U N I V E R S I D A D N A C I O N A L A U T O N O M A D E M E X I C O

FACULTAD DE ESTUDIOS SUPERIORES
CAMPUS ARAGON

INTEGRACION DE LAS TELECOMUNICACIONES
"CREACION DE UNA RED UTILIZANDO FRAME RELAY"

T E S I S

Q U E P A R A O B T E N E R E L T I T U L O D E

I N G E N I E R O M E C A N I C O E L E C T R I C I S T A

P R E S E N T A

S E R G I O L A R A M A R T I N E Z

ASESOR: ING. ADRIAN PAREDES ROMERO

SAN JUAN DE ARAGON, EDO. DE MEXICO MAYO DEL 2007

Integración de las Telecomunicaciones

“Creación de una Red utilizando Frame Relay”

Sergio Lara Martínez

Dedicatoria

A mis Padres: Por todo el apoyo que siempre me han brindado y por el amor, respeto y admiración que tengo hacia ellos.

A Concepción Feria: Por el apoyo incondicional que me brindó para poder concluir mi bachillerato.

Contenido

Introducción

El presente trabajo describe los fundamentos básicos para entender el funcionamiento de las telecomunicaciones porque muestra los servicios por cobre que se utilizan actualmente para comunicarse a otro sitio, así como para conectarse a Internet; Los servicios son mostrados en la norma americana y europea para que el lector conozca las diferentes velocidades y tecnologías con las que se puede transferir la información.

Se describen también las diferentes tecnologías y topologías que se utilizan en la red LAN, el Modelo OSI necesario para poder identificar algún problema en la conexión de la red, las diferencias entre IPv6 e IPv4, los diferentes estándares utilizados en voz sobre IP (VoIP), así como las técnicas y estándares de compresión para poder transmitir la voz por un enlace de baja velocidad.

En la parte final se crea una red utilizando tecnología Frame Relay, empleando routers de la marca Cisco como equipo Terminal donde se muestran las partes que lo componen, conectores y tarjetas empleadas para tener comunicación con otro dispositivo, así como la configuración que tiene que tener el router y el switch de Frame Relay utilizado por las compañías telefónicas, el cual servirá para crear la conexión entre los sitios.

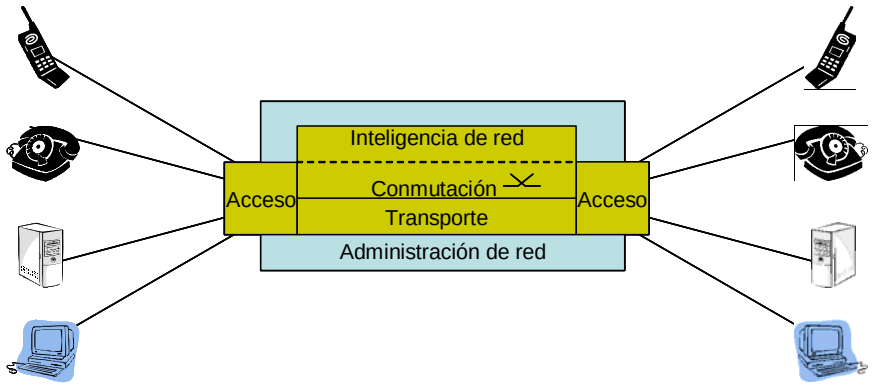
Objetivo

Diseñar una red de telecomunicaciones que permita establecer comunicación permanente con otros sitios de forma segura utilizando la tecnología Frame Relay para proveer los servicios de voz y datos en el mismo medio de transmisión.

Capitulo 1

Elementos de la Red Telefónica

Modelo de Red



Modelo de Red.

El modelo de Red es la representación esquemática de todos lo equipos y funciones que interactúan al efectuarse una llamada telefónica.

Los elementos que lo conforman son:

- Equipos Terminales.
- Accesos.
- Equipo de Conmutación
- Equipo de Transmisión.
- Sistema de Administración de Red.
- Inteligencia de la Red.

Equipos Terminales: Son todos los equipos que permiten originar o terminar una llamada, sea de voz o de datos. Se incluyen entre otros, teléfonos fijos y celulares, computadoras, equipo de video, etc.

Accesos: Son los medios físicos a través de los cuales se conectan los equipos terminales a la red. Por ejemplo, cable de cobre, microondas, fibra óptica, etc.

Equipo de Conmutación: Son los equipos que se encargan de dirigir las llamadas dentro de la red, a fin de que alcancen su destino final.

Equipo de Transmisión: Son los equipos y medios que conectan a los diferentes nodos de una red. Por ejemplo, equipos de transmisión de fibra óptica, radios de microondas, satélites, etc.

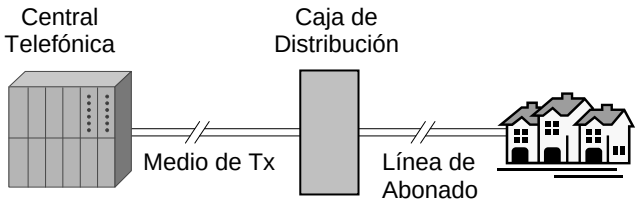
Sistema de Administración de Red: Equipos dedicados a la operación, mantenimiento y supervisión del funcionamiento de la red. Se incluyen tareas como adición de usuarios, estadísticas, alarmas, etc.

Inteligencia de Red: Sistemas dedicados a proporcionar servicios avanzados a los usuarios. Por ejemplo, números 800, etc.

Línea de abonado

La línea de abonado es el par de cables de cobre que llegan al usuario del teléfono, desde la central telefónica más cercana. La línea de abonado es el acceso del usuario telefónico a la red telefónica.

Las líneas telefónicas que llegan a casas habitación son generalmente transportadas por vía aérea o subterránea.



Línea de Abonado.

Actualmente existen compañías que usan como medio de transmisión señales de radio, a fin de evitar el gasto que representa el tendido de cableado de cobre.
La finalidad de la línea de abonado es transportar la señalización que permite establecer la llamada, así como la información de voz o datos una vez establecida.

Centrales de Conmutación

Una central de conmutación es el equipo que nos permite:

- Conectar entre sí a los abonados de la central.
- Conectar a los abonados de la central a los equipos de la misma central que proporcionan algún servicio (mensajes, hora, etc.).
- Conectar a los abonados de la central con los abonados de otra central.
- Llevar un registro de todas las conexiones (llamadas) a fin de poder efectuar la tasación y cobro de cada una de ellas.

Medio de Transporte o Transmisión

Se entiende por medio de transmisión todo aquel medio físico que nos permite llevar de un punto a otro la información.

Los medios de comunicación más comúnmente usados en telecomunicaciones son:

- Alambres de cobre: cable telefónico, cable coaxial, cableado de redes, etc.
- Atmósfera: señales de televisión, radio, celulares, etc.
- Fibra óptica: comunicación intercontinental entre ciudades, entre centrales, etc.
- Espacio: comunicación satelital, radioaficionados, etc.

Equipo Terminal

Un equipo terminal es el dispositivo que nos permitirá acceder a la red de comunicaciones, con la finalidad de establecer un intercambio de información con otro equipo terminal que funcionará como destino.

Ejemplos de equipos terminales son:

- Teléfonos fijos y celulares.
- Computadoras.
- Televisión interactiva.
- Equipo de fax.

Digitalización de la voz, Técnica PCM

La red de transporte lleva únicamente información digital, por lo que siendo la voz humana una señal analógica, se hace necesario digitalizarla.

En telefonía, se utiliza la técnica PCM (Pulse Code Modulation) para llevar a cabo la digitalización de la señal de voz.

La técnica PCM consiste en representar muestras instantáneas de una señal analógica mediante palabras digitales en un tren de pulsos en serie.

Las etapas en las que se divide la técnica PCM son:

Filtrado

La voz humana genera frecuencias que van desde los 0 a los 4Khz.
En la técnica PCM se limita el ancho de banda al rango de 300 a los 3400 Hz mediante la utilización de filtros pasa banda.

Teorema de Nyquist

Este teorema establece que para poder reconstruir sin distorsión una señal muestreada, la tasa de muestreo debe ser al menos el doble de la frecuencia máxima de la señal original.

Si consideramos que la voz humana no genera frecuencias arriba de los 4Khz, entonces la frecuencia de muestreo mínima será:

Frecuencia muestreo = 2 x Frecuencia Max.
Frecuencia muestreo = 2 x 4 Khz = 8 Khz
Esta es la frecuencia de muestreo que se usa en la técnica PCM.

Muestreo

En PCM, se toman 8000 muestras de la señal en cada segundo (una cada 125μseg). A cada valor muestreado se le asigna una palabra de 8 bits.
El resultado es un tren de pulsos en serie que tiene una velocidad de 64Kbps.

Velocidad = (8000 muestras / seg) x (8 bits / muestra)

Velocidad = 64000 bits / seg

Cuantificación

La cuantificación es el método por el cual se asigna un valor de un número finito de combinaciones a una muestra de una señal analógica en función de su valor de amplitud.

El número posible de combinaciones estará dado por el tamaño de la palabra binaria que se usará para codificar el valor muestreado.

Codificación

El proceso de codificación consiste en asignar un grupo de bits para representar el valor de la muestra en forma binaria.

En PCM se usa una longitud de palabra de 8 bits para cada muestra cuantificada.

Compansión

Con la finalidad de hacer más eficiente y con mayor calidad la transmisión de la señal, se le hace un ajuste conocido como compansión.

El proceso consiste en comprimir el rango de la amplitud de la señal antes de transmitirla y luego se descomprime al llegar a su destino.

De esta forma se logra tener un mayor número de niveles de cuantización para las señales pequeñas y un número menor para las señales grandes.

Este proceso se puede ejecutar de dos formas: una conocida como la ley μ usada en Norteamérica y Japón, y ley A, usada en Europa y el resto del mundo.

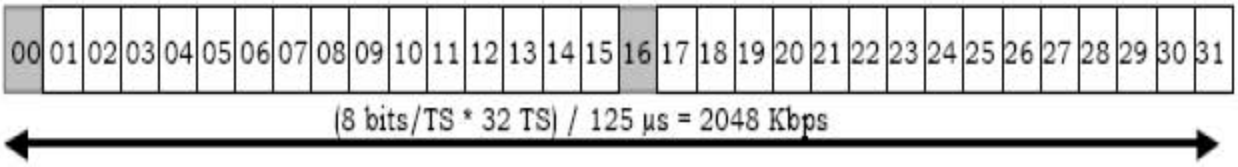
Multiplexación

El multiplexaje consiste en intercalar en el tiempo muestras de diferentes señales a fin de transmitir la información de todas ellas en serie y sobre un mismo canal.

En PCM se utiliza el multiplexaje por división de Tiempo (TDM: Time Division Multiplexing), que consiste en intercalar en el tiempo muestras de diferentes señales (canales) a fin de transmitir la información de todas ellas en serie y sobre un mismo canal.

La velocidad de cada canal es de 64 Kbps, por lo que la velocidad del tren resultante será la suma de cada una de las velocidades de los canales que forman el tren.

La norma europea define un tren o patrón que consta de 30 canales de información, más uno de sincronía y uno de señalización, para formar la trama básica conocida como E1 con una velocidad de 2.048 Mbps.



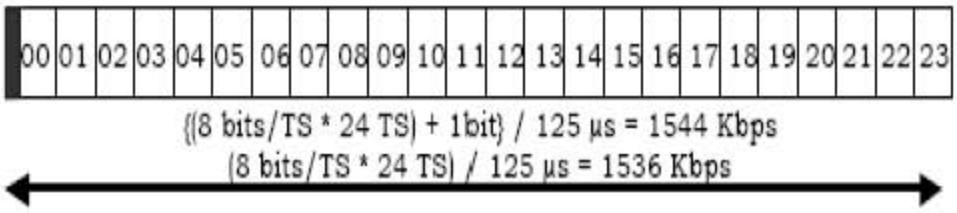
Trama E1

La norma americana define un tren o patrón que consta de 24 canales de información más un bit de sincronía.

Si cada canal de información es un paquete de 8 bits:

{(24 paquetes * 8 bits) + 1 bit de sincronía} = 193 bits, entre la duración de 125 microsegundos de cada muestra.

De esta manera se forma la trama básica conocida como T1 con una velocidad de 1.544 Mbps.



Trama T1

Capacidad de Transporte

Dados los altos niveles de tráfico entre centrales, es necesario multiplexar los E1 a jerarquías superiores, estos es, transmitir la información en anchos de banda más grandes. Por su gran capacidad y confiabilidad, el medio más usado para transmitir estás jerarquías, es la fibra óptica.

La capacidad de transporte se clasifica de acuerdo a las siguientes tres tablas, dependiendo del ancho de banda o velocidad y de la norma usada.

	Norma Americana			Norma Europea		
Jerarquía	Denominación	No. De Canales de Voz	Ancho de Banda	Denominación	No. De Canales de Voz	Ancho de Banda
PDH	DS0	1	64 Kbps	DS0	1	64Kbps
	T1	24	1544 Kbps	E1	30	2048 Kbps
	T2	96	6312 Kbps	E2	120	8448 Kbps
	T3	672	44736 Kbps	E3	480	34368 Kbps

Jerarquía PDH

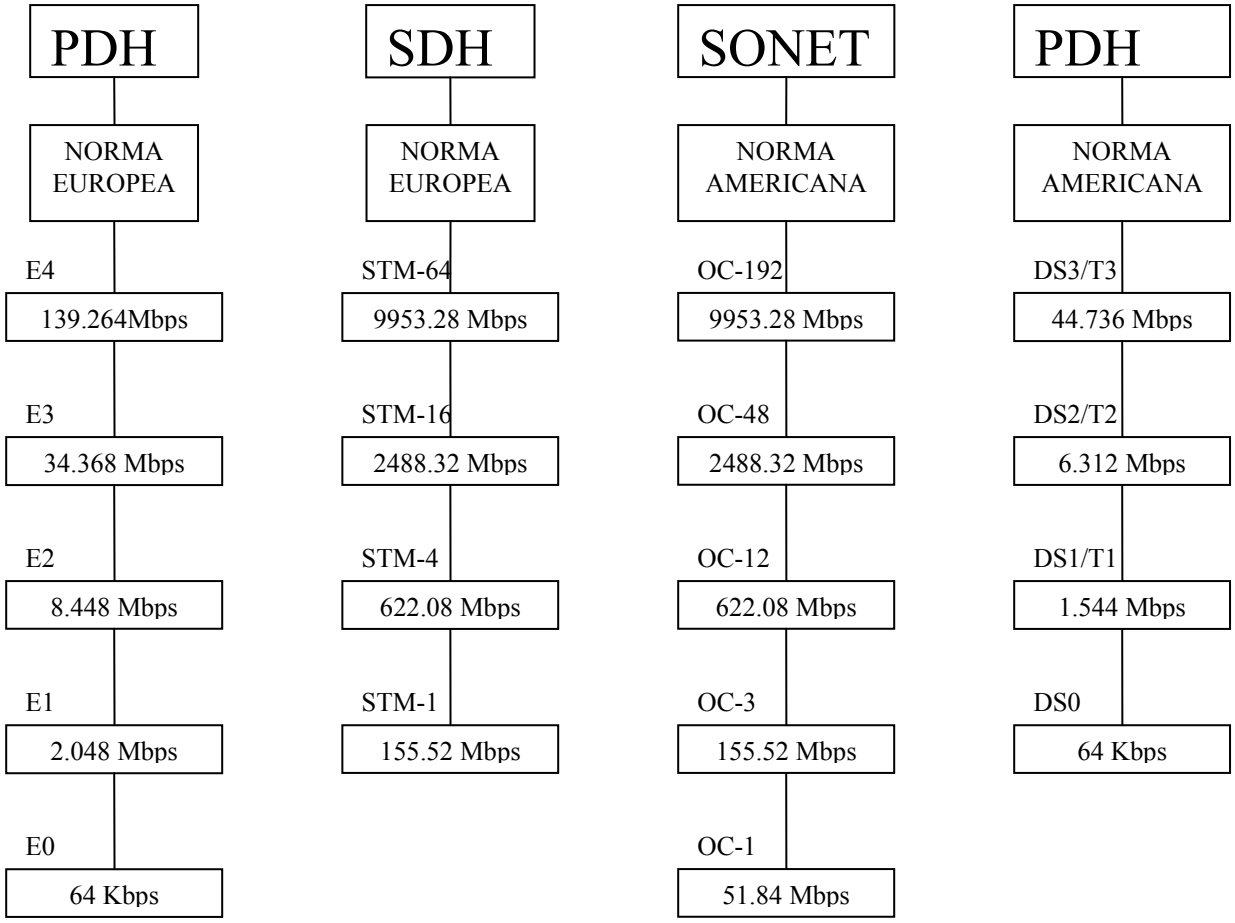
	Norma Americana		
Jerarquía	Denominación	No. De Canales de Voz	Ancho de Banda
SONET	OC-1	640	51840 Mbps
	OC-3	1920	155.520 Mbps
	OC-24	5120	1244.16 Gbps
	OC-192	122880	9953.28 Gbps

Jerarquía SONET

	Norma Europea		
Jerarquía	Denominación	No. De Canales de Voz	Ancho de Banda
SDH	STM-1	1920	155.52 Mbps
	STM-4	7680	622.08 Mbps
	STM-16	30720	2488.32 Mbps
	STM-64	122880	9953.28 Mbps

Jerarquía SDH

Jerarquías para Transmisión de Señales Digitales



PDH

NORMA EUROPEA
E4 = 4 x E3
E3 = 4 x E2
E2 = 4 x E1
E1 = 32 X E0

NORMA AMERICANA
DS3 = 7 x T2
DS2 = 4 x T1
DS1 = 24 x DS0

SONET

NORMA AMERICANA
OC-192 = 4 x OC-48
OC-48 = 4 x OC-12
OC-12 = 4 x OC-3
OC-3 = 3 x OC-1

SDH

NORMA EUROPEA
STM-64 = 4 x STM-16
STM-16 = 4 x STM-4
STM-4 = 4 x STM-1

PDH.- Plesiochronous Digital Hierarchy
DS.- Digital Signal.

SONET.- Synchronous Optical Network.
OC.- Optical Carrier.
SDH.- Synchronous Digital Hierarchy.
STM.- Synchronous Transport Module.

Línea Digital de Abonado (DSL)

Las líneas digitales de abonado (DSL, Digital Subscriber Line) son las tecnologías que permiten usar un ancho de banda grande sobre el par de cobre que llega a los abonados.

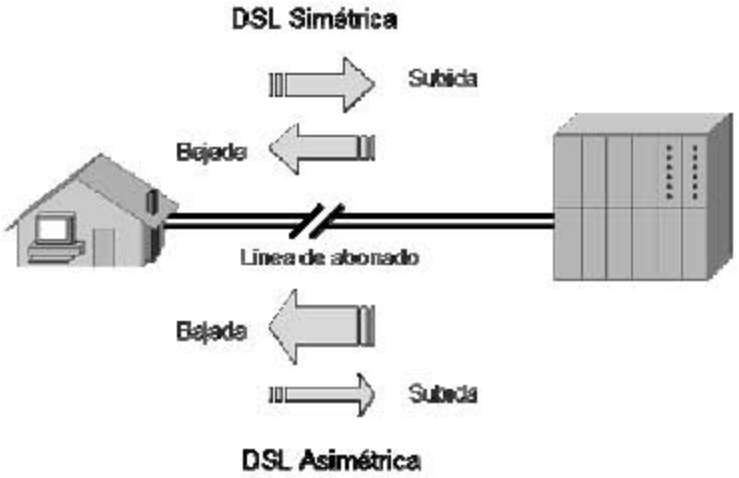
Estas conexiones no requieren el uso de ninguna etapa de amplificación ni repetidor. Son totalmente compatibles con la infraestructura actual.

Línea Digital de Abonado

DSL requiere el uso de equipos terminales tipo módem en el lado del usuario y de la central. En la central, este equipo, conocido como Multiplexor de acceso a DSL, permite sobreponer la información de datos a la señal de voz. En el lado del usuario, el separador o splitter separa la señal de voz de la de datos, pasando esta última al módem ADSL y de ahí a la aplicación de datos.

DSL emplea dos tipos de configuraciones:

- Simétrica. Cuando el ancho de banda de bajada es el mismo que el de subida.
- Asimétrica. Cuando el ancho de bajada es diferente al de subida. Usualmente el ancho de banda de bajada es mayor al de subida.



Configuraciones en DSL

Los tipos de DSL más usados son:

- IDSL. Líneas Digitales de Usuario Básico.
- HDSL. Líneas Digitales de Usuario de Alta Velocidad.
- HDSL-2. Líneas HDSL de Segunda Generación.
- SDSL. Líneas Digitales de Usuario Simétricas.
- ADSL. Líneas Digitales de Usuario Asimétricas.
- RADSL. Líneas Digitales de Usuario de Velocidad Adaptable.
- VDSL. Líneas Digitales de Usuario de Muy Alta Velocidad.

TIPO	VELOCIDAD DE SUBIDA	VELOCIDAD DE BAJADA	DISTANCIA MÁXIMA A CENTRAL [Km]	No. DE PARES
ADSL-1	16 Kbps	1.544 Mbps	5.5	1
ADSL-2	256 Kbps	3 Mbps	3.6	1
ADSL-3	640 Kbps	8 Mbps	2.4	1
IDSL	144 Kbps	144 Kbps	5.5	1
HDSL	2.048 Mbps	2.048 Mbps	4.2	2
HDSL-2	1.544 Mbps	1.544 Mbps	3.6	1
S-HDSL	768 Kbps	768 Kbps	4.2	1
SDLS	2.048 Mbps	2.048 Mbps	4.2	1
A-VDSL	2.3 Mbps	13 – 52 Mbps	0.3 – 1	1
S-VDSL	26 Mbps	26 Mbps	0.3 – 1	1

Tipos de DSL

Las líneas DSL básicas son similares a un canal BRI de ISDN. Emplea dos canales de 64 Kbps para información y un canal de señalización de 16 Kbps. Voz y Datos son transmitidos simultáneamente.

Las DSL asimétricas tienen un ancho de banda alto de bajada y un ancho de banda bajo en subida. Existen tres tipos:

- ADSL-1. Opera a una distancia máxima de 5.5 Km sobre líneas no cargadas a 1.5 Mbps. Se emplea para video codificado con calidad similar a VHS.
- ADSL-2. Opera a 3 Mbps a una distancia máxima de 3.6 Km.
- ADSL-3. Opera a 8 Mbps a una distancia máxima de 2.4 Km.

Sus principales aplicaciones son para bajar información de la red y en general, se usan en condiciones de tráfico variable.

Las DSL de alta velocidad (HDSL) transmiten en dos direcciones sobre dos pares de cobre. Esto permite tener servicios de E1 usando la infraestructura actual.

Las HDSL-2 operan en un solo par de cobre y permiten transmitir un ancho de banda de 1.544 Mbps. Es la primer configuración estandarizada, por lo que es la de más amplio uso.

Las S-HDSL se usan en aplicaciones que requieren ancho de banda variable y velocidades de transmisión de datos simétricas. Permite tener varias aplicaciones trabajando a diferentes capacidades.

Las DSL de velocidad adaptable se usan cuando se requiere un ancho de banda variable y permiten diferentes velocidades de transmisión dependiendo de las características de la línea. Esto es, si baja la calidad de la línea, se disminuye el ancho de banda.

Las DSL de muy alta velocidad permiten un ancho de banda asimétrico de hasta 52 Mbps en una dirección. Para estas velocidades se necesita que la infraestructura de red sea de fibra óptica y únicamente el último tramo de acceso sea de cobre. Tiene un alcance muy corto, no más de 1 Km.

Capitulo 2

Redes de Datos

Clasificación Geográfica de las Redes

Una clasificación de las redes corresponde a la restricción geográfica, es decir, por el área física que cubren, estas son:

- LAN
- MAN
- WAN
- PAN

LAN, Local Area Network

Una Red de Área Local (LAN) es un sistema de transmisión de datos que permite que un cierto número de dispositivos independientes se comuniquen entre sí dentro de un área geográfica limitada, por lo regular de algunos kilómetros.

MAN, Metropolitan Area Network

Una Red de Área Metropolitana, está diseñada para extenderse a lo largo de una ciudad entera, se utiliza en gran medida para la interconexión de LAN corporativas.

Una MAN puede ser propiedad de una empresa privada o puede utilizar los servicios ofrecidos por las compañías de telefonía local.

WAN, Wide Area Network

Una Red de Área Amplia (WAN), proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de video sobre grandes áreas geográficas que pueden extenderse a un país, un continente o incluso el mundo entero.

PAN, Personal Area Network

Las redes de área personal denominadas PAN, están conformadas por los dispositivos personales que permiten la interacción con la red, dentro de los cuales se tiene a las PDA (Personal Digital Assistant) y los teléfonos celulares.

Topologías y Protocolos

Topología

Una Topología, definen la forma de organización con la cual, los dispositivos o nodos se conectan al medio de comunicación dentro de la estructura de la red.
Existen dos tipos básicos de topologías; La Topología Física y La Topología Lógica.

Topología Física

Es determinada por la forma en la que físicamente los elementos o nodos de la red están interconectados entre sí.

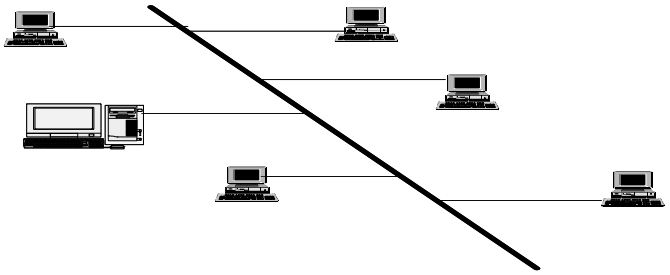
Topología Lógica

Se determina por el protocolo de comunicación, quien es el encargado de definir la forma de acceso al medio, el cual, determina bajo que reglas viaja la información dentro de la red.

Clases de Las Topologías

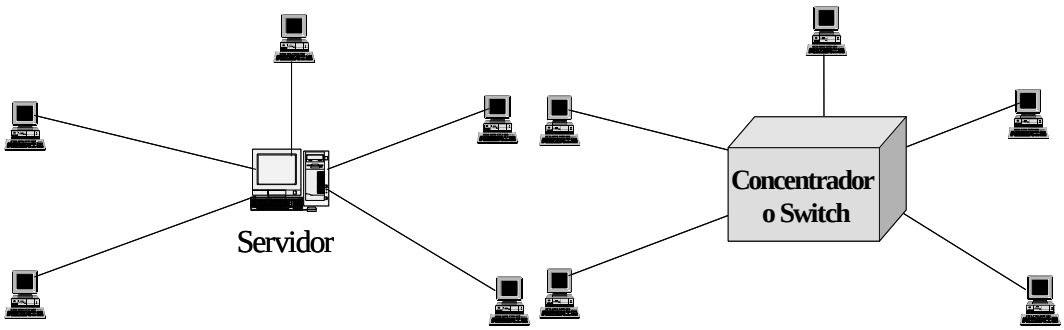
Topología De Bus

- Todos los dispositivos de la red, están enlazados por un solo cable.
- La información viaja en ambos sentidos.
- Utilizado con el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- Es difícil de aislar las fallas, ya que si el bus se interrumpe, todas las transmisiones se inhabilitan.



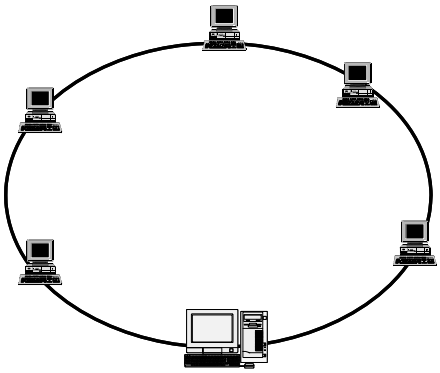
Topología De Estrella

- La comunicación se centraliza en un dispositivo que se encarga de retransmitir la información al nodo correspondiente.
- Cada uno de los nodos cuenta con un enlace hacia el dispositivo central, aislando las posibles fallas.
- Es utilizado por el Protocolo POLLING (poleo), comúnmente empleado en redes con minicomputadoras.
- Normalmente se implementa en Ethernet mediante un arreglo de concentradores o switches.



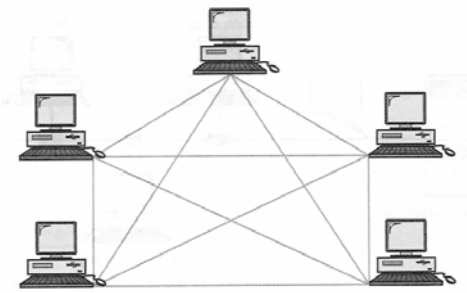
Topología De Anillo

- Todos los nodos de la red están conectados en serie, a través de un solo cable, describiendo un ángulo de 360°.
- La información viaja ordenadamente en un solo sentido.
- Una ruptura del anillo implica la inhabilitación de la red.
- Utilizado con el Protocolo TOKEN PASSING.
- Implementado con tecnologías Token Ring/IEEE 802.5 y FDDI.



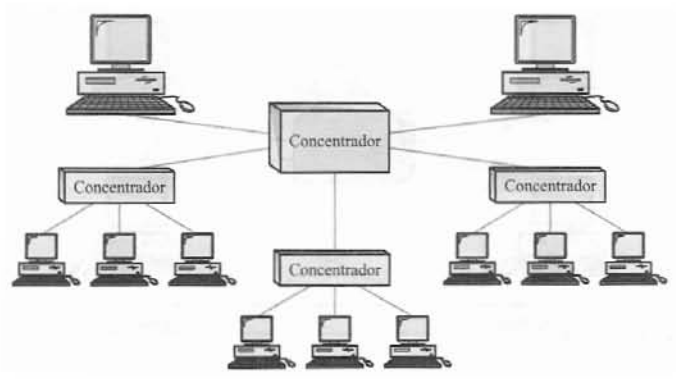
Topología En Malla

- Cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo.
- El enlace dedicado conduce el tráfico únicamente entre los dos dispositivos que conecta, por lo tanto, si un enlace falla no inhabilita al resto de la red.
- Permite garantizar la privacidad y seguridad de la red.
- Su instalación implica un gran número de cables, mayor costo y el uso de hardware especial para la conexión.



Topología En Árbol

- Es una variante de la estrella.
- En un árbol se conectan concentradores secundarios a uno llamado principal quien controla el tráfico de la red.
- Los concentradores secundarios pueden ser activos o pasivos, el concentrador principal siempre es activo.
- La principal ventaja de un árbol es el aumento en el número de nodos y la distancia de la red.



Protocolos

Son un conjunto de reglas establecidas que permiten realizar la comunicación entre dos o más nodos de la red.

Protocolos Por Demanda

Este tipo de protocolos demandan el uso del medio de comunicación, para lo cual realizan un sondeo del mismo para determinar su posible uso.
Un ejemplo, es el protocolo CSMA/CD (Carrier Sense Multiple Access/Collission Detection), utilizado en la tecnología Ethernet bajo la norma IEEE 802.3

Protocolos Por Distribución

Este tipo de protocolos permiten la distribución de la comunicación en forma ordenada, para lo cual, dependerá del protocolo en particular que se esté usando.

El protocolo Polling, basa su distribución en una serie de “Preguntas-Respuestas” entre el servidor que centraliza la comunicación y los nodos.

El protocolo Token Passing se implementa en un anillo físico por el cual viaja una señal en circulación continua, denominada “token”, el cual lleva el control de la comunicación entre los nodos de la red. Si un nodo no recibe la señal en un período especifico, emite una alarma indicando la existencia de un problema y de su localización.

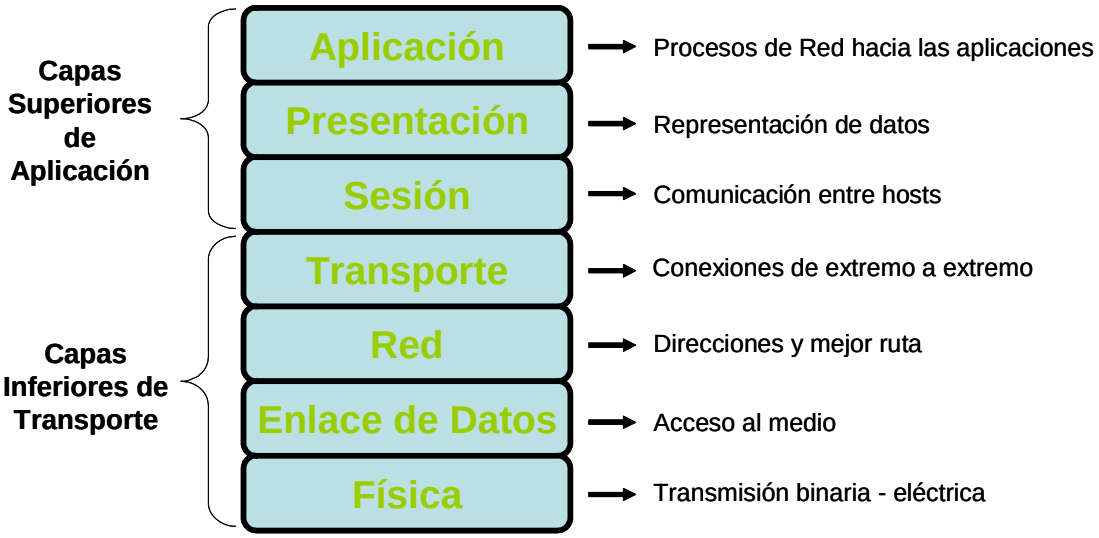
Modelo OSI

OSI, Open System Interconnection, es el modelo de referencia que describe cómo se transfiere la información, desde una aplicación de software en una computadora a través del medio de transmisión hasta una aplicación de software de otra computadora.

El modelo OSI se inició a finales de los años 70´s por la Organización Internacional de Estándares (ISO) y fue adoptado en 1984.

El objetivo del modelo OSI es permitir la comunicación entre sistemas distintos sin que sea necesario cambiar la lógica del hardware o el software subyacente.

El modelo OSI tiene siete capas, divididas en dos grupos. Las tres capas superiores definen como las aplicaciones en estaciones finales se comunicarán con cada una de los otros usuarios. Las cuatro capas inferiores definen como la información es transmitida extremo-a-extremo.



CAPA 7 - NIVEL DE APLICACIÓN

Procesos de red a aplicaciones.

- Proporciona servicios de red a procesos de aplicación (como correo electrónico, transferencia de archivos y emulación de terminales).

CAPA 6 - NIVEL DE PRESENTACIÓN

Representación de datos.

- Garantizar que los datos sean legibles para el sistema receptor.
- Formato de los datos.
- Estructuras de los datos.
- Negocia la sintaxis de transferencia de datos para la capa de aplicación.

CAPA 5 - NIVEL DE SESIÓN

Comunicación entre hosts.

- Establece, administra y termina sesiones entre aplicaciones.

CAPA 4 - NIVEL DE TRANSPORTE

Conexiones de extremo a extremo

- Se ocupa de aspectos de transporte entre hosts.
- Confiabilidad del transporte de datos.
- Establecer, mantener, terminar circuitos virtuales.
- Detección y recuperación de fallas.
- Control de flujo de información.
- Soporta servicios orientados y no orientados a la conexión.

CAPA 3 - NIVEL DE RED

Direccionamiento y mejor ruta.

- Proporciona conectividad y selección de ruta entre dos sistemas finales.
- Dominio de enrutamiento.
- Utilización de protocolos de ruteo.

CAPA 2 - NIVEL DE ENLACE DE DATOS

Acceso a los medios.

- Permite la transferencia confiable de los datos a través de los medios.
- Direccionamiento físico.
- Topología de red.
- Notificación de errores.
- Control de flujo.

Se divide en dos subcapas:

1- LLC (LOGIC LINK CONTROL)
2- MAC (MEDIA ACCESS CONTROL)

CAPA 1 - NIVEL FÍSICO

Transmisión binaria.

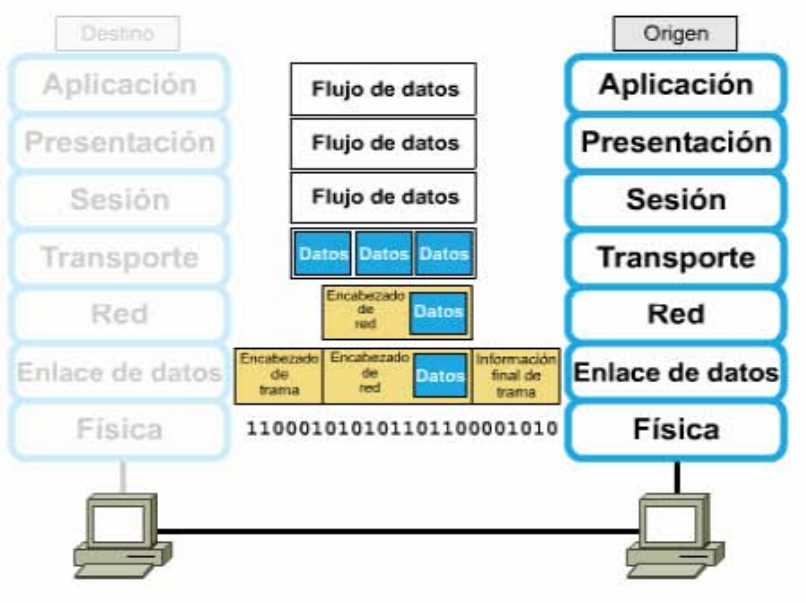
- Cables.

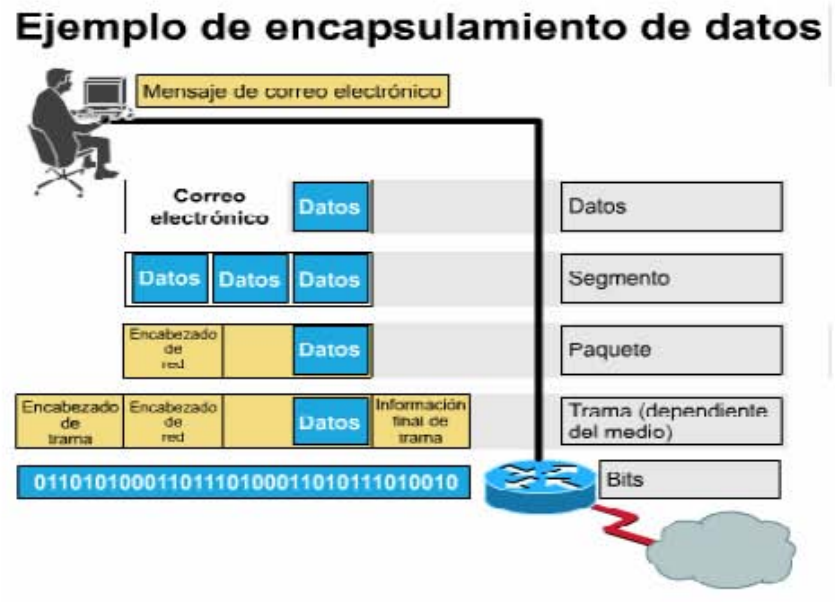
- Conectores.
- Voltajes.
- Velocidad de datos.

Encapsulamiento

El encapsulamiento, es el proceso de agregar información particular de cada uno de los niveles OSI a los datos originales que serán transmitidos.

Esta información se agrega en forma de encabezados y colas a los datos al pasar por cada nivel y solo podrá ser retirada en el receptor por el nivel correspondiente homólogo.



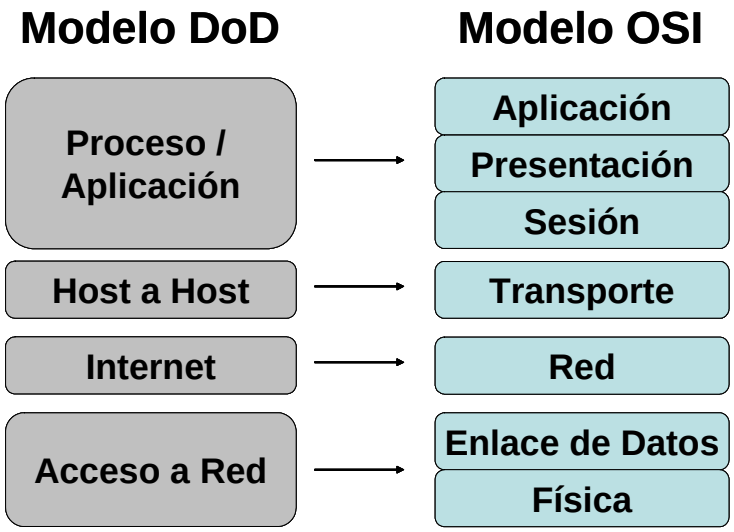


Suite TCP/IP

La Suite TCP/IP (Transmisión Control Protocol/Internet Protocol) fue creada por el Departamento de Defensa (DoD) para asegurar y preservar la integridad de la información, así como también para mantener comunicaciones en el caso de una guerra catastrófica.

Modelo DoD

El modelo DoD es básicamente una versión reducida del modelo OSI. Este modelo está compuesto de cuatro en lugar de 7 capas como el modelo OSI.



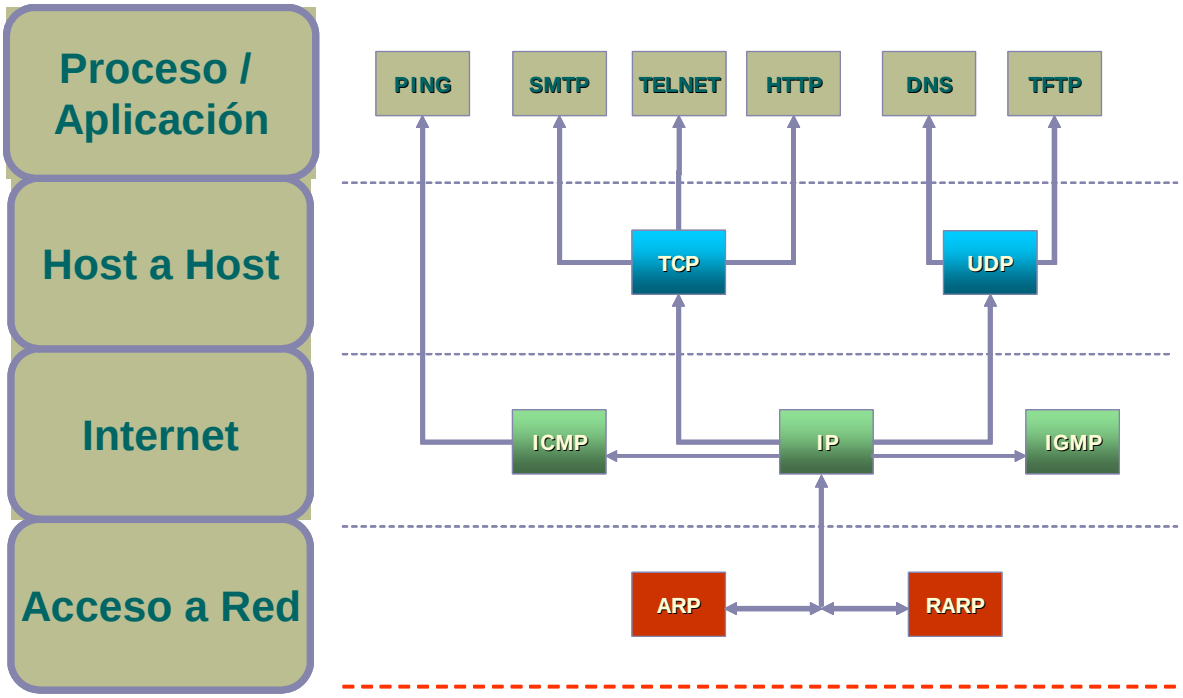
El modelo DoD y OSI son parecidos en diseño y concepto, además de que tienen funciones similares en capas similares.

La capa de Proceso/Aplicación define protocolos para aplicaciones de comunicación nodo a nodo y también controla especificaciones de la interfase de usuario.

La capa de Host a Host se compara con las funciones de la capa de Transporte del modelo OSI, definiendo protocolos para establecer el nivel de servicio de transmisión para las aplicaciones. Desempeña tareas tales como las de crear comunicación extremo a extremo confiable y asegurar la entrega de información libre de errores. Maneja la secuencia de paquetes y mantiene la integridad de la información.

La capa de Internet corresponde a la capa de Red del modelo OSI, designando los protocolos relacionados a la transmisión lógica de paquetes sobre la red entera. Se hace cargo del direccionamiento de hosts dándoles una dirección IP (Internet Protocol), además de manejar el ruteo de paquetes entre múltiples redes.

La capa de Acceso a la Red controla el intercambio de información entre el host y la red. Supervisa el direccionamiento físico y define protocolos para la transmisión física de la información. El equivalente de la capa Física y Enlace de Datos.



El protocolo TCP/IP consta de dos protocolos que funcionan en la capa 4 del modelo OSI (Capa de Transporte): TCP y UDP.

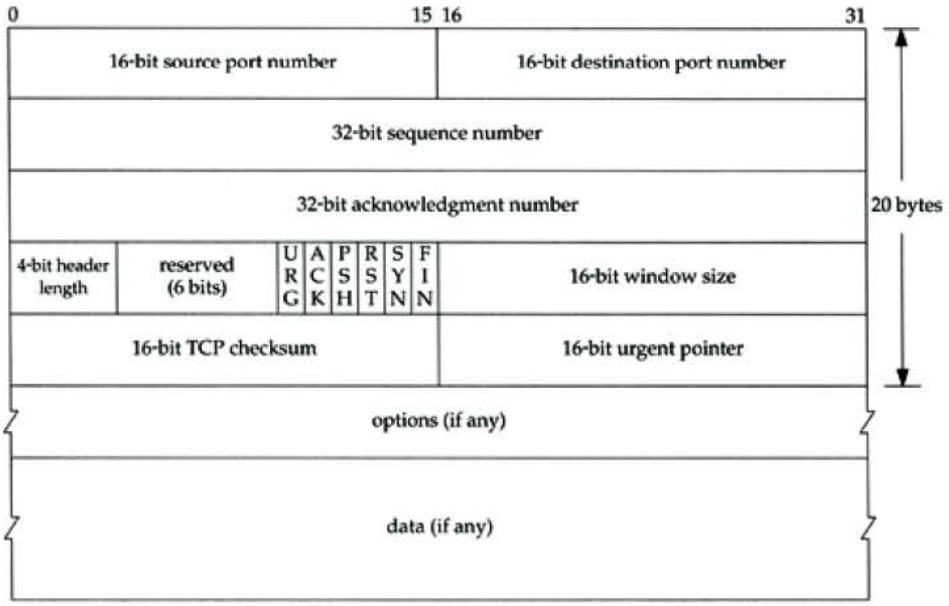
TCP ofrece un circuito virtual entre aplicaciones de usuario final.

- Orientado a conexión.
- Confiable.
- Divide los mensajes salientes en segmentos.
- Reensambla los mensajes en la estación destino.
- Vuelve a enviar lo que no se ha recibido.
- Reensambla los mensajes a partir de segmentos entrantes.

UDP transporta datos de manera no confiable entre hosts.

- No orientado la conexión.
- Poco confiable.
- Transmite mensajes (llamados datagramas del usuario).
- No ofrece verificación de software para la entrega de segmentos (poco confiable).
- No reensambla los mensajes entrantes.
- No utiliza acuses de recibo.
- No proporciona control de flujo.

Cabecera TCP



Source Port Y Destination Port: Identifican el número de puerto con el cual los procesos de origen y destino de las capas superiores reciben los servicios TCP.

Sequence Number: Especifica el número que se asigna al primer byte de datos en el mensaje actual.

Acknowledgment Number: Contiene el número de secuencia del siguiente byte de datos que el emisor del paquete espera recibir.

Header Length: Indica la longitud del encabezado TCP en palabras de 32 bits.

Reserved: Se establece en cero

Bits de Código: Funciones de control usados para iniciar y terminar una sesión.

- *Urg*: Indica que el campo *Urgent Pointer* es válido.
- *Ack*: Indica si el campo *Acknowledgment Number* es válido.
- *Pusk*: Indica que el receptor debe pasar estos datos a la aplicación lo antes posible.
- *Rst*: Inicializar la conexión.
- *Syn*: Sincroniza los números de secuencia para iniciar una conexión.
- *Fin*: Indica que el transmisor terminó de enviar información.

Window Size: Especifica el número de bytes que el receptor puede aceptar.

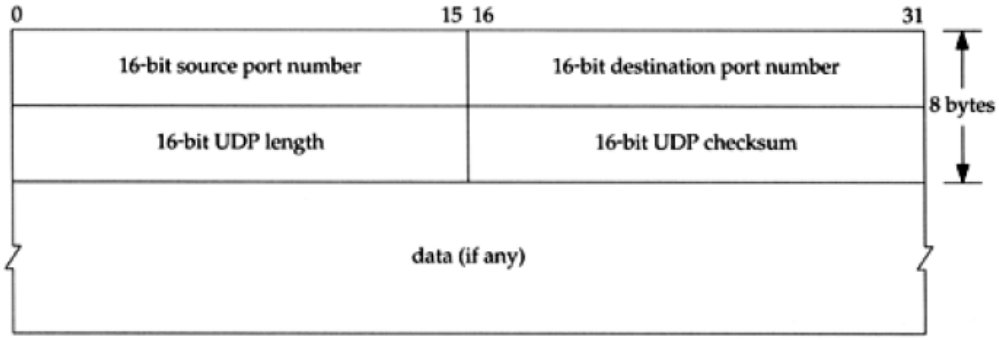
TCP Checksum: Indica si el segmento se dañó durante el viaje o se transmitió correctamente.

Urgent Pointer: Es válido sí la bandera *Urg* esta encendida, este campo indica que este número se agregue al número de secuencia.

Options: Tamaño máximo de segmento TCP.

Data: Datos de protocolo de capa superior.

Cabecera UDP



Source Port: Número del puerto de aplicación del hosts que está enviando la información.

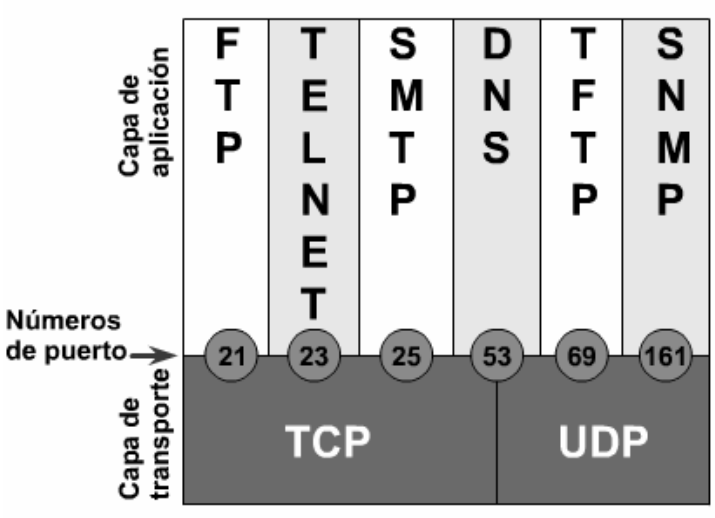
Destination Port: Número del puerto de la aplicación solicitada en el host destino.

UDP Lenght: Longitud del encabezado de UDP y de la información UDP.

UDP Checksum: Indica si el segmento se dañó durante el viaje o se transmitió correctamente.

Data: Información de la capa superior.

Números De Puerto



Otros protocolos que usan TCP y UDP

TCP	UDP
Telnet 23	SNMP 161
SMTP 25	TFTP 69
HTTP 80	DNS 53
FTP 21	
DNS 53	

Protocolos De La Capa De Internet

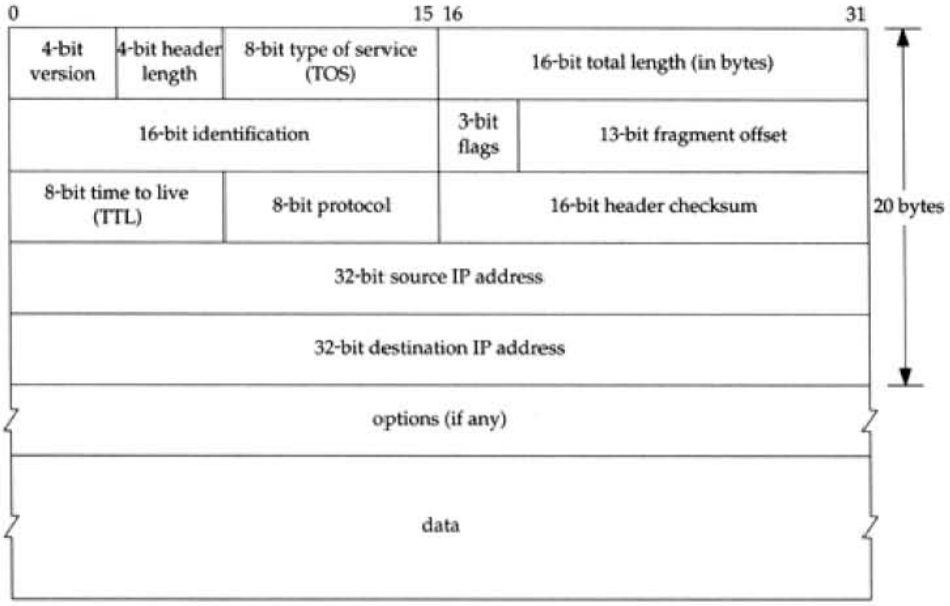
Los protocolos en la Capa de Internet son los siguientes:

- Internet Protocol (IP).
- Internet Control Message Protocol (ICMP).
- Address Resolution Protocol (ARP).
- Reverse Address Resolution Protocol (RARP).
- Proxy ARP.

Internet Protocol (IP)

El protocolo de Internet (IP) busca la dirección de cada paquete, usa la tabla de ruteo y decide por donde el paquete será enviado; Esto lo hace escogiendo la mejor ruta.
IP recibe segmentos desde la capa de Host a Host y los fragmenta en datagramas (paquetes). IP reensambla los datagramas y los hace segmentos en el lado receptor. A cada datagrama le es puesta la dirección IP del transmisor y del receptor. Cada router (Dispositivo de capa 3) que recibe un datagrama hace decisiones de ruteo basadas en la dirección IP de destino del paquete.

Cabecera IP



Version: En este campo se define la versión de IP que se esta corriendo, actualmente la versión es la 4.

Header Length: Este campo indica la longitud del encabezado en palabras de 32 bits. Normalmente es de 20 bytes. Sin embargo al ser un campo de 4 bits la longitud del encabezado puede ser mayor de 64 octetos.

Type Of Service. Los primeros 3 bits de este campo no son utilizados, así como un bit que no ha sido definido por lo que esta en 0. De los 4 bits restantes solo uno puede estar encendido. Si todos los bits se encuentran apagados indican un servicio normal.

Total Length: Este campo indica la longitud total del datagrama IP en bytes, como es un campo de 16 bits, la longitud de un datagrama IP puede ser de hasta 65535 bytes.

Identification: Este campo lleva un número generado por el nodo origen para identificar el datagrama que se esta enviando. La utilidad de este campo se incrementa cuando existe fragmentación en el trayecto del datagrama.

Flags: Este campo se utiliza para fines de fragmentación, consiste en 3 bits, el primer bit no esta definido. El segundo bites denominado DF (Don't Fragment), si este esta encendido indica que el datagrama no puede ser fragmentado. El tercer bit MF (More fragment) indica que existen más fragmentos para este datagrama.

Fragment Offset: Este campo indica la posición del datagrama en relación con el comienzo de los datos originales, lo cual permite que el proceso IP del destino reconstruya adecuadamente el datagrama original.

Time To Live: Este campo indica el número máximo de saltos que un datagrama puede dar (255), en cada salto el número de esta campo se decrementa en 1, cuando este campo tiene un valor 0 y no se ha alcanzado el destino el datagrama se descarta y el nodo fuente es informado con un mensaje ICMP.

Protocol: Este campo identifica el protocolo de capa superior que esta encapsulado en el datagrama IP.

Header Checksum: Este es un checksum solo para el encabezado IP, debido a que no es un protocolo confiable, no implementa detección y corrección de errores en el campo de información.

Source IP Address: Dirección IP origen.

Destination IP Address: Dirección IP destino.

Internet Control Message Protocol (ICMP)

El protocolo ICMP trabaja en la Capa de Red y es usado por IP para diferentes servicios. ICMP es un protocolo de administración y proveedor de servicio de mensajes para IP. Sus mensajes son transportados como datagramas IP.

Algunos eventos comunes y mensajes que usa ICMP son:

Destino Inalcanzable: Si un router no puede enviar un datagrama IP, el router usa ICMP para enviar un mensaje de regreso al transmisor, avisandole de la situación.

Buffer Lleno: Si el buffer de memoria del router para recibir datagramas está lleno, el router usará ICMP para enviar este mensaje hasta que la congestión disminuya.

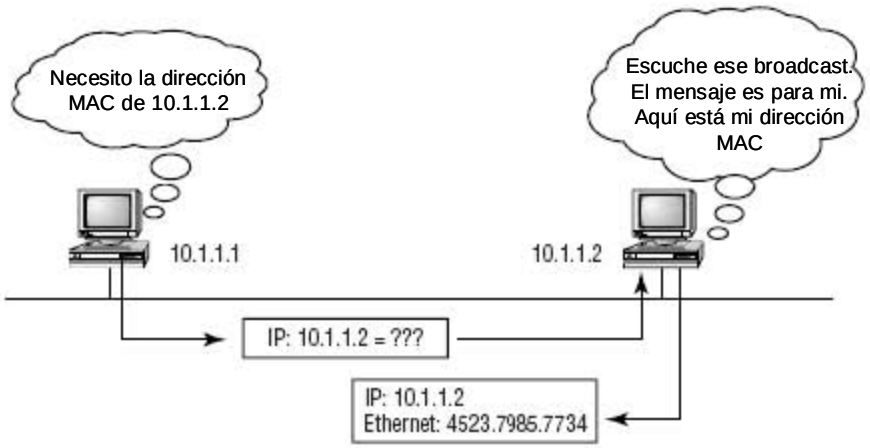
Saltos (Hops): Cada datagrama IP es asignado a un cierto número de routers, llamados Saltos (hops), para atravesar; Si se alcanza el límite de saltos antes de llegar a su destino, el último router que recibe

el datagrama lo borra y utiliza ICMP para mandar un mensaje de defunción, informando a la máquina transmisora de la eliminación de su datagrama.
Ping: Ping (Packet Internet Groper) usa mensajes de ecos de ICMP para verificar la conectividad física y lógica de máquinas en una red.

Traceroute: Es usado para descubrir la ruta que el paquete o datagrama toma para atravesar la red, para lo cual usa descansos o interrupciones de ICMP.

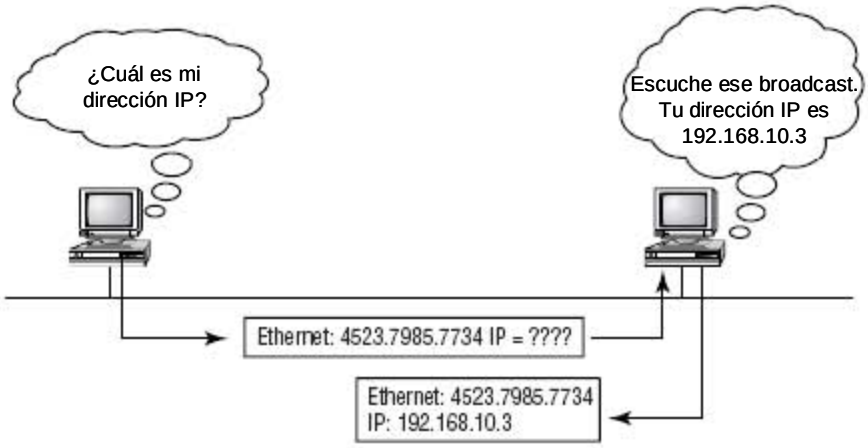
Address Resolution Protocol (ARP)

Encuentra la dirección física (MAC Address) de un host desde una dirección IP conocida.



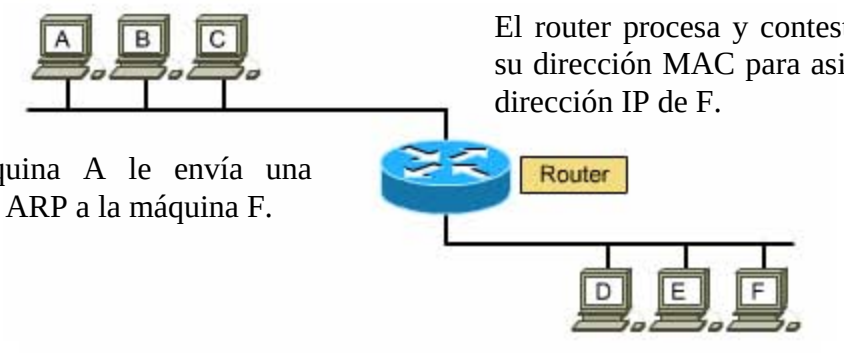
Reverse Address Resolution Protocol (RARP)

Encuentra la dirección IP de un host desde una dirección física (MAC Address).



Proxy Address Resolution Protocol (Proxy ARP)

El protocolo ARP proxy es una variante del protocolo ARP. En este caso, un dispositivo intermedio (por ejemplo un router) envía una respuesta ARP, de parte de un nodo final, hacia el host que realiza la petición. Los routers que ejecutan el protocolo ARP proxy capturan paquetes ARP. Responden enviando sus direcciones MAC a aquellas peticiones en las que la dirección IP no se ubica dentro la gama de las direcciones de la subred local.



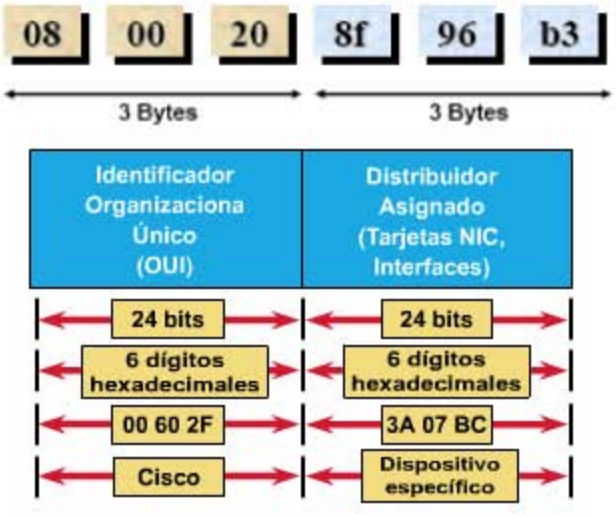
La máquina A le envía una petición ARP a la máquina F.

El router procesa y contesta a A con su dirección MAC para asignarla a la dirección IP de F.

Direccionamiento Físico

- Una dirección física es un identificador único a nivel de hardware que viene integrado en cada interfase de red (NIC, Network Interfaec Card).
- Las direcciones físicas, en la mayoría de los casos NO se pueden alterar.
- Los estándares de red más comunes hacen uso de direcciones físicas de 6 bytes a las cuales llamamos direcciones MAC (establecidas por la IEEE).
- Su representación es en forma Hexadecimal. Ejemplo: 08:00:20:8f:96:b3

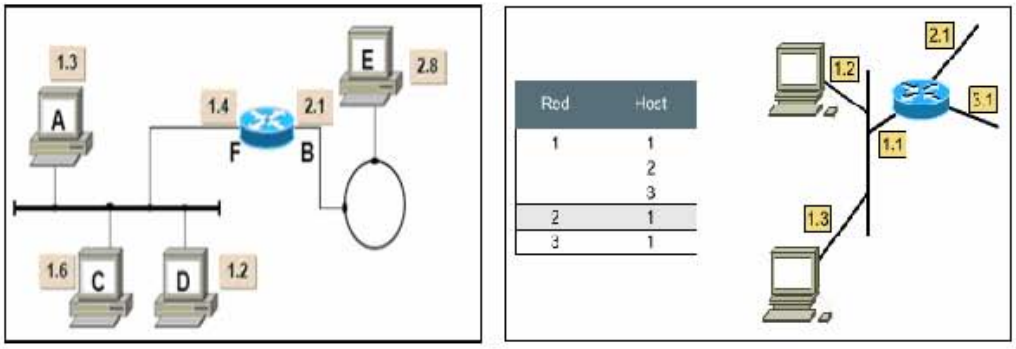
Formato de una dirección MAC:



- Los 3 primeros Bytes los asigna IEEE al Fabricante (Identifican al fabricante).
- Los 3 últimos Bytes los asigna el fabricante arbitrariamente.

Direccionamiento Lógico

- Las direcciones físicas solo sirven para intercomunicar equipos interconectados en una red local, debido a que su nomenclatura solo hace referencia a interfases de red.
- Las direcciones lógicas, a diferencia de las físicas no se encuentran configuradas en el hardware, se configuran por software.
- Su formato varía según la arquitectura de red que se utilice (Apple Talk, Novell IPX, TCP/IP, etc.).

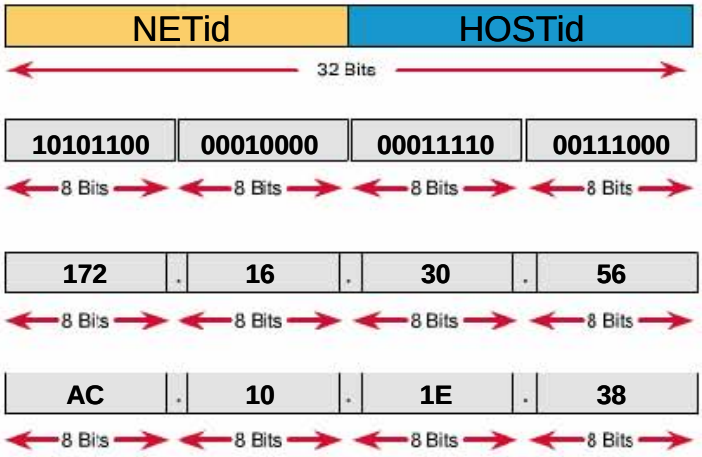


Direccionamiento IP

- Una dirección IP es un identificador numérico asignado a cada máquina en una red IP.
- Una dirección IP proporciona información de un host y de la red a la cual pertenece.
- Una dirección IP es una dirección de software, no una dirección física.

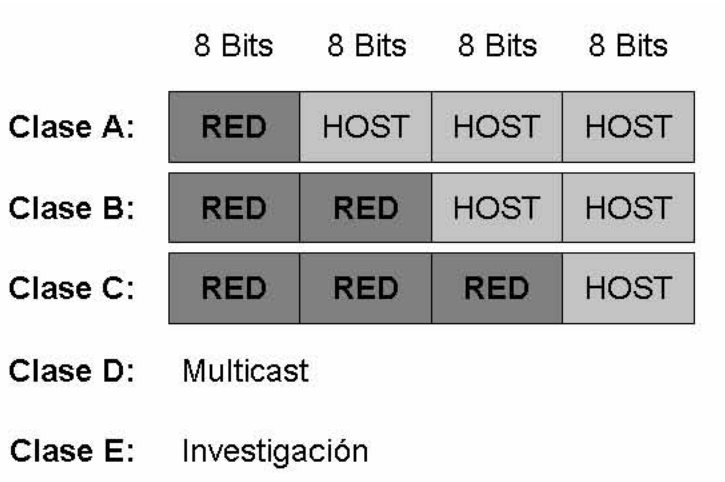
El direccionamiento fue designado para permitir a un host en una red comunicarse con otro host en una red diferente, sin importar en que tipo de LAN los host están participando.
Una dirección IP consiste de 32 bits de información (4 bytes). Estos bits son divididos en cuatro secciones referidos como octetos o bytes, cada byte está compuesto de 8 bits.
Se puede expresar la misma dirección IP utilizando uno de los tres métodos, aunque es más común que se ocupen los dos primeros:

- Decimal: 172.16.30.56
- Binario: 10101100.00010000.00011110.00111000
- Hexadecimal: AC.10.1E.38



Las direcciones IP se dividen en 5 clases: **A, B, C, D** y **E**.
Cada clase se identifica por el número de bits destinados para el NETid.
En cada clase se tiene un número diferente de redes y hosts por red de acuerdo al tamaño del NETid y del HOSTid respectivamente (a excepción de las clases **D** y **E**).

Resumen del Rango de Redes

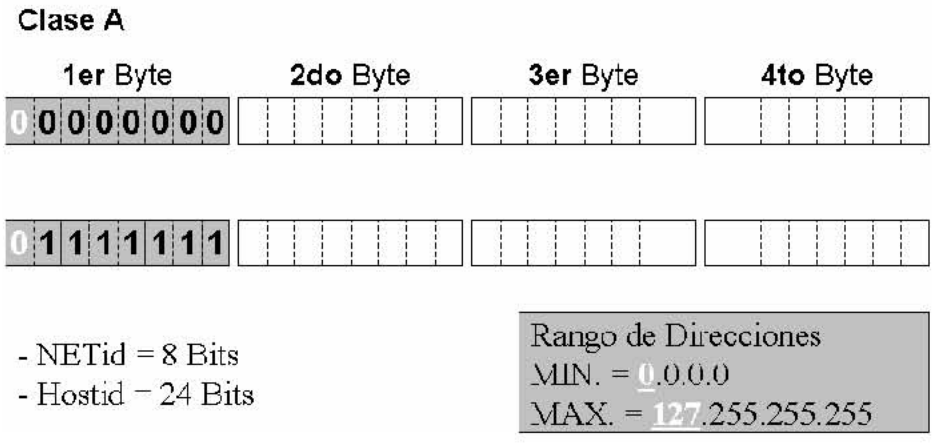


El primer bit del primer byte en una Red Clase A deben estar siempre en cero.

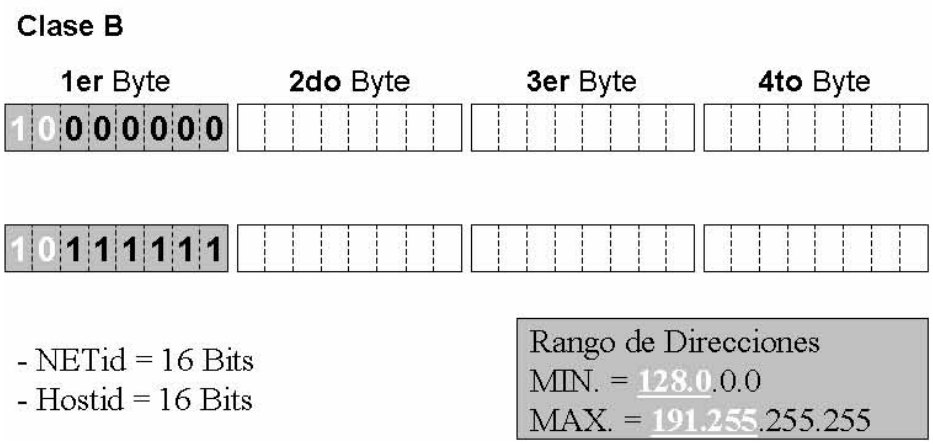
Considerando la siguiente dirección de red:

0xxxxxxx

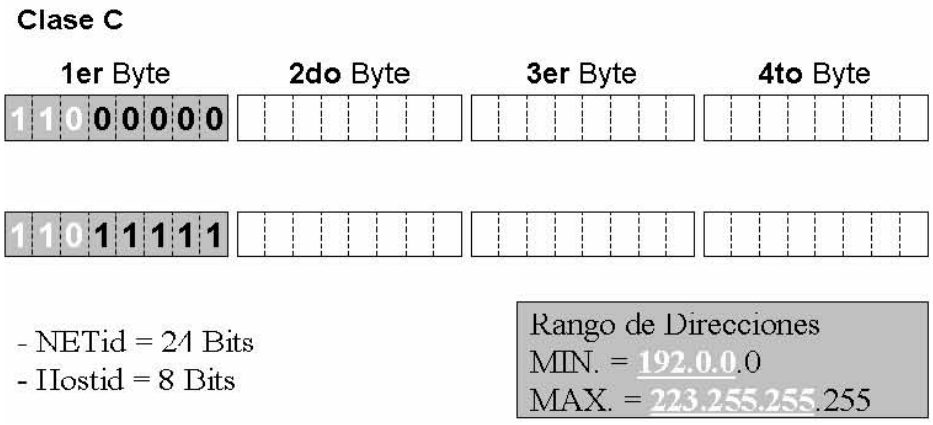
Si primero se cambian los 7 bits restantes a 0 y después a 1, se encontrará el rango de direcciones de red de la Clase A



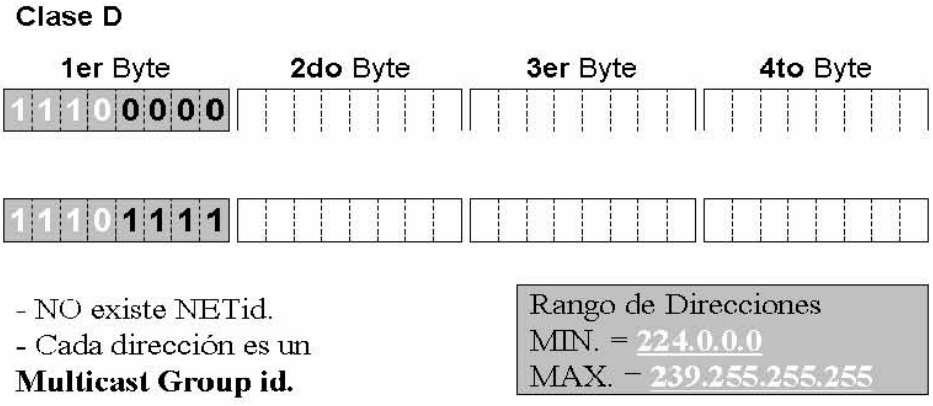
En la red de Clase B, el primer bit del primer byte debe estar siempre en 1, pero el segundo bit debe estar siempre en 0. Si se cambian los otros 6 bits a 0's y después a 1's se encontrará el rango de la red de Clase B.

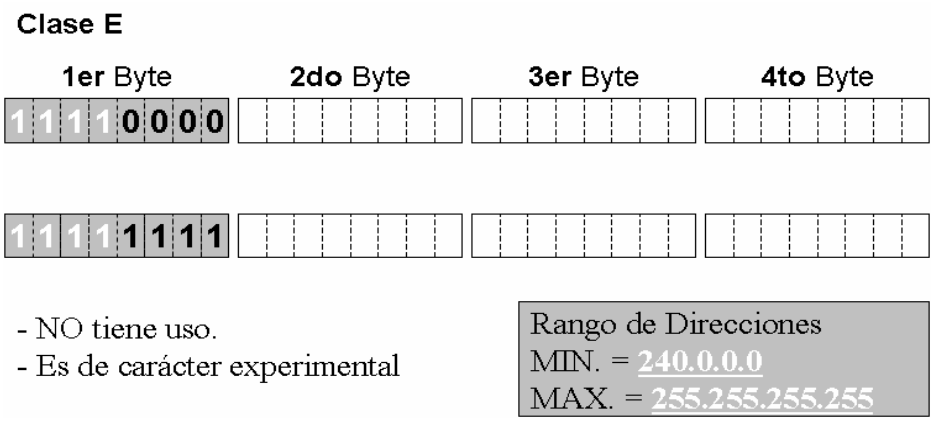


Para una red Clase C, los dos primeros bits del primer byte u octeto siempre deben estar en 1, pero el tercer bit no debe estar en 1. Si se cambian los otros 5 bits a 0's y después a 1's se encontrará el rango de la red de Clase C.



Las direcciones entre 224 y 225 son reservadas para las redes de Clase D y E. La clase D (224-239) es usada para direcciones multicast y la Clase E (240-255) para propósitos científicos o experimentales.





Direcciones IP Reservadas

Dirección	Función
Dirección de Red, todos los bits en 0's	Interpretada como "Ésta red o segmento".
Dirección de Red, todos los bits en 1's	Interpretada como "Todas las redes".
Red 127.0.0.1	Reservada para pruebas de loopback. Designa el nodo local y permite a ese nodo enviar paquetes de prueba asimismo sin generar tráfico de red.
Dirección de Nodo, todos los bits en 0's	Interpretada como "Dirección de Red" o cualquier host en una red específica.
Dirección de Nodo, todos los bits en 1's	Interpretada como "Todos los nodos" en la red especificada; por ejemplo, 128.2.255.255 significa "Todos los nodos" de la red 128.2 (Dirección de Clase B).
Dirección IP con todos los bits en 0's	Usada por los routers Cisco para designar la ruta default. También se le puede llamar "Cualquier Red".
Dirección IP con todos los bits en 1's	Broadcast a todos los nodos en la red actual.

Direcciones IP Privadas

Estas direcciones pueden ser usadas en una red privada, pero no pueden ser enrutadas a través de Internet. Están diseñadas con el propósito de crear una medida de seguridad, pero también ahorran valuable espacio de direcciones IP.
Para poder enrutar tráfico desde una red privada a través de Internet se usa algo llamado NAT (Network Address Translation), el cual toma una dirección privada y la convierte para su uso en Internet.

Espacio de Direcciones IP Privadas

Clase de Red	Espacio de Dirección Privado
Clase A	10.0.0.0 hasta 10.255.255.255
Clase B	172.16.0.0 hasta 172.31.255.255
Clase C	192.168.0.0 hasta 192.168.255.255

Direcciones de Broadcast

Broadcast de Capa 2: Los paquetes son enviados a todos los nodos de una LAN.

Broadcast de Capa 3: Los paquetes son enviados a todos los nodos de la red.

Unicast: Los paquetes son enviados a un solo host de destino.

Multicast: Los paquetes son enviados desde un simple origen y transmitidos a muchos dispositivos en diferentes redes.

Mascara De Red

Conjunto de 32 bits que sirve para identificar las partes del NETid y del HOSTid de una dirección IP.

En una máscara de red:

- Todos los bits igual a "**1**" identifican la parte del NETid.
- Todos los bits igual a "**0**" identifican la parte del HOSTid

Para las clases A, B y C el NETid ya está definido, por lo tanto, las máscaras de red son:

CLASE "A"

255	**.**	**0**	**.**	**0**	**.**	**0**
11111111	**.**	**00000000**	**.**	**00000000**	**.**	**00000000**

CLASE "B"

255	.	255	.	0	.	0
11111111	.	11111111	.	00000000	.	00000000

CLASE "C"

255	.	255	.	255	.	0
11111111	.	11111111	.	11111111	.	00000000

Estas máscaras se conocen como: máscaras naturales.

Todo host que requiera interactuar con otros en TCP/IP debe tener configurado forzosamente una dirección IP y su correspondiente máscara de red.

Una máscara de red asociada a una dirección IP se puede representar de dos maneras, Ejemplo:

IPv6 (Internet Protocol Version 6)

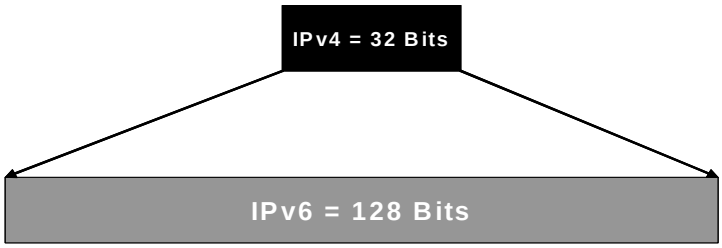
Como una solución a las limitaciones de IPv4, el Internet Enginnering Task Force (IETF), creó el proyecto IPv6 o IPng (Internet Protocol Next Generation).
En noviembre de 1994, el RFC 1752 "The Recommendation for the IP Next Generation" se convirtió en un estándar para el sucesor de IPv4.
IPng es llamado también IPv6.

Características

- IPv6 incrementa el tamaño de las direcciones de 32 a 128 bits.
- Soporta niveles en la jerarquía de direccionamiento.
- Sistema de configuración de direcciones.
- Simplificación de la cabecera.
- Mayor flexibilidad para extensiones y nuevas opciones.
- Capacidades de control de flujo.
- Capacidad de autenticación y privacidad de datos.
- Movilidad.
- Seguridad e integridad de datos.
- Calidad de servicio, QoS.

- Soporte a tráfico multimedia en tiempo real.
- Aplicaciones multicast y anycast.
- Mecanismos de transición gradual de IPv4 a IPv6.

Direccionamiento



IPv4

- 32 bits o 4 bytes de longitud.
- 4,200,000,000 posibles nodos direcionables.

IPv6

- 128 bits o 16 bytes: cuatro veces los bits de IPv4.
- 3.4 * 1038 posibles nodos direccionables.
- 340,282,366,920,938,463,374,607,432,768,211,456.
- 5 * 1028 direcciones.

Representación de Direcciones en IPv6

Existen tres formas para representar direcciones IPv6 mediante cadenas de texto:

1. La forma más indicada es mediante la estructura x:x:x:x:x:x:x:x donde los valores x son los valores hexadecimal de cada bloque de 16 bits de la dirección.

Ejemplo:
FEDC:BA09:6543:1234:FDCE:7564:BA98:7651

2. El segundo método permite agrupar largas series de ceros, para hacer más legibles las direcciones; El uso de "::" indica múltiples grupos de 16 bits a 0.

Ejemplos:
1080:0:0:0:8:800:200C:417A podría representarse como 1080::8:800:200C:417A
FFF01:0:0:0:0:0:0:43 podría representarse como FF01::43

Sólo puede usarse "::" una vez en una dirección.

3. El tercer método resulta el más indicado para representar direcciones IPv6 que contengan direcciones IPv4, los 2 últimos bloques de 16 bits se representan como 4 bloques de 8 bits mostrando sus valores en decimal, como IPv4.
Ejemplos:

0:0:0:0:0:0:13.1.68.3 ó ::13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38 ó ::FFFF:129.144.52.38

Los diferentes tipos de direcciones son especificados por los bits de mayor peso de la dirección, cada tipo tiene asignado un prefijo, de longitud variable para cada tipo.

Características de Direcciones IPv6

- Las direcciones IPv6 se asignan a interfaces lógicas.
- Una interfaz puede tener múltiples direcciones únicas. Cualquiera de las direcciones asociadas a las interfaces de los nodos se puede utilizar para identificar de forma única al nodo.
- Las direcciones tiene ámbitos de acción.
  - Link Local
  - SiteLocal
  - Global

Tipos de Direcciones IPv6

Unicast

Identificador para una interfaz individual. Un paquete IPv6 unicast, es encaminado a una única interface, especificada por la dirección. Una dirección unicast IPv6 tiene una estructura similar a una IPv4.
Existen múltiples formatos, como mínimo, un nodo considerará una dirección IPv6 como un identificador sin estructura interna.

Anycast

Identificador para un conjunto de interfaces. Un paquete IPv6 anycast es encaminado a una y sólo una de las interfaces identificadas por la dirección. El paquete será encaminado a la interface más cercana, de acuerdo con las técnicas de medida de distancia de las estrategias de enrutamiento. Una dirección anycast no podrá nunca aparecer como dirección origen, ni podrá ser asignada a ningún host, sólo podrán ser asignadas a un router.

Multicast

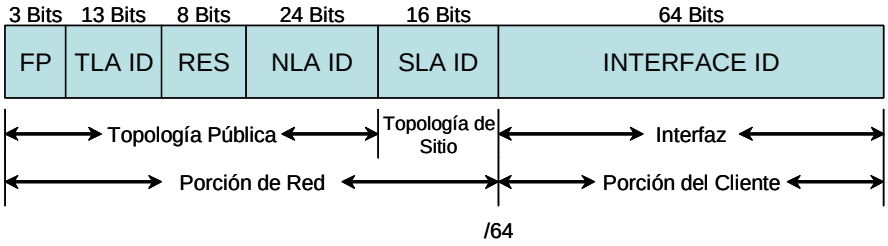
Identificador para un conjunto de interfaces o nodos. Un nodo puede pertenecer a cualquier número de conjunto multicast. Un paquete IPv6 multicast es encaminado a todas y cada una de las interfaces identificadas por la dirección.

8-Bits	4-Bits	4-Bits	112-Bits
1111 1111	Tiempo de Vida	Ámbito	Identificador de Grupo

Tiempo de Vida	
0	Si es Permanente
1	Si es Temporal

Ámbito	
1	Node
2	Link
5	Site
8	Organization
E	Global

Arquitectura Jerárquica De Direcciones IPv6



FP	Format Prefix (001)
TLA ID	Top-Level Aggregation Identifier
RES	Reservado para uso futuro
NLA ID	Next-Level Aggregation Identifier
SLA ID	Site-Level Aggregation Identifier
INT ID	Interface Identifier

IPv6 ha sido diseñado para proporcionar una alta escalabilidad de espacio de direcciones que puedan ser particionadas en una flexible y eficiente jerarquía de ruteo global.

TLA (Top Level Aggregation): Son esencialmente puntos de tránsito público (intercambio) donde los proveedores establecen sus puntos de conexiones.

NLA (Next Level Aggregation): Son direcciones que representan proveedores grandes y redes corporativas globales. Cuando una NLA es un proveedor, éste asigna estas direcciones a sus suscriptores. Los suscriptores con el mismo proveedor tienen direcciones IP con un prefijo NLA común.

SLA (Site Level Aggregation): Son bloques de direcciones contiguas asignadas por suscriptores, utilizadas por organizaciones individuales para crear su propia jerarquía de direccionamiento local e identificar subnet y host.

Interface ID: Usada para identificar una interface IPv6 en una red.

Ejemplos de IPv6

Aggregatable Global Unicast Address

• pTLA UNAM	3FFE:8070::/28 (Pruebas)
• sTLAUNAM	2001:0448::/35 (Producción)
• pNLAUNAM	3FFE:1300:14::/48
• pNLACIC-IPN	3FFE:8070:1008::/48
• pNLACUDI	3FFE:8070:1006::/48
• dirUNAM	3FFE:1CFF:0:F4::2/64
• dirUNAM	3FFE:8070:1:2::1/64

Autoconfiguración en IPv6

Dos tipos de autoconfiguración:
Stateless: un router participa en la configuración de la dirección IPv6del host.

Stateful (DHCP para IPv6): un servidor de DHCP IPv6 configura a los hosts con una dirección y otros parámetros de IPv6.

Protocolos de ruteo de IPv6

- RIPng o RIPv6 (RFC 2080, RFC 2081).
- BGP4+ (RFC 2283, RFC 2545).
- OSPFv6 (RFC 2740).
- EIGRPv6.

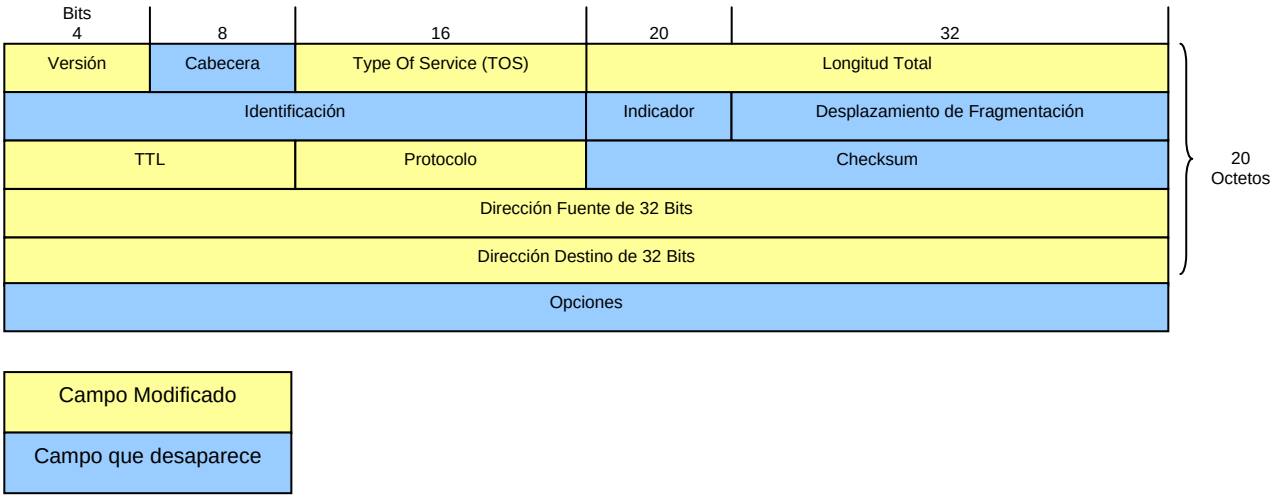
Seguridad en IPv6

Dos tipos de mecanismos de seguridad:

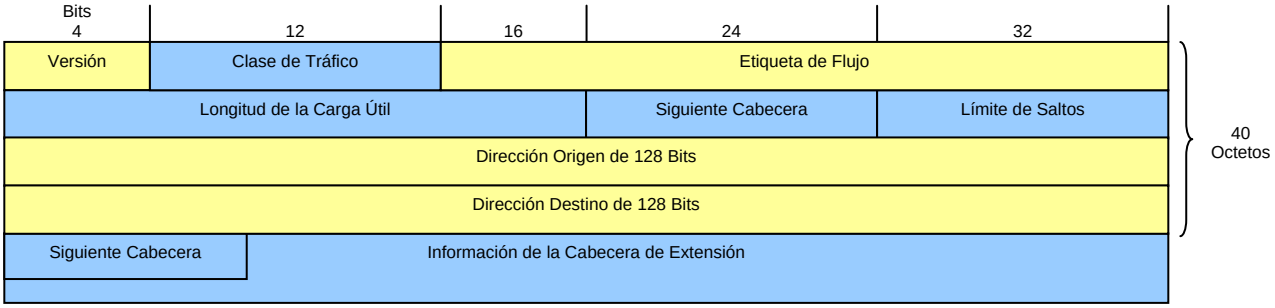
- *Authentication*: autenticación de los paquetes, realizada con el Authentication Header (RFC 2402).
- *Payload Security*: encriptación "Extremo a Extremo" del paquete, realizada con el Encapsulating Security Payload Header (RFC 2406).

Cabecera IPv4 e IPv6

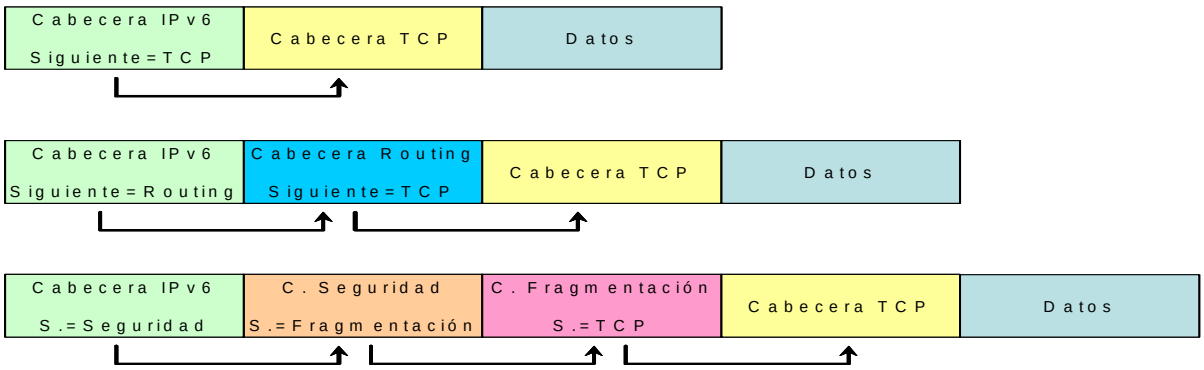
IPv4



IPv6



El valor del campo "siguiente cabecera" indica cual es la siguiente cabecera. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destinos finales. Hay una única excepción: cuando el valor de este campo es cero, indica opción de examinado y proceso "salto a salto" (hop-by-hop).



Cabeceras Extendidas

- En IPv6, la información diferente es codificada en cabeceras separadas, entre la cabecera IPv6 y la cabecera del nivel superior.
- Cada cabecera extendida es identificada con un valor en el campo siguiente cabecera.
- Un paquete IPv6 puede contener ninguna, una o más cabeceras extendidas.
- Las cabeceras deben ser procesadas en el orden en que aparezcan, el receptor no puede buscar una cabecera en concreto y procesarla antes que las anteriores.
- Si en el procesamiento de las cabeceras, un nodo se encuentra con un valor en siguiente cabecera que le es desconocido, el paquete debe ser descartado y un nivel superior (ICMP), se encargará de enviar un error al origen.
- Cada cabecera extendida debe tener una longitud en octetos múltiplo de 8, para mantener la alineación a 8 octetos a cabeceras posteriores.

Cabecera Opciones Salto A Salto: Se usa para contener información que deberá ser examinada por cada nodo que encamine el paquete hacia su destino.

Cabecera De Enrutamiento: Es utilizada por el remitente para indicar uno o más nodos que el paquete debe visitar en su recorrido.

Cabecera De Fragmento: Es utilizada por el origen del paquete IPv6 para enviar paquetes cuyo tamaño excede el mínimo MTU en el camino del paquete, la fragmentación solo la lleva a cabo el nodo origen.

Cabecera De Opciones En Destino: Se usa para contener información que sólo debe ser examinada por el nodo destino.

Cabecera De Autenticación: Proporciona soporte para integridad de datos y autenticación de paquetes IP. El contenido del campo de datos de autenticación dependerá del algoritmo de autenticación especificado en cada caso, que son establecidos por estándares basados en asociaciones de seguridad.

Cabecera De Encriptación: Ésta es el área direccionada por el servicio de encapsulamiento de Seguridad de Carga (ESP, Encapsulating Security Payload), los paquetes protegidos por las técnicas de encriptación pueden tener muy altos niveles de privacidad e integridad. ESP proporciona encriptación en la capa de red, esto es disponible para todas las aplicaciones en una alta estandarización.

Orden De Las Cabeceras

Cuando existe más de una cabecera extendida en el mismo paquete, el orden de las cabeceras debe ser el siguiente:

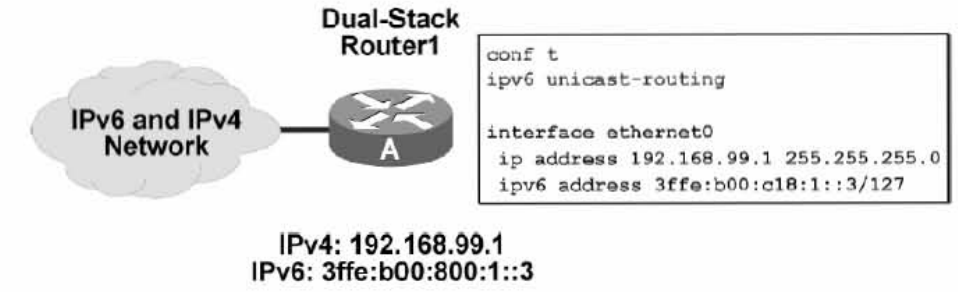
- Cabecera IPv6.
- Opciones Salto a Salto.
- Opciones en destino. Para opciones que deban ser procesadas por el destino final y por los destinos marcados en la cabecera de enrutamiento.
- Enrutamiento.
- Fragmentación.
- Autenticación.
- Opciones de seguridad para la carga.
- Opciones en destino. Para opciones que solo deban ser procesadas por el destino final.
- Cabecera de nivel superior.

Transición de IPv4 a IPv6

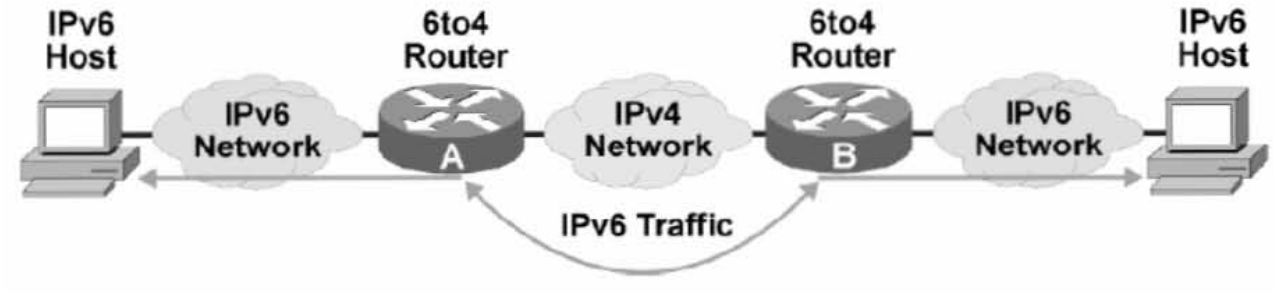
Dos mecanismos principales (RFC 1933):

- Capa IP dual: Los ruteadores y hosts soportan IPv4 y IPv6 simultáneamente.
- Túneles de IPv6 sobre IPv4: Los paquetes IPv6 se encapsulan con encabezados de IPv4 para transportarse por redes de IPv4. Existen dos tipos de de túneles: configurados (manuales) y automáticos.

Mecanismo Dual-Stack



Mecanismo de Túnel



Capitulo 3

Tecnologías LAN

Token Ring

La red Token Ring fue desarrollada por IBM en los años setenta. La especificación IEEE 802.5 es prácticamente idéntica a la red Token Ring de IBM, y absolutamente compatible con ella. El término Token Ring se refiere tanto al Token Ring de IBM como a la especificación 802.5 del IEEE.

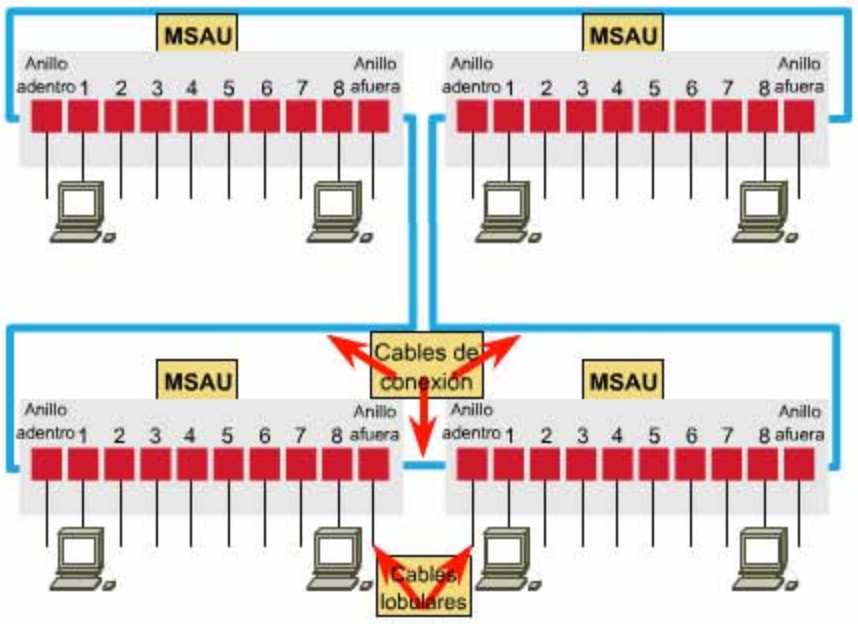
Tiene las siguientes características:

- Topología Física: Estrella o anillo.
- Topología Lógica: Anillo.
- Protocolo de acceso al medio: Token passing.
- Velocidad de transmisión: 4 o 16 Mbps.
- Dispositivos: MSAU, Multi Station Access Unit

	Red Token Ring de IBM	IEEE 802.5
Velocidad de los datos	4 ó 16 Mbps	4 ó 16 Mbps
Estaciones/segmentos	260 (Par trenzado blindado) 72 (Par trenzado sin blindaje)	250
Topología	Estrella	No especificado
Medios	Par trenzado	No especificado
Señalización	Banda base	Banda base
Método de acceso	Transmisión de tokens	Transmisión de tokens
Codificación	Diferencial Manchester	Diferencial Manchester

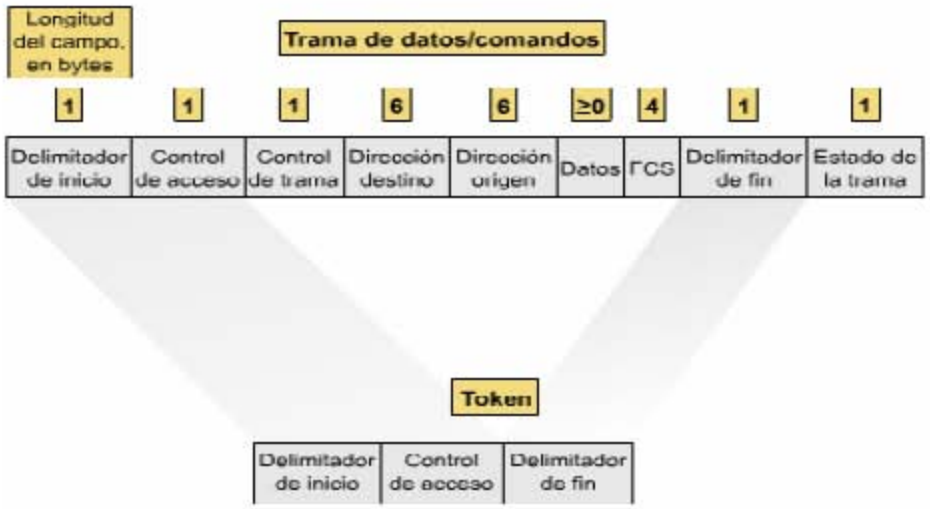
Token Ring vs IEEE 802.5

Las estaciones de red Token Ring de IBM (que a menudo usan STP y UTP como medios) están conectadas directamente a las MSAU y se pueden conectar entre sí por medio de cables para formar un anillo grande. Los cables de conexión unen las MSAU con otras MSAU adyacentes a ellas. Cables lobulares conectan las MSAU con las estaciones. Las MSAU incluyen relays bypass para eliminar estaciones del anillo.



Conexión Física de la red Token Ring de IBM.

Formato de la Trama IEEE 802.5 y Token Ring



Delimitador De Inicio: Es un campo que viola el código de línea utilizado en el resto de la trama para indicar que es el primer byte de la misma.

Control De Acceso: Contiene 3 bits de prioridad (los bits mas significativos), 3 bits de reservación (los bits menos significativos), un bit de token/frame y un bit de monitoreo que es utilizado por la estación monitorea de la red.

Control De Trama: Este campo indica si la trama lleva información de capas superiores o información de control.

Dirección Origen Y Destino: Dirección MAC de 6 octetos.

Datos: Contiene información de capas superiores.

Fcs: Frame Check Sequence. Contiene el resultado de la operación de CRC que hace el transmisor a la trama de información.

Delimitador De Fin: Byte que identifica el final de una trama o un token.

Estado De La Trama. Se utiliza para terminar una trama de datos/comandos. Este campo incluye el indicador de confirmación de dirección y el indicador del copiado de la trama.

FDDI Y CDDI

La comisión normalizadora ANSI X3T9.5 a mediados de los años 80's creó el estándar Interfaz de Datos Distribuida por Fibra (FDDI). Después de completar las especificaciones, el ANSI envió la FDDI a la Organización Internacional de Normalización (ISO), la cual creó entonces una versión internacional de dicha interfaz que es absolutamente compatible con la versión estándar del ANSI.

La FDDI especifica una LAN con topología de anillo doble, método de acceso de estafeta circulante a 100 Mbps que utiliza fibra óptica.

La tecnología FDDI utiliza una arquitectura de anillo doble a través del cual fluye tráfico en direcciones opuestas para ofrecer mayor confiabilidad y robustez en la red.

FDDI utiliza la fibra óptica como medio de transmisión principal sin embargo, existe la especificación CDDI sobre cobre.

La fibra óptica tiene varias ventajas, tales como, seguridad, confiabilidad y desempeño, además la fibra es inmune a la interferencia eléctrica causada por frecuencias de radio y campos electromagnéticos.

FDDI, permite transmitir a una velocidad de 100 Mbps y una distancia de 2 km, si utiliza fibra multimodo y distancias aún mayores si utiliza fibra óptica monomodo.

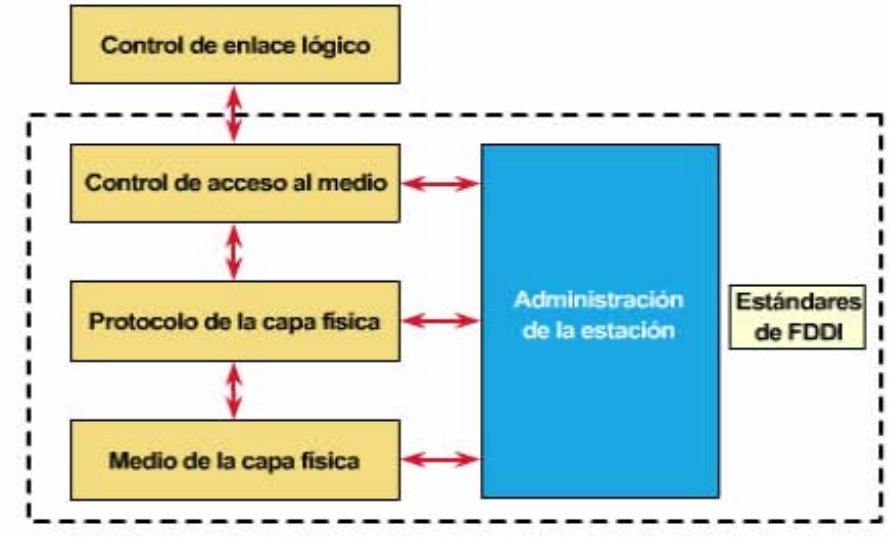
FDDI tiene cuatro especificaciones para su funcionamiento:

MAC, Media Access Control: define cómo se accesa al medio de transmisión, incluyendo el formato de trama, el manejo de la estafeta, el direccionamiento, los algoritmos para el cálculo de CRC y el mecanismo de recuperación de errores.

PHY, Protocolo de la Capa Física: define los procedimientos de codificación o decodificación, los requerimientos de temporización y el entramado.

PMD, Protocolo Dependiente del Medio Físico: define las características del medio de transmisión, incluyendo los enlaces por fibra óptica, los niveles de potencia, las tasas de error, los componentes ópticos y los conectores.

SMT, Administración de las Estaciones: define la configuración de las estaciones de FDDI, la configuración del anillo y las características de control del anillo, incluyendo la inserción y eliminación de la estación, inicialización, aislamiento y recuperación de fallas, la programación y recopilación de estadísticas.



Especificaciones de FDDI

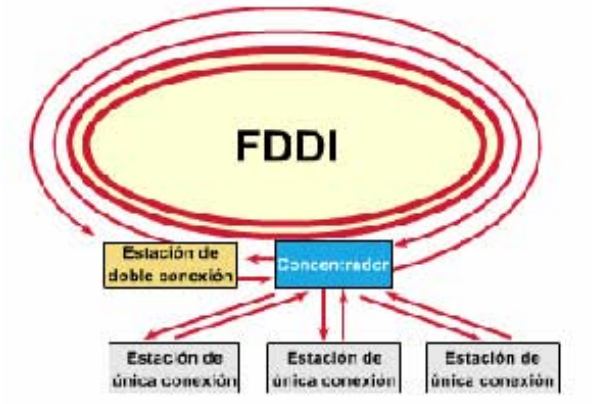
Dispositivos FDDI

El estándar FDDI define tres tipos de dispositivos:

SAS, Estaciones De Una Conexión: éstas se conectan solamente al anillo principal por medio de un concentrador, por lo tanto, los equipos no afectan de ninguna forma al anillo.

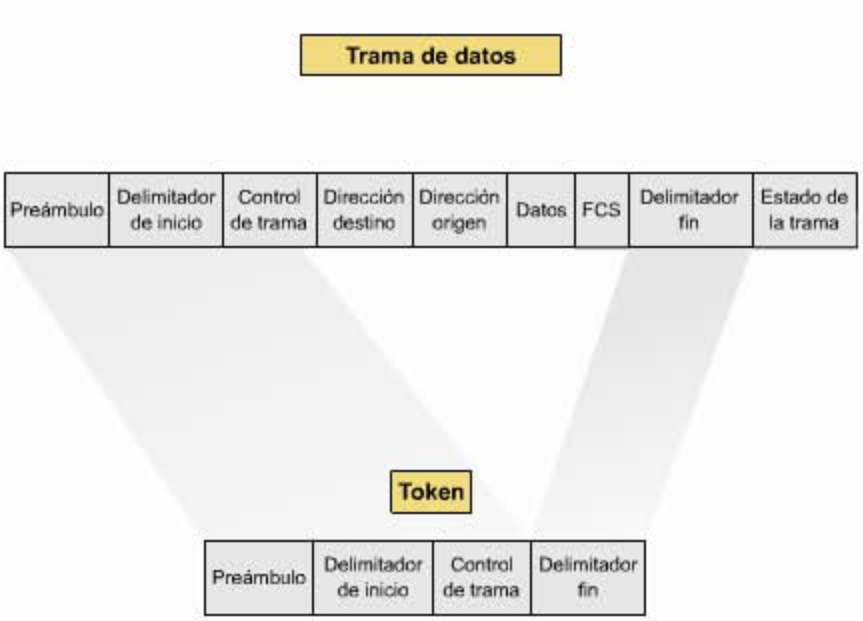
DAS, Estaciones De Doble Conexión: éstas constan de dos puertos con los cuales se conectan a los dos anillos, sin embargo, sí los DAS se desconectan o apagan afectarán al anillo.

DAC, Concentrador De Doble Conexión: es el bloque principal de una red FDDI. Se conecta directamente a ambos anillos y asegura que, sí cualquier SAS se encuentra en falla o apagado no se afectará al anillo.



Dispositivos de FDDI

Formato De La Trama FDDI



Preámbulo: Es una secuencia única que prepara a cada estación para recibir la trama entrante, sincroniza la trama con el reloj de cada estación.

Delimitador De Inicio: El delimitador de inicio indica el comienzo de la trama con un patrón de bits único que puede ser identificado por el nodo FDDI a cualquier hora en el flujo de recepción de datos.

Control De La Trama: Indica la clase de servicio, la longitud del campo de dirección y el tipo de trama.

Direccion De Destino: Especifica la dirección de la estación o estaciones a la cual esta dirigida la trama. El campo DA puede contener la dirección de una única estación (unicast), de un grupo de estaciones (multicast) o de todas las estaciones (broadcast).
Dirección Origen: Especifica la dirección de la estación que envía la trama.

Datos: El campo de datos es usado para transmitir la carga de información por la trama.

Secuencia De Verificación De Trama (Fcs): FDDI usa un chequeo de redundancia cíclica de 32 bits para asegurar que el contenido de la trama esta libre de errores. El CRC es el mismo que se usa en Ethernet, Token Ring y otros protocolos IEEE 802.

Delimitador Final: Contiene símbolos que marca el final de la trama.

Estado De La Trama: Permite que la estación de origen determine si se ha presentado un error y si la trama fue confirmada y copiada por una estación receptora.

Copper Distributed Data Interface, CDDI

La CDDI, Interface de Datos Distribuidos por Cobre, es la Implementación de los protocolos de FDDI a través de par trenzado de cobre. Utiliza una tasa de transferencia de 100 Mbps y una arquitectura de

anillo doble para dar redundancia, soporta una distancia de 100metros desde la máquina al concentrador.

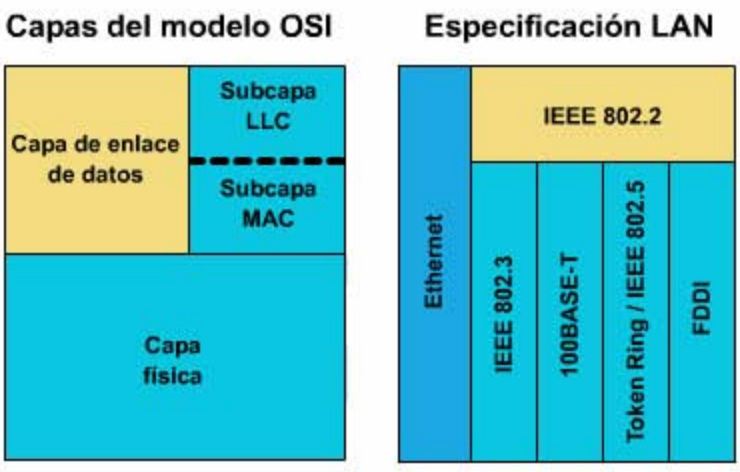
La tecnología CDDI está definida por el ANSI X3T9.5. El nombre oficial del estándar es TP-PDM, Dependiente del Medio Físico por Par Trenzado.

ETHERNET

La arquitectura de red Ethernet tiene su origen en la década de los '60 en la Universidad de Hawai, donde se desarrolló el método de acceso utilizado por Ethernet, es decir, el CSM/CD (acceso múltiple con detección de portadora y detección de colisiones). El centro de investigaciones PARC (Palo Alto Research Center) de Xerox Corporation desarrolló el primer sistema Ethernet experimental a principios de los años 70's. Este sistema sirvió como base de la especificación 802.3 publicada en 1980 por el Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronic Engineers (IEEE).

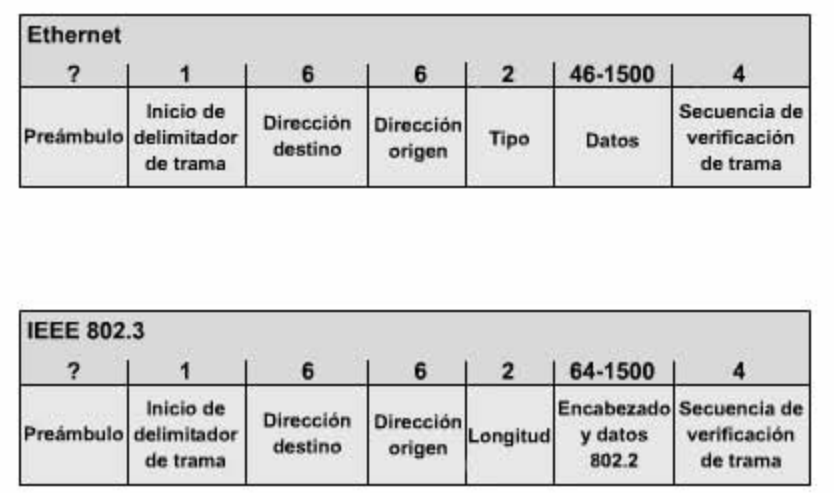
Poco después de la publicación de la especificación IEEE 802.3 en 1980, Digital Equipment Corporation, Intel Corporation y Xerox Corporation desarrollaron y publicaron conjuntamente una especificación Ethernet denominada "Versión 2.0" que era sustancialmente compatible con la IEEE 802.3.

Similitudes y Diferencias entre las capas 1 y 2 del Modelo OSI



Ethernet proporciona servicios que corresponden a las Capas 1 y 2 del modelo de referencia OSI.
IEEE 802.3 especifica la capa física, la Capa 1 y la porción de acceso al canal de la capa de enlace de datos, la Capa 2, pero no define un protocolo de Control de Enlace Lógico.
Tanto Ethernet como IEEE 802.3 se implementan a través del hardware.

Formato de las Tramas



Ethernet						
?	1	6	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección destino	Dirección origen	Tipo	Datos	Secuencia de verificación de trama

IEEE 802.3						
?	1	6	6	2	64-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección destino	Dirección origen	Longitud	Encabezado y datos 802.2	Secuencia de verificación de trama

Preámbulo: Es un patrón alternado de unos y ceros que informa a las estaciones de recepción que una trama está por llegar. La trama Ethernet incluye un byte adicional que es equivalente al campo de inicio de trama (SOF) de la trama IEEE 802.3

SOF (Start Of Frame): Es un byte delimitador en IEEE 802.3 que termina con dos bits 1 consecutivos, que sirven para sincronizar la recepción de las tramas de todas las estaciones de la LAN.

Direcciones de Destino y Origen: Son las direcciones MAC de la tarjeta de red. 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): Éste parámetro específica el protocolo de la capa superior que recibe los datos al terminar el proceso Ethernet.

Longitud (IEEE 802.3): Indica la cantidad de bytes de datos del siguiente campo.

Datos (Ethernet): Éste campo tiene una longitud mínima de 46 bytes de datos.

Datos (IEEE 802.3): La trama tiene un tamaño mínimo de 64 bytes, si los datos que contiene no son suficientes para llenarla al mínimo se insertan bytes de relleno para asegurar que la longitud de la trama sea al menos de 64 bytes.

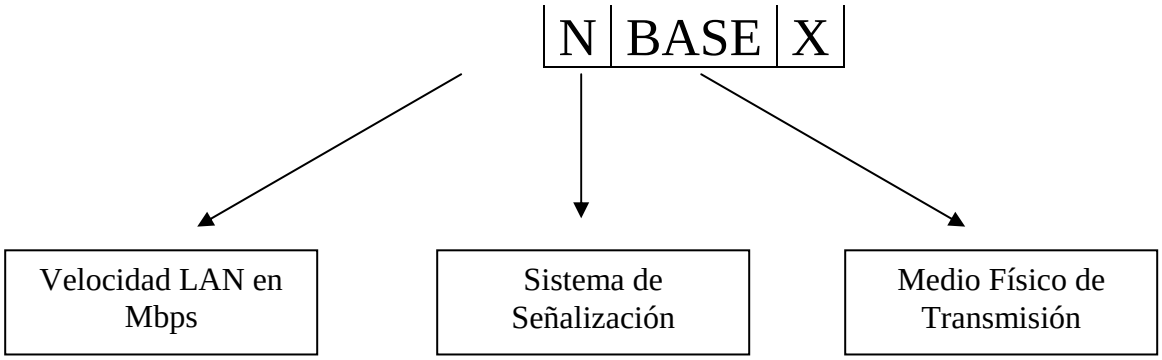
FCS (Frame Check Sequence): Esta secuencia contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

El Protocolo CSMA / CD (Carrier Sense Multiple Access / Collision Detection)

El mecanismo de acceso al medio utilizado por Ethernet se denomina Portadora Sensible a Acceso Múltiple con Detección de Colisiones (CSMA/CD), estandarizado por la IEEE en la recomendación 802.3.

Cada estación que desea transmitir deben comprobar que el medio de transmisión esta libre, sí está ocupado deben esperar a que se libere para realizar su transmisión y evitar las colisiones.

Nomenclatura IEEE 802.3



Tipos de ETHERNET (802.3)

Tipo	Medio	Ancho de banda máximo	Longitud de segmento máxima	Topología física	Topología lógica
10BASE5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10BASE-T	UTP CAT 5	10 Mbps	100 m	Estrella; Estrella extendida	Bus
10BASE-FL	Fibra óptica multimodo	10 Mbps	2000 m	Estrella	Bus
100BASE-TX	UTP CAT 5	100 Mbps	100 m	Estrella	Bus
100BASE-FX	Fibra óptica multimodo	100 Mbps	2000 m	Estrella	Bus
1000BASE-T	UTP CAT 5	1000 Mbps	100 m	Estrella	Bus

Capitulo 4

Tecnologías de Transporte

Términos WAN

CPE (Customer Premises Equipment): Es el equipo propiedad del cliente o subscriptor y ubicado en el edificio o site del mismo.

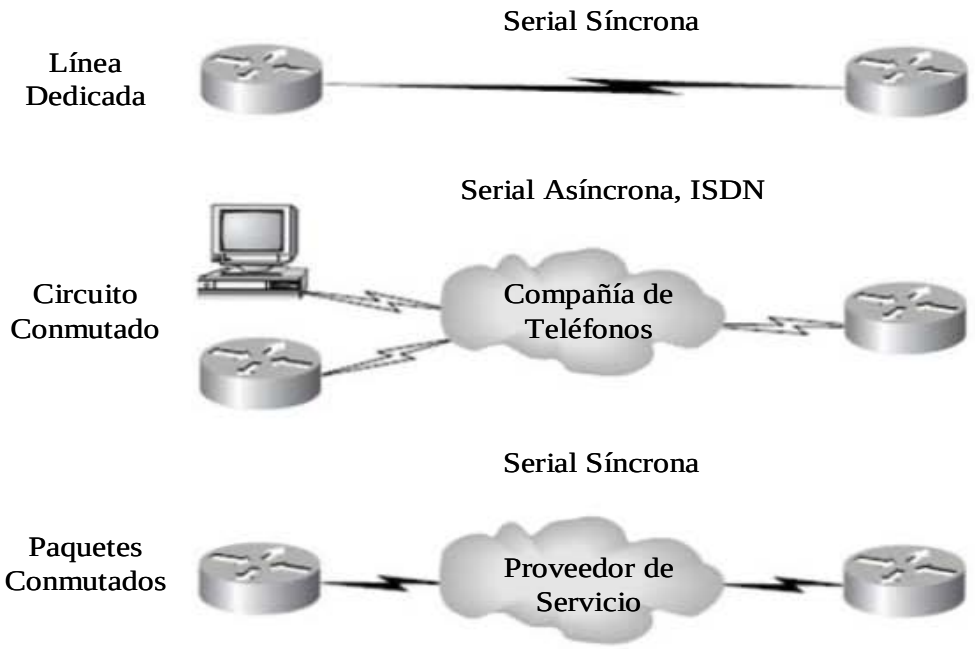
Punto de Demarcación: Es el lugar donde la responsabilidad del proveedor de servicios termina y el CPE comienza. Es generalmente un dispositivo (en el cuarto de telecomunicaciones) propiedad e instalado por la compañía de telecomunicaciones. El cliente es responsable de cablear (demarcación extendida) desde esta caja al CPE, el cual es usualmente una conexión a un CSU/DSU o interfase ISDN

Loop Local (Última Milla): El Loop Local ó última milla conecta la demarcación a la oficina de conmutación más cercana, llamada Oficina Central.

CO (Central Office): Este punto conecta a los clientes a la red de conmutación del proveedor. Una Oficina Central (CO) es a veces llamada como punto de Presencia (Point of presence, POP).

Toll Network: Es una línea troncal dentro de la red del proveedor WAN. Esta red es una colección de switches e instalaciones propiedad del ISP (Internet Service Provider).

Tipos de Conexión WAN



Líneas Dedicadas: Estas son referidas como una conexión punto a punto. Una línea dedicada es una ruta de comunicación WAN pre-establecida desde el CPE a través del switch DCE al CPE del sitio remoto, permitiendo a las redes DTE comunicarse a cualquier hora sin requerir alguna solicitud para poder enviar información. Usan líneas seriales síncronas hasta 45 Mbps. Las encapsulaciones HDLC y PPP son frecuentemente usadas en líneas dedicadas.

Circuitos Conmutados: Se paga únicamente el tiempo que se usa. Ninguna información puede transmitirse antes de que una conexión end-to-end se haya establecido. Los circuitos conmutados usan modems dial-up o ISDN y es usada para transferir información en bajo ancho de banda.

Paquetes Conmutados: Este es un método de conmutación WAN que permite compartir ancho de banda con otras compañías para ahorrar dinero. Frame Relay y X.25 son tecnologías de paquetes conmutados. Ofrece tasas de transmisión desde 56 Kbps hasta 45 Mbps.

Transmisión Serial

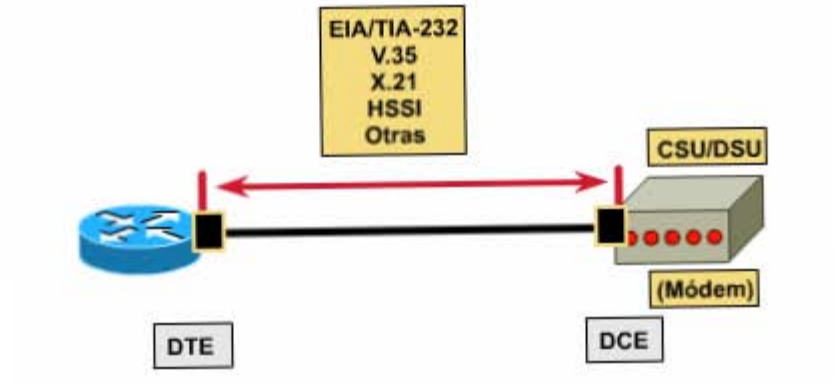
Los conectores seriales WAN usan la transmisión serial, la cual toma lugar un bit en un tiempo sobre un canal. Las transmisiones en paralelo pueden pasar por lo menos 8 al mismo tiempo, pero todas las WANs usan transmisión serial.

Los routers Cisco usan un conector serial de 60 pines propietario, también usan una conexión serial pequeña propietaria que es 1:10 el tamaño del cable serial básico de 60 pines. Este es llamado smart-serial. El tipo de conector que se tiene en el otro extremo del cable depende del proveedor de servicio o de los requerimientos del dispositivo Terminal.

Las diferentes conexiones disponibles son:

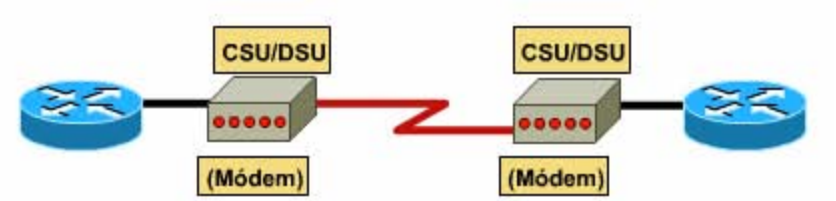
- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35
- X.21
- G.703
- EIA-530

Los enlaces seriales son descritos en frecuencia o ciclos por segundo (hertz). La cantidad de información que puede ser transportada dentro de estas frecuencias es llamada ancho de banda. El ancho de banda es la cantidad de información en bits por segundo que un canal serial puede transportar.



Equipo DTE (Data Terminal Equipment) y DCE (Data Terminal Equipment)

Las interfases del router son por default Data Terminal Equipment (DTE), y ellas se conectan con los Data Communication Equipment (DCE), por ejemplo a un CSU/DSU (Unidad de Servicio de Canal / Unidad de Servicio de Información; Channel Service Unit / Data Service Unit).
El CSU/DSU se conecta en el punto de demarcación y es la última responsabilidad del proveedor de servicio.



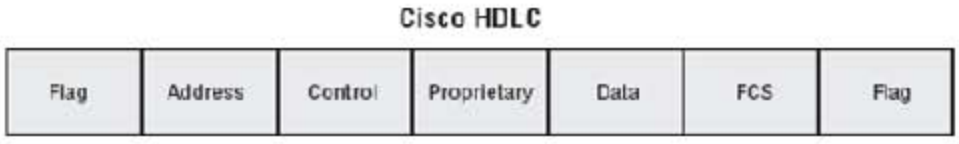
El dispositivo DCE (CSU/DSU) de la red provee el reloj a la interfase DTE conectada (interfase serial del router).

Protocolo High-Level Data-Link Control (HDLC)

El protocolo HDLC es un protocolo estándar de la capa de enlace de datos orientado a bits, derivado de SDLC (Synchronous Data Link Control) y desarrollado por ISO, ha sido implementado de diferentes formas por cada fabricante. HDLC especifica un método de encapsulación para la información sobre enlaces de datos seriales síncronos usando caracteres de trama y corrección de errores. HDLC es un protocolo punto a punto usado en líneas dedicadas.

En los protocolos orientados en bytes, el control de la información es codificada usando el byte entero. Los protocolos orientados a bit pueden usar simples bits para representar el control de la información. En los protocolos orientados a bit se incluyen SDLC, LLC, HDLC, TCP, IP entre otros.

HDLC es la encapsulación por default usada en los routers Cisco sobre enlaces seriales síncronos. El HDLC de Cisco es propietario por lo que no se comunicará con otra implementación de HDLC de otro fabricante.



Cada Fabricante en HDLC tiene su propio campo de información de propiedad para soportar entornos multiprotocolos.

Soporta únicamente entornos de un simple protocolo.

Frame Relay

Frame Relay fue originalmente diseñado para usarse en interfases de Redes Digitales de Servicios Integrados (RDSI o por sus siglas en ingles ISDN).

Frame Relay es una tecnología de conmutación de paquetes. Las redes de conmutación de paquetes habilita estaciones terminales para dinámicamente compartir el medio de Tx y el ancho de banda. Los paquetes de longitud variable son usados para transferencias más eficientes y flexibles. Cada paquete viaja a través de una serie de switches en una red Frame Relay para alcanzar su destino. Opera en la capa física y de enlace de datos del modelo de referencia OSI, pero depende de los protocolos de capa superior como TCP para la corrección de errores.

Frame Relay utiliza circuitos virtuales para realizar conexiones a través de un servicio orientado a conexión.

Circuitos Virtuales

Frame Relay es una red de conmutación de paquetes que utiliza circuitos virtuales.
Una conexión física entre un DTE y un DCE puede transportar varios circuitos virtuales en el nivel de red, siendo cada circuito responsable de información de datos o de control.

Existen dos tipos de circuitos virtuales: los Circuitos Virtuales Permanentes (PVC) y Circuitos Virtuales Conmutados (SVC).

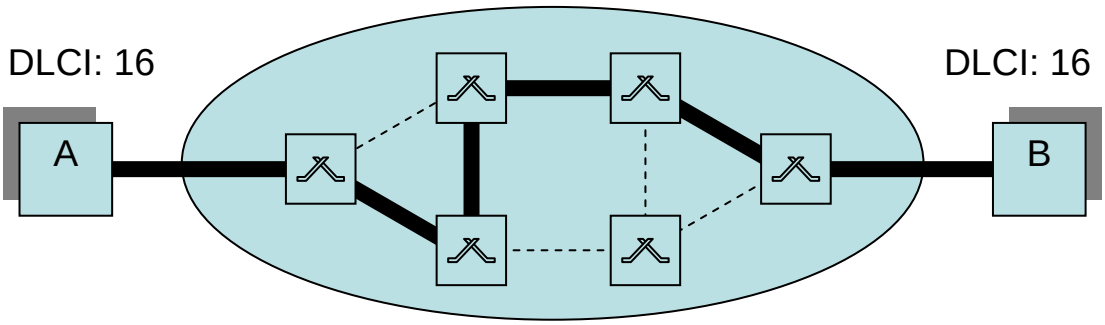
SVC, Switching Virtual Circuit (Circuito Virtual Conmutado): Son conexiones temporales que se utilizan para conectar dos equipos terminales que van a transferir datos de forma no continua. Cada vez que se requiera la transferencia de datos se crea un nuevo circuito virtual. El proceso de creación de un Circuito Vitual Conmutado, consta de los siguientes pasos:

- Establecimiento.
- Conexión.
- Transferencia.
- Liberación.

PVC, Permanent Virtual Circuit (Circuito Virtual Permanente): Son conexiones permanentes entre dos equipos terminales, se utilizan en transferencias de datos frecuentes y constantes a través de la red Frame Relay.
Los PVCs, siempre operan en alguno de los siguientes estados:

- Transferencia de Datos
- Ocioso

A diferencia de un SVC, el PVC no requiere hacer el establecimiento y finalización del circuito cada vez que se quiera transmitir.
Los DLCI son permanentes y son asignados por el proveedor de la red de Frame Relay.

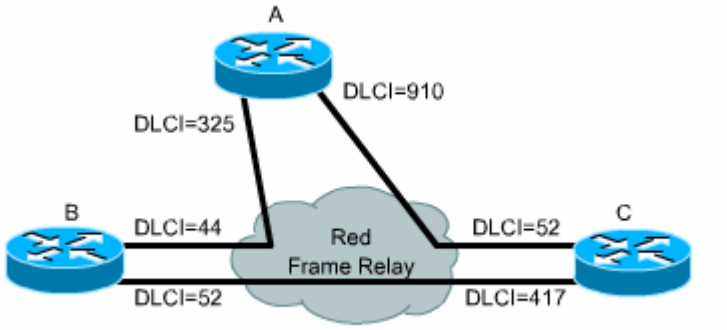


Establecimiento de un Circuito Virtual

DLCI, Data Link Connection Identifier

Los PVC de Frame Relay son identificados por los DLCI. Los DLCI de Frame Relay solo tienen importancia local, es decir, los DLCI se pueden repetir en otro switch Frame Relay. Dos dispositivos DTE conectados por un circuito virtual pueden utilizar un valor DLCI distinto para referirse a la misma conexión.

Frame Relay 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.



Control de Tráfico

Las estrategias de congestión requieren que Frame Relay realice medidas del control de tráfico para determinar cuándo deberán activarse los bits BECN, FECN y DE, así como cuándo debe descartarse una trama.
Existen varios parámetros para controlar el tráfico, estos son:

1. Tasa de Información Comprometida (CIR).
2. Intervalo de Medición de la Tasa Comprometida (Tc).

3. Tamaño comprometido de ráfaga (Bc).
4. Tamaño de ráfaga en exceso (Be).

CIR, Committed Information Rate (Tasa de Información Comprometida): Se define como la tasa de información media o promedio que se va a transmitir medida en bits por segundo y que la red está dispuesta a soportar en condiciones normales de operación.

Tc, Intervalo de Medición de la Tasa Comprometida: Se refiere al intervalo de tiempo sobre el que se miden las tasas de transferencia de información. El valor de Tc no es configurado directamente en los routers, es calculado después de que los valores de Bc y el CIR son configurados.

Bc, Committed Burst Size (Tamaño Comprometido de la Ráfaga): Es el número máximo de bits que la red garantiza entregar durante el intervalo de tiempo Tc, bajo circunstancias normales.

$$Tc = \frac{Bc}{CIR}$$

Be, Excess Bursa Size (Tamaño de la Ráfaga en Exceso): Es el número máximo de bits sobre el CIR que la red intentará entregar durante un Tc.

Todas las tramas que sean transmitidas a una tasa superior al CIR, se marcan como tramas elegibles para descarte en la red.

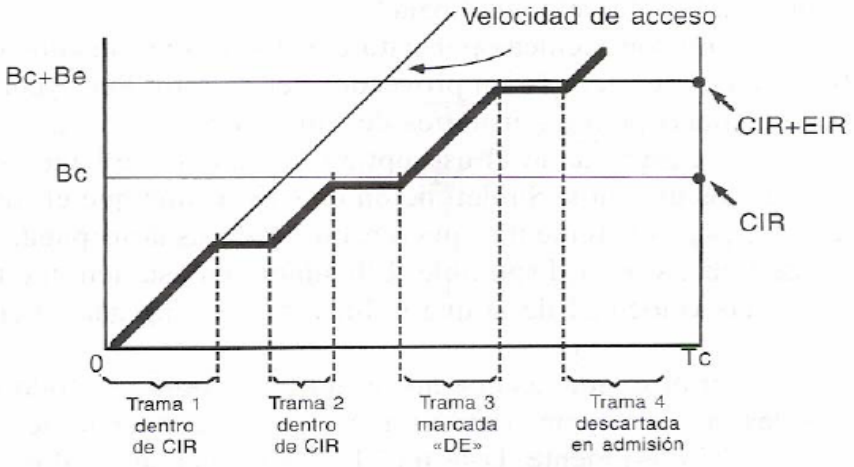
El tamaño del exceso de ráfaga, medido en bits por segundo, se denomina EIR (Excess Information Rate), el cual se calcula de la siguiente forma:

$$EIR = \frac{Be}{Tc}$$

La tasa máxima de información transmitida es:

$$CIR + EIR = \frac{(Bc + Be)}{Tc}$$

Cuando la tasa máxima es excedida, las tramas inmediatamente son descartadas.



Congestión en Frame Relay

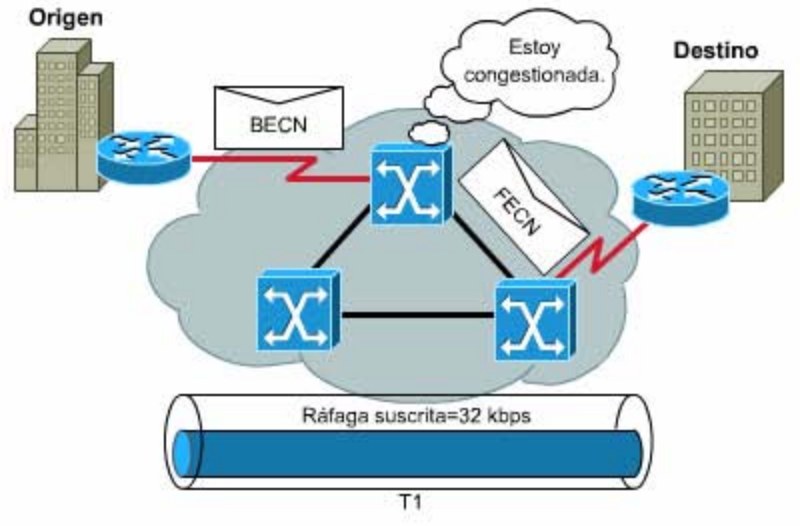
Cuando se empiezan a descartar tramas y se solicita retransmisión, se dice que la red se encuentra en estado de Congestión, para lo cual, Frame Relay implementa dos mecanismos de notificación de congestión:

- Forward Explicit Congestion Notification (FECN).
- Backward Explicit Congestion Notification (BECN).

Notificación explícita de la congestión (FECN): Bit establecido en una trama que notifica a un DTE que el dispositivo receptor debe iniciar procedimientos para evitar la congestión. Cuando un switch Frame Relay detecta la existencia de congestión en la red, envía un paquete FECN al dispositivo destino, indicando que se ha producido la congestión.

Notificación de la congestión retrospectiva (BECN): Bit establecido en una trama que notifica a un DTE que el dispositivo receptor debe iniciar procedimientos para evitar la congestión. Cuando un switch Frame Relay detecta congestión en la red, envía un paquete BECN al router origen, instruyendo al router para que reduzca la velocidad a la cual está enviando los paquetes, si el router recibe cualquier BECN durante el intervalo de tiempo actual, reduce la velocidad de transmisión un 25%.

Indicador de posible para descarte (DE): Bit establecido que indica que la trama se puede descartar para darle prioridad a otras tramas si se produce congestión. Cuando el router detecta congestión de red, el switch Frame Relay descarta en primer lugar los paquetes con el bit DE. El bit DE se establece en el tráfico sobresuscrito (es decir, el tráfico recibido después de alcanzar el CIR).



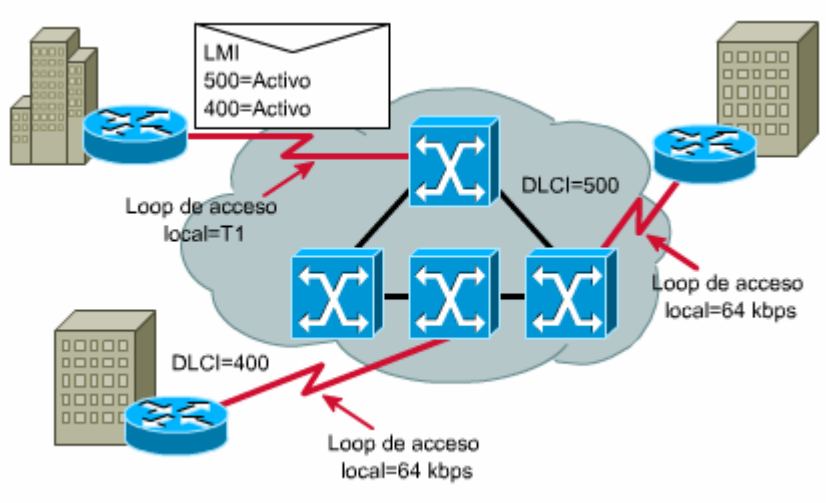
LMI, Local Management Interface (Interfaz de Administración Local)

Estándar de señalización entre el equipo terminal del abonado (CPE) y el switch Frame Relay a cargo del manejo de las conexiones y mantenimiento del estado entre los dispositivos. Las LMIs pueden incluir soporte para un mecanismo de mensajes de actividad, que verifica que los datos fluyan; un

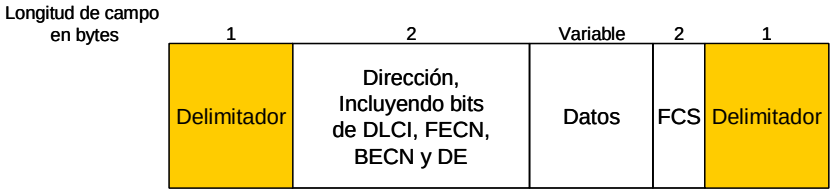
mecanismo de multicast, que puede proporcionar al servidor de red su DLCI local; direccionamiento de multicast, que permite utilizar algunos DLCI como direcciones de multicast (destinos múltiples) y la capacidad para otorgar a los DLCI significado global (toda la red Frame Relay), en lugar de simplemente significado local (los DLCI se utilizan solamente para el switch local); y un mecanismo de estado que indica el estado de los DLCI que el switch conoce.
Existen varios tipos de LMI y esta señalización debe de ser igual tanto en el router como en el switch Frame Relay. Se manejan tres tipos de LMI: cisco, ansi y q933a.

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.



Trama de Frame Relay



Delimitador: Indica el principio y el final de la trama Frame Relay.

Dirección: Indica la longitud del campo de dirección, aunque las direcciones Frame Relay 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 Frame Relay. 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.

ATM, ASynchronous Transfer Mode (Modo de Transferencia Asíncrona)

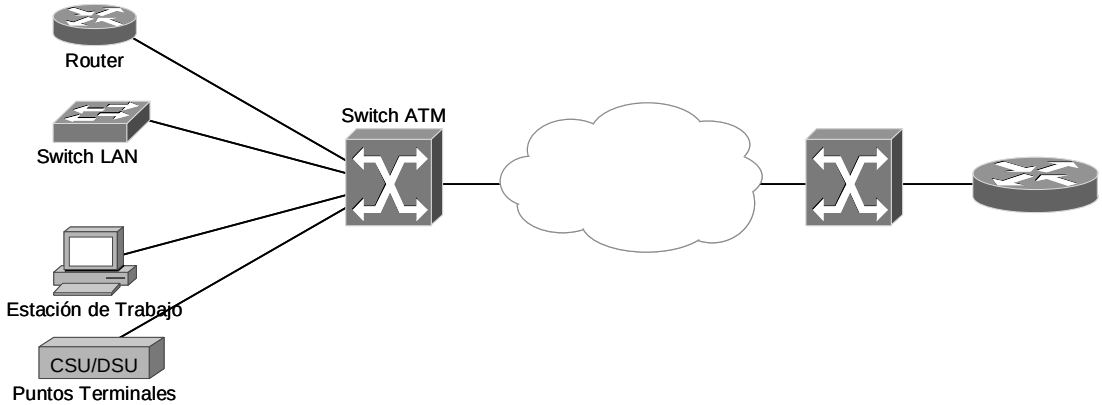
ATM es una tecnología de conmutación de celdas y multiplexaje que reúne los beneficios de la conmutación de circuitos con los de conmutación de paquetes. Proporciona un ancho de banda expandible desde algunos megabits por segundo hasta muchos gigabits por segundo. Debido a su naturaleza asíncrona, ATM es más eficiente que las tecnologías síncronas.

Dispositivos e interfaces ATM

Una red ATM está formada por un switch ATM y puntos terminales de ATM.

Un switch ATM es responsable del transporte de celdas a través de una red ATM. El proceso es el siguiente: El switch ATM acepta la celda entrante de un punto terminal de ATM u otro switch, a continuación, lee y actualiza la información contenida en la cabecera de la celda y rápidamente, conmuta la celda a una interfase de salida para enviarla a su destino.
Un punto terminal de ATM (o sistema terminal) contiene un adaptador de interfase de red ATM, tales como, estaciones de trabajo, ruteadores o switches LAN.

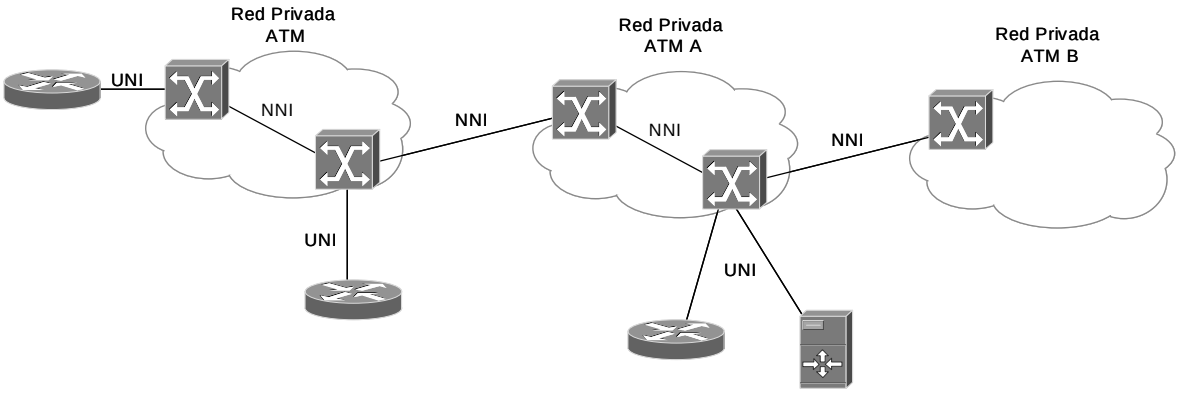
Dispositivos de La Red ATM



Interfases de red ATM

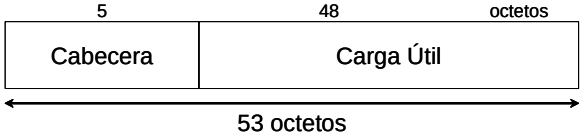
Una red ATM consta de un conjunto de switches ATM interconectados a través de enlaces o interfases punto a punto de ATM. Los switches ATM soportan dos tipos principales de interfases:

- UNI, User Network Interface (Interfase de Red del Usuario): La UNI conecta los sistemas terminales hacia un switch ATM
- NNI, Network Node Interface (Interfase de Nodo de Red): La NNI conecta dos switches ATM.



Celda ATM y su Cabecera

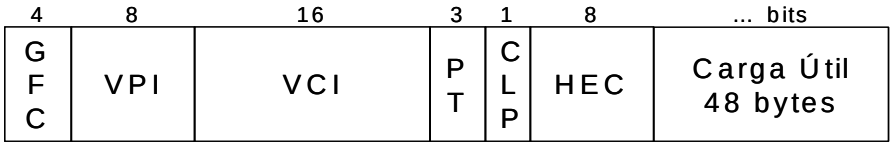
La unidad de datos básica en una red ATM se denomina celda, la cual es de tamaño fijo. Cada celda consta de 53 octetos. Los primeros 5 octetos contienen información de la cabecera de la celda, los restantes 48 octetos contienen la información del usuario denominada “carga útil”. Las celdas pequeñas de tamaño fijo son muy adecuadas para la transferencia de tráfico de voz y video, ya que dicho tráfico no tolera retardos que surgen por esperar a que un paquete grande de datos descargue su información.



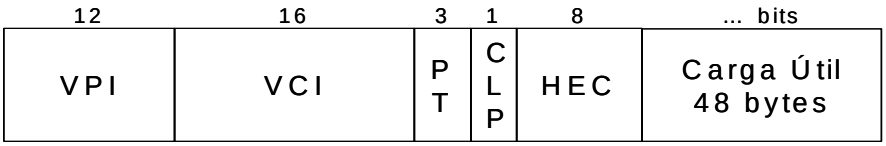
Campos de La Cabecera

Como se había mencionado antes, la cabecera de la celda ATM tiene dos posibles formatos: UNI o NNI.

Cabecera UNI



Cabecera NNI



La cabecera UNI consta de seis campos y la cabecera NNI consta de 5 campos ya que no contiene el campo GFC de la UNI, los campos son:

GFC, Generic Flow Control (Control de Flujo Genérico): Proporciona funciones locales como la identificación de múltiples estaciones que comparten una sola interfase de ATM.

VPI, Virtual Path Identifier (Identificador de Trayectoria Virtual): En conjunto con el VCI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en camino hacia su destino.

VCI, Virtual Channel Identifier (Identificador del Canal Virtual): Junto con el VPI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en ruta a su destino.

PT, Payload Type (Tipo de Carga Útil): Indica en el primer bit si la celda contiene datos del usuario o datos de control. Si la celda contiene datos del usuario, el segundo bit indica si hay saturación y el tercer bit indica si la celda es la última de una serie de celdas que representan una sola trama AAL5

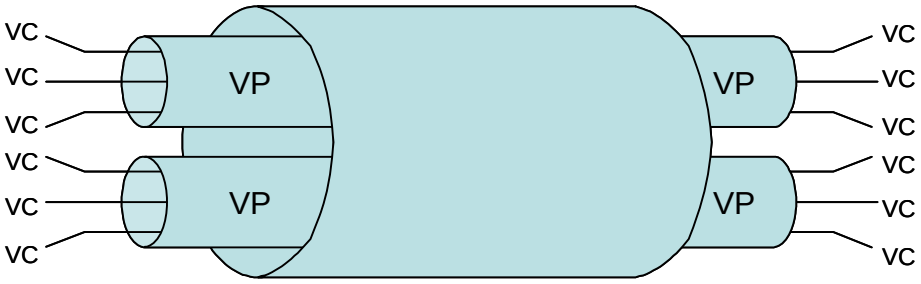
CLP, Cell Loss Priority (Prioridad de Pérdida de Celda): Indica si la celda se debe eliminar al encontrar un alto grado de saturación a su paso por la red. Si el bit CLP es igual a 1, la celda se deberá eliminar para dar preferencia a las celdas cuyo bit CLP sea igual a cero.

HEC, Header Error Check (Control de Errores de Cabecera): Este campo calcula la suma de verificación sólo en la cabecera misma.

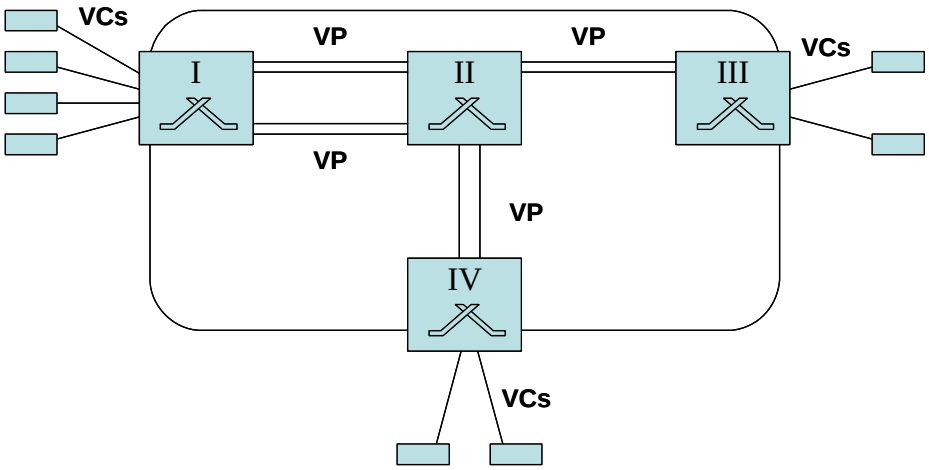
Conexiones Virtuales De ATM

ATM proporciona un servicio de transporte de celdas orientado a la conexión, esto significa que se debe establecer un VC (Canal Virtual) a través de la red ATM antes de cualquier transferencia de datos. Hay dos tipos de conexiones:

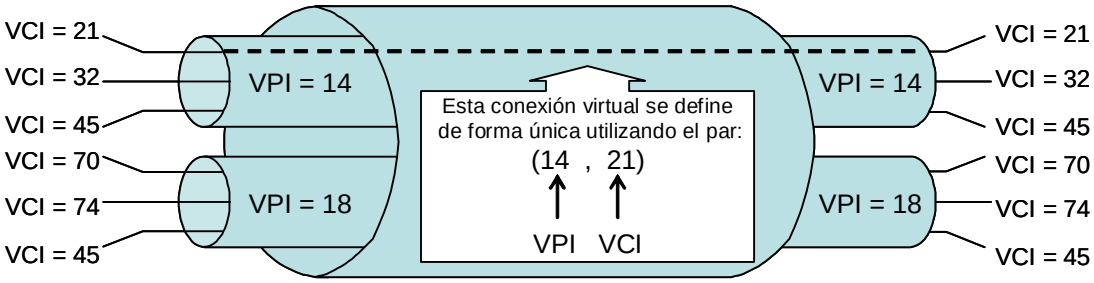
- Trayectorias Virtuales, que se identifican por medio del identificador de trayectoria virtual VPI.
- Canales Virtuales, los cuales se identifican por la combinación de un VPI y un VCI.



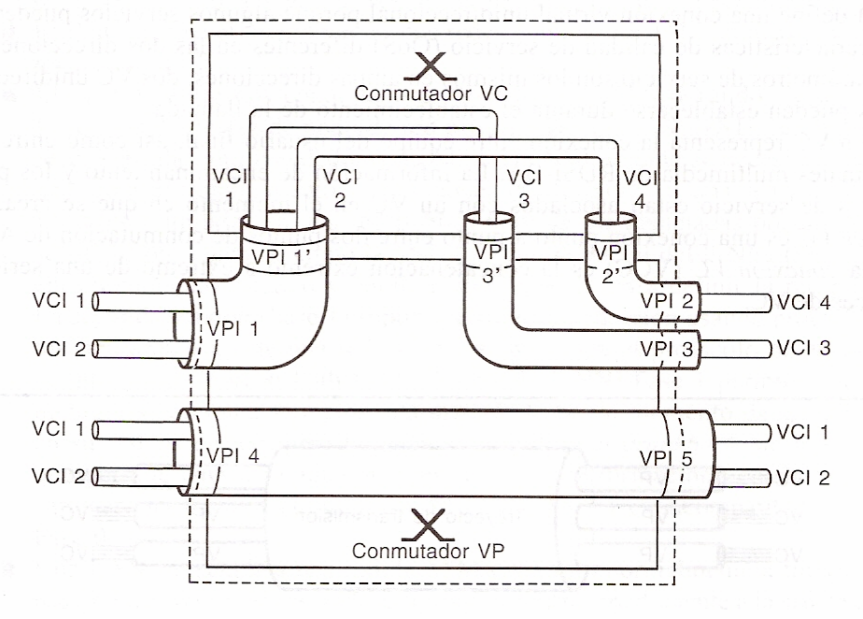
Ejemplo de Conexiones Vp y Vc



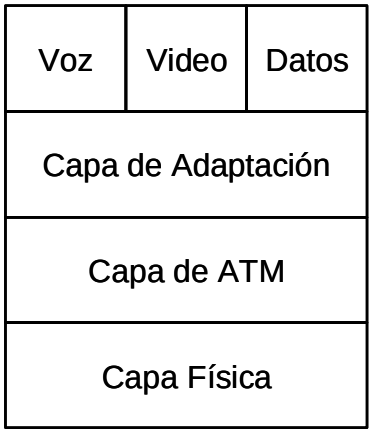
Identificadores de Conexión



Conmutación de Vp y Vc



Modelo De Referencia ATM



La arquitectura de ATM consiste de la capa física, la capa de ATM, la capa de adaptación de ATM y de las capas superiores que permiten que varias aplicaciones corran arriba de ATM. La capa de ATM y la capa de adaptación de ATM no corresponden a alguna de las capas del modelo de referencia OSI por lo que es erróneo referirse a la capa de ATM como la capa de enlace de datos.

Capa Física

La capa física de ATM es responsable del transporte de celdas entre equipos de ATM adyacentes, que puede incluir dispositivos de usuario final, conmutadores ATM privados o de la red pública, esta capa tiene cuatro funciones:

- Convertir los bits en celdas.
- Controlar la transmisión y recepción de bits en el medio físico.
- Supervisar los límites de las celdas de ATM.
- Empaquetar las celdas en un tipo de trama adecuado para enviarlas a través del medio físico.

Capa ATM

La capa ATM es responsable de la preparación de la cabecera de la celda ATM. Recibe la información de los subniveles AAL y le agrega los 5 bytes de la cabecera para conformar la celda de 53 bytes.
La capa ATM proporciona una plataforma de procedimientos comunes para la conmutación de las celdas, siendo responsable del transporte de celdas de nodo a nodo por la red de ATM y proporciona un servicio de conmutación de celdas orientado a la conexión.

Calidad de Servicio (Quality of Service, QoS)

Cada conexión de ATM está asociada con una categoría de QoS. Hay seis categorías diferentes que son provistas por la capa de ATM.

CBR, (Constant Bit Rate, Tasa de Bits Constante): Esta diseñada para usarse en aplicaciones de tiempo real que transmiten a una tasa de bits constante.

VBR, (Variable Bit Rate, Tasa de Bits Variable): Esta diseñada para aplicaciones que transmiten a una tasa variable de bits; Se divide en dos subclases:

- RT-VBR, (Real-Time VBR, Tasa de Bits Variable en Tiempo Real): Esta diseñada para aplicaciones en tiempo real que transmiten a una tasa variable de bits tales como video codificado y voz.
- NRT-VBR, (Non-Real-Time VBR, Tasa de Bits Variable No en Tiempo Real): Esta diseñada para aplicaciones sensitivas al retraso que transmiten a una tasa variable de bits pero que no tiende a utilizarse en tiempo real.

ABR, (Available Bit Rate, Tasa de Bits Disponible): Entrega las celdas a la misma velocidad. Si hay más capacidad en la red, la velocidad mínima puede incrementarse.

UBR, (Unspecified Bit Rate, Tasa de Bits No Especificada): Esta diseñada para aplicaciones que son tolerantes al retraso por lo que es un servicio de mejor entrega posible que no garantiza nada.

GFR, (Guaranteed Frame Rate, Tasa de Trama Garantizada): Esta diseñada para soportar aplicaciones no en tiempo real que solo requieren garantizar una tasa mínima de bits.

AAL, ATM Adaptation Layer (Capa de Adaptación de ATM)

La capa de adaptación de ATM (AAL) está situada entre la capa de ATM y las capas superiores. AAL convierte el tráfico generado por las capas superiores a carga útil de ATM y provee diferentes tipos de servicios a las capas superiores.

AAL consiste de dos subcapas:

- Subcapa de Convergencia (Converge Sublayer, CS): Este nivel divide el flujo de bits en segmentos de 47 bytes y los pasa a la subcapa SAR inferior.
- Subcapa de Segmentación y Reensamblado (Segmentation And Reassembly sublayer, SAR): Este nivel acepta una carga de 47 bytes y añade una cabecera de un byte, en seguida pasa los 48 bytes a la capa ATM.

Categorías de AAL

AAL1: Se usa para servicios orientados a conexión sensibles a los retrasos que requieren trasmitir información con una tasa de bits constante (CBR), como voz, audio y video.

AAL2: Se usa para servicios orientados a conexión que soportan transferir información con una tasa de bits variable (VBR).

AAL3 Y AAL4: AAL3 se usa para apoyar servicios con tasa de bits variable orientados a conexiones. Estos servicios de datos con ráfagas no requieren mantener relaciones de temporización entre el origen y el destino. AAL4 se usa para apoyar servicios en modo de mensajes o en modo de corriente para sistemas de datos (no voz ni video); también se diseño para apoyar los servicios sin conexiones, aunque la ITU-T también contempla que este tipo proporcione operaciones aseguradas en las que el tráfico perdido pueda retransmitirse. A medida que el estándar de AAL maduró, se hizo evidente que los tipos originales no eran apropiados. Por lo tanto, AAL3 y AAL4 se combinaron por ser muy similares.

AAL5: Denominada Capa de Adaptación Simple y Eficiente (SEAL); Está definida para aplicaciones de cualquier tipo de datos en forma punto a punto, por lo cual no se necesita información de corrección de errores y secuenciamiento, ya que se asume que todas las celdas viajan secuencialmente y el resto de las funciones ya han sido proporcionadas por los niveles superiores.

SONET/SDH

SONET/SDH es una red portadora (de transporte) basada en tecnología óptica que utiliza operaciones síncronas entre los componentes de la red. El término SONET se usa en Norteamérica y SDH se usa en casi todo el resto del mundo.

SONET/SDH es un estándar de red integrado en el que es posible transportar todo tipo de tráfico. El estándar SONET/SDH se basa en la tecnología de fibra óptica que tiene un mejor desempeño en comparación con los sistemas de microondas y cable.

SONET/SDH elimina la sobrecarga de la multiplexión punto a punto empleando técnicas nuevas en el proceso de preparación. Estas técnicas se implementan en un nuevo tipo de equipo llamado multiplexor de agregar/liberar (ADM, Add/Drop multiplexer).

Redes Síncronas

Las primeras redes digitales se diseñaron de modo que operaran como sistemas asíncronos, de manera que cada terminal de la red trabaja con su propio reloj, por lo que no se sincronizan con un punto de referencia central.

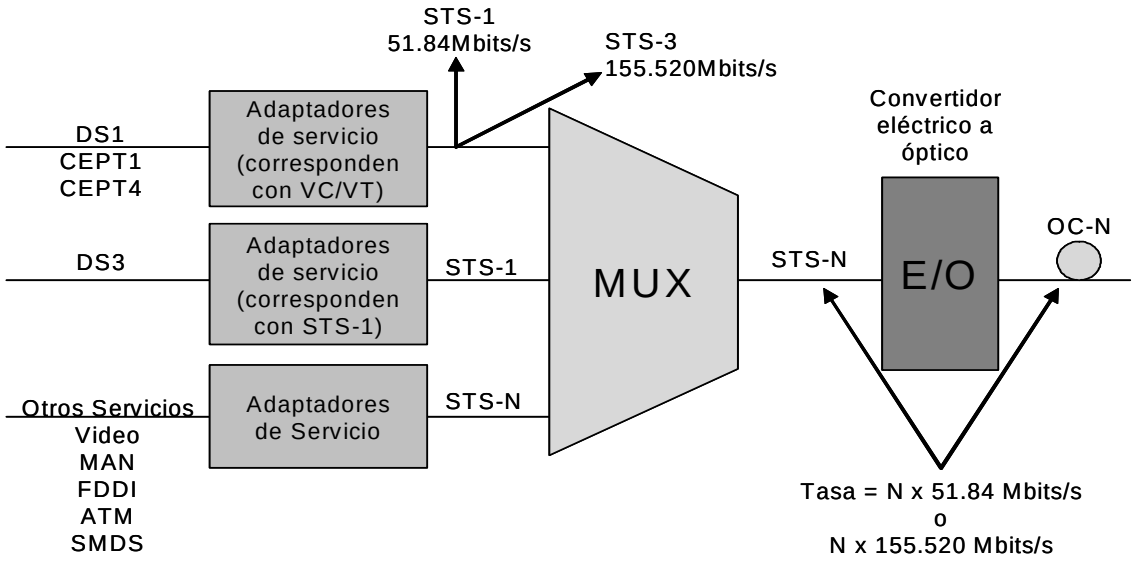
SONET/SDH se basa en transmisión síncrona, lo que implica que la frecuencia promedio de todos los relojes de la red es la misma (síncrona) o casi la misma (plesíncrona). De esta manera, los relojes se remiten a un punto de referencia muy estable y se hace innecesario alinear los flujos de datos o sincronizar los relojes. En las situaciones en las que las frecuencias de referencia podrían variar, SONET/SDH emplea apuntadores para que los flujos puedan flotar dentro del paquete de la carga útil. De hecho, la temporización síncrona es la clave de los apuntadores, debido a que permite asignar y alinear con gran flexibilidad la carga útil dentro del paquete de transmisión.

Estándares

La topología SONET/SDH se basa en estándares desarrollados por el Instituto Nacional Americano de Estándares (ANSI, American Nacional Standard Institute) y la Asociación de Estándares de Portadoras de Intercambio (ECSA, Exchange Carriers Standards Association). Aunque SONET se diseño para dar cabida a la señal DS3 norteamericana (de Mbits/s), la ITU-T utilizó SONET para el desarrollo y publicación de la Jerarquía Digital Síncrona (SDH).

Topología SONET/SDH

Las señales de usuario, sean T1, ATM o E1, se convierten (transforman) a un formato estándar llamado señal de transporte síncrono (STS, Synchronous Transport Signal) que es el bloque de construcción básico de la jerarquía de multiplexión. La STS es una señal eléctrica y la notación STS-n implica que el adaptador de servicio puede multiplexar la STS en múltiplos enteros más altos de la tasa base. La tasa base es de 51.84 Mbits/s en Norteamérica y de 155.52Mbits/s en Europa, para SONET y SDH respectivamente. La tasa base de SDH en Europa es una señal multiplexada STS-3 (51.84 * 3 = 155.520 Mbits/s).



E/O = Convertidor de eléctrico a óptico
OC = Portadora óptica
STS = Señal de Transporte Síncrona
VC = Contenedor Virtual
VT = Tributaria Virtual

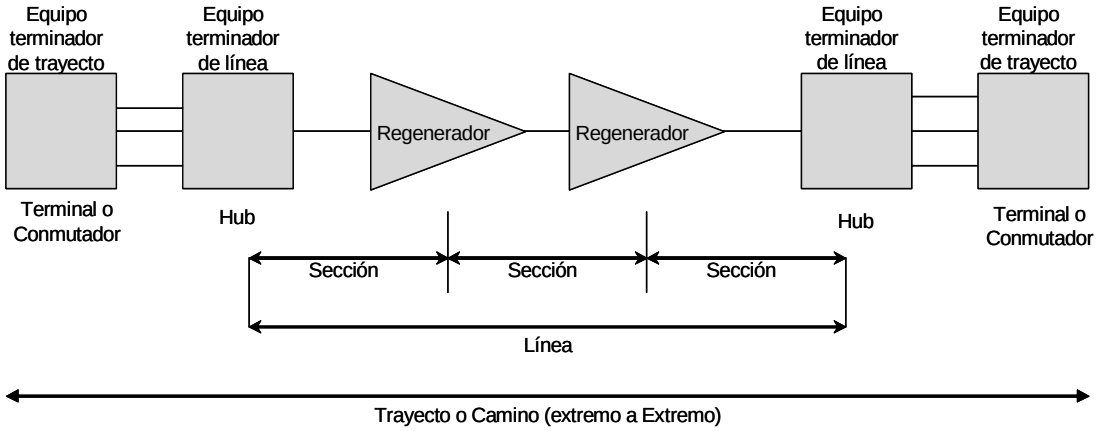
Los adaptadotes de servicio pueden aceptar cualquier señal. El propósito del adaptador de servicio es establecer una correspondencia entre tales señales y paquetes STS-1 o múltiplos de éstas. En Norteamérica, todo el tráfico se convierte inicialmente en una señal STS-1 síncrona a 51.84Mbits/s o más. En Europa, los adaptadores de servicio convierten la carga útil en una señal STS-3 (155.520Mbits/s).

Las señales de más baja velocidad primero se multiplexan en tributarias virtuales (VT, Virtual Tributaries, un término norteamericano) o contenedores virtuales (VC, Virtual Containers, un término europeo), que son cargas útiles más bajas que STS-1. Luego, varias STS-1 se multiplexan para formar una señal STS-n. Estas señales se envían a un convertidor de eléctrico a óptico (E/O) donde se efectúa una conversión a una señal óptica OC-n.

Configuración del Camino

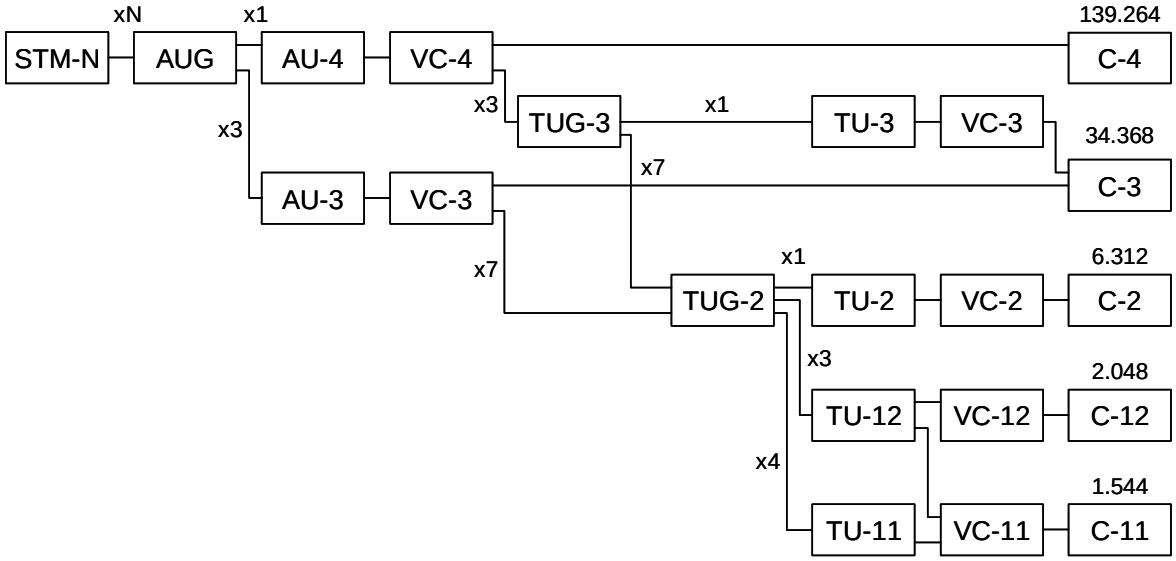
Se emplean tres tipos de equipos en un sistema SONET/SDH:

- Equipo Terminador de Trayecto: Es una terminal o un multiplexor, y se encarga de transformar la carga útil del usuario (DS1, CEPT4, FDDI, etc.) a un formato estandarizado.
- Equipo Terminador de Línea: Es un hub, el cual presta servicios al equipo terminador de trayecto, sobre todo multiplexión, sincronización y conmutación de protección automática.
- Equipo Terminador de Sección: Es un regenerador, que desempeña funciones de alineación de tramas, reempaquetado y monitoreo de errores. Este equipo se encarga de recibir y regenerar las señales.



Estructura de Multiplexión

Esta estructura es muy similar a la SONET de ANSI.



En el nivel más bajo, se introducen contenedores (C) en contenedores virtuales (VC). El propósito de esta función es crear un paquete de carga útil de VC uniforme. La jerarquía SDH cubre diversos contenedores (que van desde los 1.544Mbits/s hasta los 139.264Mbits/s). A continuación los VC se alinean con las unidades tributarias (TU). Esta alineación implica relleno de bits para que todas las entradas tengan la misma tasa de transferencia de bits. Después, los VC se alinean con las TU implementando operaciones de procesamiento de apuntadores.
Estas funciones iniciales permiten multiplexar la carga útil en grupos de TU (TUG). xN indica el entero de multiplexión empleado para multiplexar las TU en los TUG. El siguiente paso es multiplexar los TUG en VC de un nivel más alto, y los TUG-2 y 3 se multiplexan en VC 3 y 4. Estos VC se alinean con relleno de bits para las unidades de administración (AU) que finalmente se multiplexan en el grupo de AU (AUG). Esta carga útil se multiplexa entonces con un entero N par en el módulo de transporte síncrono (STM, Synchronous Transport Module).

Término	Contenido	Uso
C-n	n = 1 a 4	Contiene carga útil en el nivel de multiplexión más bajo
VC-n	n = 1, 2	Contiene un solo C-n más VC POH
VC-n	n = 3, 4	Contiene C-n, TUG-2 o TU-3, más POH para el nivel específico
TU-n	n = 1 a 3	Contiene VC más apuntador a Unidad Tributaria
TUG-2	(TU-n) =1, 3, 4	Contiene diversas TU-n
TUG-3	TU-3, 7 TUG-2s	Contiene TU-3, 7 TUG-2
AU-n	n = 3, 4	Contiene VCs más apuntador a AU
STM-1	n = 1, 3 AUGs	Contiene n señales STM-1 multiplexadas en forma síncrona

POH = Sobrecarga de Trayecto
C = Contenedor
VC = Contenedor Virtual
TU = Unidad Tributaria
TUG = Grupo de Unidad Tributaria
AU = Unidad Administrativa
STM = Módulo de Transporte Síncrono

Relaciones entre Niveles

Estas son las relaciones entre los niveles OC, STS y SDH.

STS (Trama de SONET)	OC (SONET)	Velocidad (Mbps)	STM (SDH)
STS-1	OC-1	51,840	
STS-3	OC-3	155,520	STM-1
STS-9	OC-9	466,560	STM-3
STS-12	OC-12	622,080	STM-4
STS-18	OC-18	933,120	STM-6
STS-24	OC-24	1,244,160	STM-8
STS-36	OC-36	1,866,230	STM-12
STS-48	OC-48	2,488,320	STM-16
STS-96	OC-96	4,976,640	STM-32
STS-192	OC-192	9,953,280	STM-64

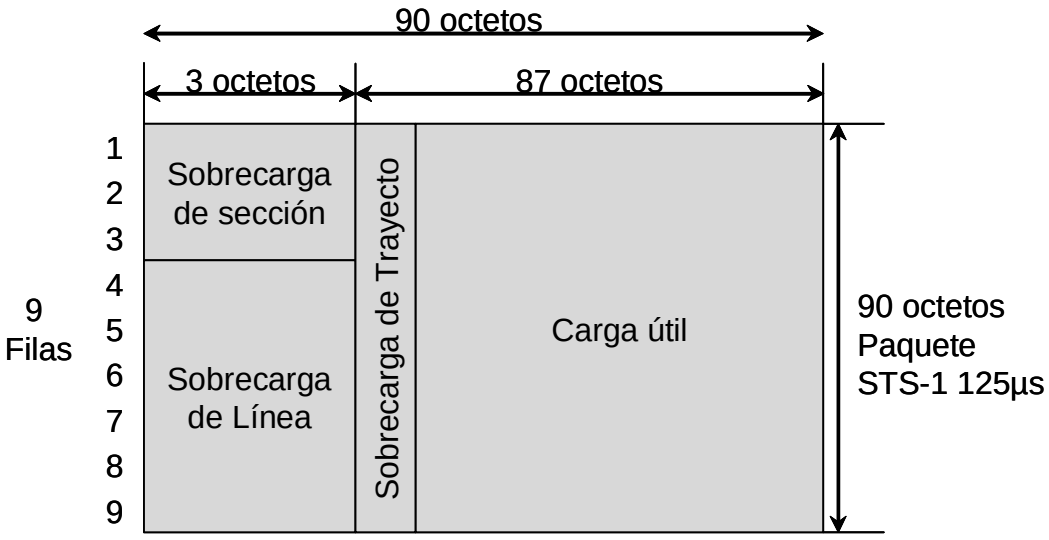
La señal de transporte síncrono (STS) de nivel 1 constituye la base para la señal de portadora óptica (OC) de nivel 1. OC-1 constituye los cimientos de la jerarquía de señales ópticas síncronas. Las señales de nivel más alto se derivan por multiplexión de las señales de nivel más bajo.

Formato de la Trama de SONET y SDH

La unidad de transmisión básica para SONET es la trama STS-1. SDH comienza en el nivel STS-3. Todos los niveles se componen de octetos de ocho bits que se transmiten en serie por la fibra óptica.

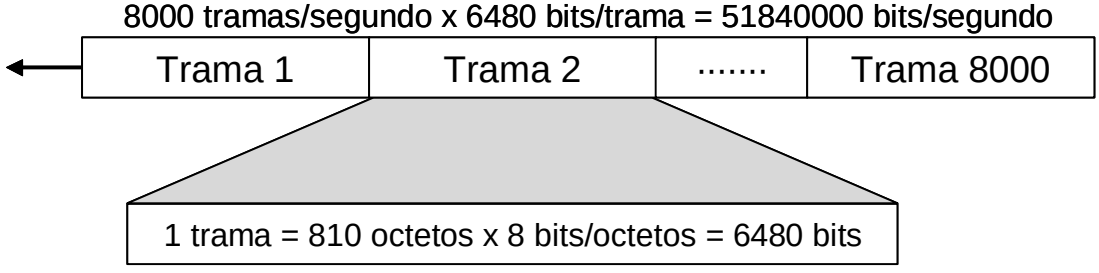
La trama SONET STS-1 consiste de 90 columnas y 9 filas de octetos de ocho bits y lleva 810 octetos o 6480 bits.

Las primeras tres columnas de la trama contienen sobrecarga de transporte, que se divide en 27 octetos, de los cuales nueve se asignan a la sobrecarga de sección y 18 a la sobrecarga de línea. Las otras 87 columnas constituyen el paquete de carga útil síncrona (SPE, Synchronous Payload Envelope) de STS-1 (aunque la primera columna de la capacidad del paquete se reserva para la sobrecarga del trayecto de STS).

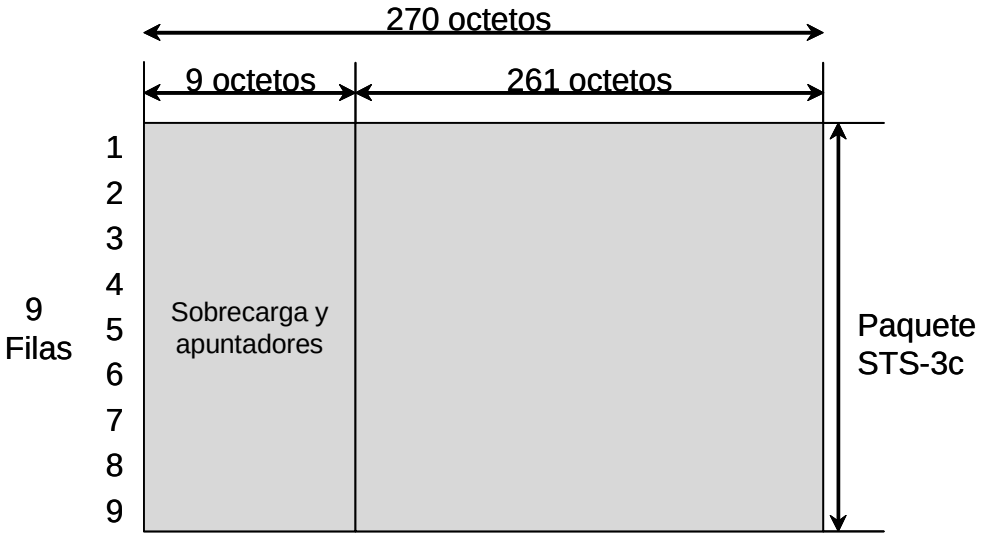


90	Octetos
x 9	Filas
x 8	Bits por octeto
6480	
x 8000	Ranuras de 125µs de bits por segundo
51,840,000	o 51.840 Mbits/s

SONET/SDH transmite 8000 tramas/segundo: por lo tanto, la longitud de la trama es de 125 microsegundos(µs). Este proceso se traduce en una tasa de transferencia de 51.840 Mbits/s (6480 x 8000 = 51,840,000).



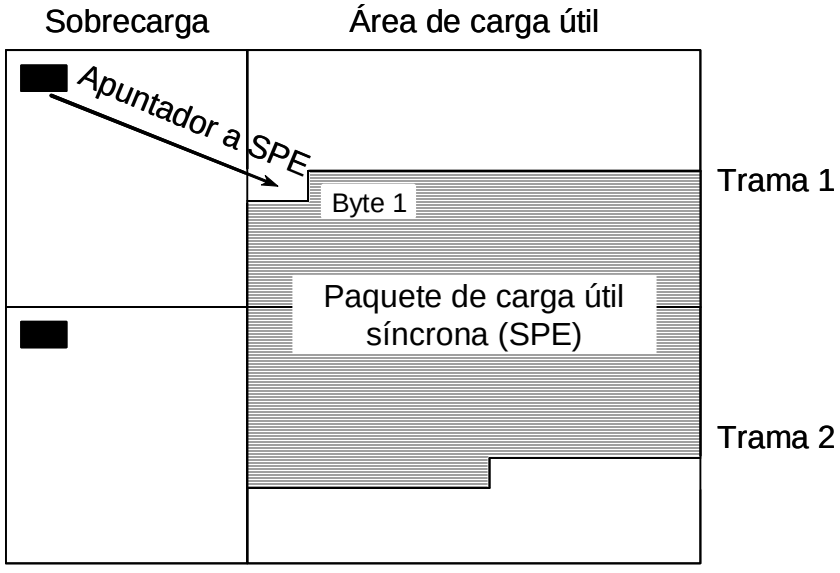
La trama SDH inicia en STS-3. La cual consiste en tres paquetes STS-1 y opera a una tasa de bits de 155.520 Mbits/s (51.840 * 3 = 155.520 Mbits/s).



3 Paquetes STS-1,
51.840
x 3
155,520,000 o 155.520 Mbits/s

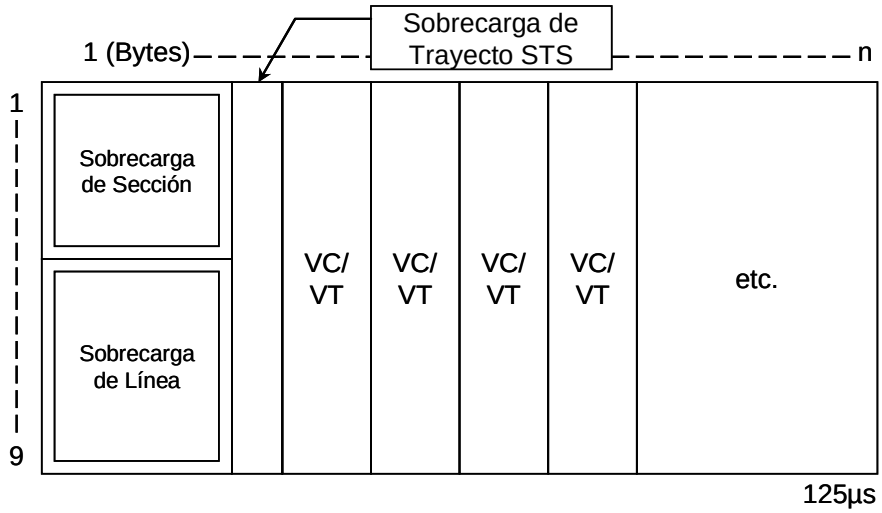
Apuntadores

SONET/SDH usa un concepto llamado apuntadores para manejar las variaciones de temporización en una red. El propósito de los apuntadores es permitir que la carga útil flote dentro del paquete. El apuntador es un valor de distancia que muestra la posición relativa del primer octeto de la carga útil. Durante la transmisión por la red, si ocurre cualquier variación en la temporización, basta con incrementar o decrementar el apuntador para compensar dicha variación.



Tributarias Virtuales o Contenedores Virtuales

SONET/SDH soporta un concepto llamado tributarias virtuales (VT) o contenedores virtuales (VC); El primer término se usa en SONET y el segundo en SDH. Mediante el uso de apuntadores y valores de distancia, los VT/VC como DS1, DS3 se pueden transportar en el paquete SONET/SDH. El estándar incluye reglas estrictas y concisas sobre la forma en que diversos VT/VC se hacen corresponder con el paquete SONET/SDH.
Los VT/VC se usan para soportar niveles subSTS-1, que son señales de baja velocidad.



MPLS (Multiprotocol Label Switching)

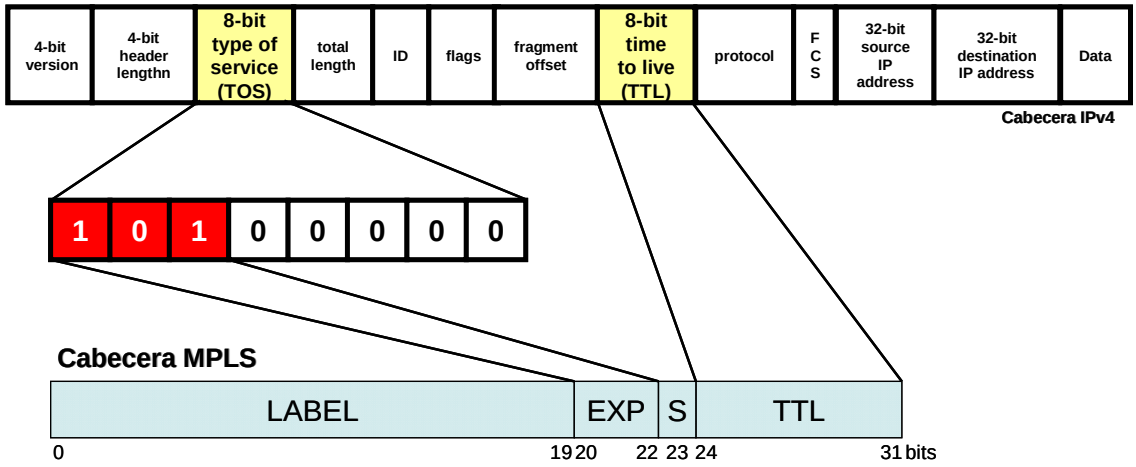
El objetivo de MPLS (MultiProtocol Label Switching) es ofrecer un método de conmutación de paquetes que no genere mucha carga a los routers de una red. Esta conmutación rápida se consigue gracias a la utilización de etiquetas de longitud fija. Estas etiquetas se insertan entre la cabecera de red y la de enlace.

Las principales características del uso de etiquetas son:

- Las etiquetas son asociadas a un flujo específico de datos unidireccional.
- La conmutación de paquetes etiquetados es muy simple dado que los routers conmutan según la etiqueta.
- MPLS puede utilizarse con casi cualquier protocolo (por ejemplo IPv4 ó IPv6).

El encapsulado de las cabeceras MPLS depende del tipo de medio sobre el cual esté montada la red. Interesa que la cabecera MPLS introduzca poca carga al paquete.

La cabecera de MPLS está compuesta de 4 octetos (32 bits).



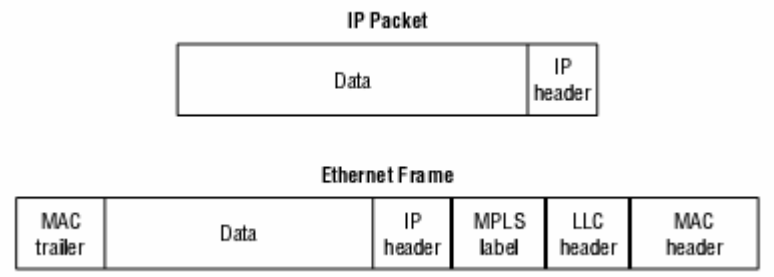
Label, (Etiqueta): Este campo es la etiqueta misma y tiene 20 bits de longitud. Con 20 bits puede haber cerca de un millón de etiquetas.

Experimental (EXP): El campo experimental tiene 3 bits de longitud y es usado para conectar el paquete IP estándar ToS (Tipo de Servicio, Type of Service) con la CoS (Clase de Servicio, Class of Service) de MPLS.

S (Stack bit, bit de apilamiento): Es usado para indicar lo último de la pila. Un valor de 1 en este campo indica el fondo o la última etiqueta de la pila.

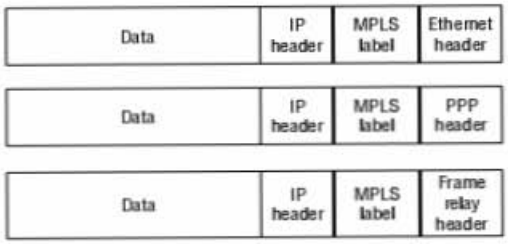
TTL, (Time To Live, Tiempo de Vida): Este campo desde IP TTL (o el campo de límite de saltos, Hop limit field en Ipv6) es decrementado por uno y a su vez copiado dentro del campo TTL en la etiqueta de MPLS. Si este campo llega a 0, el paquete será descartado. El campo TTL tiene 8 bits de longitud.

Ubicación de la Etiqueta de MPLS



La etiqueta de MPLS se encuentra entre la cabecera de la Capa 2 y la Capa 3. La pila de etiqueta de MPLS es a veces referida como “shim header” debido a la ubicación entre la carga de las dos cabeceras.

La etiqueta de MPLS puede estar entre diferentes encapsulaciones tipo trama. En donde la ubicación de la etiqueta es la misma.



Debido a que la etiqueta está antes de la cabecera de la capa 3, el router la ve primero por lo que ahora puede enviar paquetes basados en etiquetas de MPLS en lugar de la cabecera de la capa 3; Es por eso que se dice que en MPLS, el tráfico IP es conmutado en lugar de enrutado.

Arquitectura de MPLS

Hay dos componentes que conforman la arquitectura de MPLS: Control y Envío.

Control

El plano de control de la arquitectura de MPLS es responsable de unir una etiqueta a las rutas de red y distribuir esas uniones entre otros routers habilitados con MPLS.
Debido a que las etiquetas son unidas a rutas de red, se necesita tener una tabla de ruteo y para obtenerla es necesario un protocolo de ruteo. El mecanismo para intercambiar la etiquetas es hecho por dos protocolos: TDP y LDP.

TDP, Tag Distribution Protocol: Este protocolo es propiedad de Cisco y es usado para unir tags (las cuales son las mismas que las etiquetas de MPLS) a rutas de red en la tabla de ruteo.

LDP, Label Distribution Protocol: Este protocolo es la versión IETF del TDP de Cisco. LDP es usado para unir labels (etiquetas) a rutas de red.
La base de Información de Etiqueta (Label Information Base, LIB) es una lista de etiquetas de entrada con etiquetas de salida junto con interfases de salida e información del enlace.

Envío

Cuando se utiliza la información que se creó y almacenó en el plano de control, el componente de envío de la arquitectura de MPLS es conocido como el plano de envío (forwarding plane), o el plano de datos (data plane).

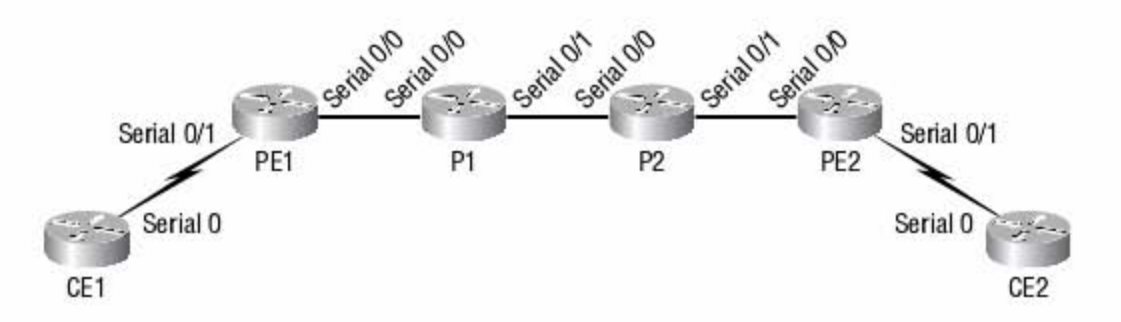
La tabla de ruteo es construida en el plano de control y almacenada en el plano de envío. Para las etiquetas, la LIB (Base de Información de Etiqueta) es construida en el plano de control y únicamente

aquellas etiquetas en uso residen en la LFIB (Base de Información para el Envío de la Etiqueta). La LFIB está bajo la LIB.

Un componente adicional que reside en el plano de reenvío es la FIB (Base de Información de Envío). La FIB es construida por la CEF (Cisco Express Forwarding, Envío Rápido de Cisco). La FIB es esencialmente una versión de reserva de la tabla de ruteo de IP que elimina la necesidad de una ruta alterna o de reserva. Para que funcione MPLS o la conmutación de etiquetas, CEF debe estar habilitado.

La conmutación de Tags propiedad de Cisco fue el precursor de MPLS y es la tecnología en la que el estándar de MPLS esta basado.

Componentes de la Red de MPLS



Los routers en la red están etiquetados como CE1, PE1, P1, P2, PE2 y CE2, estos nombres son los acrónimos para:

CE, un dispositivo en la frontera del cliente: Este es un router que se conecta a la red del cliente y al proveedor del servicio.

PE, un dispositivo en la frontera del proveedor: Este es un componente del equipo del proveedor del servicio que conecta a un cliente dentro de la red del proveedor.

P, un dispositivo del proveedor: Este es un componente del equipo del proveedor del servicio que existe completamente en la red del proveedor y únicamente se conecta a otro dispositivo de algún proveedor de servicio (no a clientes).

En resumen, Los routers PE y P son routers conmutadores de etiquetas. Hay dos tipos de estos routers:

LSR, Router Conmutador de Etiquetas (Label Switch Router, LSR): Es un router/switch que es capaz de enviar paquetes basados en etiquetas. El CE, o los dispositivos del cliente no son LSRs y solo pueden manejar paquetes sin etiquetas.

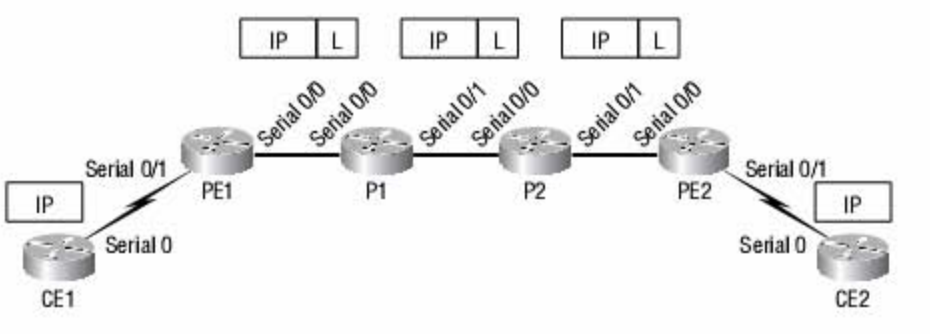
Edge-LSR, Router Conmutador de Etiquetas en la Frontera (Edge Label Switch Router, Edge-LSR): Es un término más específico para los routers PE. Un Edge-LSR es un dispositivo en la frontera que es

también un LSR. Para una red MPLS, este es un dispositivo que toma tráfico IP sin etiquetas, le agrega una etiqueta de MPLS y conmuta el tráfico al siguiente LSR. El Edge-LSR también toma tráfico etiquetado, remueve la etiqueta y lo envía al siguiente salto. Un dispositivo PE es un Edge-LSR en redes basadas en MPLS.

LSP, Caminos Conmutados de Etiquetas (Label-Switched Paths, LSP): Es una ruta unidireccional de LSRs que el paquete etiquetado debe seguir para alcanzar un destino en particular.

Aplicaciones de MPLS

Uno de los principios básicos de MPLS es que los paquetes son conmutados en lugar de enrutados. Cuando un paquete de la red del cliente entra en la red del proveedor del servicio, éste está sin etiqueta; El router en el borde de la red del proveedor del servicio acepta la entrada de este paquete y le aplica una etiqueta. El nuevo paquete etiquetado sigue un LSP a través de la red del proveedor del servicio y es conmutado; Cuando el paquete deja la red MPLS del proveedor del servicio, la etiqueta es removida y otra vez se convierte en un paquete IP sin etiqueta.



Desde que los paquetes reciben etiquetas en la frontera de la red por el Edge-LSR y esas etiquetas son usadas por cada LSR en la red del proveedor del servicio para conmutar tráfico, existen aplicaciones para MPLS tales como Virtual Private Networks (VPNs) y Calidad de Servicio (QoS).

Capitulo 5

Voz sobre IP (VoIP)

Voz sobre IP (VoIP) y Telefonía IP

Voz sobre IP: Es una aplicación de voz que es generada desde una PC o un teléfono hecho para esta tecnología, que viaja por la red LAN en un mismo sitio o se provee de una conexión a través de una WAN.

Telefonía IP: Es una aplicación de voz sobre IP y en la cual se llevan servicios básicos de telefonía tradicional como transferencia de llamada, conferencia, sígueme, llamada en espera, grupos de trabajo, retención de llamada, etc.

Estándares empleados para Voz sobre IP

Los estándares empleados son la Fuerza de Trabajo de Internet (Engineering Task Force, IETF), quien es un grupo global en el que participan especialistas tecnológicos, vendedores, personal que proporciona servicios de Internet, telecomunicaciones, personal de gobierno, etc., todos estos con el fin de obtener estándares de trabajo y convivencia entre los diferentes sistemas.
La convergencia ha tomado la migración de servicios tales como voz, video y datos a una simple y consolidada red como Internet.

IETF sigue desarrollando los estándares sobre Internet, son muchos y variados entre los principales están H323, SIP, MGCP y MEGACO para redes de voz sobre IP.

Estándar H.323

El estándar H.323 proporciona los fundamentos de audio, video y comunicaciones de datos a través de las redes basadas en IP.
El H.323 tiene muchas recomendaciones por parte de la ITU, es decir, el conjunto de estándares para comunicaciones sobre redes de Área Local que no garantizan la calidad de servicio (QoS).
H.323 dirige el control de llamada, administra multimedia y el ancho de banda, así como las interfaces entre LANs y otras redes.

Arquitectura del Estándar H.323

El estándar H.323 define cuatro componentes básicos de comunicación:

- Terminales.
- Gateways.
- Gatekeepers.
- Multipoint Control Units.

Terminales: Son puntos finales sobre la LAN; Todos estos puntos deben soportar la comunicación de voz. Video y datos son opcionales por lo que deberán soportar el estándar H.245, el cual se emplea para negociar el uso del canal y las capacidades.

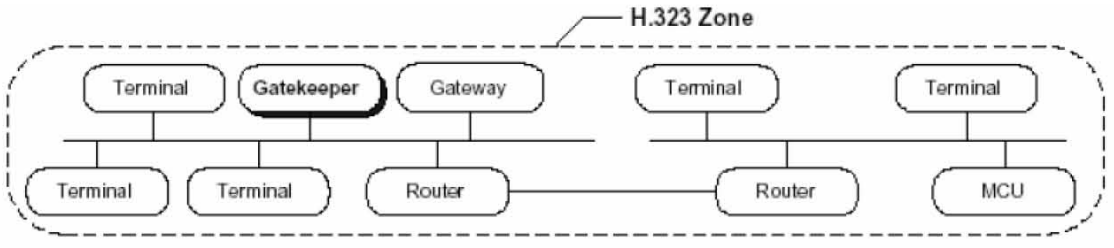
Se requieren de otros tres componentes:

- RAS: Los mensajes RAS controlan las funciones de registro en los gatekeepers, admisión de llamadas, control de ancho de banda y control de estado.
- Q.931: Es el sistema de señalización utilizado para el establecimiento, mantenimiento y liberación de las llamadas.
- RTP/RTCP: Permite la transmisión y control de los paquetes de voz en tiempo real.

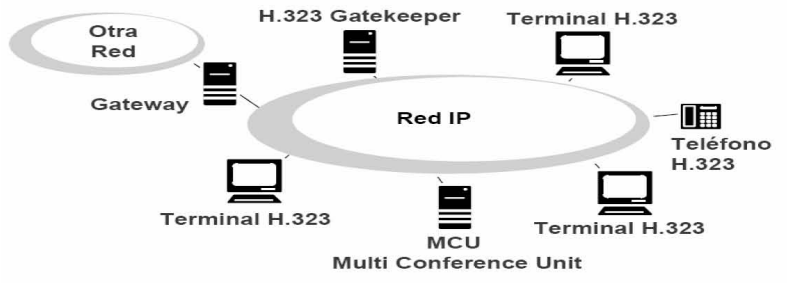
Gateway: es opcional en la conferencia H.323, este elemento proporciona muchos servicios, el más común es la conversión entre los puntos finales de H.323 y otros tipos de terminales. Establece el enlace entre las terminales analógicas de la red PSTN.

Gateway H.323/Red pública

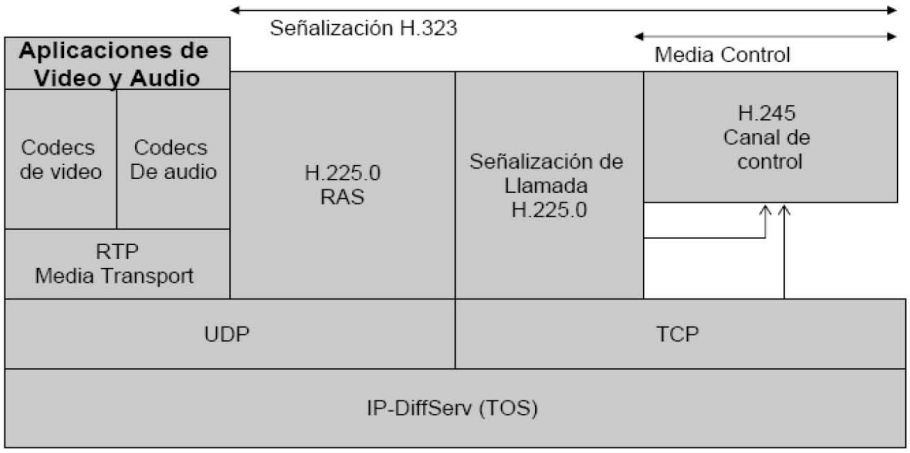
Gatekeeper: es el componente más importante de la red H.323. Actúa como el punto central de todas las llamadas en una zona y proporciona el control de servicios para registrar los puntos terminales.
El Gatekeeper tiene dos funciones principales de control, la primera traslada la dirección de red de las terminales y gateways a IP, la segunda es el manejo del ancho de banda.



Multipoint Control Units (MCU): Soporta conferencias entre tres o más puntos finales.
Bajo H.323 un MCU consiste en un Controlador Multipunto (MC). El MC maneja las negociaciones H.245 entre todas las terminales para determinar las capacidades comunes de audio y video.

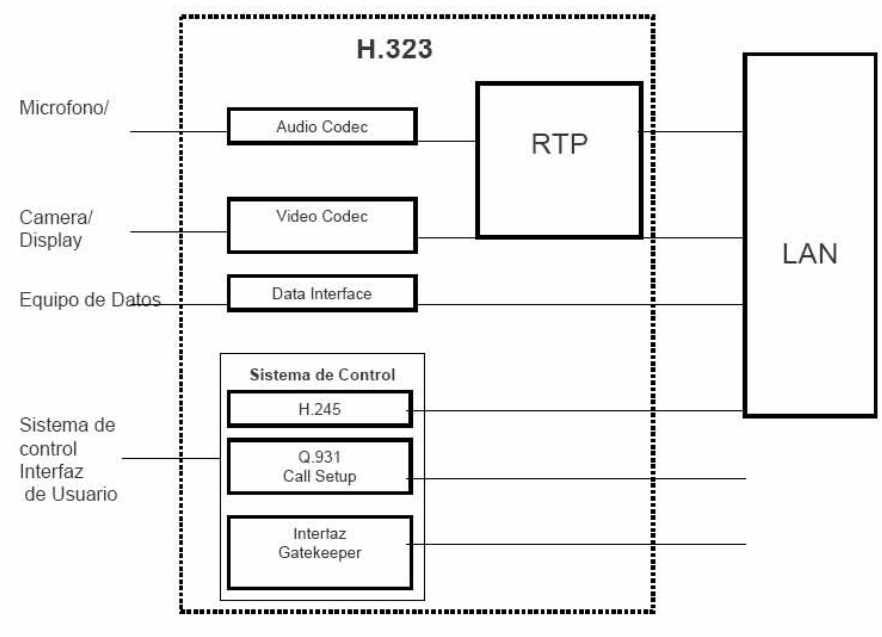


Protocolos H.323



Video		Audio		Control			Datos
H.261 H.263 Codecs de video		G.711 G.722 G.723 G.729 Codecs de audio		H.225 Terminal a Señalización Del Gatekeeper	Q.931 Señalización De Llamada	H.245 Canal de control	T.120 Terminal para Compartir datos
RTP	RTCP	RTP	RTCP				

Estructura Funcional H.323

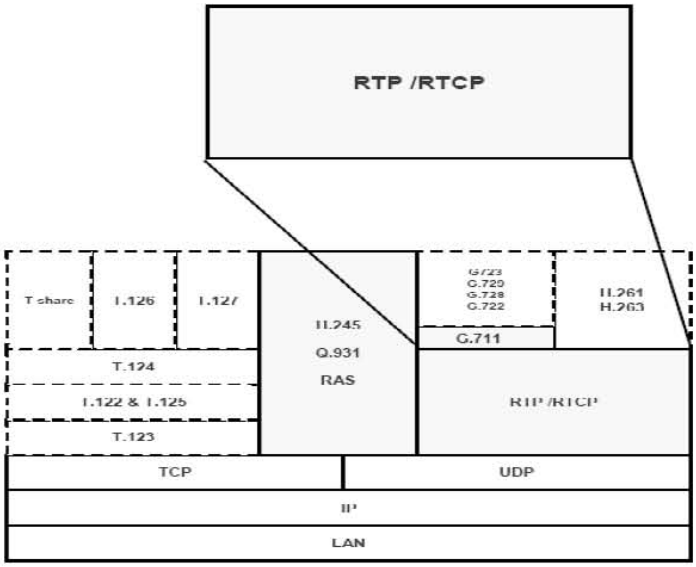


Transporte H.323

RTP, Real Time Protocol (Protocolo de Tiempo Real): Proporciona servicio de entrega extremo a extremo para el tráfico en tiempo real. RTP corre sobre UDP, así que al final ninguno se entera si los paquetes se entregaron.

RTCP, Real Time Control Protocol (Protocolo de Control de Tiempo Real): Monitorea la calidad de servicio, identifica el origen y proporciona retroalimentación en los reportes de calidad de servicio. Proporciona información de la parte que envía, tal como el nombre y número de teléfono.

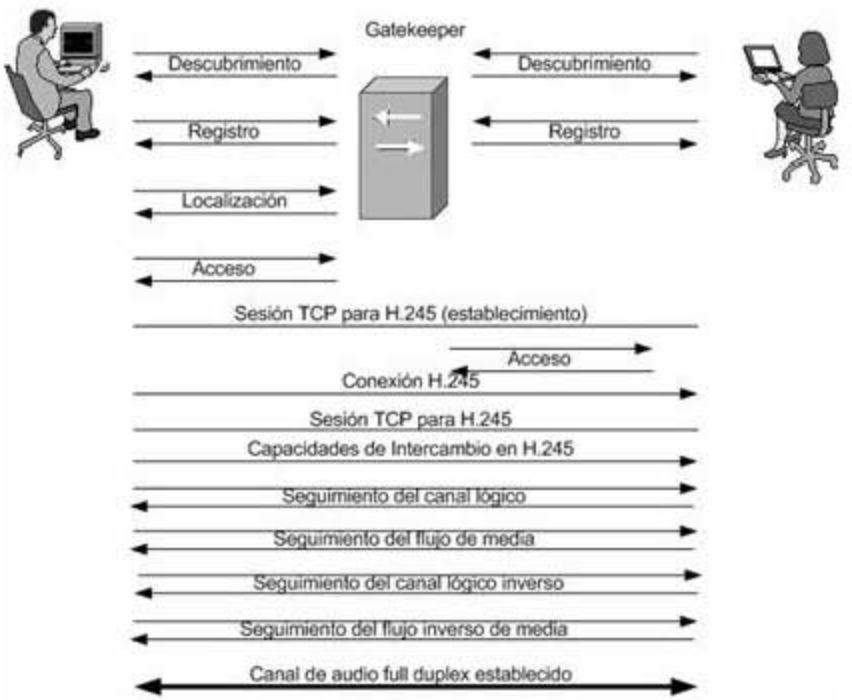
RTP y RTCP se emplea en SIP también.



RAS (Registro, Admisión y Estatus)

Los mensajes RAS y los procedimientos se describen en la recomendación H.225.0 de la ITU.
La comunicación RAS entre los puntos finales y el GK se realiza sobre UDP a la dirección IP del GK sobre el puerto UDP 1719.
Existen métodos manuales y automáticos usando multicast IP. Si el GK ha sido preconfigurado en el punto final, el registro es un simple intercambio de mensajes.

Establecimiento de Llamada



Session Initiated Protocol (SIP)

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP

SIP es un protocolo de control de la capa de aplicación que puede establecer, modificar y terminar sesiones multimedia (conferencias) tales como llamadas de telefonía por Internet. SIP también puede invitar participantes a sesiones ya existentes tales como conferencias multicast. Los medios pueden ser agregados (y removidos) desde una sesión existente. SIP transparentemente soporta mapeo de nombre

y servicios de redireccionamiento lo cual soporta mobilidad personal; Los usuarios pueden mantener un su identificador sin importar su localización en la red.

Componentes Funcionales en SIP

Existen dos elementos fundamentales, los agentes de usuario (UA) y los servidores.

User Agent (UA): Consisten en dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS). Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones. Un UAS es una entidad lógica que genera respuestas a las peticiones SIP. Ambos se encuentran en todos los agentes de usuario, así permiten la comunicación entre diferentes agentes de usuario mediante comunicaciones de tipo cliente-servidor.

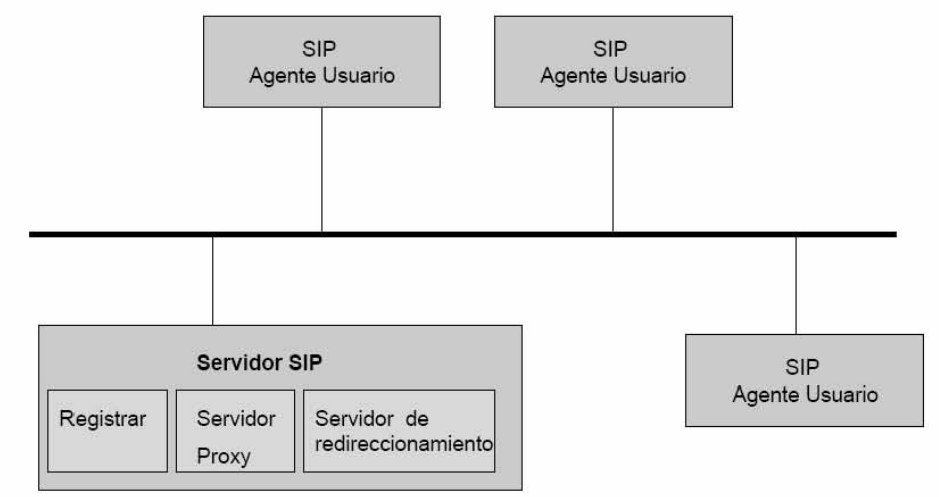
Los servidores SIP pueden ser de tres tipos:

- *Proxy Server*: Retransmiten solicitudes y deciden a qué otro servidor deben remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios.

- *Registrar Server*: Es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

- *Redirect Server*: Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

Modelo SIP



Capacidades SIP

User Location (Localización del Usuario): Los usuarios tienen la capacidad de moverse a otras localidades y recibir las características de telefonía desde cualquier localidad remota vía el registro remoto.
User Availability (Disponibilidad de Usuario): SIP define un código de respuesta muy explícito para proporcionar la información detallada acerca de la disponibilidad del usuario actual.

User Capabilities (Capacidades del Usuario): Es la determinación del medio y los parámetros a ser usados en el. SIP usa el formato del protocolo SDP para la negociación de los parámetros.

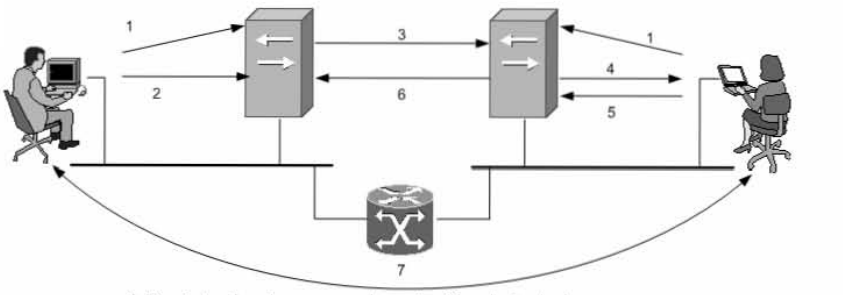
Session Setup (Establecimiento de Sesión): SIP contiene un punto de establecimiento punto a punto y conferencias multipunto, así como simples llamadas en punto final de señalización a través del servidor proxy.

Session Managment (Administración de Sesión): Se incluye la transferencia y terminación de las sesiones, modificación de los parámetros de la sesión e invocando servicios. La mayoría de las características de telefonía son soportadas con SIP.

Protocolos para establecer sesión en SIP

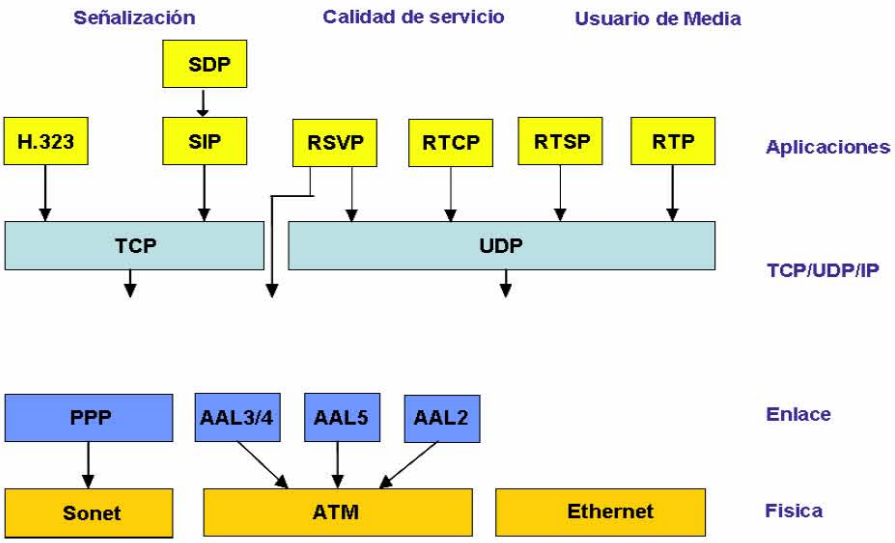
SIP es un componente que puede ser usado con otros protocolos de IETF para construir una arquitectura multimedia completa. Esta arquitectura incluye protocolos como el RTP (Real-time Transport Protocol) para transportar información en tiempo real, RTSP (Real-Time Streaming Protocol) para controlar la entrega del flujo de medio; MEGACO (Media Gateway Control Protocol) para controlar gateways hacia la PSTN, y el protocolo SDP (Session Description Protocol) para describir sesiones multimedia. Sin embargo, la funcionalidad y operación básica de SIP no depende de ninguno de estos protocolos.

Llamadas en SIP



1 Registro hecho por cada estación de trabajo
2 Bob inicia la llamada enviando una invitación y SDP
3 El servidor SIP entrega la invitación hasta todos los servidores SIP conocidos en la red
4 El servidor SIP de Alice entrega la invitación a la parte llamada
5 Alice acepta la invitación y regresa SDP
6 El servidor SIP regresa un ACK a la parte llamante
7 Finalmente la conversación telefónica

Señalización de SIP



Media Gateway Control Protocol (MGCP)

MGCP es un protocolo usado por los controladores gateway de medios (MGC, también conocidos como call agents "agentes de llamada") para controlar los gateways de medios (MG, Media Gateway). MGCP está basado en un paradigma maestro/esclavo en el cual MGC es el maestro que provee los comandos al MG (esclavo). El MG reconoce el comando, lo ejecuta y notifica al MGC de la salida (exitosa o no). En esta arquitectura, el MG maneja las funciones de medios, tales como la conversión de la multipexión por división de tiempo (TDM)/ señales analógicas dentro de Protocolo de transporte de Tiempo Real (RTP)/ ráfagas del Protocolo de Control de Tiempo Real (RTCP). MGC maneja las funciones de señalización de llamada.

En este modelo, la inteligencia del control de llamada reside en el MGC, y el MG es la entidad esclavo que actúa en base a los comandos del MGC.

Los mensajes de MGCP son transportados sobre UDP. Debido a que UDP no garantiza la entrega de mensajes, los mensajes son retransmitidos si es necesario.
MGCP tiene sus orígenes de otros protocolos: Simple Gateway Control Protocol (SGCP) e Internet Protocol Device Control (IPDC). MGCP version 1.0 está descrito en el RFC 2705.

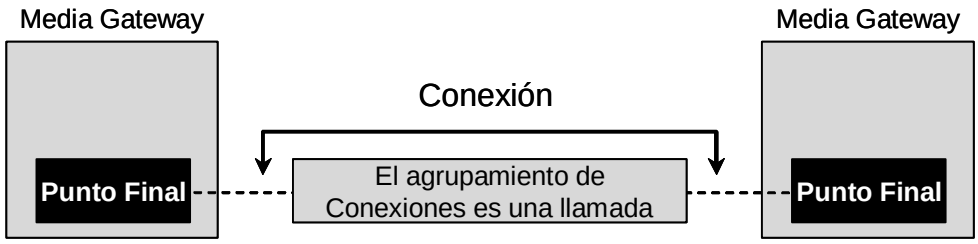
MGCP usa Session Description Protocol (SDP) para describir las sesiones de medios. SDP describe los parámetros de la sesión del flujo del medio entre los MGs tales como las direcciones IP, el puerto UDP, la descripción de RTP y las capacidades de conferencia multimedia. La especificación SDP define diferentes tipos de medios; MGCP sin embargo limita el uso de SDP a dos tipos de medios: circuitos de audio y circuitos de acceso a datos.

Los agentes de llamada usan los siguientes parámetros de SDP en los gateways de telefonía:

- El puerto UDP indica el puerto de transporte usado para recibir paquetes RTP desde el gateway remoto.
- El uso de direcciones IP en el gateway remoto, y en el gateway local o en la conferencia de audio multicast direccionan el intercambio de paquetes RTP.
- El medio de Audio especifica el codec.

Modelo MGCP

El MGCP asume un modelo de conexión en el cual las construcciones básicas son puntos finales y conexiones. Las conexiones son agrupadas en llamadas. Una o más conexiones pueden pertenecer a una llamada.



Puntos Finales: Los puntos finales son entidades físicas o lógicas que existen en un MG.

Un ejemplo de un punto final físico es una interfase en un MG que termina un circuito originado desde un switch de la red de telefonía pública conmutada (PSTN).
Un ejemplo de un punto final lógico es un punto final de servidor de anuncio que toca los anuncios basados en un comando desde el agente de llamada.

Puntos finales físicos típicamente requieren instalación de hardware, donde la creación de puntos finales lógicos puede ser desempeñada en software.

Cada punto final es identificado por un identificador que tiene dos componentes:
- El nombre del dominio del MG que contiene los puntos finales
- Un nombre local o identificador dentro del gateway.

Conexiones: Las conexiones pueden ser punto a punto o a multipunto.

Una conexión punto a punto es una asociación entre dos puntos finales con el propósito de transmitir información entre ellos. Se establece una conexión multipunto conectando el punto final a una sesión multipunto.

Cada conexión es designada localmente por un identificador de conexión y es caracterizado por sus atributos.

Los puntos finales que están involucrados en una conexión pueden estar en gateways separados o en el mismo gateway.

Llamadas: Un grupo de conexiones componen una llamada.

Los agentes de llamada asignan los identificadores, loa cuales son únicos para cada llamada y son globalmente únicos a través del sistema. Un único identificador enlaza todas las conexiones que están asociadas en la llamada. Este identificador habilita el conteo o la tasación conforme transcurre la llamada.

Comandos y Mensajes en MGCP

MGCP es un protocolo basado en texto, el cual envuelve mensajes y comandos

Los comandos de control de llamada básica son usados en la interacción de cada llamada:

- Create Connection (CRCX), Crea la conexión.
- Modify Connection (MDCX), Modifica la Conexión.
- Delete Connection (DLCX), Borra la Conexión.

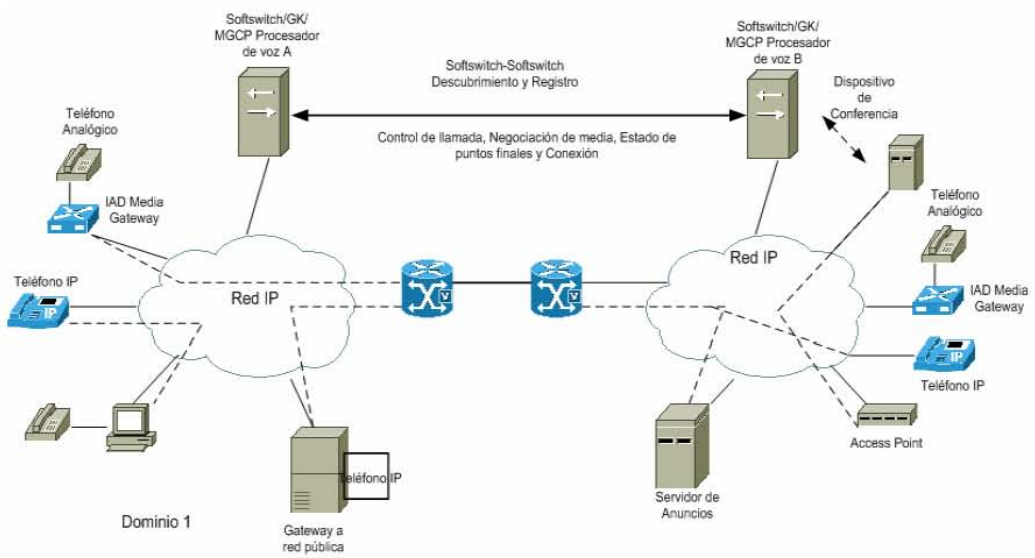
Los comandos de control de llamada avanzada son los siguientes:

- Notification Request (RQNT), Solicita al gateway el reporte de la ocurrencia de ciertos eventos.
- Notify (NTFY): El gateway reporta la ocurrencia de estos eventos al MGC usando este comando.

Los comandos de administración no están directamente relacionados al control de la llamada pero el MGC y el gateway intercambian información uno a otro sobre eventos no relacionados a la llamada. Por ejemplo, un gateway puede experimentar un problema de hardware en alguno de sus puntos finales y necesita informar al MG respecto a esto.

- AuditEndPoint (AUEP), Revisión del Punto Final.
- Audit Connection (AUCX), Revisión de la Conexión.
- RestartIn-Progress (RSIP), Reinicio en Progreso.
- EndpointConfiguration (EPCF), Configuración del Punto Final.

Señalización MGCP



Protocolo Megaco/H.248, Media Gateway Control Protocol

H.248 (como es conocido en ITU) o MEGACO (como es conocido en la IETF) es similar a MGCP en términos de arquitectura y propósito.

Las construcciones principales en el modelo de conexión de H.248 son Terminaciones, Contextos y Comandos.

Una Terminación: Es el origen de una o más serie de medios.

Un Contexto: Es una asociación entre una colección de terminaciones.

Una terminación puede estar únicamente en un contexto en cualquier tiempo. Un contexto de tipo especial es el contexto nulo que contiene todas las terminaciones que no están en otro contexto. Por ejemplo, en un gateway de acceso, todas las líneas disponibles son representadas por terminaciones en el contexto nulo.

Comandos: Son utilizados para manipular las terminaciones y contextos.

El comando Add agrega una terminación al contexto. El comando subtract remueve una terminación desde un contexto y puede resultar en el contexto siendo liberado si no permanecen terminaciones. EL comando move mueve una terminación desde un contexto a otro. El comando modify cambia el estado de la terminación.

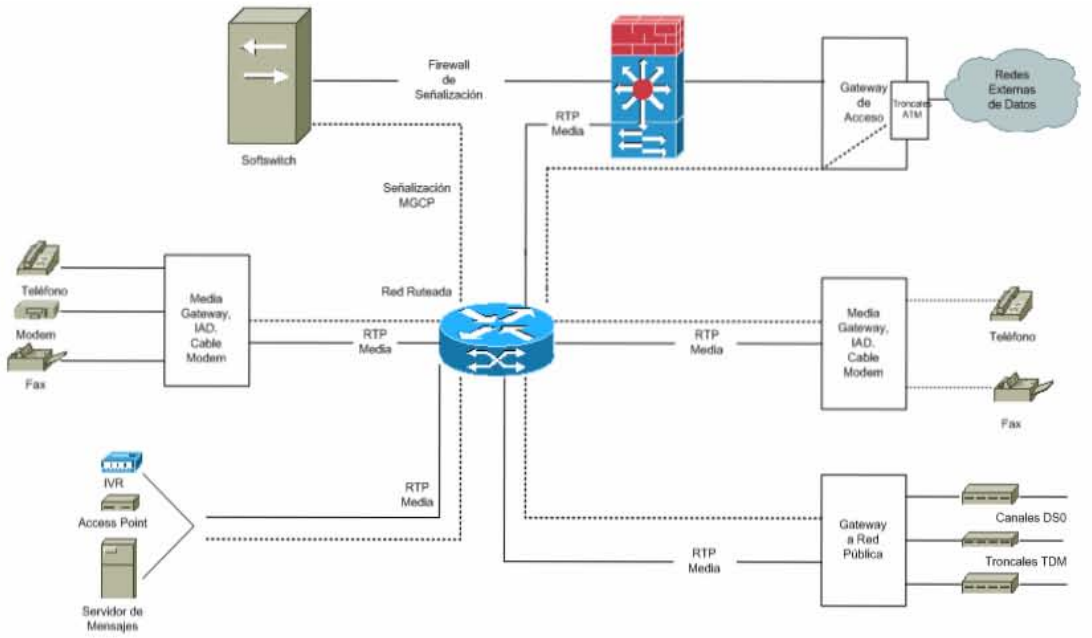
Los demás comandos son parecidos a los que se utilizan en MGCP

- Add.
- Modify.

- Substract.
- Move.
- Audit Value.
- Audit Capabilities.
- Notify.
- Service Change.
- Reply.

En MGCP una terminación se parece a un punto final y un contexto se parece a una llamada. También el comando add es similar al comando CRCX (Crear Conexión) y el comando Subtract es similar al comando DLCX (Borrar Conexión).

Señalización MGCP/Megaco



Técnicas de Compresión

Para una comunicación de voz en un solo sentido es suficiente un ancho de banda de 64 kbps. Para la red LAN no es ningún problema alcanzar este rango, pero para enlaces dial-up o incluso para algunos enlaces WAN esto no es posible debido a que saturarían el enlace, es por eso que son utilizados esquemas de compresión para reducir el ancho de banda requerido para la comunicación de voz.

Retardo causado por compresión

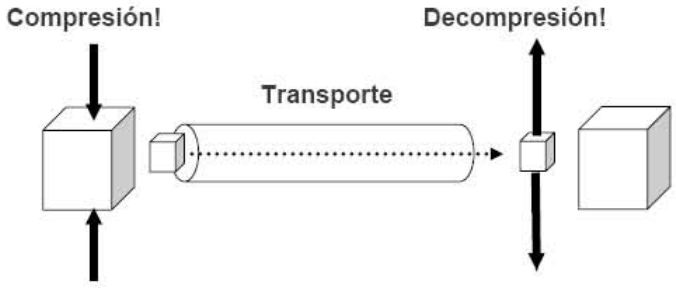
La compresión y descompresión de voz digitalizada introduce una cierta cantidad de retardo en la comunicación.

El primero es introducido debido a los cálculos que deben ser realizados (procesamiento) propios del algoritmo de compresión, este depende de la capacidad y el rendimiento del sistema.

El segundo es introducido por algunas técnicas de compresión en el cual se necesita una porción de la señal que sigue a la que esta siendo procesada "look ahead" para el proceso de descompresión de la señal.

Codificación/decodificación de Voz

- Audio (y Video).
- Codificación/ Decodificación.
- Compresión de payload.
    - Gasto de procesamiento
    - Ancho de banda



La Codificación y Proceso de Trama

Entrada analógica – Señal de voz (o video)
Muestreo
- Ejemplo: muestreo de 8 kHz <=> Una muestra cada 0.125 ms

Codificación
- El volumen de datos depende del codec empleado
- Requerimientos de procesamiento dependiendo del codec

Empaquetado
- Típicamente de 5 -30 ms el tamaño de la trama dependiendo del codec

Paquetes IP por segundo
- Aplicación / depende del producto
- Paquetes por segundo (pps)
- Típicamente 30-300 paquetes por segundo

Estándares de Compresión

Los estándares más conocidos son los G. De la ITU-T y los estándares GSM ETSI.
Los más utilizados son:

- *G.711*: Algoritmos que opera a 64 Kbps utiliza PCM y produce una trama de 125 microsegundos con alta calidad.
- *G.722*: Algoritmo que opera a 48, 56 o 64 kbps y se refiere como un codificador de banda ancha.
- *G.723.1*: Algoritmo que opera a 5.3 y 6.4 kbps; Utiliza ACELP para la menor velocidad y MP-MLQ para la alta. Este algoritmo produce tramas de 30 milisegundos y un retardo total de 37.5 milisegundos.
- *G.726*: Algoritmo que opera a 16, 24, 32 y 40 kbps; Utiliza ADPCM. El algoritmo produce una trama de 0.125 milisegundos.
- *G.728*: Algoritmo que opera a 16 kbps. Utiliza LD-CELP. Produce una trama de 0.625 milisegundos y un retardo total de 0.625 milisegundos.
- *G.729a*: Algoritmo que opera a 8Kbps. Utiliza una versión compleja de CS-ACELP. Este algoritmo produce una trama con 10 milisegundos y un retardo total de 15 milisegundos.

Recomendaciones de Diseño

El CODEC G.711 provee la mejor calidad de voz, es recomendado para utilizarse en los ambientes LAN en donde el ancho de banda está disponible; G.729 provee una buena reducción de ancho de banda con una mínima perdida en la calidad de la voz por lo que es recomendado utilizarlo en los ambientes WAN.

Calidad de Voz

El principal requerimiento en la valoración y configuración de una red es mantener la calidad de voz y la funcionalidad al usuario.
Los principales puntos que afectan la calidad de voz son los siguientes:

- *Retardo (Delay) de Propagación*: Esta afectado directamente por la distancia de los puntos que se comunican.

- *Retardo (Delay) del Transporte*: Este factor es debido a los dispositivos (routers, bridges, hubs, firewalls, etc.) que se encuentran entre el hablante y la persona que escucha.

- *Retardo de Paquetización*: Es el tiempo que se llevan los codificadores (codecs) en convertir una señal analógica a digital y viceversa.

- *Retardo por Jitter*: Cuando existen muchas variaciones en el tiempo de llegada de los paquetes de voz, se introduce un buffer llamado Jitter para suavizar las repeticiones. La paquetización y el buffer jitter son los que deciden cuanto tiempo estará empleando el equipo de VoIP.

- *Pérdida de Datos*: Los paquetes de datos usan RTP. Aunque cada uno de los datagramas RTP lleva una secuencia, no existe el tiempo necesario para retransmitir los paquetes perdidos. Cualquier pérdida de paquetes afecta directamente a la calidad de voz.

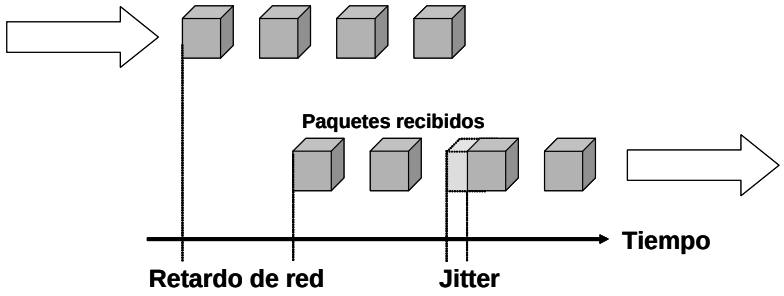
- *Ancho de Banda*: El consumo de ancho de banda es mayor de lo que se cree. El codec G.729 tiene un payload de 8 kbps pero el uso del ancho de banda es mayor, es decir, si se envían paquetes cada 30 ms, el tamaño del datagrama será de 30 bytes por datagrama. Además se le agregan 40 bytes del encabezado RTP, y 2 encabezados adicionales por enlace. Para un flujo en ambos sentidos para G.729, el consumo de ancho de banda es mayor.

Tolerancia al Jitter

Si cada bloque que contiene una parte de señal de voz digitalizada fuera reproducido en el destino inmediatamente al llegar, la calidad de la comunicación sería muy mala, debido a que cada paquete normalmente llega a su destino con ligeras diferencias en su delay, algunas veces el bloque sería reproducido antes que el previo terminara y otras veces quedarían espacios entre el final de un bloque y el principio de otro. Debido a que el Jitter es algo que ocurre en forma continua, este puede ser muy molesto para los participantes en una conversación.

Retardo y Jitter

- El retardo de red es típicamente de 100-300 ms.
- La variación en el retardo da como resultado el Jitter.



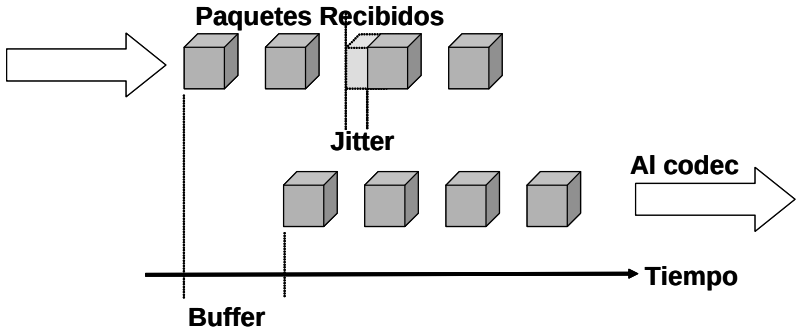
Buffering

Una técnica simple para evitar el jitter al momento de reproducir la señal de voz en el destino, es el introducir buffering; En vez de reproducir los paquetes de voz en el momento en que estos llegan a su destino, es introducida una cierta cantidad de retardo (Delay); Debido a que esto es realizado para todos los paquetes, existe una alta probabilidad de que cuando sea reproducido un paquete el siguiente este disponible inmediatamente.

En la práctica, normalmente solo una pequeña cantidad de buffering es necesaria para eliminar el Jitter, existen métodos para calcular el Jitter y poder determinar la cantidad de buffering necesitada.

Buffer de Paquetes

- El Buffer se realiza en la recepción constante del jitter.
- El tamaño típico de un buffer es de 50-100 ms.



Retardo (Delay)

Un delay grande puede ser desastroso para una conversación. El delay total puede ser categorizado en dos tipos:

- *Fijo*: Este es el delay total, el cual siempre esta presente debido a:
  - Muestreo (se debe tener primero la muestra de señal para poderla digitalizar).
  - Compresión (introducido por lo algoritmos de compresión).
  - Transmisión (debido a la capacidad de los enlaces).
  - Descompresión (introducido por lo algoritmos de descompresión).
  - Buffering (se produce artificialmente para compensar el Jitter).

- *Variable*: Este es causado por encolamiento de los paquetes en los Routers, congestiones en la red, etc.

Supresión de Silencio

En una conversación, usualmente solo una persona habla a la vez. En voz paquetizada esto da la oportunidad de ahorrar ancho de banda debido a que los paquetes que contienen solo silencio no necesitan ser enviados.

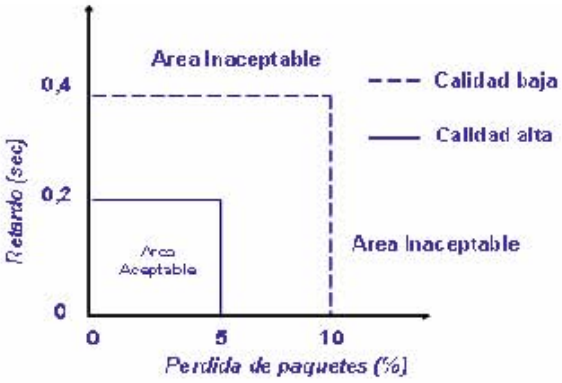
Una técnica simple es revisar si el paquete contiene muestras con un valor por encima de cierta frontera, si no hay, se puede considerar que se esta en silencio y el paquete puede ser descartado.

La supresión de silencio tiene un efecto no deseable menor. Debido a que los paquetes con silencio son descartados, no existe ningún sonido del lado del que recibe, ni siquiera ruido de ambiental, lo cual puede hacer pensar al que esta hablando que se ha perdido la conexión. La solución a este efecto es el introducir artificialmente ruido ambiental del lado en donde se esta suprimiendo el silencio.

Medición de la Calidad de la Voz

La medición de la calidad de voz ha sido subjetiva.
La principal medición subjetiva se conoce como MOS (Mean Opinión Score) y está descrita en la ITU recomendación P.800. Existe la recomendación ITU G.107 en la cual se define el modelo E, en donde se obtiene el valor R que va de 100 (excelente) a 0 (pobre) y se hace la relación en MOS de 5 a 1.

Calidad de voz percibida



Capitulo 6

El Router

El Router

El router es un dispositivo de capa 3 que envía la información en base a la dirección IP que se tenga de destino.

Componentes

El router está compuesto de los siguientes componentes:

CPU: Ejecuta instrucciones codificadas en el sistema operativo (y sus subsistemas), para desempeñar las operaciones básicas necesarias para cumplir la funcionalidad del Router, por ejemplo, todas las funciones de ruteo.

WIC Slots: Son puertos para Tarjetas de Interfase WAN (WAN Interface Card, WIC).

NM Expansion Slot: Puerto de expansión para instalar un módulo de red (Network Module ó NM) WAN o LAN.

LAN: Estos son los controladores LAN integrados en la tarjeta madre (motherboard). Se tienen puertos Ethernet, Fast Ethernet, Gigaethernet y Token Ring. La disponibilidad va a depender del modelo específico de cada router.

AIM Socket: En este socket se pueden insertar las tarjetas del Módulo de Interfase Avanzada (Advanced Interface Module, AIM). Este es un socket de 100-pin que permite funciones que no requieren una conexión externa (tales como compresión, encriptación, etc.).

System Bus (Bus de Sistema): Es usado para la comunicación entre la tarjeta de CPU y las tarjetas de interfases (entre otras).

CPU Bus (Bus de CPU): Este es usado por el CPU para acceder a varios componentes del sistema y transferir instrucciones y datos desde una dirección de memoria específica.

Host PCI Bridge: Esta es la interfase puente entre el bus del CPU y el bus de sistema (PCI bus, donde los módulos de red y otras tarjetas de interfase son conectadas).

Memoria: La memoria es usada en varias formas para algunos propósitos de almacenamiento tales como guardar el sistema operativo (Cisco IOS Software), la configuración, el bootstrap, etc.

Tipos de Memoria en el Router

Las diferentes memorias que se utilizan en el router son:

- BootROM
- Flash
- Dynamic RAM, (DRAM)
- Non-Volatile RAM (NVRAM)

BootROM: Es usada por el código de diagnostico de inicio almacenado permanentemente (ROM Monitor). La tarea principal de la BootROM es la de desempeñar algunos diagnósticos de hardware durante el reinicio del Router (Power On Self Test – POST), y cargar el Cisco IOS software desde la Flash a la memoria. La BootROM no es borrable, pero está colocada en un módulo por lo que puede ser remplazada.

FLASH: Es usada para el almacenamiento permanente de una imagen completa del Cisco IOS software en una forma comprimida.

DRAM: Es usada al mismo tiempo que se ejecuta el Cisco IOS software (y sus subsistemas), tablas de ruteo, running configuration, etc.

NVRAM: Es usada para almacenamiento permanente grabable de la startup-configuration.

Secuencia de Inicio (Boot)

Paso 1: Después de encender el Router, el ROM Monitor inicia primero. La función del ROMMON/BOOTSTRAP es importante en el inicio del Router, y desempeña las siguientes operaciones al inicio:

- Configura las opciones del registro al encender: Activa los registros del control del proceso y la de otros dispositivos para el acceso por el puerto de consola, así también como el registro de configuración.
- Ejecuta los diagnósticos de encendido: Las pruebas son ejecutadas en la NVRAM y DRAM (escribiendo y leyendo varios patrones de datos).
- Inicializa el hardware: La inicialización del hardware o tarjetas instaladas en el equipo es ejecutada, también la memoria (DRAM, SRAM, etc.) es iniciada.
- Inicializa las estructuras del software.
- La inicialización de la estructura de datos de la NVRAM, así como la información sobre la secuencia de inicio.
- La información sobre dispositivos accesibles es activada en la tabla del dispositivo inicial.

Paso 2: EL ROMMON busca la imagen de software Cisco IOS en la Flash., si el Router no encuentra una imagen válida en la Flash éste no va a funcionar, por lo que se tendrá que copiar una imagen en la memoria flash para que el Router opere correctamente.

Paso 3: Después de encontrar la imagen, el Router la descomprime y la carga dentro de la DRAM.
EL software IOS de Cisco desempeña funciones importantes durante el arranque, tales como:

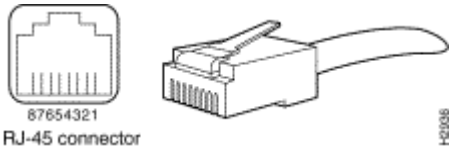
- Reconocer y analizar las interfases, así como otro hardware.
- Acomodo de Buffers.
- Lectura de la configuración (startup-config) desde la NVRAM a la RAM (running-config).

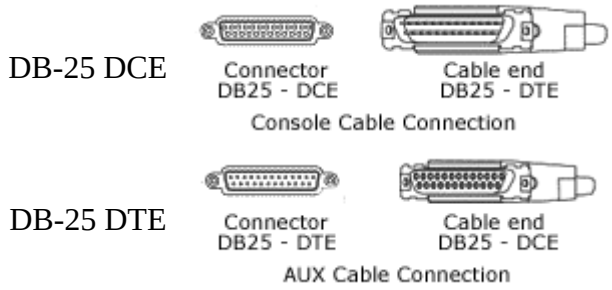
Ejemplo de una secuencia de arranque de un Router 2611

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 65536 Kbytes of main memory
program load complete, entry point: 0x80008000, size: 0x43b7fc

Self decompressing the image:
################################################################################################################
################################################################################################################
################################################################################################################
########################## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 17-Apr-01 04:55 by kellythw
Image text-base: 0x80008088, data-base: 0x8080853C

cisco 2611 (MPC860) processor (revision 0x203) with 56320K/9216K bytes of memory.
Processor board ID JAD05020BV5 (1587666027)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Press RETURN to get started!
00:00:09: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:00:09: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
00:00:09: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
00:00:09: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
00:00:10: %SYS-5-CONFIG_I: Configured from memory by console
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
00:00:13: %SYS-5-RESTART: System restarted -- Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 17-Apr-01 04:55 by kellythw
router>
```

Tipos de conectores para el puerto de Consola y AUX de routers Cisco

Los Routers de Cisco manejan tres tipos de conectores para usarse en el puerto de Consola o en el puerto AUX:

Conector	Imagen
RJ-45	

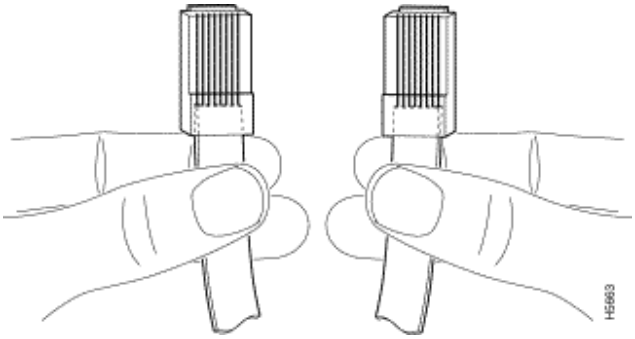


Los productos de Cisco usan los siguientes tipos de cables RJ-45:

- Straight-through o Derecho.
- Crossover o Cruzado.
- Rolled o Inverso.
- RJ-45 a DB9 Female

Cómo identificar un cable RJ-45

Para identificar el tipo de cable RJ-45, se sostienen los dos extremos del cable, de esta manera se pueden ver los colores de los cables dentro de los conectores.



Norma de cableado 568-A

Pin #	Par #	Función	Color del Cable
1	3	Transmite +	Blanco / Verde
2	3	Transmite -	Verde
3	2	Recibe +	Blanco / Naranja
4	1	Telefonía	Azul
5	1	Telefonía	Blanco / Azul
6	2	Recibe -	Naranja
7	4	Respaldo	Blanco / Marrón
8	4	Respaldo	Marrón

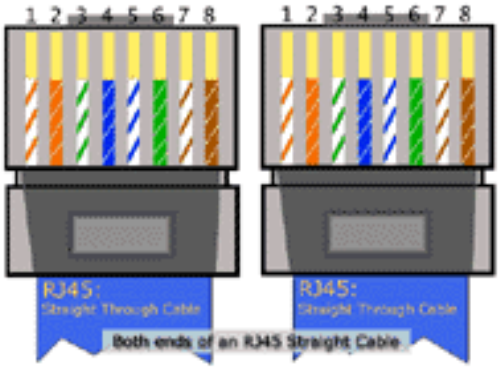
Norma de Cableado 568-B

Pin #	Par #	Función	Color del Cable
1	2	Transmite +	Blanco / Naranja
2	2	Transmite -	Naranja
3	3	Recibe +	Blanco / Verde
4	1	Telefonía	Azul
5	1	Telefonía	Blanco / Azul
6	3	Recibe -	Verde
7	4	Respaldo	Blanco / Marrón
8	4	Respaldo	Marrón

Se examina la secuencia del color de los cables para determinar el tipo de cable RJ-45, como sigue:

Cable Straight-through o Derecho

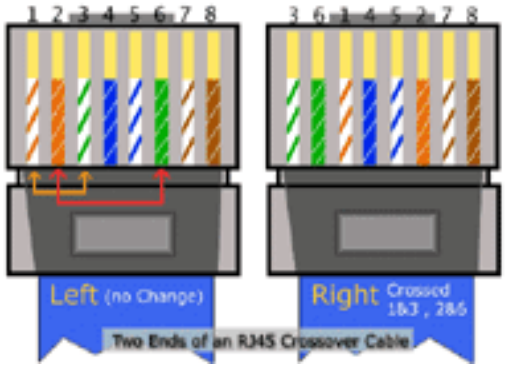
Igual pinado en ambos extremos.



Se utiliza en:
Router a Hub o Switch
Servidor a Hub o Switch
Estación de trabajo a Hub o Switch

Cable Crossover o Cruzado

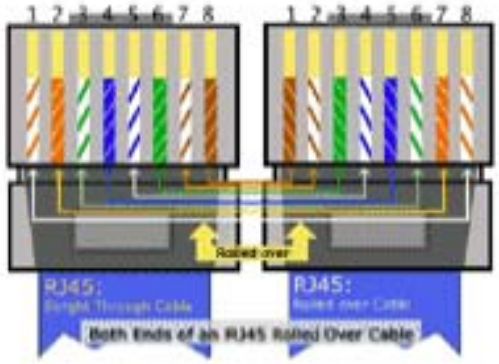
Se cruza el par 1-2 de un extremo con el 3-6 del otro, y el par 3-6 del primer extremo con el 1-2 del otro.



Se utiliza en:
Uplinks entre switches.
Hubs a switches.
Hub a Hub.
Puerto de un router a otro puerto de un router.
Conectar dos terminales directamente.

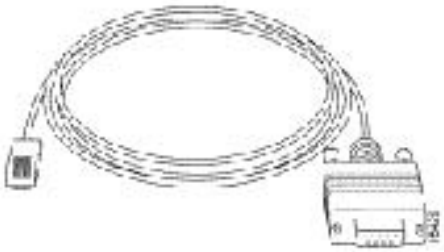
Cable Rolled o Inverso

El pinado en ambos extremos es inverso: 1-2-3-4-5-6-7-8 en un extremo, 8-7-6-5-4-3-2-1 en el otro.



Se utiliza en:
Conectarse al Puerto Consola de un dispositivo.

RJ-45 a DB-9 Female



Éste cable es también conocido como Cable de Consola (Management Cable) porque no requiere ningún adaptador ya que éste está integrado.

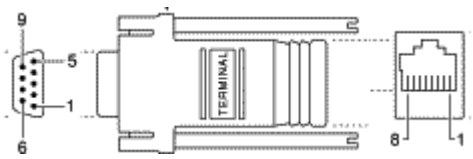
Adaptadores

Hay dos tipos de adaptadores necesarios para conectar una PC a un Router:

- Adaptador RJ-45 a DB-9
- Adaptador RJ-45 a DB-25

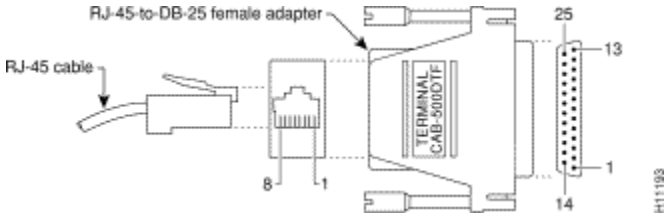
Adaptador RJ-45 a DB-9

Este adaptador conecta un Router a una PC en un puerto COM.



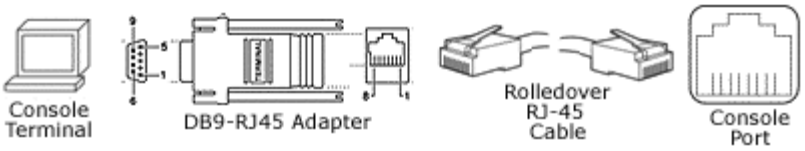
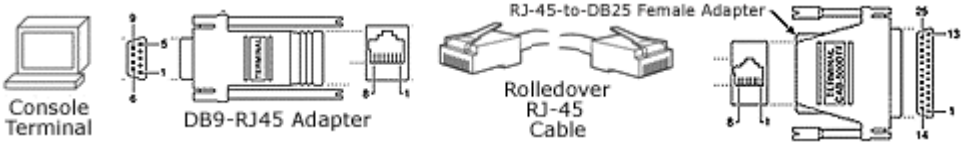
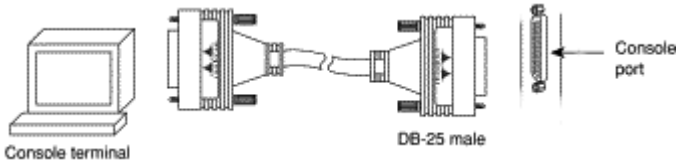
Adaptador RJ-45 a DB-25

Este adaptador conecta un Router a una PC en un puerto Serial.



Combinación de conexión del puerto Consola

Las maneras más comunes de conexión al puerto consola de un Router son:

Console Port	Cable	Adapter for PC	Adapter for Console Port
RJ-45	RJ-45 Rolled	DB-9 / DB-25	None
			
DB-25 DCE	RJ-45 Rolled	DB-9 / DB-25	RJ-45-to-DB-25
			
DB-25 DCE	DB-25	None	None
			

RJ-45	RJ-45-to-DB-9[1]	None	None

Criterio de Conexión

Dispositivo Terminal con dispositivo de acceso (Hub o Switch): *Cable Derecho*
Dispositivo de acceso entre sí: *Cable Cruzado*
Dispositivo de acceso con Router: *Cable Derecho*

Conexión al router para configurarlo

La configuración al router se puede hacer de diferentes maneras:

Puerto Consola

Conexión física: cable consola con conector RJ-45.
Requiere la utilización de un programa de emulación de terminal (por ejemplo Hyperterminal)
9600 baudios
8 bits de datos
Paridad ninguna
Bit de parada 2
Control de flujo ninguno
Por defecto no requiere password

Puerto Auxiliar

Conexión Física: cable consola con conector RJ-45.
Se puede utilizar también para configuración directa (no sólo por módem). Requiere la utilización de un programa de emulación de terminal (por ejemplo Hyperterminal).
9600 baudios
8 bits de datos
Paridad ninguna
Bit de parada 2
Control de flujo hardware
Por defecto no requiere password.

Terminal Virtual

Conexión física: se accede desde una terminal conectada a la red en cualquier punto de la misma.
Requiere la utilización del programa de emulación de terminales Telnet.
Por defecto requiere password, aunque ésta no esté configurada. Si no se configura el password, el router no permitirá el acceso por terminal virtual.

Modos al acceder al router

Hay diferentes modos en los que se puede presentar el prompt del IOS, además de que cada modo tiene diferentes opciones a ejecutar:

Modo Setup: Proceso paso a paso de la configuración de un router. Se activa automáticamente durante el proceso de inicialización cuando el router no puede encontrar un archivo de configuración válido en la NVRAM. Tiene dos opciones:

- Basic Managment: Sólo permite realizar una configuración básica para asegurar conectividad al router.
- Extended Setup: Permite además configurar algunos parámetros globales y las interfases.

Para abortar el desarrollo del modo setup se utiliza la combinación de teclas: Ctrl+C
Al terminar el proceso, el sistema muestra la nueva configuración y requiere la confirmación para grabarla y utilizarla.

Rommon> (ROM Monitor Mode, Modo monitor de ROM): Esta opción se presenta cuando hay un problema al cargar la IOS en la flash o simplemente se está accediendo a este modo de forma manual.

Router> (EXEC Mode, Modo usuario): Esta opción presenta algunos comandos sólo para visualizar información del software, hardware, estadísticas, flash, etc. pero sin poder cambiar o agregar parámetros en la configuración.

Router# (Privileged EXEC Mode, Modo Privilegiado): En este modo se pueden realizar cambios o agregar parámetros en la configuración, además de que se cuenta con más comandos para el monitoreo del equipo. Para acceder a este modo se debe de teclear enable en el modo usuario.

Router(config)# (Modo de configuración global): En este modo se pueden agregar o cambiar los parámetros que están en la configuración raíz; Se pueden agregar mapas, subinterfases y otras interfases de acuerdo a lo que se requiera.
Para acceder a la configuración global se teclea: configure Terminal

Router (config-mode) # (Otros modos específicos de configuración):

- Interface.
- Subinterface.
- Line.
- Router

Para acceder a estos modos de configuración primero se accede a la configuración global y después se teclea la interfase o línea a la cual se quiere ingresar. Para salir se teclea Ctrl + Z
Ejemplo:

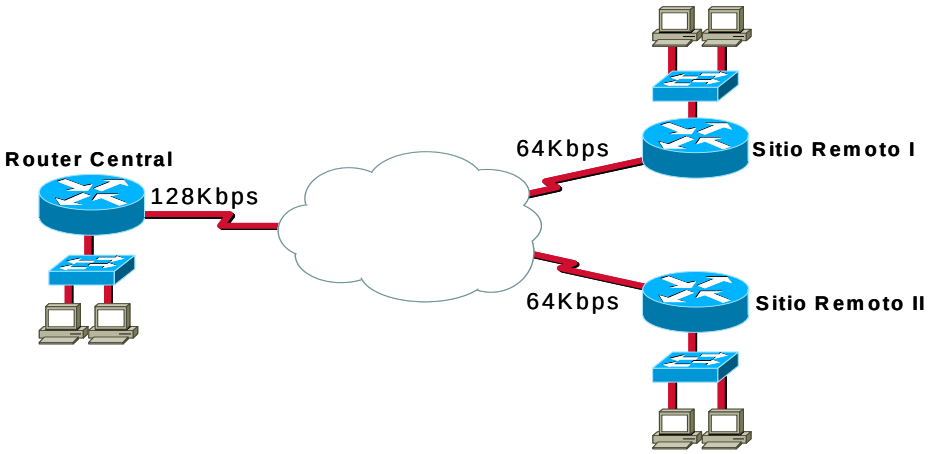
```
Router#configure terminal
Router(config)#interface [interface]
Router(config-if)#ip address [dirección] [máscara]
Router(config-if)#no shutdown
Router(config-if)#Ctrl + z
Router#
```

Capitulo 7

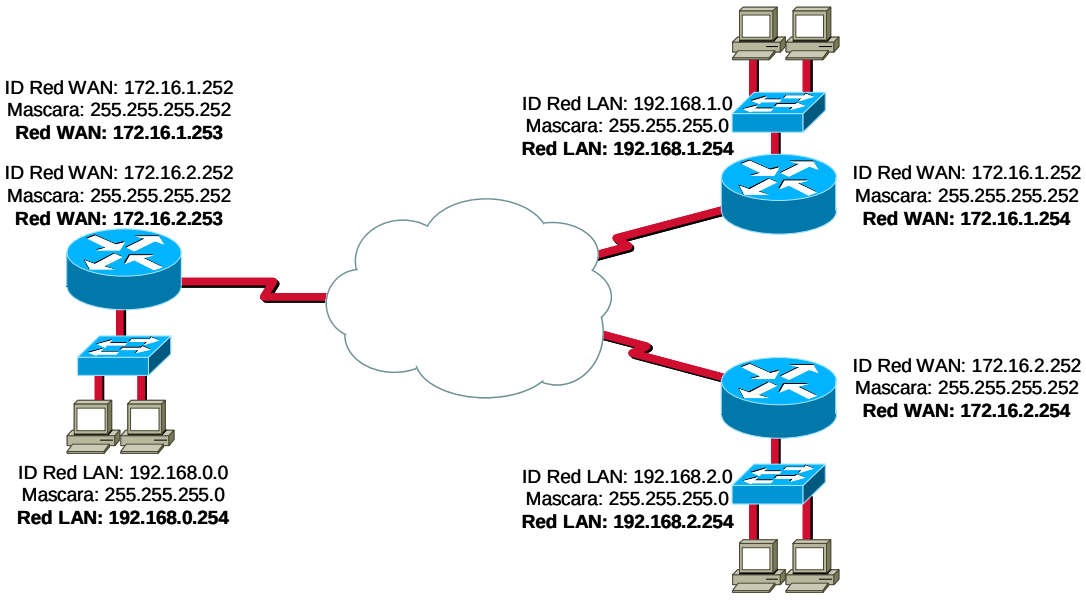
Creación de una Red utilizando Frame Relay

Para una empresa, una buena opción al momento de expandirse es utilizar enlaces de Frame Relay porque en ellos se puede emplear en el mismo enlace canal de voz para comunicarse al sitio sin generar cargos de larga distancia.

Tomemos como ejemplo una empresa la cual quiere abrir dos sucursales; El esquema de la red quedaría de la siguiente manera:



El ancho de banda que tendrá el nodo central será de 128Kbps y los dos sitios de 64Kbps cada uno. El ancho de banda del enlace central deberá ser mayor o igual a la suma del ancho de banda de los PVCs que se conectan a este enlace.
Esta empresa tiene 20 PCs en operación y cada una de ellas tiene un direccionamiento el cual únicamente funcionaba internamente debido a que no tenía comunicación con otro sitio. A raíz de la expansión de la red se tiene que hacer un adecuado direccionamiento para futuras expansiones y no desperdiciar direcciones IPs, siendo así una red escalable. Además, una red escalable le permite al router hacer un mejor enrutamiento de los paquetes.
El direccionamiento IP que vamos a utilizar es el siguiente:



	ID de la Red	Nodo Central	Sitio Remoto 1	Sitio Remoto 2
Dirección WAN	172.16.1.252	172.16.1.253	172.16.1.254	
	172.16.2.252	172.16.2.253		172.16.2.254
Dirección LAN	192.168.0.0	192.168.0.254		
	192.168.1.0		192.168.1.254	
	192.168.2.0			192.168.2.254

Configuración del Router

Para configurar el Router Cisco se accede desde el puerto de consola, se presiona enter para poder acceder y después el comando enable para entrar en el modo privilegiado.

```
Router Con0 is now available


Press RETURN to get started!


Router>enable
Router#
```

Con el commando “show running-config” desplegaremos la configuración que tiene el equipo.

```
Router#show running-config

Building configuration...
Current configuration : 625 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
ip subnet-zero
!
!
!
!
!
interface FastEthernet0/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial0/0
  no ip address
  no ip directed-broadcast
  shutdown
!
!
ip classless
!
!
!
line con 0
line aux 0
line vty 0 4
  login
!
end

Router#
```

Configuración de las Interfases en el Router

Estando dentro del equipo, se ingresa el comando "hostname" para cambiar el nombre del router y saber que equipo es el que estaremos modificando; Para modificar la configuración del router se ingresa el comando "configure terminal".

En la interfase de la FastEthernet 0/0 se configurará lo siguiente:

- Descripción de la interfase.
- Dirección IP.
- Modo de operación “full-duplex”.
- El comando “no shutdown” para activar la interfase.

```
Router(config)#hostname Router_Central
Router_Central(config)#
Router_Central(config)#interface FastEthernet0/0
Router_Central(config-if)#description RED DE AREA LOCAL
Router_Central(config-if)#ip address 192.168.0.254 255.255.255.0
Router_Central(config-if)#full-duplex
Router_Central(config-if)#no shutdown
09:16:21 %LINK-3-UPDOWN:  Interface Fastethernet0/0, changed state to up

09:16:21 %LINEPROTO-5-UPDOWN: Line protocol on Interface Fastethernet0/0, changed state to up

Router_Central(config-if)#
```

Se ingresa ahora a la interfase serial 0/0 en la cual no se utilizará una dirección IP debido a que se utilizarán sub-interfases para varios PVCs.

En esta interfase se configurará lo siguiente:

- Descripción del enlace.
- Ancho de banda.
- Tipo de encapsulación "Frame Relay".
- El comando "frame-relay traffic-shaping" que servirá para que se pueda ingresar voz en el enlace de Frame Relay.
- Tipo de LMI (Local Management Interface) el cual tiene 3 opciones "cisco, ansi y q933a", en donde el más utilizado es el ansi que es el que entrega la compañía proveedora del servicio.
- El comando "no shutdown" para activar la interfase.

```
Router_Central(config)#
Router_Central(config)#interface Serial0/0
Router_Central(config-if)#description ENLACE PRINCIPAL
Router_Central(config-if)#bandwidth 128
Router_Central(config-if)#no ip address
Router_Central(config-if)#encapsulation frame-relay
Router_Central(config-if)#frame-relay traffic-shaping
Router_Central(config-if)#frame-relay lmi-type ansi
Router_Central(config-if)#no shutdown
09:17:04 %LINK-3-UPDOWN:  Interface Serial0/0, changed state to up

09:17:04 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

Router_Central(config-if)#
```

Creación de Subinterfases en el Router

Se configurarán sub-interfases para utilizarse varios PVCs en el mismo enlace; Se configurará lo siguiente en cada sub-interfase:

- EL número de la sub-interfase asociada al número del DLCI provisto por el proveedor del servicio para identificar más rápido el PVC.
- Descripción del enlace.
- Ancho de Banda utilizado.
- Dirección IP.
- DLCI que se utilizará en la subinterfase.
- El comando “class” seguido del nombre que identificará el mapa asociado.
- El comando “vofr cisco” que se utiliza para activar los canales de voz.

```
Router_Central(config)#interface Serial0/0.16 point-to-point
Router_Central(config-subif)#description CONEXION CON SITIO REMOTO I
Router_Central(config-subif)#bandwidth 64
Router_Central(config-subif)#ip address 172.16.1.253 255.255.255.252
Router_Central(config-subif)#frame-relay interface-dlci 16
Router_Central(config-fr-dlci)#class FR64-VOZ
%Creating new map-class.
Router_Central(config-fr-dlci)#vofr cisco
Router_Central(config-fr-dlci)#^Z
Router_Central#

Router_Central(config)#interface Serial0/0.17 point-to-point
Router_Central(config-subif)#description CONEXION CON SITIO REMOTO II
Router_Central(config-subif)#bandwidth 64
Router_Central(config-subif)#ip address 172.16.2.253 255.255.255.252
Router_Central(config-subif)#frame-relay interface-dlci 17
Router_Central(config-fr-dlci)#class FR64-VOZ
Router_Central(config-fr-dlci)#vofr cisco
Router_Central(config-fr-dlci)#^Z
Router_Central#
```

El comando "class" se utiliza para asociar la sub-interfase con un mapa, el cual contiene parámetros que configurarán el ancho de banda del enlace así como el del canal de voz.
En este caso se está utilizando el nombre de "FR64-VOZ" el cual nos ayudará a identificar el mapa que se está utilizando en esta sub-interfase en caso de tener varias y con diferentes anchos de banda.

Creación de un Mapa

Para configurar el mapa se agregan los siguientes parámetros que son utilizados en la red de Frame Relay:

```
Router_Central(config)#map-class frame-relay FR64-VOZ
Router_Central(config-map-class)#frame-relay cir 64000
Router_Central(config-map-class)#frame-relay bc 640
Router_Central(config-map-class)#frame-relay be 0
Router_Central(config-map-class)#frame-relay mincir 64000
Router_Central(config-map-class)#frame-relay fair-queue
Router_Central(config-map-class)#frame-relay voice bandwidth 48000
Router_Central(config-map-class)#frame-relay fragment 80
Router_Central(config-map-class)#no frame-relay adaptive-shaping becn
Router_Central(config-map-class)#^Z
Router_Central#
```

Asignación del número del Canal de Voz en los puertos

Para asignar el número del canal de voz y se puedan comunicar a este sitio, se ingresará lo siguiente:

```
Router_Central(config)#dial-peer voice 1 pots
Router_Central(config-dial-peer)#destination-pattern 100
Router_Central(config-dial-peer)#port 1/0/0
Router_Central(config-dial-peer)#
```

```
Router_Central(config-dial-peer)#dial-peer voice 2 pots
Router_Central(config-dial-peer)#destination-pattern 100
Router_Central(config-dial-peer)#port 1/0/1
Router_Central(config-dial-peer)#
Router_Central(config-dial-peer)#dial-peer voice 3 pots
Router_Central(config-dial-peer)#destination-pattern 100
Router_Central(config-dial-peer)#port 1/1/0
Router_Central(config-dial-peer)#
Router_Central(config-dial-peer)#dial-peer voice 4 pots
Router_Central(config-dial-peer)#destination-pattern 100
Router_Central(config-dial-peer)#port 1/1/1
Router_Central(config-dial-peer)#^Z
Router_Central#
```

Para comunicarse a otro sitio, se ingresa lo siguiente:

- El dial-peer que se utilizará para identificar el marcado.
- El número de destino.
- La interfase y el DLCI que se utilizará como salida para comunicarse.

```
Router_Central(config)#dial-peer voice 101 vofr
Router_Central(config-dial-peer)#destination-pattern 101
Router_Central(config-dial-peer)#session target Serial0/0 16
Router_Central(config-dial-peer)#
Router_Central(config-dial-peer)#dial-peer voice 102 vofr
Router_Central(config-dial-peer)#destination-pattern 102
Router_Central(config-dial-peer)#session target Serial0/0 17
Router_Central(config-dial-peer)#^Z
Router_Central#
```

Protocolo de Ruteo

Para comunicarse el router con otros nodos, necesita de un protocolo de ruteo. El protocolo deberá tener configuradas las redes directamente conectadas para poder hacer el enrutamiento de paquetes a su destino; Existen diversos protocolos, por ejemplo: Rip, OSPF, IGRP, EIGRP, IS-IS, BGP; En este caso utilizaremos EIGRP con el sistema autónomo 1.

Se configure lo siguiente en el protocolo de ruteo:

- El AS (Sistema Autónomo) que se utilizará, que deberá ser el mismo en cada router que se conecte.
- Las redes directamente conectadas.

```
Router_Central(config)#router eigrp 1
Router_Central(config-router)#network 172.16.0.0
Router_Central(config-router)#network 192.168.0.0
Router_Central(config-router)#
Router_Central#
```

Todo lo realizado anteriormente se realiza en los otros dos nodos cambiando la sub-interfase de acuerdo al sitio y cambiando el número a marcar por canal de voz.

Configuración Final en los Routers

La configuración en el Router Central quedaría de la siguiente manera:

```
Router_Central#show running-config

Building configuration...
Current configuration : 625 bytes
!
!
version 12.1
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname Router_Central
!
enable password cisco
ip subnet-zero
!
!
!
interface FastEthernet0/0
 description RED DE AREA LOCAL
 ip address 192.168.0.254 255.255.255.0
!
!
interface Serial0/0
 description ENLACE PRINCIPAL
 bandwidth 128
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
!
interface Serial0/0.16 point-to-point
 description CONEXION CON SITIO REMOTO I
 bandwidth 64
 ip address 172.16.1.253 255.255.255.252
 frame-relay interface-dlci 16
  class FR64-VOZ
  vofr cisco
!
!
interface Serial0/0.17 point-to-point
 description CONEXION CON SITIO REMOTO II
 bandwidth 64
 ip address 172.16.2.253 255.255.255.252
 frame-relay interface-dlci 17
  class FR64-VOZ
  vofr cisco
!
router eigrp 1
 network 172.16.0.0
 network 192.168.0.0
!
map-class frame-relay FR64-VOZ
 no frame-relay adaptive-shaping
 frame-relay cir 64000
 frame-relay bc 640
 frame-relay be 0
 frame-relay mincir 64000
 frame-relay fair-queue
 frame-relay voice bandwidth 24000
 frame-relay fragment 80
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer cor custom
!
dial-peer voice 1 pots
 destination-pattern 100
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 100
 port 1/0/1
!
dial-peer voice 3 pots
 destination-pattern 100
 port 1/1/0
!
dial-peer voice 4 pots
 destination-pattern 100
 port 1/1/1
!
!
dial-peer voice 101 vofr
 destination-pattern 101
 session target Serial0/0 16
!
dial-peer voice 102 vofr
 destination-pattern 102
 session target Serial0/0 17
!
!
!
banner login ^C
ACCESO RESTRINGIDO, CUALQUIER ABUSO SERA CASTIGADO
^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
End
```

La configuración del Sitio Remoto I quedaría de la siguiente manera:

```
Sitio_Remoto_I#show running-config

Building configuration...
Current configuration : 625 bytes
!
version 12.1
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname Sitio_Remoto_I
!
enable password cisco
ip subnet-zero
!
!
!
interface FastEthernet0/0
 description RED DE AREA LOCAL
 ip address 192.168.1.254 255.255.255.0
 speed 100
 full-duplex
!
interface Serial0/0
 description SITIO REMOTO I
 bandwidth 64
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/0.16 point-to-point
 description CONEXION CON ROUTER CENTRAL
 ip address 172.16.1.254 255.255.255.252
 frame-relay interface-dlci 16
  class FR64-VOZ
  vofr cisco
!
!
router eigrp 1
 network 172.16.0.0
 network 192.168.0.0
!
!
map-class frame-relay FR64-VOZ
 no frame-relay adaptive-shaping
 frame-relay cir 64000
 frame-relay bc 640
 frame-relay be 0
 frame-relay mincir 64000
 frame-relay fair-queue
 frame-relay voice bandwidth 24000
 frame-relay fragment 80
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 101
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 101
 port 1/0/1
!
dial-peer voice 100 vofr
 destination-pattern 100
 session target Serial0/0 16
!
dial-peer voice 102 vofr
 destination-pattern 102
 session target Serial0/0 16
!
banner login ^C
ACCESO RESTRINGIDO, CUALQUIER ABUSO SERA CASTIGADO
^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

La configuración del Sitio Remoto II quedaría de la siguiente manera:

```
Sitio_Remoto_II#show running-config

Building configuration...
Current configuration : 625 bytes
!
version 12.1
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname Sitio_Remoto_II
!
enable password cisco
ip subnet-zero
!
!
interface FastEthernet0/0
 description RED DE AREA LOCAL
 ip address 192.168.2.254 255.255.255.0
 speed 100
 full-duplex
!
interface Serial0/0
 description SITIO REMOTO II
 bandwidth 64
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/0.17 point-to-point
 description CONEXION CON ROUTER CENTRAL
 ip address 172.16.2.254 255.255.255.252
 frame-relay interface-dlci 17
  class FR64-VOZ
  vofr cisco
!
router eigrp 1
 network 172.16.0.0
 network 192.168.0.0
!
!
map-class frame-relay FR64-VOZ
 no frame-relay adaptive-shaping
 frame-relay cir 64000
 frame-relay bc 640
 frame-relay be 0
 frame-relay mincir 64000
 frame-relay fair-queue
 frame-relay voice bandwidth 24000
 frame-relay fragment 80
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 102
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 102
 port 1/0/1
!
dial-peer voice 100 vofr
 destination-pattern 100
 session target Serial0/0 17
!
dial-peer voice 101 vofr
 destination-pattern 101
 session target Serial0/0 17
!
banner login ^C
ACCESO RESTRINGIDO, CUALQUIER ABUSO SERA CASTIGADO
^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Equipo Utilizado por la Compañía Proveedora del Servicio

La compañía proveedora del servicio, utiliza equipos NTU (Network Terminal Equipment) en donde entregan el servicio.
Hay diferentes tipos de NTU donde entregan el servicio: Martis, Tellabs, Watson, Metrodata, donde se configuran los Time slots (Ts) para proporcionar el enlace solicitado.

Estos son algunos ejemplos de NTU:

Equipo o Tarjeta Tellabs

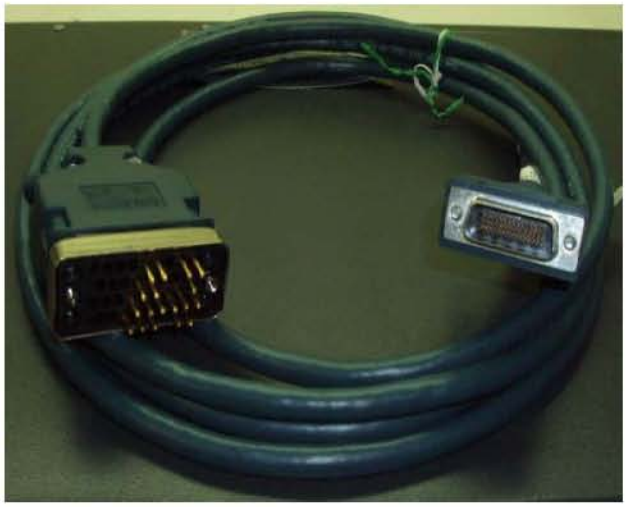
Equipo o Tarjeta Watson

Equipo o Tarjeta Adtran

Parte posterior de equipo Tellabs

Las NTUs se conectan a la tarjeta serial del router con un cable V.35 a serial

Tarjeta WIC-1T



Cable V.35 a Serial

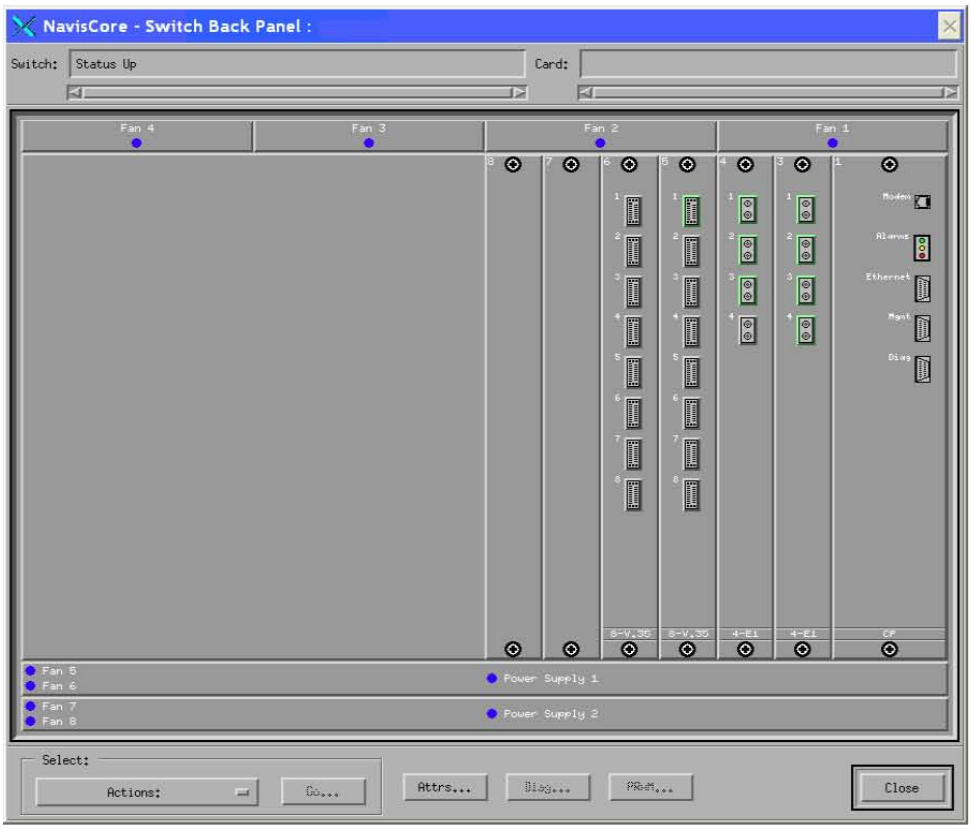
La compañía proveedora del servicio, tiene switches Frame Relay en toda la Republica Mexicana, los cuales se interconectan por enlaces STM-16, STM-4, y E1s.

Los switches de Frame Relay son como el siguiente:

En la parte posterior de estos equipos se encuentran los puertos útiles para conectar la NTU o conectar el router. Este equipo se encuentra en las centrales telefónicas, donde se descanaliza para entregar enlaces desde los 64Kbps hasta E1s para después distribuirlo a lo conocido como la última milla; En ocasiones este tipo de equipo lo tiene algún cliente en su sitio porque está utilizando varios E1s.

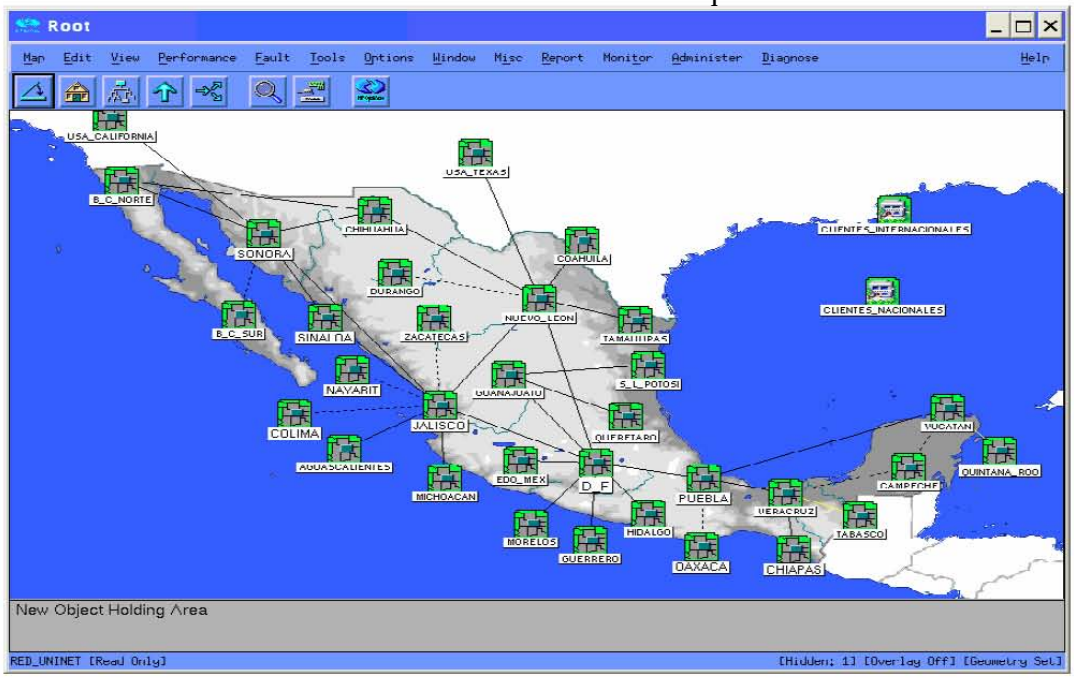
La operación de estos equipos incurre en la utilización de un software que los administra de manera remota, en donde se muestra la parte posterior del equipo y los puertos que se pueden utilizar para entregar el servicio.

La imagen siguiente es una muestra de la parte posterior del switch mostrado anteriormente pero desde el software que lo administra de manera remota:



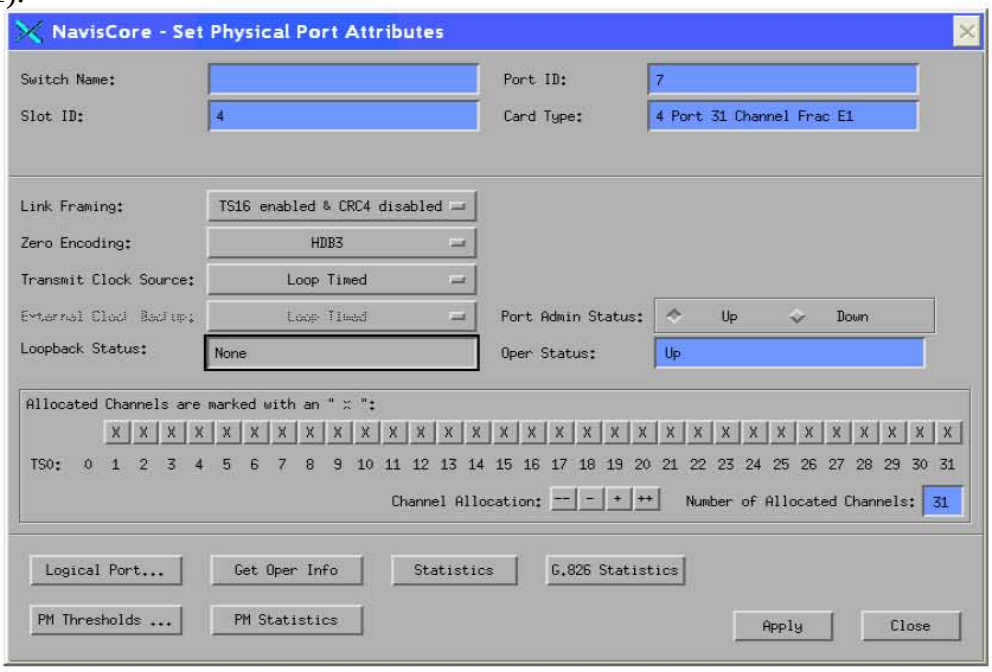
Configuración del Switch de Frame Relay

De manera remota se accede al switch de acuerdo a la ubicación que tiene el sitio del cliente.



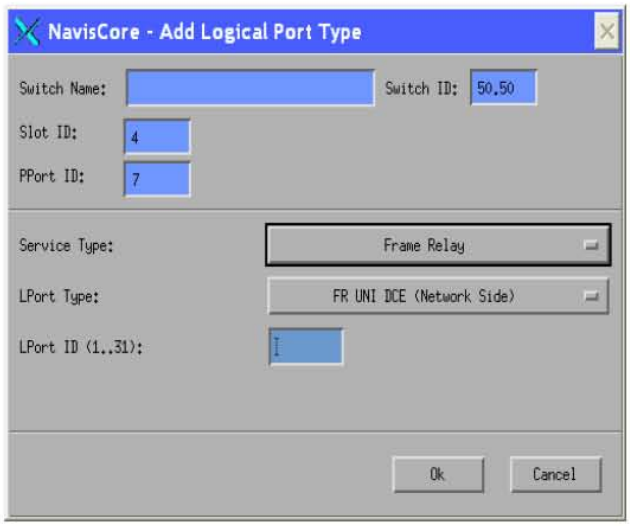
Puerto Físico del Switch

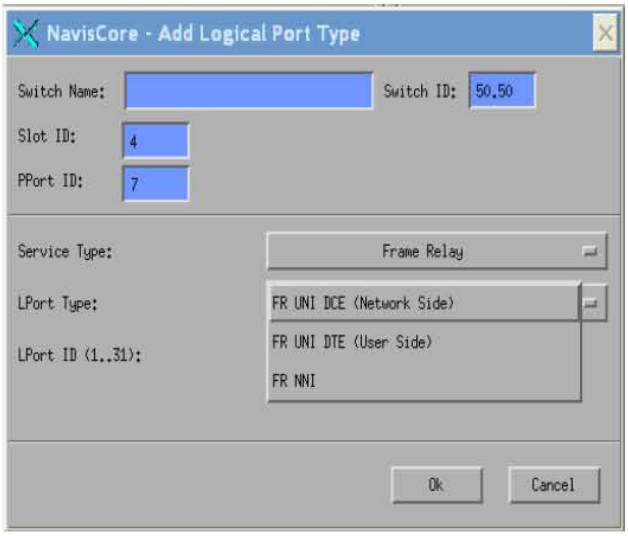
El puerto físico es la salida que tiene el switch en donde se entregará el servicio. Para configurarlo se accede al puerto físico del switch de manera remota y se configura la capacidad completa del puerto (que es un E1).



Puerto Lógico del Switch

Después de configurar el puerto físico, se tiene que configurar el puerto lógico.
El puerto lógico sirve para asignar a un cliente cierta cantidad de ancho de banda en el E1 del puerto físico.



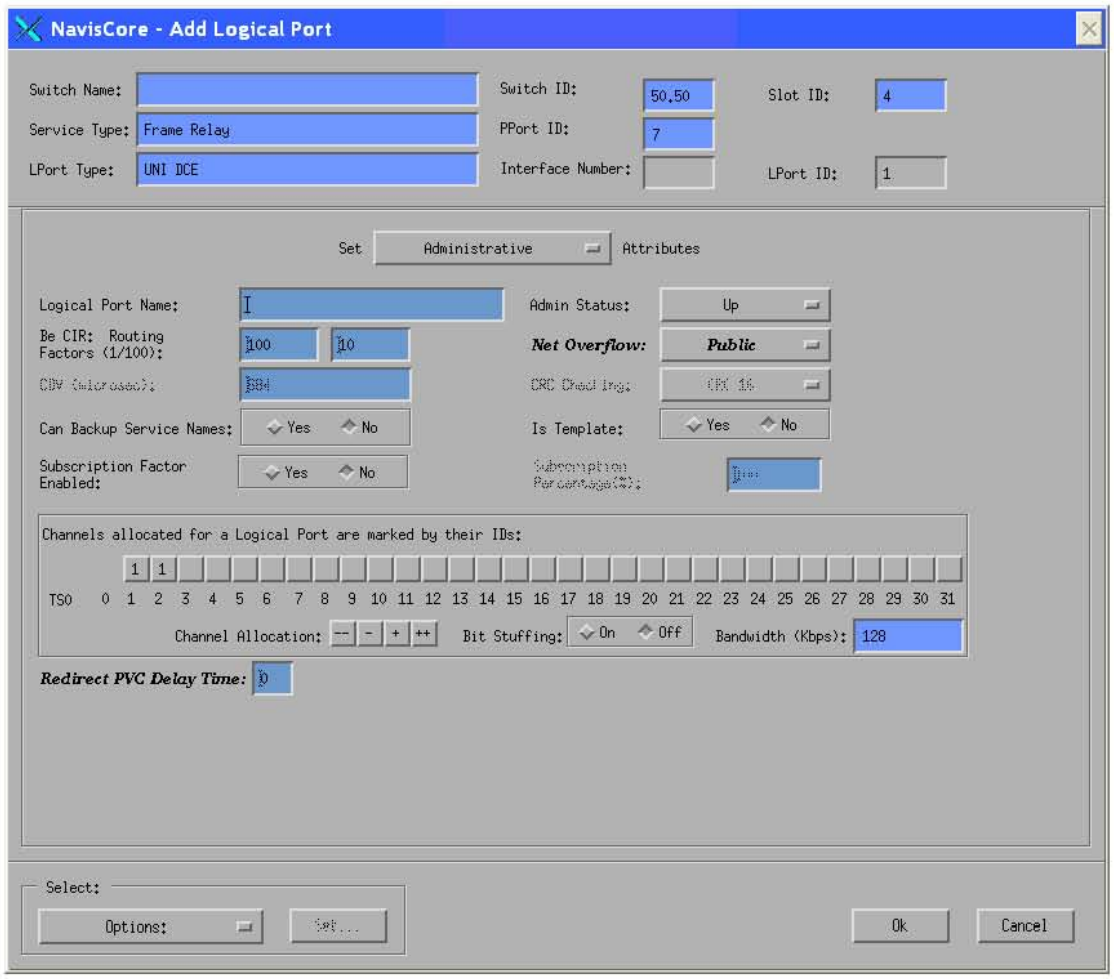


En la creación del puerto lógico se emplean diferentes tipos para entregar el servicio:

- FR UNI DCE (Network Side), Frame Relay User-Network Interface Data Communications Equipment: El switch entrega el reloj de sincronía o velocidad del enlace.
- FR UNI DTE (User Side), Frame Relay User-Network Interface Data Terminal Equipment: El equipo del cliente entrega el reloj de sincronía o velocidad del enlace.
- FR NNI, Frame Relay Network to Network Interface: El switch se conecta con otro switch.

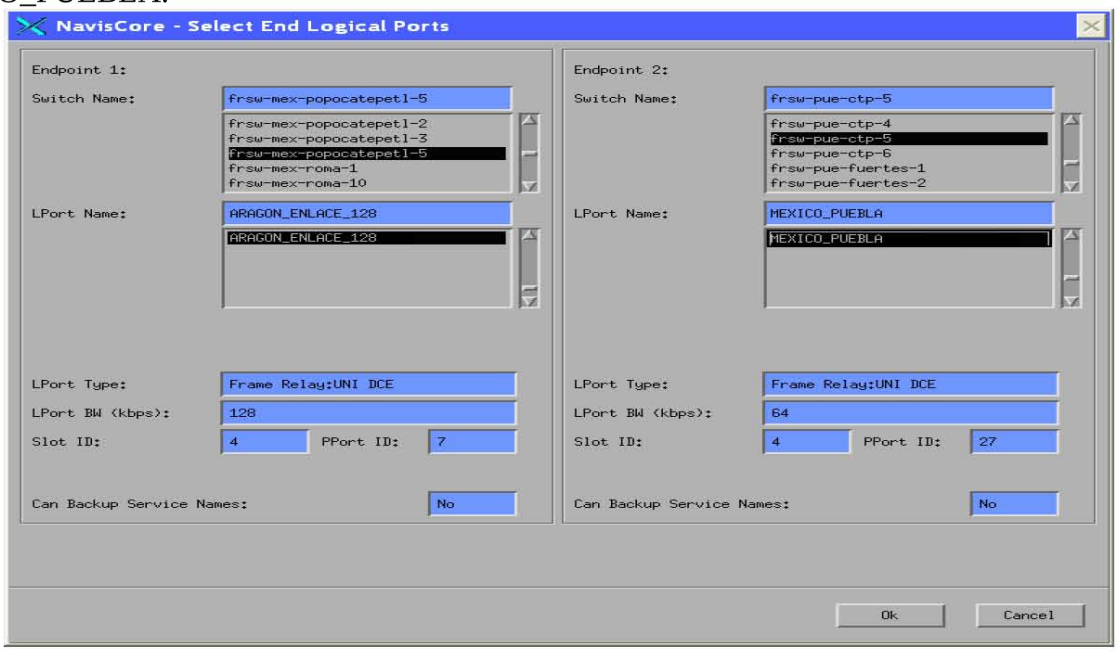
En la opción LPort ID se agrega un número del 1 al 31 (que son los correspondientes al E1) para identificar los Ts (Time slots) que se están empleando en el puerto lógico.

Para finalizar la creación del Puerto Lógico, se seleccionan los canales o Ts (Time slots) que se emplearán en el enlace. En este caso se utilizarán solo dos Ts para proporcionar 128Kbps en el nodo central y un Ts para cada uno de los sitios remotos.

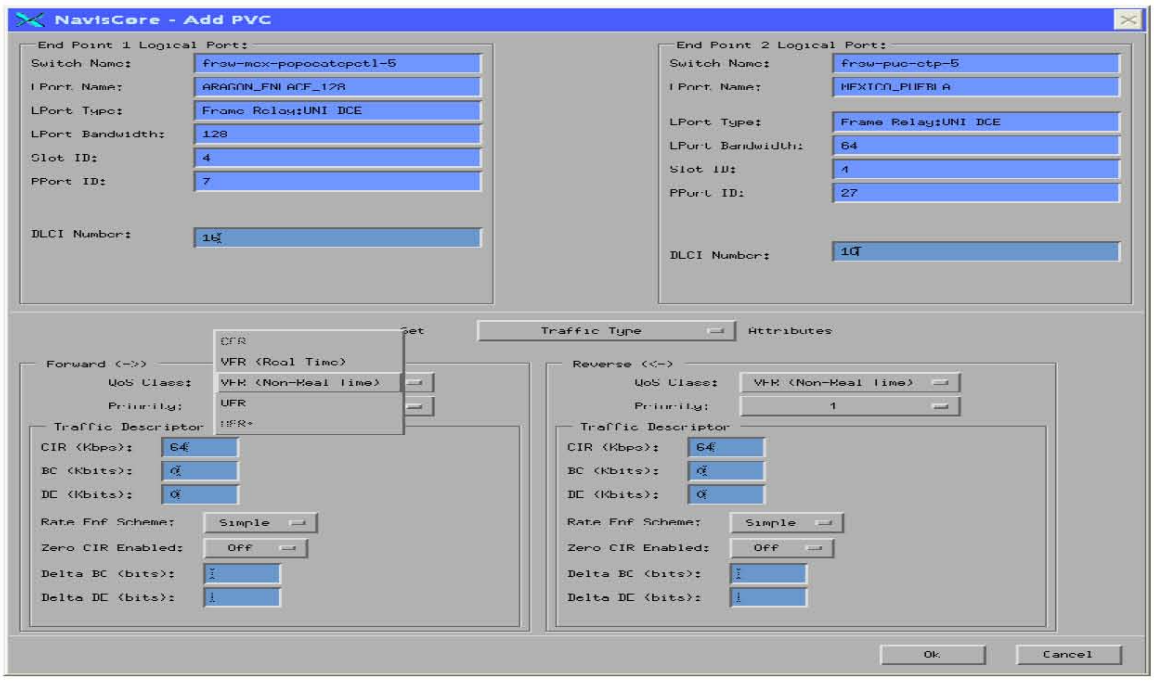


Creación del PVC en el Switch de Frame Relay

Primero se seleccionan los puertos lógicos configurados anteriormente en el switch para poder crear el PVC entre ellos.
En este caso se crearon los puertos lógicos con el nombre de ARAGON_ENLACE_128 y MEXICO_PUEBLA.



Después de seleccionar los puertos lógicos se tiene que configurar el nombre del PVC, el CIR que tendrá el enlace, el DLCI que se utilizará para identificarlo, la clase de QoS y la prioridad que tendrá el servicio.

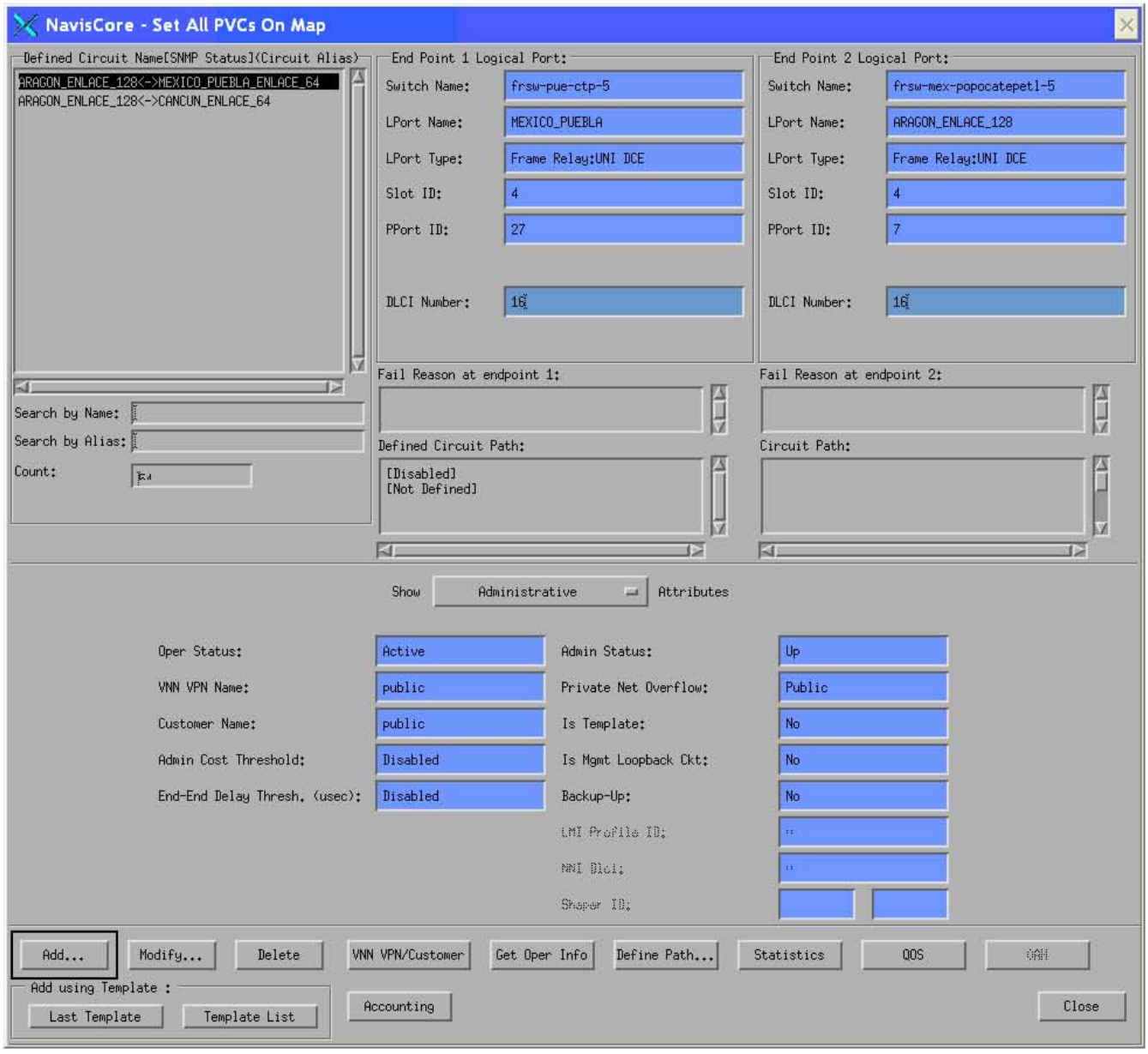


Revisión de los PVCs en el Switch de Frame Relay

Los PVCs se pueden verificar en el software si están activos, quedando de la siguiente manera:

El enlace de ARAGON_ENLACE_128 tiene conexión con los enlaces: MEXICO_PUEBLA_ENLACE_64 y CANCUN_ENLACE_64.

Si el enlace está activo, en la opción de Fail Reason at endpoint no debe aparecer ninguna de las dos puntas, en caso contrario se mostrará hacia que punta el enlace está caído.



Revisión de los PVCs en el Router

En el router central y en los sitios remotos, se puede verificar si el PVC ya está activo. Primero aplicamos el comando “show ip interface brief” para revisar el estado de las interfases; Si el Status y el protocolo aparece down el PVC está inactivo.

```
Router_Central#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.0.254   YES NVRAM  up                    up
Serial0/0                  unassigned      YES manual up                    up
Serial0/0.16               172.16.1.253    YES manual up                    up
Serial0/0.17               172.16.2.253    YES manual up                    up
```

También podemos aplicar el siguiente comando “show frame-relay pvc” para revisar el estado del PVC.
Si el PVC está activo, en el estado del PVC se muestra ACTIVE, si se observa DELETED o INACTIVE, el PVC ha sido borrado o está fuera de servicio.

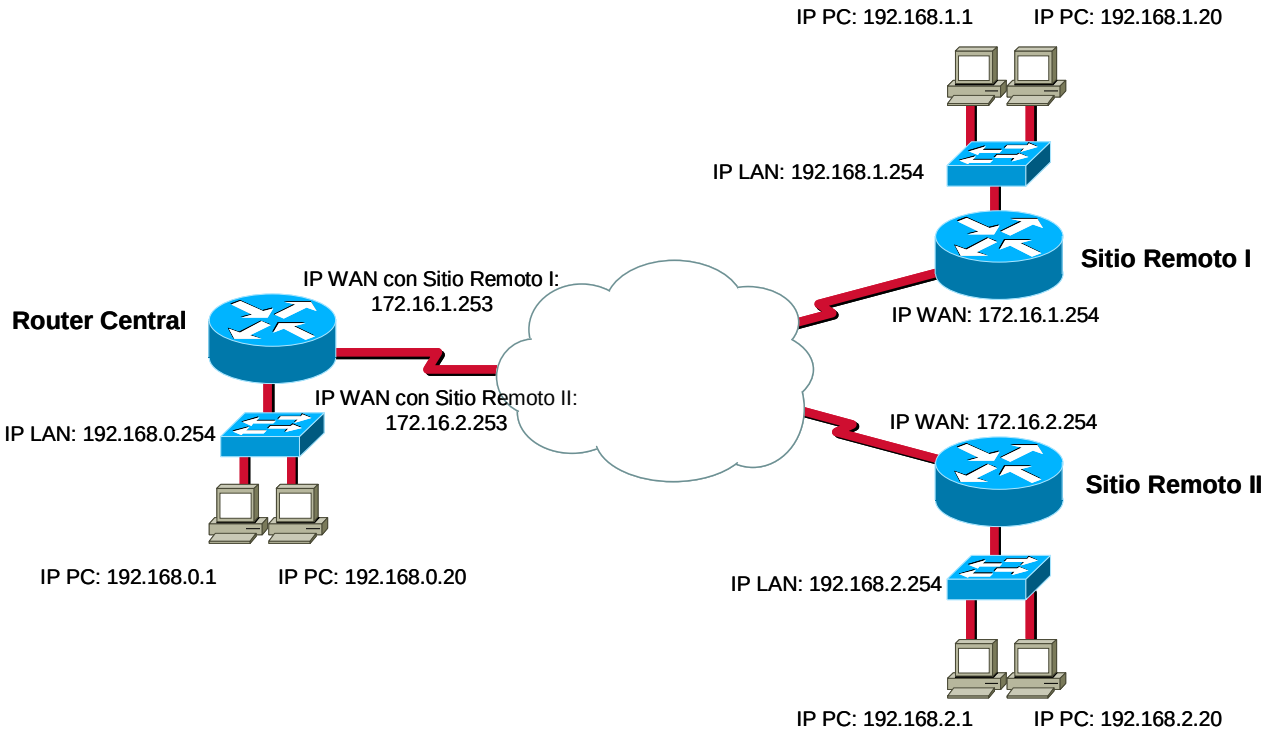
```
Router_Central#show frame-relay pvc 16

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.16

  input pkts 1             output pkts 4            in bytes 564
  out bytes 2246           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 4         out bcast bytes 2246
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:02:41, last time pvc status changed 00:00:00

Router_Central#show frame-relay pvc 17

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0.17

  input pkts 2             output pkts 5            in bytes 1123
  out bytes 2820           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 5         out bcast bytes 2820
  5 minute input rate 1000 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
  pvc create time 00:02:42, last time pvc status changed 00:00:01
```

Se puede mostrar el estado de las sub-interfases con el comando “show interfaces”

```
Router_Central#show interfaces

Serial0/0.16 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.1.253/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never

Serial0/0.17 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.2.253/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never
```

Comunicación con los sitios por Datos y Canal de Voz

Para verificar si ya se tiene comunicación desde el router a los otros sitios e inclusive a las PCs que se tienen conectadas, se manda un ping desde la PC con dirección IP 192.168.0.1 conectada en la red Lan del Router Central hacia la IP WAN del router del sitio I y II, además de mandarlo también a una PC que está dentro de la red local de cada sitio.



Desde la PC con IP 192.168.0.1 se manda un ping a la dirección IP WAN del router del Sitio Remoto I

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Reply from 172.16.1.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.1.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.1.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.1.254 ;bytes=32 time=22ms TTL=254

Ping Statistics for 172.16.1.254:
    Packets Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

Ahora a una PC que está en la red LAN del Sitio Remoto I

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.1.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.1.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.1.1 ;bytes=32 time=22ms TTL=254

Ping Statistics for 192.168.1.1:
    Packets Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

La comunicación con el Sitio Remoto I ha sido exitosa.

Se manda un ping a la dirección IP WAN del router del Sitio Remoto II

```
C:\>ping 172.16.2.254

Pinging 172.16.2.254 with 32 bytes of data:

Reply from 172.16.2.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.2.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.2.254 ;bytes=32 time=22ms TTL=254
Reply from 172.16.2.254 ;bytes=32 time=22ms TTL=254

Ping Statistics for 172.16.2.254:
    Packets Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

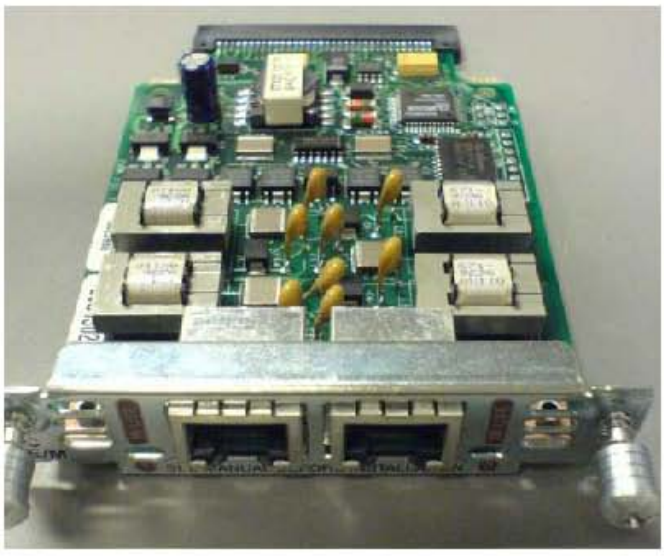
Ahora a una PC que está en la red LAN del Sitio Remoto II

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.2.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.2.1 ;bytes=32 time=22ms TTL=254
Reply from 192.168.2.1 ;bytes=32 time=22ms TTL=254

Ping Statistics for 192.168.2.1:
    Packets Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

La comunicación por datos hacia los dos sitios remotos ha sido exitosa; Ahora se procede a revisar los canales de voz.

En los tres routers (Router Central, Sitio Remoto I y Sitio Remoto II) se tienen instaladas tarjetas FXS, estas tarjetas proveen el tono de invitación a marcar y funcionan conectando un teléfono analógico en cualquier puerto de la tarjeta; Hay tarjetas FXO y E&M que necesitan de un conmutador para que provea la señalización y genere el tono de invitación a marcar.

Tarjeta VIC-2FXS



Tarjeta VIC-2E&M

Se utiliza el comando “show voice call summary” para ver el estado de los puertos.

```
Router_Central#show voice call summary
PORT         CODEC    VAD VTSP STATE              VPM STATE
============ ======== === ==================== ======================
1/0/0           -         -  -                      FXSLS_ONHOOK
1/0/1           -         -  -                      FXSLS_ONHOOK
1/1/0           -         -  -                      FXSLS_ONHOOK
1/1/1           -         -  -                      FXSLS_ONHOOK
```

Con el comando “show dial-peer voice summary” se puede verificar el plan de marcación que se tiene en el router, en donde se indica el número de destino que se tiene en los puertos así como el número que se tiene que marcar para que el router enrute la llamada por el DLCI 16 o 17.

```
Router_Central#show dial-peer voice summary
dial-peer hunt 0
              AD                                      PRE PASS
TAG    TYPE   MIN  OPER PREFIX    DEST-PATTERN       FER THRU SESS-TARGET   PORT
1      pots   up   up             100                 0                     1/0/0
2      pots   up   up             100                 0                     1/0/1
3      pots   up   up             100                 0                     1/1/0
4      pots   up   up             100                 0                     1/1/1
101    vofr   up   up             101                 0  syst Serial0/0 16
102    vofr   up   up             102                 0  syst Serial0/0 17
```

Cuando se realice una llamada por el canal de voz se puede verificar con el comando “show voice call summary”. Para saber si se estableció la llamada, tiene que aparecer CONNECT y el codec que se está empleando para comprimir la voz al enviarla por el enlace.

```
Router_Central#show voice call summary
PORT         CODEC    VAD VTSP STATE              VPM STATE
============ ======== === ==================== ======================
1/0/0           g729r8    y  S_CONNECT             FXSLS_CONNECT
1/0/1           g729r8    y  S_CONNECT             FXSLS_CONNECT
1/1/0           -         -  -                      FXSLS_ONHOOK
1/1/1           -         -  -                      FXSLS_ONHOOK
```

Para finalizar se puede corroborar la llamada con el comando “show call active voice brief”, además de que despliega el número de donde se está llamando y hacia donde.

```
Router_Central#show call active voice brief

12B4 : 24087028hs.1 +251 pid:1 Answer 100 active
 dur 00:01:38 tx:3212/96223 rx:1032/30960
 Tele 1/0/0:259: tx:99830/30960/0ms g729r8 noise:-53 acom:19  i/0:-50/-45 dBm

12B4 : 24087176hs.1 +103 pid:3 Originate 101 active
 dur 00:01:38 tx:1032/34056 rx:3212/99438
 FR cisco-switched [Serial0/0 16 37] vad:Y dtmf:N seq:N g729r8 (30)

12B7 : 24094192hs.1 +867 pid:2 Answer 100 active
 dur 00:00:21 tx:817/24305 rx:834/25020
 Tele 1/0/1:261: tx:28040/25030/0ms g729r8 noise:-47 acom:14  i/0:-43/-28 dBm

12B7 : 24094346hs.1 +713 pid:3 Originate 102 active
 dur 00:00:21 tx:834/27522 rx:817/25127
 FR cisco-switched [Serial0/0 17 38] vad:Y dtmf:N seq:N g729r8 (30)
```

De esta manera la comunicación por datos y por el canal de voz ha sido revisada.

Conclusiones

Las diferentes tecnologías y capacidades de transporte que se pueden utilizar actualmente permiten una comunicación más eficiente y rápida, esto aunado con el uso de IPv6 en un futuro, hará que cada dispositivo tenga una dirección IP y se pueda administrar o controlar de manera remota.

Dado que se continúa utilizando IPv4, se mostró el direccionamiento que se emplea en los diferentes rangos de redes, así como las direcciones privadas y reservadas que se pueden o no utilizar; Con un adecuado direccionamiento se logrará que se tenga una red escalable sin desperdiciar direcciones IPs en el caso de una expansión a futuro.

El modelo OSI y el modelo DoD describen como se transfiere la información, lo que permite que en caso de falla se pueda analizar o determinar en que parte de la comunicación se tiene el problema.

Se hace una descripción del router como dispositivo de capa 3 del Modelo OSI, debido a que con él se va a realizar la conexión a nivel WAN, o dicho en otras palabras, permitirá que se tenga comunicación con otros nodos en diferente ubicación. Además, se muestra la manera de identificar un cable RJ45, así como la norma de cableado para poder conectar un dispositivo al router y tener comunicación con él.

Para finalizar, se hace el uso de la tecnología de Frame Relay para crear una red, como una alternativa de bajo costo para poder tener conexión por voz y datos, logrando de esta manera reducir los gastos de llamadas en LD sin emplear dispositivos o configuración adicional debido a que los teléfonos que se utilizan son analógicos y únicamente se conectan al router en los puertos de voz. La configuración que se empleó en los routers hace que la red sea escalable tanto en el direccionamiento IP como en las extensiones de los sitios remotos para comunicarse por voz. La configuración en los switches de Frame Relay permitirá que se cree la conexión entre los sitios y de esta manera poder tener una red la cual tenga un buen desempeño tanto en voz como en datos.

Bibliografía

Connection-oriented networks: SONET/SDH, ATM, MPLS and optical networks.
Harry G. Perros
John Wiley & Sons Inc.
2005

http://www.rad.com/Home/0,6583,5847,00.html

Diplomado Integral de Telecomunicaciones, Sexta Versión
Centro Educativo Multidisciplinario Polanco
Modulo 4. Redes de Telefonía Inteligentes
Modulo 5. Redes de Datos y Tecnologías de Transporte
Modulo 6. Internet (TCP/IP)
Modulo 8. Voz sobre IP
2005

CCNA: Cisco Certified Network Asóciate, Study Guide
Todd Lammle
Sybex Inc. 2005

Programa de la Academia de Networking de Cisco
CCNA Semestre 1, 2 y 4
V 2.1.2
Cisco System, Inc. 2000

Building Scalable Cisco Internetworks, Student Guide
Volume 1
Version 2.2
Cisco System, Inc. 2005

http://www.ipv6.unam.mx

http://www.ipv6forum.com

Network +, Fast Pass
Bill Ferguson
Sybex Inc. 2005

Tecnologías emergentes para redes de computadoras.
Black, Uyless
Prentice Hall Hispanoamericana, S.A.
México, 1999

CCIP: MPLS Study Guide
James Reagan
Sybex Inc. 2002

Voice over IP Fundamentals, Second Edition
Jonathan Davidson, James Peters, Manoj Bhatia, Satish Kalidindi, Sudipto Mukherjee
Cisco Press 2006
Cisco Voice over IP (CVoice)
Kevin Wallace
Cisco Press 2007

Cisco Voice Gateways and Gatekeepers
Denise Donohue, David Mallory, Ken Salhoff
Cisco Press 2007

Voice over IP First-Step
Kevin Wallace
Cisco Press 2006

Inteligencia de Red
Barba Martí, Antoni
Hesselbach Serra, Xavier
Ediciones UPC 2002

Apunte rápido CCNA
Oscar Antonio Gerometta
Libronauta
2006

http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a0080094e92.shtml

http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheets_list.html

http://www.cisco.com/en/US/products/hw/routers/ps332/products_tech_note09186a0080094ce6.shtml

http://www.cisco.com/en/US/products/hw/routers/ps259/products_installation_guide_book09186a0080692b95.html

http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080091ba1.html

http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheets_list.html

http://www.cisco.com/univercd/home/home.htm

http://www.lucent.co.jp/livelink/090094038005dfdb_Brochure_datasheet.pdf

Frame Relay Configuration II, Student Guide
Lucent Technologies Inc. 2000

NavisCore Frame Relay Configuration Guide
Ascend Communications, Inc. 1998

http://www.techconcepts.com/adtran.html#TECHNICAL%20CONCEPTS%20CORPORATION

http://www.techconcepts.com/PDFs/Adtran_DSU_III_A_%20Data_Sheet.pdf

http://networking.ringofsaturn.com/RemoteAccess/adtran.php

http://www.tellabs.com/products/list.shtml

http://www.kandk.fi/tuotteet/dsl-tuotteet_ja_jarjestelmat/watson_5_g_shdsl/

http://www.vucomm.co.yu/upload/products/1117_Watson_5.pdf

http://www.kandk.fi/mp/db/file_library/x/IMG/10583/file/WATSON5.pdf

http://www.schmid-telecom.com/page.php?t=template2&templateID=167&language=en&titel=Datasheets