar un buen número de canales de voz. En el caso de señalización digital punto a punto de larga distancia, se pueden conseguir del orden de unos pocos Mbps; para distancias cortas, actualmente ya existen productos comerciales que alcanzan los 100 Mbps e incluso 1 Gbps.

### 1.5.1.1 Sin Apantallar UTP

Existen dos variantes de pares trenzados: apantallado y sin apantallar. El par trenzado no apantallado (UTP) es el medio habitual en la telefonía. No obstante, actualmente es práctica habitual en el cableado de edificios, muy por encima de

las necesidades reales de telefonía. Esto es así ya que hoy por hoy, el par sin apantallar es el menos caro de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y manipular. El par trenzado sin apantallar se puede ver afectado por interferencias electromagnéticas externas incluyendo interferencias con pares cercanos y fuentes de ruido.

#### 1.5.1.2 Apantallado STP

Una manera de mejorar las características de transmisión del par trenzado sin apantallar es embutiendo dentro de él una malla metálica, reduciendo así las interferencias. El par trenzado apantallado (STP) proporciona mejores resultados a velocidades de transmisión bajas, pero es más costoso y difícil de manipular que el anterior.

### 1.5.2 Fibra Óptica

La fibra óptica es un medio flexible y fina capaz de confinar un haz de naturaleza óptica. Un cable de fibra óptica tiene forma cilíndrica y esta formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta.

Los circuitos de fibra óptica son filamentos de vidrio (compuestos de cristales n aturales) o plástico (cristales artificiales), del espeso de un pelo (entre 10 y30 micrones). Levan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo al otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

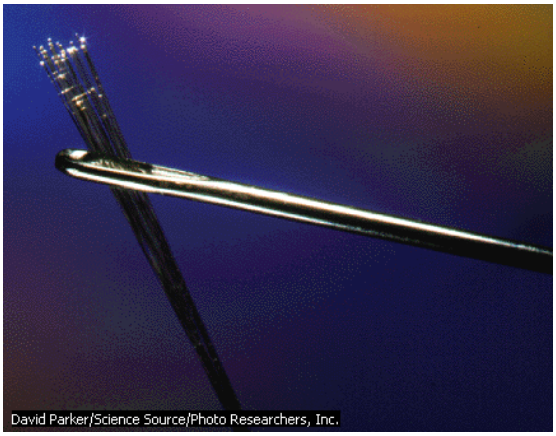



**Figura 13.** Fibra óptica

Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en pequeños ambientes autónomos (tales como sistemas de procesamiento de datos de aviones), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas).

**Funcionamiento** En un sistema de transmisión por fibra óptica existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o en luminosa, por ello se le considera el componente activo de este proceso. Una vez que es transmitida la señal luminosa por las minúsculas fibras, en otro extremo del circuito se encuentra un tercer componente el que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en energía electromagnética, similar a la señal original. El sistema básico de transmisión se compone en este orden, de señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo),

empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida.

En resumen, se puede decir que este proceso de comunicación, la fibra óptica funciona como medio de transportación de la señal luminosa, generado por el transmisor de LED's (diodos emisores de luz ) y láser.

Los diodos emisores de luz y los diodos láser son fuentes adecuadas para la transmisión mediante fibra óptica, debido a que su salida se puede controlar rápidamente por medio de una corriente de polarización. Además su pequeño tamaño, su luminosidad, longitud de onda y el bajo voltaje necesario para manejarlos son características atractivas.

**Características**

- **Mayor Capacidad.** El ancho de banda potencial, y por tanto la velocidad de transmisión, en las fibras es enorme. Experimentalmente se ha demostrado que se pueden conseguir velocidades de transmisión de cientos de Gbps para decenas de kilómetros de distancia.
- **Menor tamaño y peso.** Las fibras ópticas son apreciablemente más finas que el cable coaxial. La reducción en tamaño lleva a su vez aparejada una reducción en peso que disminuye a su vez la infraestructura necesaria.
- **Menor atenuación.** La atenuación es significativamente menor en las fibras óticas que en los cables coaxiales, además es constante en un gran intervalo.
- **Mayor separación entre repetidores.** Cuantos menos repetidores haya el coste será menor, además de haber menos fuentes de error. Para la fibra,

es práctica habitual necesitar repetidores separados entre sí por decenas de kilómetros.

### 1.5.3 Microondas

Las microondas son ondas electromagnéticas de radio situadas entre los rayos infrarrojos (cuya frecuencia es mayor) y las ondas de radio convencionales. Su longitud de onda va aproximadamente desde 1 mm hasta 30 cm. Las microondas se generan con tubos de electrones especiales como el klistrón o el magnetrón, que incorporan resonadores para controlar la frecuencia, o con osciladores o dispositivos de estado sólido especiales. Las microondas tienen muchas aplicaciones: radio y televisión, radares, meteorología, comunicaciones vía satélite, medición de distancias, investigación de las propiedades de la materia o cocinado de alimentos.

Los hornos de microondas funcionan excitando las moléculas de agua de los alimentos, lo que hace que vibren y produzcan calor. Las microondas entran a través de aberturas practicadas en la parte superior de la cavidad de cocción, donde un agitador las dispersa de forma homogénea por todo el horno. Las microondas no pueden penetrar en un recipiente de metal para calentar la comida, pero sí atraviesan los recipientes no metálicos.

Las microondas pueden detectarse con un instrumento formado por un rectificador de diodos de silicio conectado a un amplificador y a un dispositivo de registro o una pantalla. La exposición a las microondas es peligrosa cuando se

producen densidades elevadas de radiación, como ocurre en los máseres. Pueden provocar quemaduras, cataratas, daños en el sistema nervioso y esterilidad. Todavía no se conocen bien los posibles peligros de la exposición prolongada a microondas de bajo nivel.

#### 1.5.3.1 Microondas Terrestres

Básicamente un enlace vía microondas consiste en tres componentes fundamentales: el transmisor, el receptor y el canal aéreo. El transmisor es el responsable de modular una señal digital a la frecuencia utilizada para transmitir, el canal aéreo representa un camino abierto entre el transmisor y el receptor, y como es de esperarse el receptor es el encargado de capturar la señal transmitida y llevarla de nuevo señal digital.

El factor limitante de la propagación de la señal en enlaces de microondas es la distancia que se debe cubrir entre el transmisor y el receptor, además esta distancia debe ser libre de obstáculos.

Otro aspecto que se deba señalar es que en estos enlaces, el camino entre el receptor el transmisor debe tener una altura mínima sobre los obstáculos en la vía, para compensar este efecto se utilizan torres para ajustar dichas alturas.

**Antenas y torres microondas**

La distancia cubierta por enlaces microondas puede ser incrementada por el uso de repetidoras, las cuales amplifican y redireccionan la señal, es importante

destacar que los obstáculos de la señal pueden ser salvados a través de reflectores pasivos.


**Figura 14.** Antena

La señal de microondas transmitidas es distorsionada y atenuada mientras viaja desde el transmisor hasta el receptor, estas atenuaciones y distorsiones son causadas por una perdida de poder dependiente a la distancia, reflexión y refracción a obstáculos y superficies reflectoras, y a perdidas atmosféricas.

**Características de la transmisión**

El rango de microondas cubre una parte del espectro electromagnético. La banda de frecuencias está comprendida entre 2 y 40 GHz. Cuanto mayor sea la frecuencia utilizada, mayor es el ancho de banda potencial, y por tanto, mayor es la posible velocidad de transmisión.

Al igual que cualquier sistema de transmisión, la principal causa de pérdidas en las microondas es la atenuación. La atenuación aumenta con las lluvias, siendo este efecto especialmente significativo para frecuencias por encima de 10 GHz.

Otra dificultad adicional son las interferencias. Con la popularidad creciente de las microondas, las áreas de cobertura se pueden solapar, haciendo que las interferencias sean siempre un peligro potencial. Así la asignación de bandas tiene que realizarse siguiendo una regulación estricta.

Las bandas más usuales de transmisión a larga distancia se sitúan entre 4 GHz y 6Ghz. Debido a la creciente que están sufriendo estas bandas, la banda de 11 GHz se está empezando a utilizar. La banda de 12 GHz se usa para proporcionar la señal de TV a las cabeceras de distribución de TV por cable, en las que para llegar al abonado se utilizan el cable coaxial.

#### 1.5.3.2 Microondas por Satélite

En su concepción más sencilla, y quizás simplista, los satélites de radioaficionados son repetidoras voladoras. Su principal diferencia con sus equivalentes terrestres es que vuelan y que al volar se mueven.

**Funcionamiento** Un radioaficionado “A” emite una señal que es recibida por el satélite. El satélite la amplifica y la retransmite inmediatamente. El radioaficionado “B” la recibe y le contesta. Así inicia un comunicado por satélite.

Un satélite es un repetidor de radio en el cielo (transponder). Un sistema de satélite consiste de un transponder, una estación basada en tierra para controlar el funcionamiento y una red de usuario de las estaciones terrestres, que proporcionan las facilidades para transmisión y recepción de tráfico de comunicaciones, a través del sistema de satélite. Las transmisiones de satélites

se catalogan como bus o carga útil. La de bus in incluye mecanismos de control que apoyan la operación de carga útil. La de carga útil es la información del usuario que será transportada a través del sistema. Aunque en los últimos años los nuevos servicios de datos y radioemisión de televisión son más y más demandados, la transmisión de las señales de teléfono de voz convencionales (en forma analógica o digital).

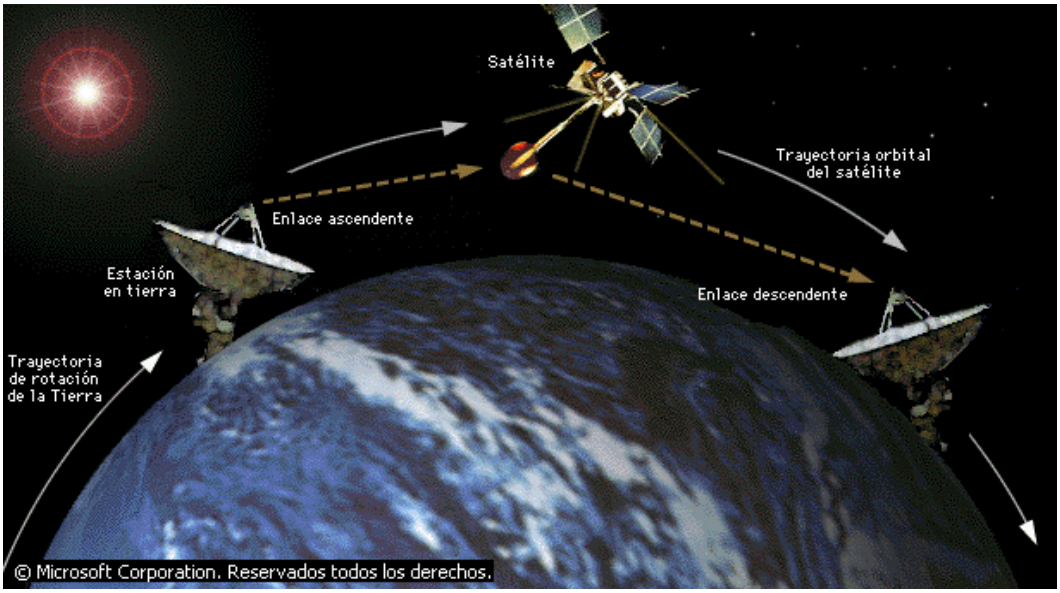



**Figura 15.** Satelite

Las comunicaciones vía satélite se componen de dos partes fundamentales: el satélite y la estación en tierra. El satélite lo componen tres unidades básicas: la unidad de combustible, los controles de telemetría y los transpondedores. Los transpondedores son la parte que se encarga de la comunicación y se compone de la antena receptora, que se encarga de recoger las señales de la estación de tierra, un receptor de banda ancha, un multiplexor de entrada y un convertidor de

frecuencia, que se utiliza para trasladar la señal de entrada a un amplificador de alta potencia y enviarlo de nuevo a la tierra.

**Función** La función principal de un satélite, es reflejar señales electromagnéticas. En el caso de un satélite de telecomunicaciones, el papel principal es recibir señales de una estación en la tierra y enviarlas a otra estación a una distancia considerable.

**Transmisión de datos** A pesar de lo que pueda parecer, la incorporación de satélite como parte de una red terrestre está altamente influenciada por tres características exclusivas de la comunicación por satélite: El retardo de propagación, un ancho de banda un poco escaso, y el ruido. El retardo de propagación quizás sea uno de los mayores problemas a la hora de incorporar satélites a las redes terrestres. Debido fundamentalmente a la gran distancia existe entre las estaciones de tierra y las órbitas de los satélites, obtenemos retardos del orden de 0.2 segundos, que pueden ocasionar grandes problemas a las estaciones que esperan la entrega de paquetes. El ancho de banda pobre, viene dado por las limitaciones físicas de la transmisión de las ondas de radio, estableciéndose un ancho de banda fijo para la transmisión. La potencia de las ondas de radio, es proporcional al cuadrado de la distancio que han viajado, de esta forma, cuando llegan a la estación correspondiente en la tierra, se han debilitado mucho, lo que facilita la inserción de ruidos.

# CAPÍTULO DOS

## TCP/IP

**2.1 CONJUNTO DE PROTOCOLOS TCP/IP**

**2.1.1 Protocolos TCP/IP de Internet y el modelos OSI**

**2.2 RELACIÓN CON LA CAPA DE RED**

**2.2.1 TCP/IP y la capa de Internet**

**2.2.2 Protocolo de mensajes de control de Internet (ICMP)**

**2.2.3 Funcionamiento de ARP**

**2.2.4 Funcionamiento RARP**

## 2.1 CONJUNTO DE PROTOCOLOS TCP/IP

### 2.1.1 Protocolos TCP/IP de Internet y el modelos OSI

El conjunto de protocolos Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) se desarrolló como parte de la investigación realizada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA). Originalmente, se desarrolló para suministrar comunicaciones a través de DARPA. Posteriormente, TCP/IP se incluyó en la Distribución del Software Berkeley de UNIX. TCP/IP es hoy el estándar de facto para las comunicaciones de internetwork y sirve como el protocolo de transporte para Internet, permitiendo que millones de computadores se comuniquen a nivel mundial.

Este currículum se centra en TCP/IP por varios motivos:

- TCP/IP es un protocolo disponible a nivel mundial que, muy probablemente, usted mismo esté usando para trabajar.
- TCP/IP es una referencia útil para comprender otros protocolos porque incluye elementos que son representativos de otros protocolos.
- TCP/IP es importante porque el router lo utiliza como una herramienta de configuración.

La función de la pila, o conjunto, de protocolo TCP/IP es la transferencia de información desde un dispositivo de red a otro. Al hacer esto, se asemeja al

modelo de referencia OSI en las capas inferiores y soporta todos los protocolos físicos y de enlace de datos.

Las capas que se ven más afectadas por TCP/IP son la Capa 7 (aplicación), la Capa 4 (transporte) y la Capa 3 (red). Dentro de estas capas se incluyen otros tipos de protocolo que tienen varios propósitos / funciones, todos ellos relacionados con la transferencia de información.

TCP/IP permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones de LAN como de WAN. TCP/IP incluye no sólo las especificaciones de las Capas 3 y 4 (como, por ejemplo, IP y TCP) sino también especificaciones para aplicaciones tan comunes como el correo electrónico, la conexión remota, la emulación de terminales y la transferencia de archivos

## 2.2 RELACIÓN CON LA CAPA DE RED

### 2.2.1 TCP/IP y la capa de Internet

La capa de Internet de la pila de TCP/IP corresponde a la capa de red del modelo OSI. Cada una de las capas tiene la responsabilidad de transportar paquetes a través de una red utilizando el direccionamiento por software.

Como se muestra en la figura, varios protocolos operan en la capa Internet de TCP/IP, que corresponde a la capa de red del modelo OSI:

- *IP* : suministra enrutamiento de datagramas no orientado a conexión, de máximo esfuerzo de entrega; no se ocupa del contenido de los datagramas; busca la forma de desplazar los datagramas al destino
- *ICMP*: aporta capacidad de control y mensajería
- *ARP* : determina direcciones a nivel de capa de enlace de datos para las direcciones IP conocidas
- *RARP* : determina las direcciones de red cuando se conocen las direcciones a nivel de la capa de enlace de datos

### 2.2.2 Protocolo de mensajes de control de Internet (ICMP)

**Internet Control Message Protocol** La estación destino o un dispositivo intermedio debe informar a la estación fuente acerca del procesamiento de datagramas, y para esto se utiliza el ICMP, el cual se encarga de transportar distintos mensajes de control o de informar al origen si se ha producido algún error durante la entrega de su mensaje. En otras palabras el ICMP maneja información de realimentación sobre problemas en el entorno de comunicación.

ICMP se puede caracterizarse de la siguiente manera:

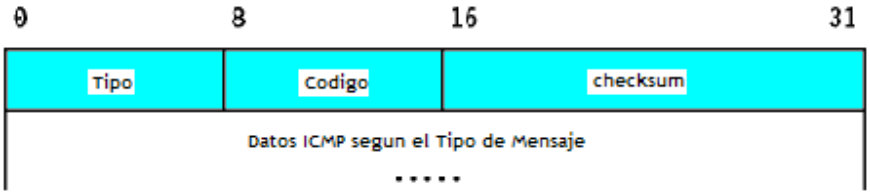
- ICMP usa IP como si ICMP fuera un protocolo del nivel superior(es decir, los mensajes ICMP se encapsulan en datagramas IP). Sin embargo, ICMP es parte integral de IP y debe ser implementado por todo módulo IP.

- ICMP se usa para informar de algunos errores, *no* para hacer IP fiable. La fiabilidad debe ser implementada por los protocolos de nivel superior que usan IP.
- ICMP puede informar de errores en cualquier datagrama IP con la excepción de mensajes IP, para evitar repeticiones infinitas.
- Para datagramas IP fragmentados, los mensajes ICMP sólo se envían para errores ocurridos en el fragmento cero. Es decir, los mensajes ICMP nunca se refieren a un datagrama IP con un campo de desplazamiento de fragmento.
- Los mensajes ICMP nunca se envían en respuesta a datagramas con una dirección IP de destino o de origen que no represente a un único host. Es decir, la dirección de origen no puede ser cero, una dirección de *looopback*, de *broadcast* o de *multicast*.
- Los mensajes ICMP nunca se envían en respuesta a mensajes ICMP de error. Pueden enviarse en respuesta a mensajes ICMP de consulta.

**Mensajes ICMP**

Los mensajes ICMP se describen en los RFCs 792 y 950, correspondientes al STD 5 y son obligatorios.

La cabecera IP del datagrama siempre tendrá un número de protocolo 1, indicando que se trata de ICMP y un servicio de tipo 0(rutina). El campo de datos de IP contendrá el auténtico mensaje ICMP.[2]




Formato te mensajes ICMP Donde Type Especifica el tipo del mensaje, el cual puede ser:

| Campo de tipo | Tipo de mensaje |
|---|---|
| 0 | Echo reply Respuesta de eco |
| 3 | Destination unreachable Destino inaccesible |
| 4 | Source quench Disminución del tráfico desde el origen |
| 5 | Redirect Redireccionar, cambio de ruta |
| 8 | Echo Request Solicitud de eco |
| 9 | Router Advertisement |
| 10 | Router Solicitation |
| 11 | Time exceeded Tiempo excedido para un datagrama |
| 12 | Parameter Problem Problema de Parámetros |
| 13 | Timestamp request Solicitud de marca de tiempo |
| 14 | Timestamp reply Respuesta de marca de tiempo |
| 15 | Information request (obsolete) Solicitud de información (obsoleto) |
| 16 | Information reply (obsolete) Respuesta de información (obsoleto) |
| 17 | Adress mask request Solicitud de máscara |
| 18 | Adress mask reply Respuesta de máscara |

**TABLA 3.** Descripción de un mensaje ICMP

[2] http://www.eduangi.com

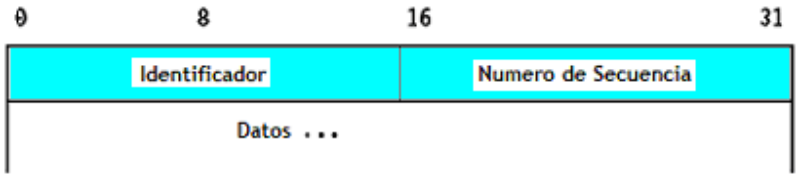
*Code* -Contiene el código de error para el datagrama del que da parte el mensaje ICMP. La interpretación depende del tipo de mensaje.

*Checksum* - Contiene el complemento a 1 de 16 bits de la suma del "*ICMP message starting with the ICMP Type field*". Para computar este *checksum* se asume en principio que su valor es cero. Este algoritmo es el mismo que el usado por IP para el cálculo de la cabecera IP. Compárese con el algoritmo de UDP y TCP que incluyen además una pseudocabecera-IP en el checksum.

*Data*- Contiene información para el mensaje ICMP. Típicamente se tratará de parte del mensaje IP original para el que se generó el mensaje ICMP. La longitud de los datos puede calcularse como la diferencia entre la longitud del datagrama IP que contiene el mensaje y la cabecera IP.

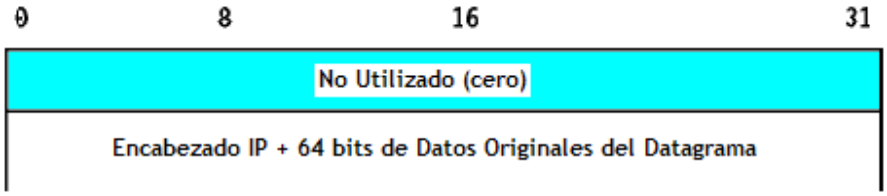
**Tipo de mensajes ICMP:**

**Echo Reply (0) respuesta de eco y Echo Request eco (8)**




*Echo* se usa para saber si existe comunicación entre 2 hosts a nivel de la capa de red. La fuente inicializa el identificador y el número de secuencia (que se utiliza cuando se envían múltiples mensajes *echo request*), añade opcionalmente algunos datos al campo de datos y envía el eco ICMP al host de destino. El código de la cabecera ICMP es cero. El receptor cambia el tipo del mensaje a *echo reply* y devuelve el datagrama al host fuente.

El siguiente formato es igual para todos los siguientes tipos de mensajes ICMP: (3) Destino inaccesible, (4) Disminución del tráfico desde el origen, (11) tiempo excedido.




**Destination Unreachable (3) Destino inaccesible**

Si este mensaje es recibido de un *router* intermedio, significa que el *router* considera la dirección IP de destino como inalcanzable. Si se recibe del *host* destino, significa que el protocolo especificado en el campo de número de protocolo del datagrama original no está activo en ese *host* o que el puerto

indicado es el que no está activo. El campo de código de cabecera tendrá uno de los siguientes valores:

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 (obsolete)*

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*

**Source Quench (4) Disminución del tráfico desde el origen**

Si se recibe este mensaje de un *router* intermedio, significa que el *router* no dispone de suficiente espacio en el buffer para almacenar los datagramas de salida para la siguiente red. Si este mensaje procede del host de destino, significa

que los datagramas entrantes llegan demasiado rápidos para ser procesados. El código de la cabecera ICMP siempre es cero.

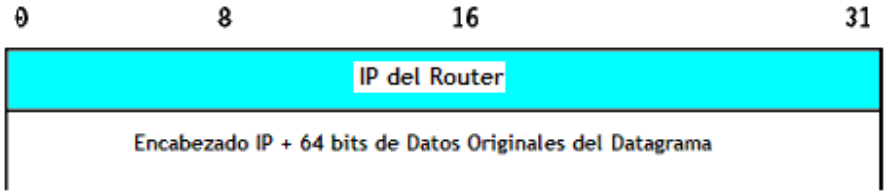
**Time Exceeded (11) tiempo excedido**

Si se recibe este mensaje de un *router* intermedio, significa que el TTL de un datagrama IP ha expirado. Si se recibe del host de destino, significa que el TTL para ensamblar el datagrama ha expirado mientras el host esperaba uno de sus fragmentos. La cabecera ICMP puede tener uno de los siguientes valores:

0 - *transit TTL exceeded*

1 - *reassembly TTL exceeded*

**Redirect (5) Redireccionar, Cambio de ruta**




Si se recibe este mensaje de un "router" intermedio, significa que el host debería enviar los siguientes datagramas para esa red al "router" cuya dirección IP se especifica en el mensaje ICMP. Este otro "router" habrá de estar siempre en la misma subred que el host que envió el datagrama y el que lo devolvió enviará el datagrama a su siguiente dirección de salto; si la dirección del "router" coincide con la dirección fuente del datagrama original, indica un bucle. Este mensaje ICMP

no se enviará si el datagrama IP contiene un ruta fuente. La cabecera ICMP tendrá uno de los siguientes valores:

0 -Network redirect

1 - Host redirect

2 - Network redirect for this type of service

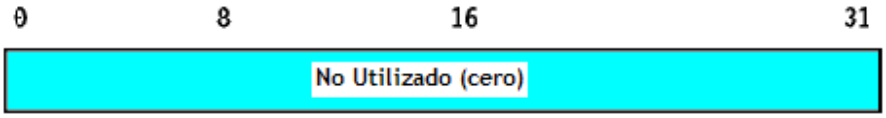
3 - Host redirect for this type of service

**Router Advertisement (9) y Router Solicitation (10)**

Los mensajes ICMP 9 y 10 son opcionales. Se describen en el RFC 1256, que es electivo.

*Router Advertisement*


*Router Solicitation*




*number* - El número de entradas del mensaje.

*entry length*- La longitud de una entrada en unidades de 32 bits. Vale 2 (32 bits para la dirección IP y 32 bits para el valor tomado por preferencia).

TTL - El número de segundos que se considerará válida una entrada.

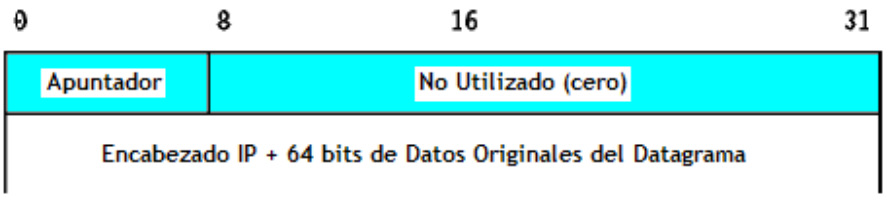
*router address* -Una de las direcciones IP del host fuente.

*preference level* - Un nivel expresado con un valor de 32 bits con signo que indica la preferencia a asignar a esta dirección al seleccionar un *router* por defecto para una subred. Cada *router* de una subred es responsable de anunciar su propio nivel de preferencia. La preferencia aumenta cuanto mayor es el valor, y viceversa. El valor por defecto es cero, que está en el centro del rango de valores. Un valor de X'80000000' -2exp31 indica que el "router" no se debería usar jamás como *router* por defecto. La cabecera ICMP es cero para ambos mensajes.

Estos dos mensajes se usan si un host o un *router*" soporta el RDP (*Router Discovery Protocol*). El uso del *multicast* está recomendado, pero se puede usar el *broadcast* si la interfaz no soporta el *multicast*. Los *router* anuncian periódicamente sus direcciones IP en subredes si han sido configurados para que lo hagan. Los anuncios se hacen en la dirección de *multicast* (224.0.0.1) o de *broadcast* limitado (255.255.255.255). el comportamiento por defecto es enviar anuncios cada 10

minutos con un TTL de 1800 (30 minutos). Los *routers* también responden a los mensajes de solicitud que puedan recibir. Pueden responder directamente al solicitante, o esperar un intervalo de tiempo aleatorio y relativamente corto y responder con un *multicast*. Los *hosts* pueden enviar solicitudes hasta que reciben una respuesta. Las solicitudes se envían a la dirección de *multicast* para todos los *routers* (224.0.0.2) o a la de *broadcast* limitado (255.255.255.255). Típicamente, tres mensajes de solicitud se envían a intervalos de 3 segundos. Alternativamente, un host puede esperar a los anuncios efectuados periódicamente. Cada vez que un host recibe un anuncio, actualiza su *router* por defecto si el nuevo anuncio tiene una preferencia superior y fija el TTL para que la entrada se ajuste al valor del nivel de preferencia. Cuando el host recibe un nuevo valor para su *router* por defecto actual, pone el valor TTL al del nuevo anuncio. Esto proporciona además un mecanismo para que los *router* se declaren no disponibles: envían un anuncio con un TTL de cero.

**Parameter Problem (12) problemas de parametro**



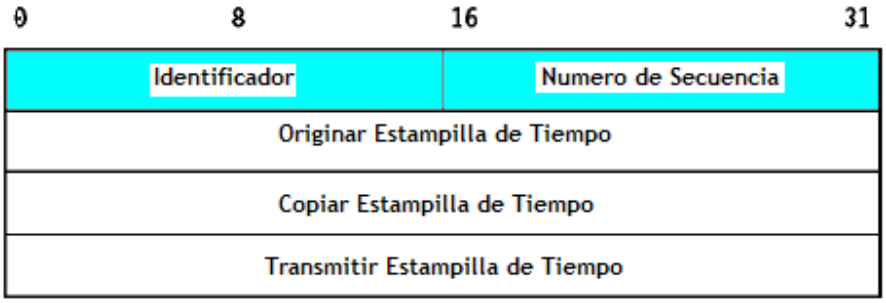

Indica que se encontró un problema durante el procesamiento de los parámetros de la cabecera IP. El campo puntero apunta al byte del datagrama original en el

que se encontró el problema. La cabecera ICMP puede tener uno de los siguientes valores:

0 - *unspecified error*

1 -*required option missing*

**Timestamp Request (13) y Timestamp Reply (14) solicitud y respuesta de marca de tiempo**

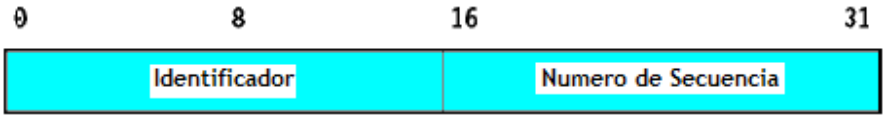



Estos dos mensajes se emplean para medir el rendimiento y para la depuración. No se emplean para la sincronización: para eso está el NTP (*Network Time Protocol*).

El host fuente envía el identificador y el número de secuencia(usado si se envían múltiples mensajes *timestamp requests*), fija su sello de tiempo y se lo envía al receptor. El host receptor fija el valor de los sellos de tiempo de recepción y de envío, cambia el tipo del mensaje a *timestamp reply* y se lo devuelve al receptor. El receptor dispone de dos sellos de tiempo en caso de que haya una diferencia sensible entre los tiempos de recepción y de transmisión, aunque en la práctica la mayoría de las implementaciones efectuarán ambas operaciones (recepción y

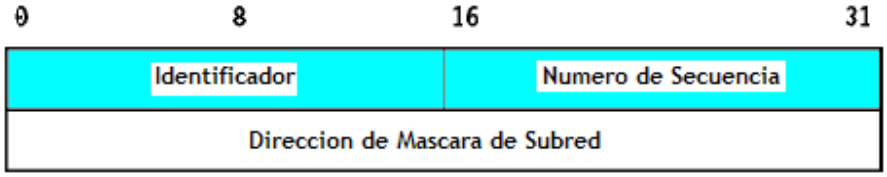
respuesta) de una sola vez, dando a los dos sellos el mismo valor. Los sellos de tiempo indican el número de milisegundos transcurridos desde la medianoche según el meridiano de *Greenwich* (GMT).

**Information Request (15) e Information Reply (16) solicitud y respuesta de informacion (obsoletos)**




El mensaje *Information Request* lo lanza un *host* para obtener una dirección IP para una red con la que está conectado. El *host* fuente envía la solicitud con la dirección IP de destino puesta a cero en la cabecera IP (refiriéndose a su propia red) y espera una respuesta de un servidor autorizado a asignar direcciones IP a otros *hosts*. La cabecera ICMP vale cero. La respuesta contendrá las direcciones IP de red en los campos de dirección fuente y dirección de destino de la cabecera IP. Este mecanismo está obsoleto.

**Address Mask Request (17) y Address Mask Reply (18) solicitud y respuesta de mascara**



El mensaje *Address Mask Request* es usado por un host cuando quiere determinar qué máscara de subred usa la red a la que está conectado. Los *hosts* se configuran con su máscara de subred, pero se puede dar el caso de una estación de trabajo sin disco, donde se deba obtener esta información de un servidor. Un host utiliza RARP para obtener su dirección IP. Para obtener una máscara de subred, el host hace un *broadcast* del mensaje *Address Mask Request*. Cualquier host en la red que se haya configurado para enviar mensajes *Address Mask Reply* rellenará esta máscara, convertirá el tipo del mensaje a *Address Mask Reply* y se lo devolverá al *host* fuente. La cabecera ICMP tiene valor cero.

### 2.2.3 Funcionamiento de ARP

**ARP (Protocolo de Resolución de direcciones)** El protocolo ARP *(Address Resolution Pro*tocol) tiene como función convertir las direcciones IP en direcciones físicas (de red y local), y al hacerlo, elimina la necesidad de que las aplicaciones sepan direcciones físicas. [5]

Los sistemas LAN usan ARP para descubrir información sobre su dirección física. Cuando una estación quiere empezar a comunicarse con otra estación local, busca la dirección de IP del otro en su tabla de ARP, que normalmente se mantiene en memoria. Si no existe una entrada para esa dirección de IP, el host difunde una solicitud de ARP que contiene la dirección de IP de destino.

[5] CISCO SYSTEMS, Inc. Academia de Networking de Cisco *Systems*: Guía del primer año.

La estación destino reconoce su dirección de IP y lee la consulta. Lo primero que hace es actualizar su propia tabla de traducción de direcciones con la dirección física del origen y luego envía de vuelta una respuesta que contiene su propia dirección de la interfaz hardware o dirección física. El origen al momento de recibir la respuesta, actualiza su tabla de ARP y queda listo para transmitir datos por la LAN.

**ARP Sustituto (proxy ARP)** Los términos *ARP sustituto (proxy, ARP) y ARP hack,* se refieren a la segunda técnica utilizada para transformar un solo prefijo IP de red en dos direcciones físicas, esta técnica sólo se aplica en redes que utilizan ARP para convertir direcciones de red en direcciones físicas. El modo de operación es el siguiente:

Cuando una estación que esta fuera de nuestra LAN, hace una petición a una estación nuestra, un dispositivo intermedio (por lo general un router) envía una respuesta ARP con su dirección física de parte de un nodo final (estación de nuestra red) a la estación solicitante.

Con la respuesta recibida la estación solicitante (la que esta fuera de nuestra LAN) actualiza su tabla ARP y utiliza la dirección recibida (dirección del Proxy) para enviar los datagramas destinados a la estación de nuestra LAN. Esto sin darse cuenta que en realidad los datagramas inicialmente se están enviando al Proxy y de ahí es que se dirigen hacia la estación destino de nuestra LAN.

Los routers que utilizan la técnica de ARP sustituto, tornan ventaja de una característica importante del protocolo ARP, a saber, la confianza. ARP está basado en la idea de que todas las máquinas cooperan y de que cualquier respuesta es legítima. La mayor parte de los anfitriones instalan asociaciones obtenidas por medio de ARP sin verificar su validez y sin mantener una consistencia. Por lo tanto, puede suceder que la tabla ARP asocie muchas direcciones IP en la misma dirección física, sin embargo, esto no viola las especificaciones del protocolo.

Algunas implantaciones de ARP no son tan poco exigentes como otras. En particular, las implementaciones ARP diseñadas para alertar a los administradores de posibles violaciones de seguridad les informarán siempre que dos direcciones IP distintas se transformen en la misma dirección física de hardware. El propósito de alertar al administrador es avisarle sobre el *spoofing,* situación en la que una máquina indica ser otra para poder interceptar paquetes. Las implantaciones de ARP en anfitriones que alertan a los administradores del posible *spoofing* no se pueden utilizar en redes que tienen routers sustitutos ARP, ya que el software generaria mensajes con gran frecuencia.

La principal ventaja de ARP sustituto es que se puede agregar a un solo router en una red sin alterar las tablas de ruteo en otros anfitriones o routers en esa red. Por lo tanto, el software ARP sustituto (proxy ARP) oculta completamente los detalles de las conexiones físicas. Además, Esta técnica puede reducir el uso del ancho de banda en enlaces WAN de baja velocidad.

La principal desventaja de ARP sustituto es que no trabaja para las redes a menos que utilicen ARP para la definición de direcciones. Además, no se generaliza para topologías de red más complejas (por ejemplo, muchos routers que interconectan dos redes físicas), ni incorpora una forma razonable para el ruteo. De hecho, la mayor parte de las implantaciones de ARP confía en los administradores para el mantenimiento manual de máquinas y direcciones, haciendo que se ocupe tiempo y se tenga propensión a los errores.

### 2.2.4 Funcionamiento RARP

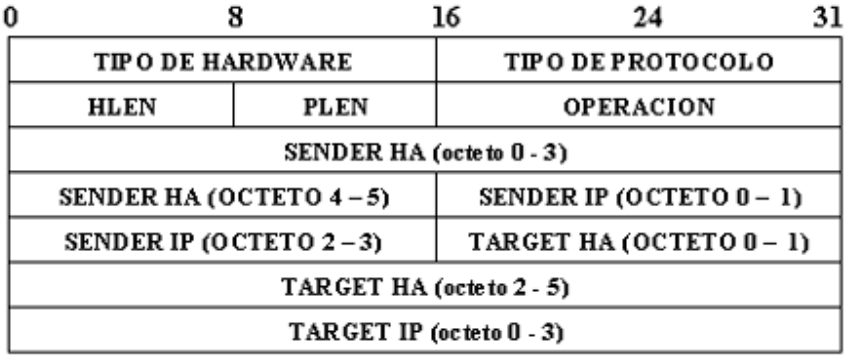
**RARP (ARP inverso)** Para ayudar a un nodo a descubrir su propia dirección de IP se diseñó una variante del ARP llamado *ARP inverso* (RARP - *reverse ARP).* El objetivo era que lo usasen las estaciones de trabajo sin disco y otros dispositivos que necesitasen obtener configuración de red de un servidor de red. [5]

La estación que usa el protocolo ARP inverso difunde una petición en la que indica su dirección física y solicita su dirección de IP. Un servidor de la red, configurado con una tabla de direcciones físicas y las correspondientes direcciones de IP responde a la petición.

ARP inverso ha sido superado por el protocolo BOOTP y su versión mejorada, el *Protocolo de configuración dinámica de host (DHCP - Dynamic Host Configuration Protocol).* Estos protocolos son más potentes y se usan para conseguir un conjunto completo de parámetros de configuración de un sistema TCP/IP.

[5] CISCO SYSTEMS, Inc. Academia de Networking de Cisco *Systems*: Guía del primer año.

**Formato De Mensaje ARP / RARP**




El campo **tipo de hardware** específica un tipo de interfaz de hardware para el que el transmisor busca una respuesta; contiene el valor 1 para Ehternet.

De forma similar, el campo **tipo de protocolo** especifica el tipo de dirección de protocolo de alto nivel que proporcionó el transmisor. Contiene $0800_{16}$ para la dirección IP.

El campo **operación** específica una solicitud ARP (1), una respuesta ARP (2), una solicitud RARP (3) o una respuesta RARP (4).

Los campos **HLEN** y **PLEN** permiten que ARP se utilice con redes arbitrarias ya que éstas especifican la longitud de la dirección de hardware y la longitud de la dirección del protocolo de alto nivel.

El transmisor proporciona sus direcciones IP y de hardware, si las conoce, en los campos **SENDER HA** y **SENDER IP**.

Cuando realiza una solicitud, el transmisor también proporciona la dirección IP del objetivo (ARP) o la dirección de hardware del objetivo (RARP), utilizando los campos **TARGET HA** y **TARGET IP**.

Antes de que la máquina objetivo responda, completa las direcciones faltantes, voltea los pares de objetivo y transmisor, y cambia la operación a respuesta. Por lo tanto, una respuesta transporta las direcciones tanto de hardware como de TP del solicitante original, lo mismo que las direcciones de hardware e IP de la máquina para la que se realizó asignación.

Tabla ARP (caché ARP)

Cada ordenador almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada a su tabla. Para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red direcciones físicas, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla. Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias. En cada línea de la tabla hay la siguiente información:

· Índice IF: indica el puerto físico

· Dirección física: dirección física del dispositivo

· Dirección IP: la dirección IP que corresponda a la dirección física

# CAPÍTULO TRES

## ENRUTAMIENTO Y DIRECCIONAMIENTO

## 3.1 DETERMINACIÓN DE RUTAS

Para el tráfico que atraviesa una nube de red, la determinación de ruta se produce en la capa de red (Capa 3). La función de determinación de ruta permite al router evaluar las rutas disponibles hacia un destino y establecer el mejor manejo de un paquete. Los servicios de enrutamiento utilizan información de topología de red al evaluar las rutas de una red. Esta información la puede configurar el administrador de red o se puede recopilar a través de procesos dinámicos ejecutados en la red.

La capa de red proporciona entrega de paquetes de máximo esfuerzo y de extremo a extremo a través de redes interconectadas. La capa de red utiliza la tabla de enrutamiento IP para enviar paquetes desde la red origen a la red destino. Después de que el router determina qué ruta debe utilizar, procede a enviar el paquete. Toma el paquete que aceptó en una interfaz y lo envía hacia otra interfaz o puerto que represente la mejor ruta hacia el destino del paquete.[5]

## 3.2 CLASES DE DIRECCION IP

Hay tres clases de direcciones IP que una organización puede recibir de parte del Registro Estadounidense de Números de Internet (ARIN) (o ISP de la organización): Clase A, B y C. En la actualidad, ARIN reserva las direcciones de Clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan

[5] CISCO SYSTEMS, Inc. Academia de Networking de Cisco *Systems*: Guía del primer año.

otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de Clase B para las medianas empresas. Se otorgan direcciones de Clase C para todos los demás solicitantes.

**Clase A**

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección de Clase A siempre es 0. Un ejemplo de una dirección IP de clase A es 124.95.44.15. El primer octeto, 124, identifica el número de red asignado por ARIN. Los administradores internos de la red asignan los 24 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase A es verificar el primer octeto de su dirección IP, cuyo valor debe estar entre 0 y 126. (127 *comienza* con un bit 0, pero está reservado para fines especiales).

Todas las direcciones IP de Clase A utilizan solamente los primeros 8 bits para identificar la parte de la red de la dirección. Los tres octetos restantes se pueden utilizar para la parte del host de la dirección. A cada una de las redes que utilizan una dirección IP de Clase A se les pueden asignar hasta 2 elevado a la 24 potencia ($2^{24}$) (menos 2), o 16.777.214 direcciones IP posibles para los dispositivos que están conectados a la red.

**Clase B**

Los primeros 2 bits de una dirección de Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP de Clase B es 151.10.13.28. Los dos primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 16 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase B es verificar el primer octeto de su dirección IP. Las direcciones IP de Clase B siempre tienen valores que van del 128 al 191 en su primer octeto.

Todas las direcciones IP de Clase B utilizan los primeros 16 bits para identificar la parte de la red de la dirección. Los dos octetos restantes de la dirección IP se encuentran reservados para la porción del host de la dirección. Cada red que usa un esquema de direccionamiento IP de Clase B puede tener asignadas hasta 2 a la 16ta potencia ($2^{16}$) (menos 2 otra vez), o 65.534 direcciones IP posibles a dispositivos conectados a su red.

**Clase C**

Los 3 primeros bits de una dirección de Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP de Clase C es 201.110.213.28. Los tres primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 8 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase C es verificar el

primer octeto de su dirección IP. Las direcciones IP de Clase C siempre tienen valores que van del 192 al 223 en su primer octeto.

Todas las direcciones IP de Clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Sólo se puede utilizar el último octeto de una dirección IP de Clase C para la parte de la dirección que corresponde al host. A cada una de las redes que utilizan una dirección IP de Clase C se les pueden asignar hasta $2^8$ (menos 2), o 254, direcciones IP posibles para los dispositivos que están conectados a la red.

### 3.3 PRINCIPIOS BÁSICOS SOBRE SUBREDES

La máscara de subred (término formal: prefijo de red extendida), le indica a los dispositivos de red cuál es la parte de una dirección que corresponde al campo de red y cuál es la parte que corresponde al campo de host. Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección IP. [6]

Para determinar la máscara de subred para una dirección IP de subred particular, siga estos pasos. (1) Exprese la dirección IP de subred en forma binaria. (2) Cambie la porción de red y subred de la dirección por todos unos. (3) Cambie la porción del host de la dirección por todos ceros. (4) Como último paso, convierta la expresión en números binarios nuevamente a la notación decimal punteada.

[6] PAQUET, Catherine. Building Scalable CISCO Networks.

## 3.4 CREACIÓN DE UNA SUBRED

La razón principal para usar una subred es reducir el tamaño de un dominio de broadcast. Se envían broadcasts a todos los hosts de una red o subred. Cuando el tráfico de broadcast empieza a consumir una porción demasiado grande del ancho de banda disponible, los administradores de red pueden preferir reducir el tamaño del dominio de broadcast.

Las direcciones de subred incluyen la porción de red de Clase A, Clase B o Clase C además de un campo de subred y un campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original para toda la red. La capacidad de decidir cómo dividir la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad para el direccionamiento al administrador de red. Para crear una dirección de subred, un administrador de red pide prestados bits de la parte original de host y los designa como campo de subred.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. La cantidad mínima de bits que se puede pedir prestada es 2. Si fuera a pedir prestado sólo 1 bit para crear una subred, entonces sólo tendría un número de red (el.0 de red) y el número de broadcast (el .1 de red). La cantidad mínima de bits que se puede pedir prestada puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

### 3.4.1 Determinación de ruta de una subred en un router

Esta práctica de laboratorio lo ayudará a comprender los principios básicos de las máscaras de subred IP y de su uso con las redes TCP/IP. La máscara de subred se puede usar para dividir una red existente en "subredes". Esto se puede hacer para 1) reducir el tamaño de los dominios de broadcast (crear redes más pequeñas con menos tráfico), 2) permitir que las LAN de distintas ubicaciones geográficas se puedan comunicar entre sí o 3) por motivos de seguridad, para separar una LAN de otra . Los routers separan subredes y el router determina si un paquete puede desplazarse desde una subred hacia otra. Cada router por el que pasa un paquete se considera como un "salto". Las máscaras de subred ayudan a que las estaciones de trabajo, los servidores y los routers de una red IP determinen si el host destino para el paquete que desean enviar está ubicado en su propia red o en otra red. Las máscaras de subred por defecto se describieron en una práctica de laboratorio anterior. En esta práctica de laboratorio se hará un repaso de la máscara de subred por defecto y luego se ocupará de las máscaras de subred personalizadas que usarán más bits que la máscara de subred por defecto al "pedir prestados" estos bits de la parte correspondiente al host de la dirección IP. Esto crea una dirección de tres partes; 1) La dirección de red original asignada, 2) la dirección de subred compuesta por los bits que se pidieron prestados 3) la dirección host compuesta por los bits que quedaron luego de haber prestado algunos bits para las subredes.

**Conceptos básicos sobre direcciones IP.**

Las direcciones de red IP son asignadas por el Centro de Informaciones de la Red de Internet (InterNIC). Si su empresa tiene una dirección de red IP clase "A", InterNIC asigna el primer octeto (8 bits) y la empresa puede usar los 24 bits restantes para definir hasta 16.777.214 hosts de la red. ¡Ésta es una gran cantidad de hosts! No es posible colocar todos estos hosts en una red física sin separarlos mediante routers y subredes. Una estación de trabajo puede estar ubicada en una red o subred y un servidor puede estar ubicado en otra red o subred. Cuando la estación de trabajo necesita recuperar un archivo del servidor, debe utilizar su máscara de subred para determinar la red o la subred en la que está ubicado el servidor. El propósito de una máscara de subred es ayudar a los hosts y routers a determinar la ubicación de la red en la que se puede ubicar al host destino. Consulte la siguiente tabla para repasar las clases de dirección IP, las máscaras de subred por defecto y la cantidad de redes y hosts que se pueden crear con cada clase de dirección de red.

| Cls | Intervalo decimal del 1er octeto | Bits de orden superior del 1er octeto | ID de Red / Host (N=Red, H=Host) | Máscara de subred por defecto | Cantidad de redes | Hosts por red (direcciones utilizables) |
|---|---|---|---|---|---|---|
| A | 1 - 126* | 0 | N.H.H.H | 255.0.0.0 | 126 (27 - 2) | 16.777.214 (2 24 - 2) |
| B | 128 – 191 | 1 0 | N.N.H.H | 255.255.0.0 | 16.382 (214 - 2) | 65.534 (2 16 - 2) |
| C | 192 – 223 | 1 1 0 | N.N.N.H | 255.255.255.0 | 2.097.150 (221 - 2) | 254 (2 8 - 2) |
| D | 224 – 239 | 1 1 1 0 | Reservado para multicast | | | |
| E | 240 – 254 | 1 1 1 1 0 | Experimental, se utiliza para fines de investigación | | | |

**TABLA 4.** Direcciones de Máscara de Subred

**El proceso de "AND".**

Explicación: Los hosts y routers utilizan el proceso de "AND" para determinar si un host destino está ubicado o no en la misma red. El proceso de AND se ejecuta cada vez que un host desea enviar un paquete hacia otro host de una red IP. Si desea conectarse a un servidor, es posible que conozca la dirección IP del servidor al que se desea conectar o simplemente puede escribir el nombre del host (por ej., www.cisco.com) y un Servidor de denominación de dominio (DNS) convertirá el nombre de host en una dirección IP. En primer lugar, el host origen compara (AND) su propia dirección IP con su propia máscara de subred. El resultado de AND es identificar la red en la que reside el host origen. Luego compara la dirección IP destino con su propia máscara de subred. El resultado del 2do AND es la red en la que está ubicado el host destino. Si las direcciones de red origen y destino son las mismas, se pueden comunicar directamente. Si los resultados son distintos, entonces están ubicados en distintas redes o subredes y se deben comunicar a través de routers o es posible que no se puedan comunicar en absoluto.[5]

AND depende de la máscara de subred. La máscara de subred por defecto para una red Clase C es 255.255.255.0 ó 11111111.111111111.111111111.00000000. Esta se compara bit por bit con la dirección IP origen. El primer bit de la dirección IP se compara con el primer bit de la máscara de subred y el segundo bit se

[5] CISCO SYSTEMS, Inc. Academia de Networking de Cisco *Systems*: Guía del primer año

compara con el segundo, etc. Si los dos bits son unos, el resultado de AND es un UNO. Si los dos bits son cero y un uno o dos ceros, el resultado de AND es un CERO. Básicamente, esto significa que una combinación de 2 unos da como resultado un UNO, cualquier otra combinación da como resultado cero. El resultado del proceso de AND es el número de red o de subred en la que está ubicada la dirección origen o destino.

**Dos redes Clase C que utilizan la máscara de subred por defecto.**

Explicación: Este ejemplo muestra la forma en que se puede utilizar una máscara de subred por defecto Clase C para determinar cuál es la red en la que está ubicado un host. Una máscara de subred por defecto no separa una dirección en subredes. Si se utiliza la máscara de subred por defecto, la red no se "divide en subredes". El host X (origen) de la red 200.1.1.0 tiene una dirección IP 200.1.1.5 y desea enviar un paquete al host Z (destino) de la red 200.1.2.0 y tiene una dirección IP 200.1.2.8. Todos los hosts de cada red están conectados a hubs o switches y luego a un router. Recuerde que en el caso de una dirección de red Clase C, el American Registry for Internet Numbers (ARIN) asigna los 3 primeros octetos (24 bits) como la dirección de red de modo que estas son dos redes Clase C distintas. Esto deja un octeto (8 bits) para los hosts de modo que cada red Clase C puede tener hasta 254 hosts (2^8 = 256 - 2 = 254).

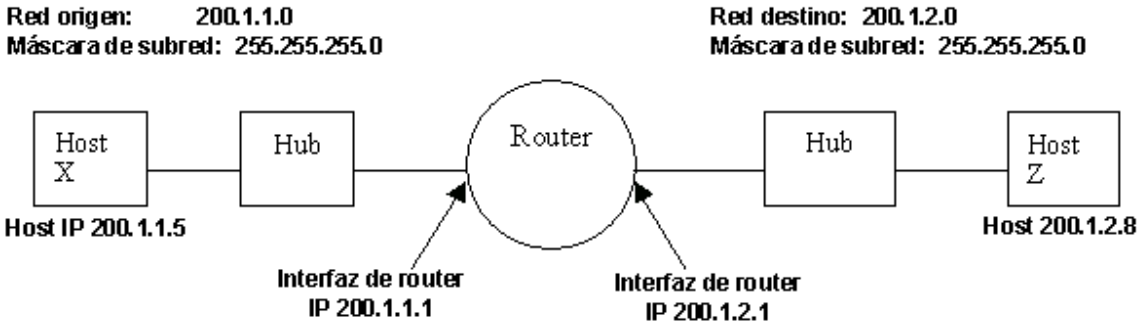



**Figura 16.** Esquema para la creación de una subred

El proceso de AND ayuda a que el paquete llegue desde el host 200.1.1.5 de la red 200.1.1.0 hasta el host 200.1.2.8 de la red 200.1.2.0 siguiendo estos pasos.

El host X compara su propia dirección IP con su propia máscara de subred utilizando el proceso de AND

| | |
|---|---|
| Dirección IP del host X 200.1.1.5 | 11001000.00000001.00000001.00000101 |
| Máscara de subred 255.255.255.0 | 11111111.11111111.11111111.00000000 |
| Resultado de AND (200.1.1.0) | 11001000.00000001.00000001.00000000 |

**TABLA 5.** Resultados de AND para una máscara de subred

NOTA: El resultado del paso 3a del proceso de AND es la dirección de red del host X, que es 200.1.1.0

A continuación, el host X compara la dirección IP del Host Z destino con su propia máscara de subred utilizando el proceso de AND.

| | |
|---|---|
| Dirección IP del Host Z 200.1.2.8 | 11001000.00000001.00000010.00001000 |
| Máscara de subred 255.255.255.0 | 11111111.11111111.11111111.00000000 |
| Resultado de AND (200.1.2.0) | 11001000.00000001.00000010.00000000 |

**TABLA 6.** Resultados 2 de AND para una máscara de subred

NOTA: El resultado del paso 3b del proceso de AND es la dirección de red del host Z, que es 200.1.2.0.

El host X compara los resultados de AND del paso A y el resultado de AND del paso B y observa que son distintos. Ahora el host X sabe que el host Z no está ubicado en su Red de área local (LAN) y que debe enviar el paquete hacia su "Gateway por defecto", que es la dirección IP de la interfaz del router de 200.1.1.1 de la red 200.1.1.0. Luego el router repite el proceso de AND para determinar cuál es la interfaz del router a través de la cual debe enviar el paquete.

**Red Clase C que utiliza una máscara de subred personalizada.**

Explicación: En este ejemplo se utiliza una sola dirección de red Clase C (200.1.1.0) y se mostrará cómo se puede utilizar una máscara de subred Clase C personalizada para determinar cuál es la subred en la que está ubicado un host y cómo enrutar paquetes desde una subred a otra. Recuerde que en el caso de una

dirección de red Clase C, ARIN asigna los 3 primeros octetos (24 bits) como la dirección de red. Esto deja 8 bits (un octeto) para los hosts de modo que cada red Clase C puede tener hasta 254 hosts (2^8 = 256 - 2 = 254).

Tal vez desea tener menos de 254 hosts (estaciones de trabajo y servidores) en una red y desea crear 2 subredes y separarlos utilizando un router por motivos de seguridad o para reducir el tráfico. Esto hará que se creen dominios de broadcast más pequeños e independientes y puede mejorar el desempeño de la red y aumentar la seguridad ya que estas subredes estarán separadas por un router. Suponga que necesita por lo menos 2 subredes y 50 hosts por subred. Como sólo tiene una dirección de red Clase C, sólo tiene 8 bits disponibles en el cuarto octeto para un total de 254 hosts posibles, debe crear una máscara de subred personalizada. Utilizará la máscara de subred personalizada para "PEDIR PRESTADOS" bits de la parte de la dirección que corresponde al host. Los siguientes pasos lo ayudarán a lograr esto:

El primer paso para "realizar la división en subredes" es determinar cuántas subredes se necesitan. En este caso, se necesitan 2 subredes. Para ver cuántos bits se deben pedir prestados a la parte de la dirección de red que corresponde al host, agregue los valores de bit de derecha a izquierda hasta que el total sea igual o mayor que la cantidad de subredes que se necesitan. Como se necesitan 2 subredes, agregue el bit uno y el bit dos, lo que equivale a tres. Esta cantidad es mayor que la cantidad de subredes que son necesarias, de modo que se deben pedir prestados por lo menos dos bits de la dirección de host comenzando desde el lado izquierdo del octeto que contiene la dirección host.

| Dirección de red 200.1.1.0 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4to octeto de bits de la dirección de host: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Valores de bits de la dirección de host (desde la derecha) | 128 | 64 | 32 | 16 | 8 | 4 | **2** | **1** |

**TABLA 7.** Valores de bits del host

(Agregue bits desde el lado derecho (el 1 y el 2) hasta obtener una cantidad mayor que la del número de subredes que son necesarias)

Una vez que sabemos cuántos bits se deben pedir prestados, los bits se toman empezando por el lado izquierdo del primer octeto de la dirección host. Cada bit que se le pide prestado al host hace que queden menos bits para los hosts. Aunque la cantidad de subredes aumenta, la cantidad de hosts por subred disminuye. Como se deben pedir prestados 2 bits del lado izquierdo, se debe indicar ese nuevo valor en la máscara de subred. La máscara de subred por defecto era 255.255.255.0 y la nueva máscara de subred "personalizada" es 255.255.255.192. El 192 proviene del valor de los dos primeros bits de la izquierda (128 + 64 = 192). Ahora estos bits se transforman en 1 (unos) y forman parte de la máscara de subred general. Esto deja 6 bits para las direcciones IP de host o 2^6 = 64 hosts por subred.

| Bits prestados por el 4to octeto para subred: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|
| Valores de bits de subred: (desde la izquierda) | **128** | **64** | 32 | 16 | 8 | 4 | 2 | 1 |

**TABLA 8.** Valores de bits de subred

Con esta información, puede crear la siguiente tabla. Los dos primeros bits son el valor binario de la subred. Los últimos 6 bits son los bits del host. Al pedir prestados 2 bits de los 8 bits de la dirección de host, se pueden crear 4 subredes con 64 hosts cada una. Las 4 redes creadas son la red "0", la red "64", la red "128" y la red "192". La red "0" y la red "192" se consideran no utilizables. Esto se debe a que la red "0" tiene sólo ceros en la parte de la dirección que corresponde a la subred y la red 192 tiene sólo unos en la parte de la dirección que corresponde a la subred.

| Nro. de subred | Valor binario de los bits de subred prestados | Valor decimal de los bits de subred | Valores (intervalo) binarios posibles de bits de host (6 bits) | Intervalo en decimales de subred / Host | ¿Utilizables? |
|---|---|---|---|---|---|
| Subred 0 | 00 | 0 | 000000 – 111111 | 0 – 63 | NO |
| Subred 1 | 01 | 64 | 000000 - 111111 | 64 - 127 | SÍ |
| Subred 2 | 10 | 128 | 000000 - 111111 | 128 - 191 | SÍ |
| Subred 3 | 11 | 192 | 000000 - 111111 | 192 - 254 | NO |

**TABLA 9.** Subredes

Tenga en cuenta que la primera subred siempre comienza en 0 y, en este caso, aumenta de 64 en 64 que es la cantidad de hosts de cada subred. Una de las formas en que se puede determinar la cantidad de hosts de cada subred o el inicio de cada subred es elevar los bits de host restantes al cuadrado. Como se han pedido prestados dos de los 8 bits para subredes y quedan seis bits, la cantidad

de hosts por subred es 2^6 ó 64. Otra de las formas para calcular la cantidad de hosts por subred o el "incremento" de una subred a la siguiente es restar el valor de la máscara de subred en decimales (192 en el cuarto octeto) a 256 (que es la cantidad máxima de combinaciones de 8 bits posibles) que equivale a 64. Esto significa que se comienza en 0 para la primera red y se agrega 64 para cada subred adicional. Si se toma la segunda subred (la red 64) como ejemplo de la dirección IP 200.1.1.64 no se puede utilizar para un ID de host porque es el "ID de red" de la subred "64" (la parte que corresponde al host son todos ceros) y la dirección IP 200.1.1.127 no se puede utilizar porque es la dirección de broadcast de la red 64 (la parte que corresponde al host son todos unos).

**Red Clase C que utiliza una máscara de subred personalizada.**

Tarea: Use la siguiente información y los ejemplos anteriores para responder las siguientes preguntas sobre las subredes.

Explicación: Su empresa ha presentado una solicitud para una dirección de red Clase C 197.15.22.0 que ha sido aprobada. Desea subdividir la red física en 4 subredes, interconectadas por routers. Necesitará por lo menos 25 hosts por subred. Deberá utilizar una máscara de subred personalizada Clase C y tendrá un router entre las subredes para enrutar el paquete desde una subred a otra. Determine la cantidad de bits que debe pedir prestados a la parte de la dirección de red que corresponde al host y luego la cantidad de bits que quedan para las direcciones de host. (Ayuda: Habrá 8 subredes)

Complete la tabla que aparece a continuación y responda las siguientes preguntas:

| Nro. De subred | Valor binario de los bits de subred prestados | Nro. de subred decimal & de los bits de subred. | Valores (intervalo) binarios posibles de bits de host (6 bits) | Intervalo en decimales de subred / Host | ¿Utilizar? |
|---|---|---|---|---|---|
| Subred 0 | 000 | 0 (197.15.22.0) | 00000 - 11111 | 0 - 31 | NO |
| Subred 1 | 001 | 32 (197.15.22.32) | 00000 - 11111 | 32 - 63 | SÍ |
| Subred 2 | 010 | 64 (197.15.22.64) | 00000 - 11111 | 64 - 95 | SÍ |
| Subred 3 | 011 | 96 (197.15.22.96) | 00000 - 11111 | 96 - 127 | SÍ |
| Subred 4 | 100 | 128 (197.15.22.128) | 00000 - 11111 | 128 - 159 | SÍ |
| Subred 5 | 101 | 160 (127.15.22.160) | 00000 - 11111 | 160 - 191 | SÍ |
| Subred 6 | 110 | 192 (127.15.22.192) | 00000 - 11111 | 192 - 223 | SÍ |
| Subred 7 | 111 | 224 (127.15.22.224) | 00000 - 11111 | 224 - 255 | NO |

**TABLA 10.** Solución para la creación de subredes

¿Qué octeto u octetos representan la parte que corresponde a la red de una dirección IP Clase C? los tres primeros octetos de izquierda a derecha.

¿Qué octeto u octetos representan la parte que corresponde al host de una dirección IP Clase C? El ultimo octeto de izquierda a derecha.

¿Cuál es el equivalente binario de la dirección de red Clase C en el ejemplo (197.15.22.0)? Dirección de red en decimales: 197.15.22.0

Dirección de red en binarios: 11000101.00001111.00010110.00000000

¿Cuántos bits de orden superior se pidieron prestados a los bits de host en el cuarto octeto? 3 bits

¿Cuál es la máscara de subred que debe usar (mostrar la máscara de subred en decimales y binarios)? Máscara de subred en decimales:255.255.255.224 Máscara de subred en binarios:11111111.11111111.11111111.11100000

¿Cuál es la cantidad máxima de subredes utilizables que se pueden crear con esta máscara de subred? 6 subredes =8-2=2*2*2-2

¿Cuántos bits quedaron en el 4to octeto para los ID de hosts? 5 bits

¿Cuántos hosts por subred se pueden definir con esta máscara de subred? 32

¿Cuál es la cantidad máxima de hosts que se pueden definir para todas las subredes para este ejemplo (suponiendo que no se pueden utilizar los números más bajos y más altos de subred ni los ID de host más bajo y más alto de cada subred)? 180=6(subredes utilizables)*30(dir IP utilizables por subred)

¿Es 197.15.22.63 una dirección IP de host válida para este ejemplo? no

¿Por qué? (o por qué no) esta dirección es de broadcast PARA LA SUBRED1.

¿Es 197.15.22.160 una dirección IP de host válida para este ejemplo? no

¿Por qué? (o por qué no) por que esta es la dirección de la subred5. El host "A" tiene una dirección IP 197.15.22.126. El host "B" tiene una dirección IP 197.15.22.129. ¿Estos hosts están ubicados en la misma subred? No

¿Por qué? Si vemos la tabla del punto 1 nos damos cuenta que estan en subredes diferentes, el HOST A Esta eN LA SUBRED3 Y HOST B EN la SUBRED4. Ademas de poderlo demostrar de la siguiente manera:

Calculamos la funcion AND para la IP del host A con su Mascara de Subred, y para la IP del host B con su Mascara de Subred.

| | |
|---|---|
| Dirección IP del host A 197.15.22.126 | 11000101.00001111.00010110.01111110 |
| Máscara de subred 255.255.255.224 | 11111111.11111111.11111111.11100000 |
| Resultado de AND (197.15.22.96) | 11000101.00001111.00010110.01100000 |
| Dirección IP del Host B 197.15.22.129 | 11000101.00001111.00010110.10000001 |
| Máscara de subred 255.255.255.224 | 11111111.11111111.11111111.11100000 |
| Resultado de AND (197.15.22.128) | 11000101.00001111.00010110.10000000 |

**TABLA 11.** Cálculos de la función AND

Si comparamos los resultados de AND para el host A CON SU MASCARA DE SUBRED con el resultado de AND para el host B CON SU MASCARA DE SUBRED observamos que son distintos. Queriendo decir que el host A y el host B no están ubicados en la misma subred.

**Determinación de ruta**

La función de determinación de ruta permite al router evaluar las rutas disponibles hacia un destino y establecer la mejor ruta para enrutar un paquete. El enrutamiento se refiere al proceso de selección de la mejor ruta a través de la cual se envían paquetes y cómo atravesar múltiples redes físicas. Esta es la base de todas las comunicaciones de Internet. La mayoría de los protocolos de

enrutamiento utilizan simplemente la ruta que es mejor y más corta, y utilizan distintos métodos para descubrir esta ruta. Los routers generalmente transfieren un paquete desde un enlace de datos a otro. Para transferir un paquete, el router utiliza 2 funciones básicas: una función de determinación de ruta y una función de conmutación. La función de conmutación permite que el router acepte un paquete de una interfaz y lo envié a otra. La función de determinación de ruta permite al router seleccionar la interfaz más adecuada para enviar un paquete, en otras palabras permite al router evaluar las rutas disponibles hacia un destino y establecer el mejor manejo de paquete. La porción de dirección de red se refiere a un puerto específico en el router que lleva a un dispositivo adyacente (router, switch) en esa dirección. El router final (conectado a la red destino) utiliza la porción de nodo de la dirección para entregar el paquete al host correcto. Este proceso se lleva a cabo en la capa de red 3. Cuando una aplicación de host necesita enviar un paquete hacia un destino de una red distinta, se recibe una trama de enlace de datos en una de las interfaces del router. El proceso de la capa de red del router examina el encabezado para determinar la red destino y luego consulta la tabla de enrutamiento que asocia las redes con las intercfaces salientes. La trama original se elimina y se descarta. El paquete se encapsula nuevamente en la trama de enlace de datos para la interfaz seleccionada y se ubica en la cola para su entrega al siguiente salto en la ruta. Este proceso tiene lugar cada vez que el paquete se conmuta a traves de otro router. En el router que se encuentra conectado a la red que contiene el host destino, el paquete se

encapsula nuevamente en el tipo de trama de enlace de datos de la LAN destino y se entrega al host destino.

### 3.4.2 Mascara de subred con IP Calculator

Aquí se trabajará con 5 routers y un esquema de direccionamiento IP. Debe obtener un esquema de direccionamiento IP correcto con una sola dirección de red Clase C (204.204.7.0) y múltiples subredes.

**Diseñar la topología física de la red.**

Debe tener por lo menos 5 routers en distintas ubicaciones geográficas. Deberá tener por lo menos una LAN Ethernet en cada router. Haga un boceto de la topología a medida que la va diseñando. Responda las siguientes preguntas para que sean de ayuda en la planificación:

1. ¿Cuántos routers tiene? 5

2. ¿Dónde están ubicados los routers? oficina1, oficina2, oficina3, oficina4, oficina5

3. ¿Cuántos switches tiene? 5

**Desarrollar un esquema de direccionamiento IP.**

Revise el boceto de la topología del paso uno. Utilizando la dirección Clase C 204.204.7.0, cree un diseño de subred para su topología. Documente el esquema indicando dónde colocará cada una de las subredes. Responda las siguientes preguntas para que sean de ayuda en la planificación.

4. ¿Cuántas LAN hay? 5

5. ¿Cuántas WAN hay? 3

6. ¿Cuántas subredes exclusivas necesita?8

7. ¿Cuántos hosts por subred (LAN y WAN) tiene? 2

8. ¿Cuántas direcciones IP (hosts + interfaces de router) se requieren? 22 (10 estaciones de trabajo y 12 interfaces de router)

9. ¿Cuál es su dirección de red Clase C? 204.204.7.0

10. ¿Cuántos bits le pedirá prestados a la porción de host de la dirección de red? 4

11. ¿Cuál es la máscara de subred? 255.255.255.240

12. ¿Cuántas subredes utilizables se permiten en total? 14 =16-2

13. ¿Cuántos hosts por subred se permiten? 14 =24 –2

**Asignar direcciones IP a cada interfaz de dispositivo.**

Utilizando la tabla, asigne una dirección IP a cada interfaz de dispositivo o intervalo de dispositivos (hosts) que requieran una dirección IP. Los switches no requieren una dirección IP, pero puede asignarles una si lo desea. Los hubs no tienen dirección IP.

| Nombre / modelo del dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway por defecto |
|---|---|---|---|---|
| Host0 | E1 | 204.204.7.18 | 255.255.255.240 | 204.204.7.17 |
| Host1 | E1 | 204.204.7.19 | 255.255.255.240 | 204.204.7.17 |
| Host2 | E0 | 204.204.7.34 | 255.255.255.240 | 204.204.7.33 |
| Host3 | E0 | 204.204.7.35 | 255.255.255.240 | 204.204.7.33 |
| Host4 | E0 | 204.204.7.50 | 255.255.255.240 | 204.204.7.49 |
| Host5 | E0 | 204.204.7.51 | 255.255.255.240 | 204.204.7.49 |
| Host6 | E0 | 204.204.7.66 | 255.255.255.240 | 204.204.7.65 |
| Host7 | E0 | 204.204.7.67 | 255.255.255.240 | 204.204.7.65 |
| Host8 | E0 | 204.204.7.82 | 255.255.255.240 | 204.204.7.81 |
| Host9 | E0 | 204.204.7.83 | 255.255.255.240 | 204.204.7.81 |

**TABLA 12.** Asignación de direcciones IP

14. ¿Cuál de las interfaces requiere que se establezca la velocidad del reloj? S0 en Lab-A, Lab-B y Lab-C

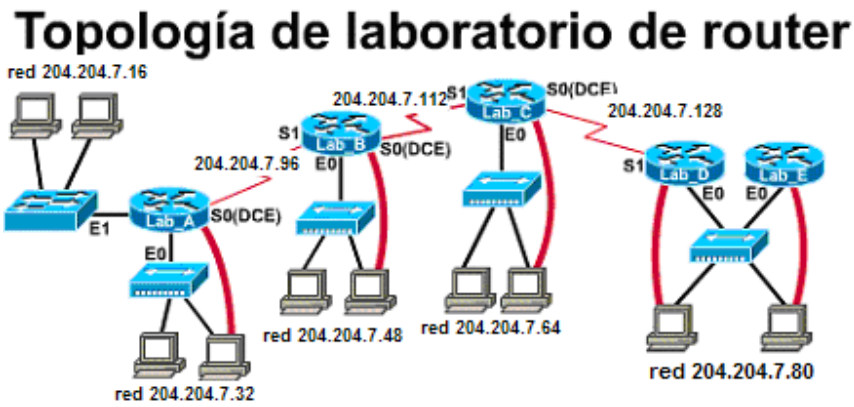



**Figura 17.** Topología del Laboratorio de Router

Los cálculos realizados anteriormente para saber cual es la mascara de subred para el ejemplo fueron hechos con IP_CALCULATOR de la siguiente manera:

1. Seleccionamos el tipo de dirección de red a la cual le calcularemos la mascara en el item address type.
2. elegimos el número de bits que se prestaran a la porción de host de la dirección de red, en subnet bits.

Este se calcula según las necesidades de la topología a usar en este caso dio como resultado 4, debido a que se querían utilizar 8 subredes y Recordando lo dicho anteriormente que para ver cuántos bits se deben pedir prestados a la parte de la dirección de red que corresponde al host, se agregan bit de derecha a izquierda hasta que el total sea igual o mayor que la cantidad de subredes que se necesitan.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Dirección de red 204.204.7.0 | | | | | | | | |
| 4to octeto de bits de la dirección de host: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Valores de bits de la dirección de host (desde la derecha) | 128 | 64 | 32 | 16 | **8** | **4** | **2** | **1** |

**TABLA 13.** Valores de bits de la dirección del Host

En este caso el resultado es 4 bits de donde se pueden crear 16 subredes

Para ver las direcciones que corresponden a cada subred se procede de la siguiente forma:

3. proporcionamos la dirección de red, en ip address de la sheet address info.
4. luego pasamos a la sheet subnet/host para ver el numero de subredes creadas con su respectivo rango de direcciones, subnet – host range.

# CAPÍTULO CUATRO

## LA CAPA DE RED EN INTERNET

**4.1 PROTOCOLO DE INFORMACIÓN DE RUTEO**

**4.1.1 Tabla de ruteo del RIP**

**4.2 PROTOCOLO DE ENRUTAMIENTO DE PASARELA INTERIOR**

**4.3 INTERIOR GATEWAY ROUTING PROTOCOL (IGRP)**

**4.4 ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)**

## 4. LA CAPA DE RED EN INTERNET

En la capa de red, la Internet puede verse como un conjunto de subredes, o sistemas autónomos (AS) interconectados. No hay una estructura real, pero existen backbone principales. Estos se construyen a partir de líneas de alto ancho de banda y enrutadores rápidos. Conectadas a los backbone hay redes regionales (de nivel medio), y conectadas a estas redes están las LAN de muchas universidades, compañías y proveedores de servicios de Internet. El responsable de mantener unida la Internet es el protocolo IP (Internet Protocol), Este se diseñó desde sus principios con la interconexión de redes en mente. Debe proporcionar el "mejor esfuerzo" para el transporte del datagrama del origen hacia el destino, sin importar si éstos están en la misma red o si hay otras redes entre ellos.[4]

### 4.1 PROTOCOLO DE INFORMACIÓN DE RUTEO

Internet se compone de una gran cantidad de sistemas autónomos (AS Un sistema autónomo está compuesto por routers, administrados por uno o más operadores, que presentan una visión coherente del enrutamiento ante el mundo exterior. El Centro de Información de la Red (NIC) asigna un sistema autónomo único a las empresas. Este sistema autónomo equivale a un número de 16 bits.

Los protocolos de enrutamiento exterior se utilizan para las comunicaciones entre sistemas autónomos, se le llama protocolo de pasarela exterior. Los protocolos de

[4] http://www.cisco.com

enrutamiento interior se utilizan dentro de un mismo sistema autónomo se llama protocolo de pasarela interior. [5]

El protocolo RIP, al igual que sus antecesores propietarios es un protocolo de ruteo que fue diseñado para funcionar como protocolo “vector distancia”. RIP fue diseñado para funcionar en redes pequeñas de pasarela interior. RIP está basado en la versión 4.3 de la distribución de UNIX de Berkeley.

En cuanto al protocolo tenemos que tener en cuenta las siguientes tres limitaciones:

El protocolo no permite más de quince saltos, limita el tamaño máximo de la red.

Problema del “conteo a infinito”. Este problema puede surgir en situaciones atípicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado.

El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetros a tiempo reales como por ejemplo retardos o carga del enlace.

RIP se especificó originalmente en RFC 1058, es un protocolo que genera muchísimo tráfico al enviar toda la tabla de ruteo en cada actualización, con la carga de tráfico que ello conlleva.

[5] CHAPPELL, Laura. Advanced Cisco Router Configuration

### 4.1.1 Tabla de ruteo del RIP

La base de datos de ruteo de cada uno de los hosts de la red que utilizan el protocolo de ruteo RIP tiene los siguientes campos:

Dirección de destino. La dirección de la red a la que se desea acceder.

Siguiente salto. El siguiente salto se define como el siguiente enrutador por el que el paquete va a pasar para llegar a su destino, este será necesariamente un vecino del enrutador origen.

Interfaz de salida del enrutador. Interfaz a la cual está conectado su siguiente salto.

Métrica. conteo de saltos, se considera como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la línea.

Temporizador. El temporizador indica el tiempo transcurrido desde que se ha recibido la última actualización de cierta ruta. RIP utiliza varios tiempos importantes, el tiempo de actualización que se establece en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos. El tiempo de actualización es considerado el tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos. El tiempo de desactivación se considera como el tiempo máximo que puede esperar un enrutador sin recibir actualizaciones de un vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que

se ha caído, con lo cual el enrutador no está activo en la red, por lo cual se establece la métrica a valor 16, es decir destino inalcanzable. El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese enrutador supuestamente caído son eliminadas de la tabla de enrutamiento.

Para obtener esta tabla, el protocolo de enrutamiento RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de enrutamiento de cada uno de los nodos o enrutadores de la red:

Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia al destino, y el siguiente salto del enrutador a esa red.

Periódicamente (cada 30 segundos) se enviará una actualización de la tabla a cada uno de los vecinos del enrutador mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de enrutamiento.

Cuando llegue una actualización desde un vecino, se añadirá el coste asociado a la red del vecino, y el resultado será la distancia y si es menor que el valor actual de la misma a esa red entonces se sustituirá por el nuevo valor.

## 4.2 PROTOCOLO DE ENRUTAMIENTO DE PASARELA INTERIOR

El protocolo de pasarela interior original de Internet fue un protocolo de vector de distancia (RIP) basado en el algoritmo Bellman-Ford. Este protocolo funcionó bien

en pequeños sistemas, pero menos bien a medida que los AS se volvieron más grandes.[5]

En 1988, la Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet) comenzó a trabajar en su sucesor. Ese sucesor llamado OSPF (Open Shortest Path First, abrir primero la trayectoria más corta), se convirtió en estándar en 1990.

El OSPF funciona haciendo una abstracción del conjunto de redes, enrutadores y líneas en un grafo dirigido en el que a cada arco se le asigna un costo (distancia, retardo, etc.). Entonces se calcula la trayectoria más corta con base en los pesos de los arcos.

Lo fundamental que hace el OSPF es representar la red como un grafo y luego calcular la trayectoria más corta de un enrutador a todos los demás.

El OSPF funciona intercambiando información entre enrutadores adyacentes, que no es lo mismo que entre enrutadores vecinos. En particular es ineficiente hacer que todos los enrutadores de una LAN hablen con todos los enrutadores de otra LAN.

Para evitar esta situación, se elige un enrutador como enrutador designado, el cual se dice que es adyacente a todos los demás enrutadores, e intercambia información con ellos. Los enrutadores que no son vecinos no se intercambian información entre ellos, se mantienen actualizados designando un enrutador de

[5] CHAPPELL, Laura. Advanced Cisco Router Configuration

respaldo para facilitar la transición en el caso que el enrutador designado primario se caiga.

### 4.3 INTERIOR GATEWAY ROUTING PROTOCOL (IGRP)

IGRP es un protocolo propietario de Cisco y se desarrolló para reemplazar a RIP. IGRP es un protocolo de enrutamiento interior por vector distancia. Los protocolos de enrutamiento por vector distancia requieren que cada router envíe toda o parte de su tabla de enrutamiento en un mensaje de actualización de enrutamiento a intervalos regulares a cada uno de sus routers vecinos. A medida que la información de enrutamiento se disemina en toda la red, los routers pueden calcular las distancias hacia todos los nodos dentro de la red. IGRP utiliza una combinación de métricas. El retardo de red, el ancho de banda, la confiabilidad y la carga son todos factores que se toman en cuenta en la decisión de enrutamiento. Los administradores de red pueden determinar las configuraciones para cada una de estas métricas. IGRP utiliza las configuraciones determinadas por el administrador o las configuraciones por defecto de ancho de banda y retardo para calcular automáticamente las mejores rutas. [5]

IGRP ofrece un amplio intervalo de métricas. Por ejemplo, la confiabilidad y la carga pueden tener cualquier valor entre 1 y 255; el ancho de banda puede tener valores que reflejen velocidades desde 1200 bps hasta 10 Gbps; y el retardo

[5] CHAPPELL, Laura. Advanced Cisco Router Configuration

puede tener cualquier valor desde 1 a 224. Los amplios intervalos de métricas permiten configuraciones de métrica adecuadas en redes con características de desempeño que varían ampliamente. Como resultado, los administradores de red pueden influir en la selección de ruta de modo intuitivo. Esto se logra evaluando cada una de las cuatro métricas, es decir, indicándole al router qué valor asignarle a una métrica en particular. Los valores por defecto relacionados con las determinaciones de valor para IGRP otorgan mayor importancia al ancho de banda, lo que hace que IGRP sea superior a RIP. A diferencia de IGRP, RIP no evalúa las métricas porque utiliza solamente una: el número de saltos.

El objetivo principal de Cisco al crear IGRP fue suministrar un protocolo sólido para el enrutamiento dentro de un sistema autónomo (AS). Un AS es un conjunto de redes bajo una administración común que comparten una estrategia de enrutamiento común. IGRP utiliza una combinación de métricas que el usuario puede configurar, incluyendo retardo, ancho de banda, confiabilidad y carga de red. IGRP publica tres tipos de rutas: interior, sistema y exterior.

Las rutas interiores son rutas entre subredes en la red conectada a una interfaz de router. Si la red está conectada a un router que no está dividido en subredes, IGRP no publica rutas interiores. Además, la información de subred no se incluye en las actualizaciones del IGRP, lo que representa un problema para las subredes IP no contiguas.

Las rutas de sistema son rutas hacia otras redes importantes dentro del AS. El router deriva las rutas de sistema desde las interfaces de red conectadas directamente y la información de ruta de sistema suministrada por otros routers que utilizan IGRP. Las rutas de sistema no incluyen información de división en subredes.

Las rutas exteriores son rutas hacia redes ubicadas fuera del AS que se consideran al identificar un gateway de último recurso. El router elige un gateway de último recurso de la lista de rutas exteriores que suministra IGRP. El router utiliza el gateway de último recurso si no tiene una mejor ruta para el paquete y el destino no es una red conectada. Si el AS tiene más de una conexión hacia una red externa, los distintos routers pueden seleccionar distintos routers exteriores como el gateway de último recurso.

IGRP ofrece una serie de funciones diseñadas para mejorar su estabilidad, incluyendo las siguientes:

**Esperas**: Cuando un router se entera de que una red está más lejos de lo que se sabía previamente, o que la red está fuera de servicio, la ruta hacia esa red se coloca en estado de espera. Durante el período de espera, la ruta se publica, pero se pasan por alto las publicaciones entrantes acerca de esa red desde cualquier router que no sea el router que originariamente publicó la nueva métrica de la red. Este mecanismo se utiliza a menudo para ayudar a evitar los loops de

enrutamiento en la red, pero tiene el efecto de aumentar el tiempo de convergencia de la topología.

Las esperas se utilizan para evitar los mensajes de actualización regulares que se producen al reinstaurar una ruta que puede no ser válida. Cuando un router deja de funcionar, los routers vecinos detectan esto por la falta de mensajes de actualización programados de forma regular. Estos routers entonces calculan nuevas rutas y envían mensajes de actualización de enrutamiento para informar a los vecinos sobre el cambio de ruta. Esta actividad inicia una ola de actualizaciones provocadas que se filtran a través de la red. Estas actualizaciones provocadas no llegan instantáneamente a cada uno de los dispositivos de la red. Por lo tanto, es posible que el Dispositivo A, al que todavía no se le ha informado acerca de la falla de la red, envíe un mensaje de actualización regular (indicando que la ruta que recién ha dejado de funcionar todavía funciona) al dispositivo B, al que recién se le ha notificado acerca de la falla de la red. En este caso, el Dispositivo B ahora contiene (y potencialmente publica) información de enrutamiento incorrecta.

Las esperas le indican al router que se mantenga en espera ante los cambios que pueden afectar las rutas durante un período de tiempo. Por regla general, se calcula el tiempo de espera para que sea un poco mayor que el tiempo necesario

para actualizar la red entera con un cambio de enrutamiento. Esto sirve para evitar los loops de enrutamiento provocados por una convergencia lenta.

**Split horizons**: Un split horizon (horizonte dividido) se produce cuando un router trata de enviar información acerca de una ruta nuevamente en la dirección desde donde provino. Por ejemplo, consideremos el gráfico: El Router 1 inicialmente publica que tiene una ruta hacia la Red A. Como resultado, no hay ningún motivo para que el Router 2 no incluya esta ruta de regreso hacia el Router 1 porque el Router 1 está más cerca de la Red A. La norma de split horizon establece que el Router 2 debe eliminar esta ruta de cualquiera de las actualizaciones que le envía al Router 1.

La norma de split horizon ayuda a prevenir los loops de enrutamiento. Por ejemplo, supongamos que la interfaz del Router 1 hacia la Red A deja de funcionar. Sin los split horizons, el Router 2 continúa informándole al Router 1 que puede llegar a la Red A (a través del Router 1). Si el Router 1 no es lo suficientemente inteligente, puede resultar seleccionando la ruta del Router 2 como una alternativa para la conexión directa que ha fallado, provocando un loop de enrutamiento. Aunque las esperas deberían prevenir esto, los split horizons se implementan en IGRP como una manera de suministrar estabilidad de protocolo adicional.

**Actualizaciones inversas**: Mientras que los split horizons deben prevenir los loops de enrutamiento entre routers adyacentes, las actualizaciones inversas tienen como objetivo impedir que se produzcan loops de enrutamiento más grandes. El aumento en las métricas de enrutamiento generalmente indican que hay loops de enrutamiento. Luego se envían actualizaciones inversas para eliminar la ruta y colocarla en espera. El router hace una actualización inversa de la ruta enviando una actualización con una métrica de infinito a un router que originalmente había publicado una ruta hacia una red. La actualización inversa de la ruta puede facilitar la convergencia rápida.

IGRP utiliza varios tipos de información de métrica. Para cada ruta a través de un AS, IGRP registra el segmento que tiene el ancho de banda más bajo, el retardo acumulado, la unidad máxima de transmisión (MTU) más pequeña y la confiabilidad y carga.

Se utilizan diversas variables para evaluar cada métrica y, por defecto, al ancho de banda se le atribuye la mayor importancia al calcular la mejor ruta. Para una red de un solo medio (tal como una red que utiliza sólo Ethernet), esta métrica se reduce a un número de saltos. Para una red de medios mixtos (por ejemplo, Ethernet y las líneas seriales que ejecutan velocidades desde 9600 baudios a T1), la ruta que tiene la mejor métrica refleja la ruta más aconsejable hacia un destino).

Un router que ejecuta IGRP envía un broadcast de actualización IGRP cada 90 segundos. Declara que una ruta es inaccesible si no recibe ninguna actualización del primer router en la ruta dentro de tres períodos de actualización (270 segundos). Después de siete períodos de actualización (630 segundos), el router elimina la ruta de la tabla de enrutamiento. IGRP utiliza la actualización flash y la actualización inversa para acelerar la convergencia del protocolo de enrutamiento. Una actualización flash es el envío de una actualización que se produce más rápido que el intervalo de actualización periódica estándar para notificar a los demás routers acerca de un cambio de métrica. Las actualizaciones inversas tienen como objetivo evitar los loops de enrutamiento de gran tamaño provocados por los aumentos en las métricas de enrutamiento. Las actualizaciones inversas se envían para eliminar una ruta y colocarla en espera, lo que evita que la nueva información de enrutamiento se utilice durante un período determinado de tiempo.

IGRP tiene un número máximo de saltos de 255, que normalmente se establece en un valor menor que el número por defecto, que es 100. Como IGRP utiliza actualizaciones provocadas (flash), el conteo hasta 100 no tarda demasiado. Sin embargo, se establece el número máximo de saltos en un número menor, a menos que tenga una red enorme. Debe ser un número por lo menos tan grande como la cantidad máxima de routers que una ruta puede tener que atravesar en la red. Si intercambia el enrutamiento IGRP con una red externa, el número de saltos debe incluir su red y esa red externa. Cuando realiza un cálculo del número de

saltos, debe tener en cuenta cómo sería la configuración si algunas líneas dejaran de funcionar.

Con la creación de IGRP a principios de los ochentas, Cisco Systems fue la primera compañía en resolver los problemas asociados con el uso de RIP para rutear paquetes entre routers interiores. IGRP es un protocolo de enrutamiento por vector-distancia que envía actualizaciones de enrutamiento a intervalos de 90 segundos, publicando las redes en un sistema autónomo en particular. Algunas de las características de diseño claves de IGRP enfatizan lo siguiente:

- Versatilidad que permite manejar automáticamente topologías indefinidas y complejas.
- Flexibilidad para segmentos con distintas características de ancho de banda y de retardo.
- escalabilidad para operar en redes de gran envergadura.

El protocolo de enrutamiento IGRP determina la mejor ruta a través de una red examinando dos métricas el ancho de banda y la demora de las redes entre los routers. Aunque puede utilizar una combinación de variables para determinar una métrica compuesta. Estas variables incluyen: ancho de banda, retardo, carga y Confiabilidad.

IGRP converge más rápido que RIP, por lo tanto se evitan los ciclos de ruteo causados por el desacuerdo entre routers sobre cual es el próximo salto a ser

tomado. Más aún, el IGRP no tiene limitación en cuanto a contador de saltos. Por lo anterior, el IGRP es utilizado en redes de gran tamaño, complejas y con diversidad de topologías. IGRP utiliza una métrica compuesta que es calculada por una suma ponderada de los valores de retardo entre redes, ancho de banda del enlace, confiabilidad y carga, donde el administrador de la red puede dar valores arbitrarios para las ponderaciones, lo que permite un grado mayor de flexibilidad. Una característica adicional de IGRP es que permite ruteo multitrayectoria, lo que permite, por ejemplo, establecer líneas de respaldo en caso de fallas. Para mejorar la estabilidad del algoritmo de vector de distancias, IGRP utiliza mensajes *Holddown* que evitan que las actualizaciones regulares enviadas por los *routers* comiencen el problema de la cuenta hasta infinito, ya que al detectar una falla, debido a la falta de actualizaciones, un *router* que detecte esto envía el mensaje Holddown para evitar que comiencen las sucesivas actualizaciones y se genere la cuenta hasta infinito. Este mensaje es un período de tiempo en el que no deben actualizarse las rutas recibidas. IGRP también utiliza las técnicas *Split Horizon* y *Poison-Reverse* en el envío de actualizaciones para prevenir *loops* información entre routers adyacentes. Finalmente, IGRP mantiene una serie de *timers* e intervalos de tiempo, entre los que se incluye un *timer* para actualizaciones (cuyo valor por defecto es 90 seg.), uno para marcar las rutas como no válidas (por defecto 3**Update*=270 seg.), uno para el tiempo de Holddown (por defecto 3**Update*+10=280 seg.) y uno para el de descarte de rutas (por defecto 7**Update*=630 seg.).

## 4.4 ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

Cisco lanzó también una nueva versión de IGRP para manipular redes de alto crecimiento y misión-crítica este es un protocolo de enrutamiento híbrido equilibrado. Esta nueva versión es conocida como EIGRP (*Enhanced* IGRP) y combina la facilidad de uso de los protocolos de ruteo de vector de distancia tradicional con las capacidades de reruteo rápido de los protocolos estado del enlace. El EIGRP consume mucho menos ancho de banda que el IGRP, porque éste es capaz de limitar el intercambio de información de ruteo para incluir solamente la información que ha cambiado. Además, es multiprotocolo pues capaz de manipular información de ruteo de AppleTalk, IPX e IP.[2]

[2] http://www.eduangi.com

## CONCLUSIONES Y RECOMENDACIONES

El desarrollo de las prácticas de los laboratorios recomendados por la Academia de *Networking* de CISCO brinda el mejor tipo de aprendizaje y es aquel basado en la experiencia. Al realizar las prácticas el estudiante se enfrentará a problemas de distintas índoles, lo cual generará "experiencia" a la hora de enfrentarse a problemas en el campo profesional.

Las tecnologías en el campo computacional avanzan a medida desmesurada, de igual forma ocurre con las tecnologías de comunicación de datos, es por esto que no siempre se van a tener las mismas tecnologías, estas estarán mejorando y saldrán nuevos dispositivos totalmente diferentes a los que se encuentran en funcionamiento hoy en día.

El Ethernet más rápido ratificado como una norma el año pasado (10 Gbps), es hasta ahora más que suficiente para la mayoría de los portadores y empresas. Gigabit Ethernet es la velocidad máxima en los backbones de las redes empresariales, donde el trafico de muchos servidores y los departamentos vienen juntos. Siempre que el próximo salto se tome, hay razones técnicas para hacer el paso más corto a 40G bps en lugar de desarrollar el 100-Gigabit Ethernet. Las interfaces de Ethernet a esta velocidad se igualarían con enlaces WAN tradicionales de OC-768, haciéndolo más sencillo diseñar equipos y redes. Los vendedores que construyan equipos para Ethernet de 40 Gbps también

pueden equilibrar el trabajo que se realizó al desarrollar interfaces en los años anteriores para la especificación de área amplia OC-768 (también de 40 Gbps).

Una velocidad de 40 Gbps podría ser lograda trayendo cuatro 10-Gigabit conexiones de Ethernet que juntos usan una agregación de enlaces, una propuesta más económica que desarrollar un nuevo tipo de interface. Si una nueva norma es desarrollada, debe ir toda hasta 100 Gbps.

Al finalizar el documento investigativo se pudo concluir que las bases brindadas por la CCNA de Cisco son buenas pero no lo suficiente. El alumno de la CCNA de Cisco queda con vacíos que le presentarán obstáculos a la hora de desarrollar cada una de las prácticas que este curso brinda. Es por esto que este documento cuenta con una base teórica acompañada de prácticas de laboratorio que brindaran al estudiante el conocimiento y la práctica necesaria para tener un buen fundamento en base a las redes de comunicación y el enrutamiento.

El propósito de los laboratorios es familiarizar a los estudiantes de la CCNA con los distintos dispositivos utilizados en *networking*, crear un cimiento cognitivo acerca del funcionamiento de las redes de comunicación y brindarle al estudiante un breve vistazo a lo que se puede enfrentar en el campo profesional.

Este trabajo proporciona al lector con la información necesaria para otorgarle al estudiante los fundamentos teóricos necesarios para diseñar y comprender el funcionamiento de una red de comunicación de datos. Se recomienda que el

lector se empape de esta teoría y a medida que vaya avanzando, este realice cada una de las prácticas realizadas para que este pueda comprender cada parte de los fundamentos básicos de redes. Es necesario mejorar el ámbito tecnológico de las prácticas, es de suma importancia conocer las nuevas tecnologías y como estas están afectando el funcionamiento de las redes de comunicación. El avance cotidiano nos trae nuevas mejoras en el campo de las redes de información y es por esta razón que debemos tener una constante actualización de las tecnologías de punta en el mercado.

## BIBLIOGRAFÍA


- ✓ CHAPPELL, Laura. Advanced Cisco Router Configuration. McMillan Technical Publishing, Indianapolis, IN. USA 2001.

- ✓ CISCO SYSTEMS, Inc. Academia de Networking de Cisco *Systems*: Guía del primer año. Segunda Edición. Pearson Educación, S.A. Madrid. 2002.

- ✓ FORD, Merilee. Tecnologías de Interconectividad de Redes. Prentice-Hall, Mexico, 1988.

- ✓ PAQUET, Catherine. Building Scalable CISCO Networks. CISCO Press, Indianapolis, IN. USA 2001.

- ✓ Enciclopedia Microsoft Encarta 2000, Microsoft Corporation 1993-1999, Redmond, WA. USA.

- ✓ Página Web de CISCO
  http://www.cisco.com

- ✓ Página Web de Actualizaciones de redes informáticas
  http://www.eduangi.com

# ANEXOS

En la carpeta “PRÁCTICAS” que se encuentra en el disco compacto correspondiente a este trabajo, se encuentran las prácticas de laboratorio correspondientes a los semestres uno y dos de la CCNA de Cisco.

En la carpeta “Documentación” se encuentra una serie de documentos utilizados en la elaboración de este trabajo.

## GLOSARIO

**Banda ancha** - Sistema de transmisión que multiplexa varias señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que un canal de grado de voz (4 kHz). En la terminología de las LAN, un cable coaxial en el que se usa señalización analógica. También se denomina *banda amplia*.

**Banda base** - Característica de una tecnología de red donde sólo se utiliza una frecuencia portadora. Ethernet es un ejemplo de una red de banda base. También denominada *banda angosta*.

**broadcast** - Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección de broadcast. Comparar con *multicast* y *unicast*.

**DCE** -**Equipo de comunicación de datos** (expansión EIA) o equipo de terminación de circuito de datos (expansión UIT-T). Los dispositivos y conexiones de una red de comunicaciones que comprenden el extremo de la red de la interfaz de usuario a red. DCE brinda una conexión física a la red, envía el tráfico y proporciona una señal de sincronización utilizada para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE.

**DLCI** -**Identificador de conexión de enlace de datos**. Valor que especifica un PVC o SVC en una red Frame Relay. En la especificación básica Frame Relay, los DLCI son localmente significativos (dispositivos conectados pueden usar diferentes valores para especificar la misma conexión). En la especificación extendida LMI, los DLCI son globalmente significativos (los DLCI especifican dispositivos finales individuales).

**DTE Equipo terminal de datos**. Dispositivo en el extremo usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. El DTE incluye dispositivos tales como computadores, traductores de protocolos y multiplexores.

**IEEE Instituto de Ingeniería Eléctrica y Electrónica**. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares que predominan en las LAN de la actualidad.

**ISO Organización Internacional para la Normalización**. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

**MAC Control de acceso al medio**. Capa inferior de las dos subcapas de la capa de enlace de datos, según la define el IEEE. La subcapa MAC maneja el acceso a los medios compartidos, por ejemplo, si se utilizara la transmisión o la contención de tokens.

**MSAU Unidad de acceso a múltiples estaciones**. Concentrador de cableado al que se conectan todas las estaciones finales de una red Token Ring. La MSAU suministra una interfaz entre estos dispositivos y la interfaz Token Ring de, por ejemplo, un TRIP Cisco 7000. A veces abreviada*MAU*.

**Subred** 1. En redes IP, una red que comparte una dirección de subred específica. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina *subnet*. Ver también *dirección IP*, *dirección de subred* y *máscara de subred*. 2. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo único y que utiliza un protocolo de acceso de red exclusivo.

**TIA Asociación de la Industria de las Telecomunicaciones**. Organización que desarrolla los estándares que se relacionan con las tecnologías de telecomunicaciones. De forma conjunta, la TIA y la EIA han formalizado estándares por ejemplo, EIA/TIA-232, para las características eléctricas de la transmisión de datos.

**Token** -Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

**Trama** Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y a la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. Los términos *datagrama*, *mensaje*, paquete *segmento* también se utilizan para describir las agrupaciones de información lógica en las distintas capas del modelo de referencia OSI y en distintos círculos de tecnología.