

Medios de Transmisión

El medio de transmisión es la vía física que conecta al transmisor con el receptor de un sistema de comunicaciones. La figura 1(a) muestra el modelo básico de un sistema de comunicación Punto a Punto, y la figura 1(b) el modelo básico de un sistema de transmisión multipunto.

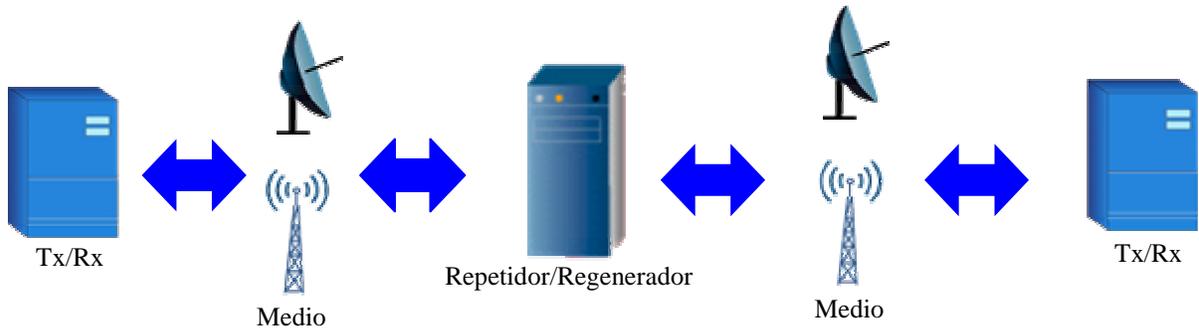


Figura 1(a): Sistema de transmisión P-P

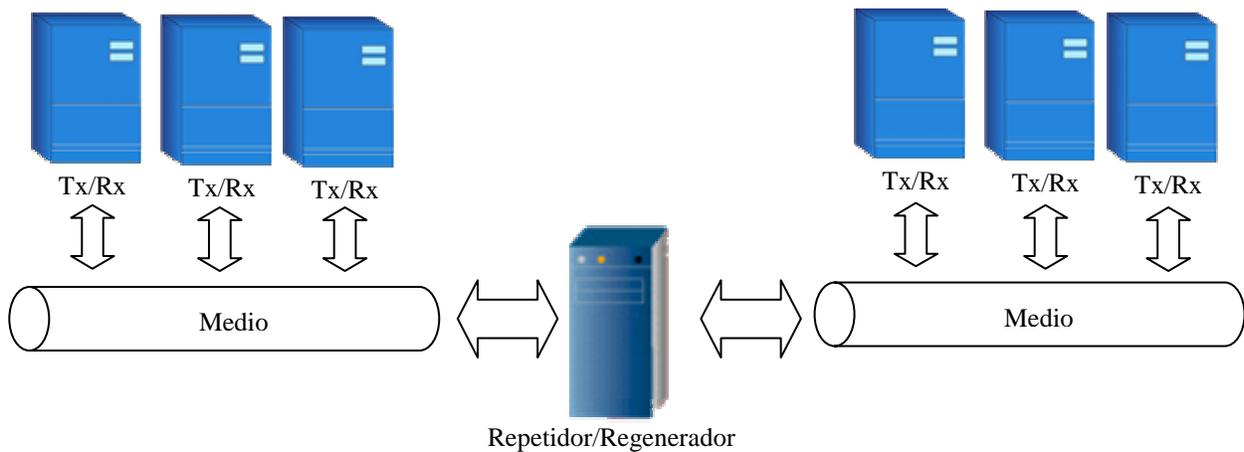


Figura 1(b): Sistema de transmisión M-P

La configuración más común entre dos dispositivos transmisores/receptores es un enlace Punto a Punto entre ellos. Estos dispositivos cuentan con las interfaces apropiadas para insertar señales análogas o digitales sobre el medio de transmisión. En este modelo puede usarse uno o más dispositivos intermedios (repetidores, amplificadores) para compensar atenuaciones u otros deterioros de transmisión.

Los medios de transmisión que utilizan señales electromagnéticas pueden clasificarse en:

Medios Guiados:

Las señales electromagnéticas son guiadas a través del camino físico. Por ejemplo par trenzado, cable coaxial, FO.

Medios no Guiados:

Las señales electromagnéticas son propagadas en todas direcciones sin existir un camino determinado. Por ejemplo el espectro de radio frecuencia, (el espacio libre).

A continuación describimos diferentes medios de transmisión usando para ello el siguiente pool de características:

- Descripción Física:
Naturaleza del medio de Tx.
- Características de Tx
Incluye tipo de señales usadas (digitales o análogas), técnicas de modulación, capacidad y rango de frecuencias.
- Conectividad
Tipo de configuración (P-P, P-M)
- Alcance Geográfico
Máxima distancia entre puntos de red.
- Inmunidad al Ruido
- Costo Relativo

Par Trenzado

El par trenzado es el medio físico más usado para la transmisión de señales análogas y digitales. Se usa en telefonía para conectar aparatos TF a centrales TF's y en la actualidad para conectar computadores a redes de área local.

Descripción Física:

Un par trenzado consiste de dos conductores (alambre) eléctricamente aislados, dispuestos a lo largo de una patrón espiral. Los conductores son de cobre o acero revestido en cobre. El cobre provee de la conducción eléctrica y el acero de resistencia mecánica. Un par trenzado actúa como una vía simple de comunicación y típicamente se agrupa un número de estos pares en un cable, con protección mecánica adicional. El hecho de trenzar cada par por separado minimiza la interferencia electromagnética entre los pares, los diámetros de los conductores varían desde los 0.4 mm hasta los 1.0 mm.

Características de Transmisión:

El par trenzado puede utilizarse tanto para transmitir señales análogas como digitales. Para el caso de señales análogas se requiere de un amplificador aproximadamente cada 5 ó 6 Km. Para el caso de señales digitales se utilizan repetidores aproximadamente cada 2 ó 3 Km.

El uso más frecuente del par trenzado es para la transmisión de la voz. Un canal de voz full-duplex standard está comprendido entre los 300Hz y 3400Hz y múltiples canales de voz pueden ser multiplexados en frecuencia (FDM) sobre un par trenzado. Para esto se utiliza un ancho de banda de 4KHz por cada canal de voz y se pueden agrupar hasta 24 canales de voz sobre un par trenzado (Ancho de Banda usado: 268KHz).

Para transmitir señales digitales sobre un canal de voz se utilizan los MODEMs. Las técnicas actuales permiten tasas de transmisión de 19.2 kbps lográndose con esto tasas de transferencias agregadas de 230 kbps. Tasas de transferencias superiores dependen fuertemente de las distancias involucradas y un límite superior razonable hoy en día es 4Mbps.

Conectividad:

El par trenzado puede ser usado tanto para conexiones punto a punto como para conexiones multipunto. Utilizando como medio multipunto el par trenzado es más barato que, por ejemplo, el cable coaxial, pero también soporta menos estaciones conectadas y presenta un rendimiento menor. La configuración punto a punto es la más usual de encontrar.

Alcance Geográfico:

El par trenzado fácilmente puede proveer conexiones punto a punto hasta de 15Km o más. Es típicamente usado para el cableado al interior de un edificio y en algunos casos para cablear edificios contiguos.

Inmunidad al ruido:

Comparado con otros medios guiados, el par trenzado es limitado en distancia, ancho de banda y tasa de transferencia. El medio es muy sensible a la interferencia y al ruido producto de su fácil acoplamiento con campos electromagnéticos. Ejemplos típicos de interferencia son campos generados por las líneas de alimentación de poder y acoplamientos producto de pares trenzados adyacentes (cross-talk).

Existen algunas medidas que se pueden adoptar para reducir la posibilidad de interferencia y estas son las siguientes: Proteger el par trenzado con una cubierta de modo de apantallar las interferencias, usar diferentes largos de trenzados entre para adyacentes reduce el cross-talk.

Costos

El uso de par trenzado es más barato que el cable coaxial y que la fibra óptica en términos de costos por unidad de largo. En términos de equipamiento para acceder a las redes, los costos por unidad son más baratos que el caso de fibra óptica y costos similares al caso del cable coaxial. Este medio presenta menor costo de instalación y mantención que los otros medios.

Cable Coaxial

Según muchos, el cable coaxial es el medio físico más versátil para las redes de área local, pero esta creencia se está desmoronando ante el creciente uso del par trenzado. Existen dos tipos de cable coaxial en uso para las redes de área local: cable de 75-ohms, usado típicamente en sistemas de CATV y el cable de 50-ohms. El cable de 50-ohms es usado para transmitir señales digitales, modalidad llamada “baseband” y el cable de 75-ohms es usado para transmitir señales análogas usando técnicas de FDM, modalidad llamada de “broadband”.

Descripción Física:

El cable coaxial consiste de dos alambres conductores eléctricamente aislados, pero está construido de forma diferente al par trenzado, lo que permite operar en un rango mayor de frecuencias. El cable coaxial está construido por un conductor cilíndrico exterior y que rodea a un conductor simple. El conductor interior puede ser sólido o conformado por hebras, y el conductor exterior puede ser sólido o tejido. El conductor interior mantiene su posición axial gracias a la disposición regular de anillos aislante o por efecto de un material dieléctrico de relleno. El conductor externo está recubierto por material vinílico o PVC para su protección. Los diámetros de los cables coaxiales varían desde los 10mm hasta los 250mm.

Características de Transmisión:

El cable coaxial de 50-ohms es usado solamente para transmisión digital usando típicamente codificación tipo Manchester. Con este medio se pueden alcanzar tasas de transferencias de 10Mbps. El cable coaxial de 75-ohms o cable CATV es usado tanto para transmisión de señales análogas como digitales. Para el caso de señalización análoga, las frecuencias de hasta 300 a 400 Mhz son posibles. La información análoga, tal como video y audio, puede ser manejada en cable de CATV de la misma forma que se realiza en el caso de radiación sobre el espacio libre de radio y TV. Cada canal de TV tiene asignado un ancho de banda de 6MHz y cada canal de radio requiere mucho menos. Para compartir el mismo medio físico por muchos canales se utiliza la técnica de FDM, en cuyo caso se dice que el cable de CATV opera en la modalidad “broadband”. Para el caso de transmisión digital de señales se dedica todo el ancho de banda a la transferencia de datos y se han logrado de hasta 50Mbps.

Conectividad:

El cable coaxial puede aplicarse tanto para conexiones punto a punto como para configuraciones multipunto. El cable de 50-ohms puede soportar del orden de 100 dispositivos por segmentos, utilizando como técnica de extensión de segmentos el uso de repeaters. El cable CATV puede soportar del orden de 1000 dispositivos, pero el uso del CATV a tasa de 50 Mbps limita entre 20 y 30 el número de dispositivos conectados.

Alcance Geográfico:

El cable coaxial en modo “baseband” limita las distancias máximas a algunos kilómetros. En el caso de redes “broadband” las redes se pueden dispersar en rangos de las decenas de kilómetros. La diferencia se explica por la integridad relativa de la

información de las señales análogas y digitales. En un ambiente urbano e industrial, la mayor parte del ruido e interferencias se encuentran en las frecuencias bajas y para el caso de transmisiones análogas, estas se pueden modular sobre una portadora lo suficientemente alta en el espectro de frecuencia de manera de evitar el ruido.

Para el caso de transmisiones de altas tasas de transferencias (50Kbps) las distancias se limitan a 1Km.

Inmunidad al ruido:

En general la inmunidad al ruido depende fuertemente de la aplicación y de las técnicas de modulación empleadas, pero el medio es menos sensible a la interferencia y al ruido que en el caso del par trenzado.

Costos:

El uso de cable coaxial es más barato que la fibra óptica, pero más caro que el par trenzado en términos de costos por unidad de largo. En términos de equipamiento para acceder a las redes, los costos por unidad son más baratos que la fibra óptica y similares que al par trenzado.

Fibra Optica

Hoy en día muchos avances están ocurriendo en el campo de la investigación de este medio de transmisión, por lo que sólo se puede mostrar una fotografía del estado de lo que hoy existe.

Descripción Física:

La fibra óptica está constituida de vidrio o plástico muy delgados dispuestos de forma tal que permiten la conducción de la luz. La fibra óptica es un cable con forma de cilindro y que consiste de tres secciones concéntricas: el núcleo o centro (core), el revestimiento (cladding) y la sobrecubierta (jacket). El centro es la sección interior y contiene una o más fibras de vidrio o plástico, estas fibras son muy delgadas (típicamente 2 a 125 μm). Cada fibra está rodeada de su revestimiento (cladding) que posee características ópticas muy diferentes respecto del centro. La capa externa llamada sobrecubierta consiste de material plástico, PVC u otro de manera de proveer la protección contra la suciedad, corrosión, y otros aspectos ambientales.

Características de Transmisión:

La fibra óptica transmite, por medio de una reflexión total interna, un rayo de luz codificado. La reflexión total puede ocurrir en cualquier medio transparente que posea un índice de refracción mayor que el del medio que lo rodea. De esta manera, la fibra óptica actúa como una guía de onda para frecuencias en el rango de 10×10^{14} hasta 10×10^{15} Hz, rango que cubre el espectro visible y parte del espectro infrarrojo.

Existen dos modos de transmisión en fibra óptica: multimodo y monomodo. En el caso de transmisión multimodo el diámetro del centro (core) es mayor que en el caso de la transmisión monomodo. Este mayor diámetro permite que ingrese un gran número de rayos de luz que tienen un ángulo distinto de cero con respecto al eje del centro de la fibra. Parte de estos rayos es reflejado y propagado a lo largo de la fibra y otra parte son absorbidos por

el material que rodea la fibra de vidrio. En el caso de la transmisión monomodo el menor diámetro del centro sólo permite que entren a la fibra rayos con ángulo cero con respecto al eje del centro. La transmisión monomodo tiene mejor rendimiento que la de propagación, puesto que en el caso multimodo existen múltiples caminos de propagación, lo que se traduce en distintos tiempos de propagación y por tanto reduce los límites de las tasas de transferencia.

Conectividad:

El uso más común de la fibra óptica es para enlaces de tipo punto a punto. El uso de esquemas multipuntos todavía presenta costos muy elevados.

Alcance Geográfico:

Las longitudes que se pueden lograr sin repetidores varían con el modo de transmisión, pero se puede señalar que distancias de hasta 6 a 8 Km se logran con la tecnología actual.

Inmunidad al ruido:

La fibra óptica no está afectada por las radiaciones ni ruidos electromagnéticos, lo que permite alcanzar elevadas tasas de transferencias sobre largas distancias. Otra característica es que por su naturaleza óptica no produce ningún tipo de radiación, lo que la hace muy apta en ambientes industriales inflamables y en oficinas donde se requiera de seguridad ante eventuales espionajes.

Costos:

Los sistemas de fibra óptica son más costosos que el uso de cable coaxial y para trenzado, en términos de valor por unidad de longitud y componentes requeridos (transmisores, receptores, conectores, etc.).

Cableado Estructurado

En la actualidad es frecuente encontrar en las empresas una gran variedad de dispositivos computacionales que dan diferentes servicios a los usuarios. Por ejemplo: PC con tarjetas Ethernet, PC con tarjetas Token Ring, terminales asincrónicos, Macintosh, impresoras, modems, etc.. Cada dispositivo posee características propias desde el punto de vista de las conexiones eléctricas y mecánicas que es necesario efectuar para que su operación sea la correcta.

Producto de la dinámica de cada empresa, a menudo es necesario cambiar el puesto de trabajo de un usuario que posee cierto tipo de dispositivos. El puesto vacante será ocupado por otra persona que probablemente empleará un dispositivo diferente para realizar su labor. Ciertamente, la experiencia es traumática si consideramos la periodicidad de la situación antes descrita. Con el paso del tiempo, desde cada puesto de trabajo en la oficina, salen tendidos paralelos, con diferentes tipos de cable, hacia el lugar donde se encuentran los recursos computacionales mayores.

La situación mencionada es más caótica de lo que parece a primera vista, dado que:

1.- Es difícil mantener un historial actualizado de todos los tendidos con distintos cables, de distintas longitudes y diámetros, que se ramifican por la organización. Entre estos encontramos coaxiales y pares metálicos de diferentes características eléctricas.

2.- Los conductos destinados para cables se saturan y generalmente no se usan todos los cables que se encuentran tendidos.

3.- En cada oportunidad, en la cual no se cuente con el tipo de cable apropiado, es necesario realizar un nuevo tendido. Las consecuencias propias de esta operación son:

- Pérdida de eficiencia por el tiempo que involucra un cambio.
- Molestias al usuario.
- Aumento de los costos de operación.

4.- Se pierde el control y la efectividad para responder ante situaciones de fallas, debido a que resulta difícil identificar un tendido para aislar una falla.

La pérdida de la capacidad para responder a este tipo de situaciones tiene las siguientes implicancias:

- Costo de oportunidad al dejar de operar.
- Molestias al usuario.
- Aumento de los costos de operación.

La técnica del Cableado Estructurado

La técnica conocida como cableado estructurado es una tendencia mundial, que surge como la solución lógica a los inconvenientes indicados anteriormente.

El cableado estructurado resuelve el problema de distribución de servicios a los usuarios finales, proporcionando gran flexibilidad y confiabilidad en las conexiones que se deben realizar.

Las premisas sobre las cuales se sustenta esta técnica son las siguientes:

- Todos los dispositivos de uso frecuente para el usuario pueden ser soportados sobre par trenzado.
- El cableado que se realiza hacia un puesto de trabajo es independiente del dispositivo a conectar.

Recomendaciones para la realización de un Cableado Estructurado

- Es conveniente realizar un estudio detallado del número de puestos de trabajo por oficina, considerando los requerimientos presentes y futuros.
La idea es que el tendido de cables para dar servicio al usuario se efectúe una sola vez en el tiempo.
- Entre todos los dispositivos que pueden ser soportados sobre par trenzado, los que tienen mayores exigencias son los conectados en Ethernet o en Token Ring

(mayores velocidades de operación). Por lo tanto, la distancia entre el punto de distribución y el puesto de trabajo no debe exceder los 100 metros, tal como lo establecen los estándares para par trenzado. Otros dispositivos soportan mayores distancias (terminales asincrónicos), pero el objetivo es independencia del dispositivo a conectar, de modo que no debería excederse, por ningún motivo, la distancia de 100 metros.

- Es conveniente que el tendido para distribución de dispositivos computacionales sea independiente del tendido para distribución telefónica. Las razones que fundamentan esta recomendación son:
 - a) El tendido para distribución telefónica no tiene exigencias severas, en cuanto a tipo de pares metálicos y distancias soportadas. De otra manera se estarían haciendo restricciones innecesarias al cableado telefónico. Por ejemplo, el número de regletas (saltos sucesivos) que se emplean para alcanzar un puesto de trabajo, producen atenuaciones a las señales de altas frecuencias, lo cual limita la distancia máxima que se puede alcanzar, desde el punto de distribución a los puestos de trabajo. Tal es el caso para las redes Ethernet y Token Ring.
 - b) El personal dedicado a la mantención de una red telefónica no tiene la preparación necesaria para manipular las regletas que contienen pares que transporten datos a alta velocidad, sobre todo si las regletas contienen pares de voz y datos a la vez.
Lo anterior no significa que los tendidos telefónicos y de datos a alta velocidad no puedan ser realizados y planeados en forma conjunta. De hecho, en un mismo conector de pared de un puesto de trabajo se podría contar con ambos servicios (voz y datos).
- Es aconsejable que el cableado hacia cada puesto de trabajo considere 8 hilos, dado que esto permite flexibilidad con las señales RS-232. Por ejemplo, permitiría la instalación de una impresora serial.

Concepto de Ancho de Banda y Velocidad de Transmisión

Como hemos visto en los temas anteriores, en todo lo que se refiere a comunicaciones, sean estas análogas o digitales, la forma de representar tanto matemáticamente, como los modelos de los sistemas de comunicaciones, se basan en la variable “frecuencia”, variable a la que el común de la gente no está acostumbrada, dado principalmente que por nuestra naturaleza entendemos el medio más bien expresado en la variable “tiempo”. De aquí que el concepto de Ancho de Banda sea bastante difícil de entender en un principio, pero vale la pena dedicar tiempo a ello dado que es parte fundamental en la técnica de comunicar. Definiremos Ancho de Banda (BW) como el rango de frecuencia que necesita un sistema para poder ser transmitido en un medio de transmisión de señales electromagnéticas. Por ejemplo, 6 Mhz en el caso de una transmisión de Televisión broadcasting, 25 Khz en el caso de transmisión FM de voz vía radio enlace, 50 Khz para radio módem digital de 128 Kb/s, etc. Ver figura 2.

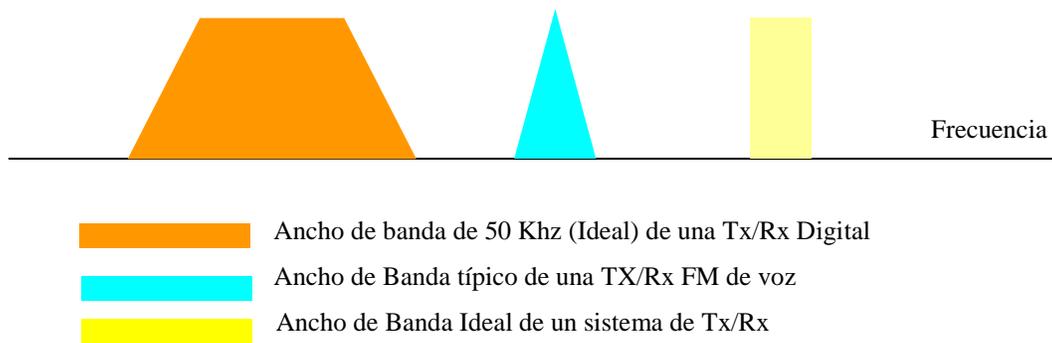


Figura 2: Representación de anchos de Banda

Otros conceptos importantes a tomar en cuenta al representar al BW de un sistema de transmisión son la Atenuación del Medio y su respuesta ante interferencias o ruido, es muy típico hoy en día encontrar tablas y mucha literatura y estudios con respecto a estos temas para cada medio de transmisión como para cada sistema, en este punto es bueno dejar en claro que los BW de los sistemas de Tx/Rx estan definidos por el sistema mismo, esto es, el diseñador del sistema decide o el mismo diseño (o modelo) del sistema le entrega los requerimientos de BW, en cambio en los medios de Tx/Rx es una variable física que no la define nadie más que el mismo material que se este utilizando para comunicar. Por ejemplo, en un sistema de Tx/Rx en donde se quiere comunicar dos computadores dentro de un estandar IEEE 802.3 a 10 Mb/s, los 10 Mb/s son definidos por el estandar y no por el cable UTP que se utiliza para realizarlo, se entiende que se eligió cable UTP pues es capaz de soportar el BW que se necesita para comunicar ambos PC's a esta velocidad.

Atenuación: este término define las pérdidas de señal en db's que sufre una señal al ser transmitida a través de un medio de Tx/Rx, este efecto es un resultado físico de transmitir y está presente en cualquier medio de transmisión, Coaxial, FO, UTP, etc. Debido a este fenómeno es que los estándares definen máximos para el largo de los cables, o distancia maxima entre Tx/Rx vía radio o cantidad de fusiones de una FO por tramo. Normalmente los sistemas de comunicaciones se defienden de este fenomeno intercalando (cuando se hace estrictamente necesario) repetidores (o amplificadores). En estricto rigor un repetidor solo se utiliza si las pérdidas por atenuación lo indican, y además siempre se trata de buscar la mejor opción de técnicas y estándares para no utilizarlos, dado esto principalmente por el aumento en la probabilidad de fallos de sistema.

Como hemos visto, el medio de transmisión define el máximo BW del que se dispone para la comunicación, por lo tanto se elige el medio dependiendo de la velocidad o cantidad de señal que deseamos transmitir, por ejemplo para 10/100 Mb/s el par trenzado es suficiente, para velocidades o distancias superiores a los 300 m ya la atenuación del par trenzado es tal que se hace necesario intercalar repetidores o cambiar de medio, típicamente se instala FO para evitar los repetidores.

Velocidad de transmisión: este término se define dependiendo en que parte del modelo de comunicación estemos, por ejemplo, a nivel físico (en el par trenzado) la velocidad de transmisión entrega una idea de con qué frecuencia están pasando los bits por el cable, en cambio a nivel intermedio la velocidad de un paquete de información nos indica a qué velocidad se está comunicando un protocolo de comunicaciones, por lo tanto el concepto de Velocidad de Transmisión esta íntimamente ligado a la posición dentro del modelo de comunicaciones que se esté utilizando, por ejemplo, pensemos que estamos comunicando dos PC's a través de sus puertos seriales mediante dos modems tradicionales de 33.6 Kb/s, si el medio nos permite enlazarnos a velocidad máxima entonces los bits por la línea telefónica estarán pasando a una razón de 2.97 e^{-5} (s), pero sin embargo dependiendo del protocolo que se esté utilizando para transmitir esta información (distintos softwares por ejemplo) es muy probable que la velocidad que finalmente logremos sea mucho menor.

Por ejemplo, una Tx/Rx serial, a 9600 bps, asincronica, en 8N1 v/s lo mismo pero en 8E1.

En el caso 8N1 se transmiten 9 bits por cada símbolo de comunicación, en el otro caso de 8E1, se transmiten 10 bits, por lo que ambas Tx/Rx se realizan a una velocidad de línea de 9600 bps, pero para el usuario final la cantidad de información que realmente pasa por el sistema no es la misma, y lo más importante de todo, ambos sistemas en realidad no son a la misma velocidad !.

Conceptos Básicos de Redes de Datos

El modelo de referencia OSI de la ISO

Hasta el momento hemos estudiado la transmisión de señales desde el punto de vista de un Tx/Rx interconectados por un medio de transmisión cualquiera, con este modelo genérico hemos sido capaces de entender como se modulan señales y como se transforman para poder acceder el medio de transmisión. Ahora la tarea es entender como estas señales conviven en un ambiente más real y no tan genérico, y sobre todo pensando que lo que deseamos es interconectar computadores. De aquí nace el concepto de Red en su forma más general y que es explicado mediante un modelo de referencia que la OSI (Organización Internacional de Normas) nombro, en su momento, OSI.

Para poder enfrentar el problema general de interconectar diferentes sistemas computacionales, la ISO genera el modelo de referencia OSI, el principio general en el que se basa este modelo es aquel según el cual un problema complejo (como lo es el de interconectar computadores) puede ser mejor manejado y explicado si se divide en varios problemas menores y más específicos. De esta forma, la función de la red de comunicaciones, se particiona en varias funciones específicas, cada una de las cuales contribuye con una parte que, en conjunto con las demás, permiten la comunicación deseada final.

El modelo se denomina formalmente, Modelo de Referencia para la Interconexión de Sistemas Abiertos (Open System Interconnect, OSI), y define las funciones necesarias para alcanzar el objetivo de interconectar sistemas digitales de cómputo. Ver figura 3

Modelo de Referencia OSI de la ISO

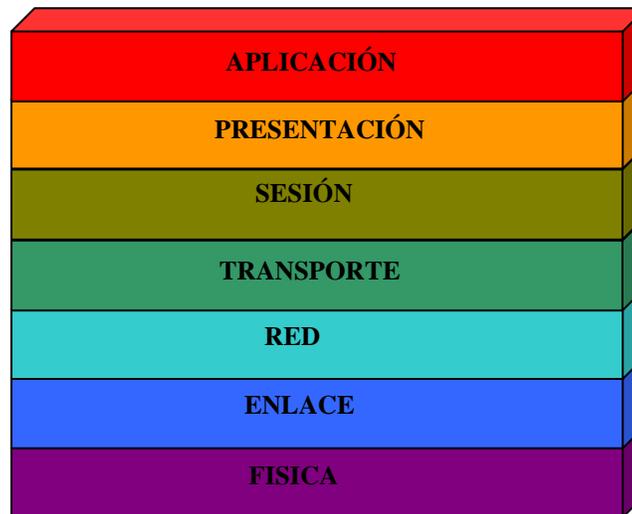


Figura 3: Los niveles del modelo OSI

El modelo de referencia OSI describe las funciones proporcionadas por cualquier sistema de interconexión de redes, en términos de niveles o capas. Es una especificación en que cada capa o nivel brinda un servicio a la capa o nivel superior y espera un servicio de la inferior.

El problema general de las comunicaciones se visualiza, de acuerdo a este modelo, como una estructura jerarquizada, compuesta de niveles, cada una de las cuales aporta una fase específica en el proceso global.

La tarea de la IOS fue definir cada una de las capas del modelo y los servicios que proporcionarían, la partición debería agrupar las funciones en forma lógica, y debería tener suficientes capas para hacer que cada una fuera manejablemente pequeña, y no demasiadas para que el modelo no se engrosara demasiado. El resultado es un modelo de siete niveles, que se describen a continuación.

En lo que sigue se definen, en términos generales, las funciones que deben ser ejecutadas en un sistema para comunicarse, desde luego se necesitan dos sistemas para poder establecer una comunicación, en el que debe existir el mismo conjunto de funciones para asegurar el fiel intercambio de señales, datos o información. El sistema de comunicaciones se mantiene dada la comunicación entre las capas pares de cada sistema comunicante, las capas pares (peer) se mantienen comunicadas por una serie de reglas o protocolos (convenciones o normas).

Los elementos claves de un protocolo son:

- **Sintaxis:** *La forma en la cual la información es intercambiada (formato, código).*
- **Semántica:** *La interpretación de la información de control para la coordinación y el manejo de errores.*
- **Sincronización (timing):** *La secuencia en que ocurren los eventos.*

Las capas o niveles del modelo OSI:

Capa Física: Está relacionada con la transmisión de un flujo de bits no estructurado sobre el medio físico; involucra parámetros tales como niveles de voltaje de señales eléctricas y la duración de cada bits en el medio; también con las características mecánicas, eléctricas y de procedimientos para establecer, mantener y desactivar el enlace físico (RS-232c, RS449, X.21, V.35, Frame Relay, etc).

Capa Enlace: Provee transferencia confiable de datos a través del enlace físico, envía bloques de datos (frames) con la sincronización necesaria, control de errores y control de flujo (HDLC, SDLC, BiSync, HDB3, etc).

Capa Red: Permite transferir los datos en forma transparente, seleccionando una ruta a través de la red. Es responsable de establecer, mantener y terminar las conexiones (X.25, IP).

Capa Transporte: Asegura transferencia confiable y transparente de datos entre puntos terminales, provee recuperación de errores y control de flujo entre extremos terminales, optimiza la utilización de los recursos empleados, desligando a los usuarios de los detalles de la transferencia misma.

Capa Sesión: Responsable del control de la comunicación entre procesos de aplicación, establece, maneja y termina las conexiones (sesiones) entre procesos cooperantes.

Capa Presentación: Ejecuta útiles transformaciones de datos de tal forma de presentar una interfaz estándar (interpretación de datos) y provee servicios de comunicación comunes: Encriptación, reformateo, compresión de texto.

Capa Aplicación: Provee servicio a los usuarios del ambiente OSI: NFS, SNMP, etc.

Dispositivos de Red

Los dispositivos constituyentes de una red dependen del tipo de topología que ella posea, cada una de ellas posee dispositivos típicos que la constituyen, por ejemplo en el caso de una LAN es común encontrar un HUB, adaptadores de red en las estaciones de trabajo y servidores de red, si la red es amplia, lo común son routers o bridges, modems, etc. Revisemos a continuación los dispositivos más comunes de acuerdo a la topología de red.

LAN

Adaptadores de red: Estos dispositivos son los encargados de comunicar a las estaciones de trabajo con la red, o dicho de otra forma conectan los computadores a la red. Normalmente son tarjetas que se instalan en los computadores como un periférico más, existen diversos fabricantes, modelos y para cada estándar de capa física, por ejemplo lo más común en estos días son las tarjetas de red ethernet, ellas pueden ser ISA o PCI o como se está dando cada vez con mayor frecuencia estos adaptadores vienen integrados “On Board” (integrados en las placas madres de los PC’s). Ellos pueden trabajar en variadas normas, por ejemplo 10BaseT, 10 Base2, Token-Ring, etc. Ver figura 4



Figura 4: Adaptadores de red (tarjetas de red)

HUB: Este dispositivo es el encargado de manejar la comunicación o administrar la comunicación entre las estaciones de trabajo de una red LAN basada en par trenzado, se puede definir como un concentrador de red LAN, este dispositivo traspasa la información desde un cable de red a otro dependiendo del origen y el destino (físico) de la información, este dispositivo es el que vino a reemplazar el Bus de comunicaciones de las redes basadas en 10Base2. Ellos también existen en variados formatos, capacidades y fabricantes, los más comunes hoy en día son los de 12 puertos Ethernet (o más) y poseen características de apilamiento (cascada) tipo Daisy-Shain o protocolos de apilamiento parecidos. Además en el último tiempo los fabricantes les han agregado capacidades de administración tipo SNMP, lo cual permite a los administradores de red responder ante fallos y optimizar recursos de red. Ver figura 5.



Figura 5: Hub de 16 puertos ethernet apilable

WS (estaciones de trabajo): Ellas son las máquinas que poseen las interfaces gráficas adecuadas para que los usuarios de la red puedan acceder a ella. Hoy en día lo más usual es encontrar computadores personales (PC's) los cuales poseen sistemas operativos con las características esenciales de comunicación en red, además de los softwares necesarios para levantar protocolos de red y entenderse con el medio.

WAN

Las redes WAN son usualmente interconexiones de redes LAN a grandes distancias, por lo tanto sus dispositivos más usuales son elementos más especializados y que cumplen funciones específicas de interconexión de redes, interfaz entre redes distintas y conmutación de información.

Módem: Este dispositivo es el encargado de transportar señales a través de líneas físicas dedicadas a los centros de comunicación más cercanos. Ellos, en definitiva, transportan las señales de las redes a interconectar entre sitios distantes geográficamente. Existen diversos tipos y diversas normas para cada uno de ellos, por ejemplo los modems conmutados que utilizan la red telefónica para comunicarse a larga distancia, los dedicados (Banda Base) que normalmente son empleados para transmitir flujos de información apreciables a distancias que no exceden los kilómetros. Ver figura 6.



Figura 6: Módem externo de sobremesa

Bridges/Routers: Estos elementos de red son los encargados (muy básicamente) de realizar los cambios necesarios a la información de las redes locales para poder transportarla hacia las demás redes conformantes de la red amplia. Ellos realizan fundamentalmente dos actividades: determinan los caminos a seguir por la información para llegar a destino y el transporte de los grupos de información (paquetes) a través de la inter-red (conmutación). La diferencia entre router y bridge se basa en el nivel de la capa OSI en la que trabajan. Los bridges trabajan a nivel 2 y los routers a nivel 3, los primeros conmutan frames y los segundos paquetes. Ver figura 7.



Figura 7: Router

Repetidores: Los repetidores aunque suelen enumerarse dentro de los dispositivos de red en estricto rigor no son tales. En realidad su función es conectar diversos segmentos de una misma red, permitiendo de esta forma extender la distancia abarcada por ésta. Son meros regeneradores de señales.

Topologías de Red

En lo esencial las redes de computadores se clasifican en redes de área local (Local Area Network, LAN), cuando su extensión geográfica no supera algunos cientos de metros, y de área amplia o extendida (Wide Area Network, WAN) cuando cubre grandes distancias, alcanzando hasta miles de kilómetros. Sin embargo, entre ellas suelen hacerse algunas clasificaciones adicionales. La descripción de las redes desde este punto de vista se presenta a continuación.

Redes de Área Local, LAN

La característica en común de este tipo de redes es que ocupan un área geográfica limitada (algunos cientos de metros), y se clasifican en:

- **Redes Punto a Punto (P-P)**
- **Redes de alta velocidad, HSLN (High Speed Local Networks)**
- **Redes homogéneas (de proveedores)**
- **Redes heterogéneas (LAN)**

Las redes Punto a Punto son constituidas por enlaces directos entre dos o más equipos computacionales. Un ejemplo simple, lo constituyen dos computadores conectados por medio de una enlace serial asincrónico.

Las redes de alta velocidad proveen comunicaciones de alta velocidad tipo P-P, entre dispositivos de gran capacidad, tales como Mainframes y dispositivos de almacenamiento masivo.

Por redes homogéneas se suele denominar a cualquier sistema de conexión entre múltiples computadoras del mismo fabricante, que se encuentren cercanos entre sí y cuyas características técnicas no encuentran expresión entre otros proveedores (sistemas propietarios o cerrados). Ejemplos de esto se encuentran entre los productos de casi todos los principales fabricantes de hardware computacional.

Las redes LAN poseen las siguientes características: Sus componentes son de bajo costo, sus velocidades son altas (típicamente 1 a 20 Mb/s, aunque cada vez más se instalan redes con velocidad nativa de 100 Mb/s), permiten un alto número de equipos conectados (hasta varios centenares), son confiables y fáciles de configurar, entre otras.

Entre las redes de área local de propósito general, cabe mencionar que las topologías de mayor importancia, por su difusión son las de bus lineal (cable coaxial) y estrellado (par trenzado), basadas en la red Ethernet de Xerox y el anillo estrellado de (token-ring) de IBM.

Redes LAN tipo Ethernet

Sin duda, la topología más usada en la actualidad para la interconexión de computadores en redes LAN heterogéneas es la del bus lineal, conformado por un cable coaxial delgado, al que se conectan los diferentes computadores. Este fue el medio concebido por Xerox, para su red Ethernet. Ver figura 8.

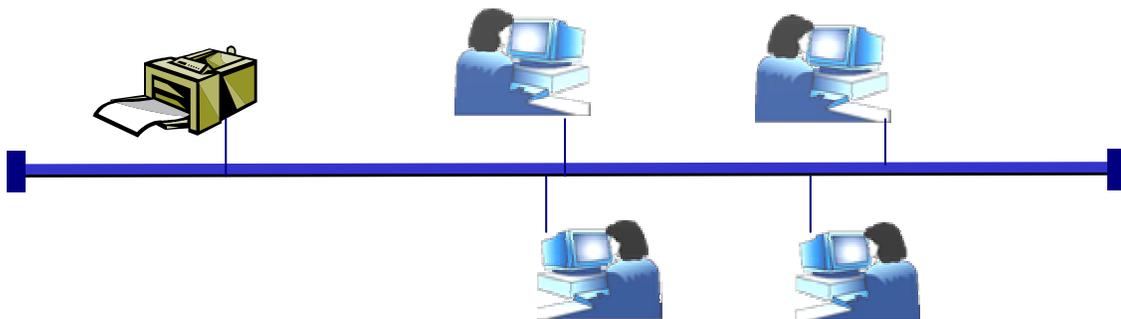


Figura 8: Red Ethernet sobre Cable Coaxial (10B2)

En los últimos años, sin embargo, se ha introducido fuertemente el cableado de redes ethernet sobre par trenzado, para lo cual se utiliza una topología de estrella, cuyo centro lo constituye un dispositivo concentrador denominado HUB. Ver figura 9.

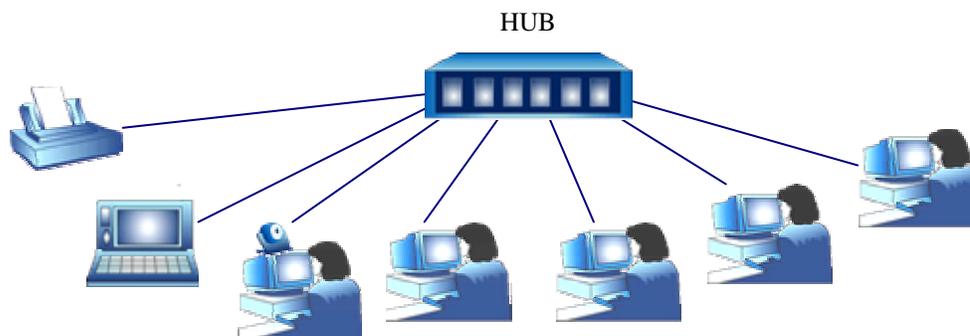


Figura 9: Red Ethernet 10BASE-T

Redes LAN Token-Ring (red de anillo con paso de testigo)

Otras de las topologías de mayor uso en redes LAN heterogéneas es el anillo estrellado, impulsado por IBM, bajo el nombre de red Token-Ring. En esta topología los computadores se cablean radialmente entre un concentrador pasivo, llamado Multistation Access Unit (MAU), como se muestra en la figura 10.

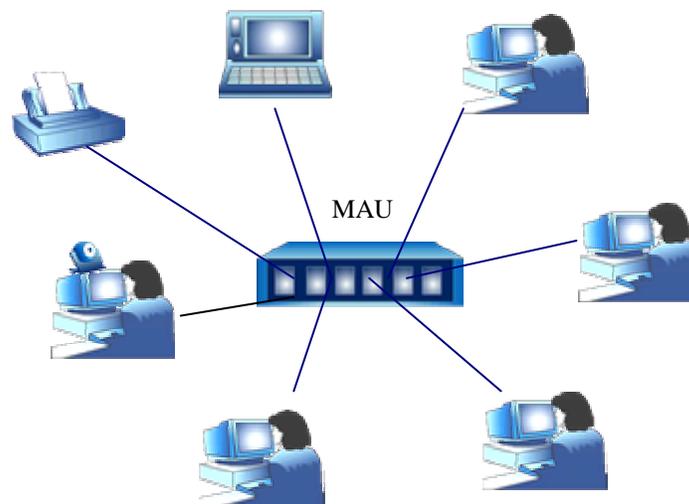


Figura 10: Red Token-Ring (conexión mecánica)

Los cables que unen a cada computador con el MAU, sin embargo, son dos pares (Uno de TX y otro de Rx), conformándose desde el punto de vista eléctrico un anillo que enlaza a los computadores, como se aprecia en la figura 11.

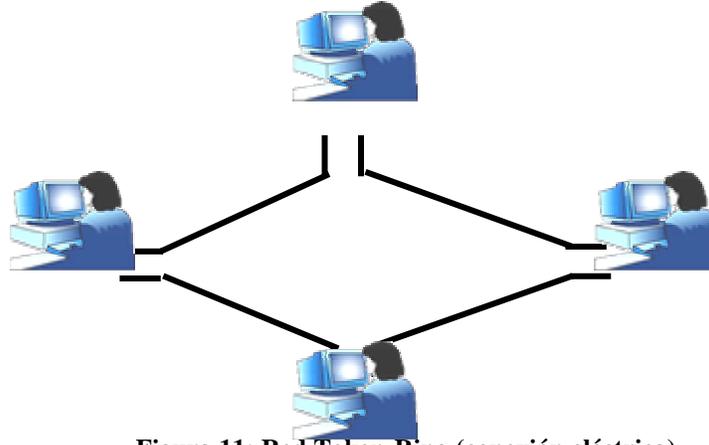


Figura 11: Red Token-Ring (conexión eléctrica)

Redes Metropolitanas

Una Red Metropolitana (Metropolitan Area Network, MAN) corresponde a una red que se extiende a través de la ciudad, normalmente basada en un anillo de fibra óptica. Este anillo sirve de enlace principal o “backbone”, interconectando equipos de diferentes proveedores y de distintas empresas. Su principal característica es su alta velocidad de transmisión (100 Mb/s, en el caso de FDDI). Ver figura 12.

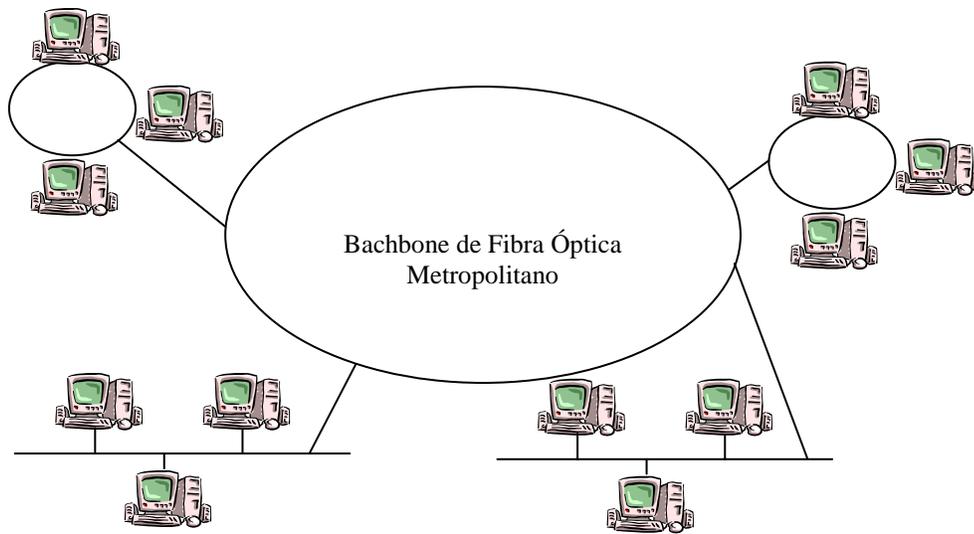


Figura 12: Metropolitan Area Network

Redes de Area Amplia

Las redes de área amplia o extendida (Wide Area Network, WAN) implementan las comunicaciones a larga distancia para sistemas de computación distribuidos, empleando con preferencias redes de comunicación públicas existentes, a través de líneas dedicadas (“leased”) o conmutadas (por circuito, como es el caso de la red telefónica, o de paquetes como las redes X.25 o Frame Relay).

Para las conexiones que requieren mayor ancho de banda se emplean enlaces punto a punto, normalmente a través de líneas dedicadas digitales (desde 64 kbps, hasta velocidades de E1).

Para las conexiones multipunto se emplea redes conmutadas de paquetes (X.25 pública o privada) y Frame Relay para mayores velocidades. Ver figura 13.

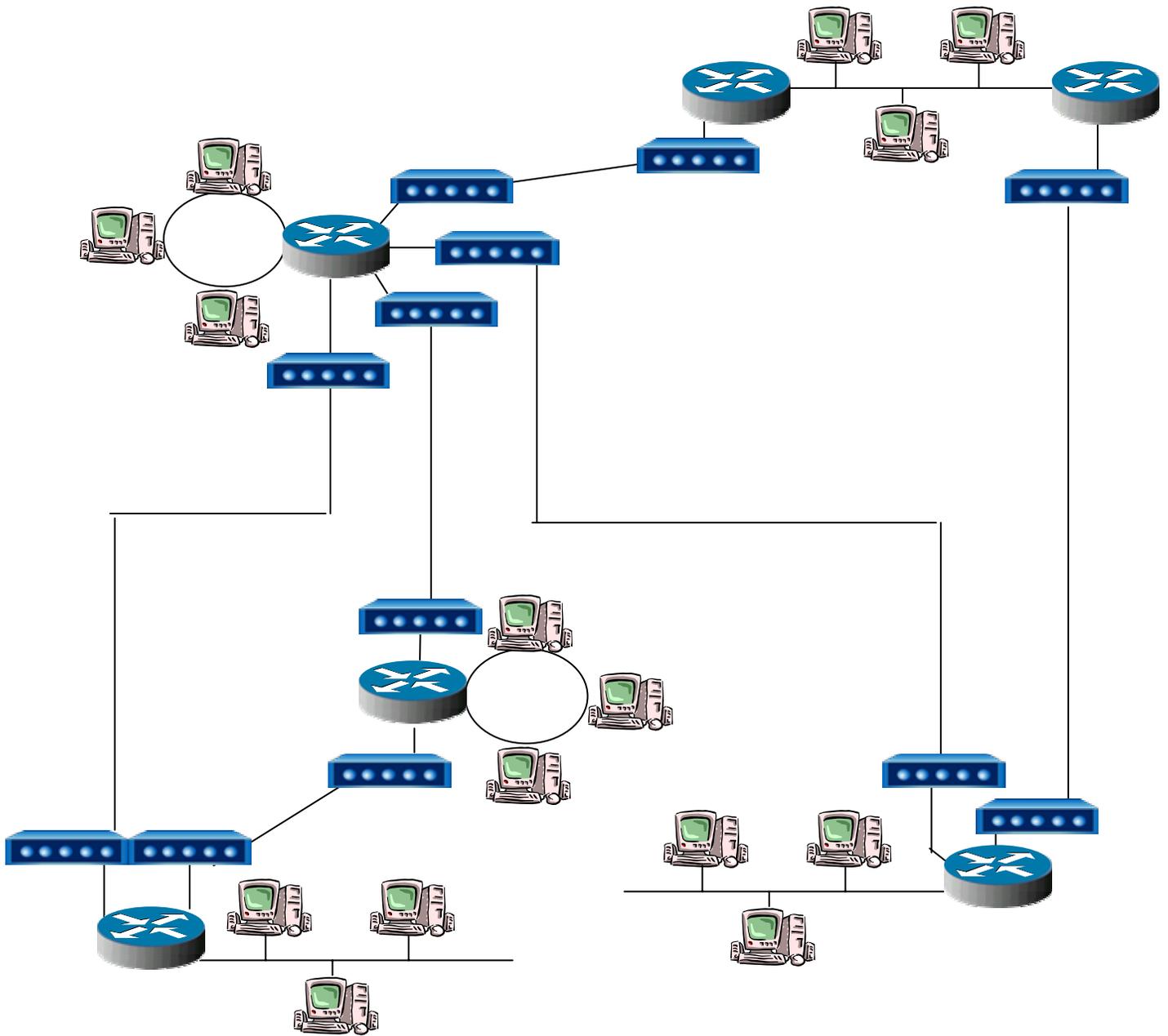


Figura 13: Red de Area Amplia

Modelo de Referencia TCP/IP

- Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.
- La red es packet-switched y está basada en un nivel de internet sin conexiones. Los niveles físico y de enlace (que juntos se llaman el "nivel de host a red" aquí) no son definidos en esta arquitectura.
- **Nivel de internet.** Los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino. No hay garantías de entrega ni de orden. Este nivel define el *Internet Protocol* (IP), que provee el ruteo y control de congestión.
- **Nivel de transporte.** Permite que pares en los hosts de fuente y destino puedan conversar. Hay dos protocolos:
 - **Transmission Control Protocol (TCP).** Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.
 - **User Datagram Protocol (UDP).** Es un protocolo no confiable y sin conexión para la entrega de mensajes discretos. Se pueden construir otros protocolos de aplicación sobre UDP. También se usa UDP cuando la entrega rápida es más importante que la entrega garantizada.
- **Nivel de aplicación.** Como en OSI. No se usan niveles de sesión o presentación.

OSI v/s. TCP/IP

- OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.
 - Servicio: lo que un nivel hace
 - Interfaz: cómo se pueden acceder los servicios
 - Protocolo: la implementación de los servicios
- TCP/IP no tiene esta clara separación.
- Porque OSI fue definido antes de implementar los protocolos, los diseñadores no tenían mucha experiencia con donde se debieran ubicar las funcionalidades, y algunas otras faltan. Por ejemplo, OSI originalmente no tiene ningún apoyo para broadcast.
 - El modelo de TCP/IP fue definido después de los protocolos y se adecuan perfectamente. Pero no otras pilas de protocolos.
 - OSI no tuvo éxito debido a
 - Mal momento de introducción: insuficiente tiempo entre las investigaciones y el desarrollo del mercado a gran escala para lograr la estandarización

- Mala tecnología: OSI es complejo, es dominado por una mentalidad de telecomunicaciones sin pensar en computadores, carece de servicios sin conexión, etc.
- Malas implementaciones
- Malas políticas: investigadores y programadores contra los ministerios de telecomunicación
- Sin embargo, OSI es un buen modelo (no los protocolos). TCP/IP es un buen conjunto de protocolos, pero el modelo no es general. Usaremos una combinación de los dos:

Nivel de aplicación
Nivel de transporte
Nivel de red
Nivel de enlace
Nivel físico

Arquitectura TCP/IP **Transmission Control Protocol/Internet Protocol**

En la actualidad, bajo la denominación TCP/IP se conoce a toda una familia (stack o suite) de protocolos, que se generó con la finalidad de permitir las comunicaciones entre hosts conectados a través de una gran variedad de redes heterogéneas (Ethernet).

Su origen se remonta al año 1969, en que la Agencia para Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de EEUU, inició un proyecto que pretendía establecer la posibilidad de construir un sistema de comunicaciones no centralizado, de propósito general, entre computadores diferentes. Este proyecto dio origen a la red conocida como ARPANET, que es parte de la Red de Datos de Defensa (DDN).

Los dos miembros principales de la familia de protocolos son: TCP (Transmission Control Protocol) e IP (Internet Protocol). Sin embargo, el conjunto comprende varios otros protocolos, como se aprecia en la figura 1.

En ella se muestra también la funcionalidad prestada por cada miembro de la suite, en términos de las capas del Modelo de Referencia OSI (Open Systems Interconnect) de la ISO, analizado anteriormente.

Como se aprecia en la figura 14, TCP/IP comprende una suite de protocolos que abarcan desde el nivel de red (capa 3) hasta el de aplicación (capa 7) del Modelo OSI. En cuanto a los medios físicos y protocolos de enlace, cabe mencionar que existen implementaciones de TCP/IP sobre todas las estructuras de importancia, como es el caso de IEEE 802.3 (CSMA/CD), IEEE 802.4 (token bus), IEEE 802.5 (Token-Ring), Ethernet, ARPANET, PDN (X.25), MILNET, etc.

OSI 5-7	FTP	TELNET	FINGER	SMTP	LPD/LPR	RLOGIN	SNMP	NFS	TFTP	BOOTP	TIME SERVICE	NAME RESOL	RWHO	PING
OSI 4	TCP							UDP						
OSI 3	IP													

Figura 14: Stack de protocolos TCP/IP

El proceso de armado y desarmado de los frames que son físicamente transmitidos por el medio físico se bosqueja en la figura 15, que muestra como, a medida que la unidad de información o mensaje a transmitir va siendo procesado por las diversas funciones de la comunicación, le son agregados campos con información específica para que las funciones correspondientes en otra parte de la red puedan recuperar el mensaje original, de manera clara y confiable.

Al transmitir el mensaje, la aplicación agrega el encabezado o header de aplicación (AH), a su vez la capa de presentación agrega el header de presentación (PH). Igual cosa efectúan las capas de sesión (SH), transporte (TH) y red (NH). La capa de enlace agrega información de framing (F), direcciones físicas (A) y de control (C). También agrega la secuencia de chequeo del frame (FCS) y, según el caso, caracteres adicionales de framing, como terminador. Este frame, ensamblado, llega finalmente al medio físico donde es transmitido simplemente como bits.

Se puede apreciar que, a medida que el mensaje va siendo procesado por los agentes que cumplen las diversas funciones especificadas por el Modelo OSI, va siendo “encapsulado” en formatos que resultan comprensibles para los agentes que operan los niveles homólogos en otras partes de la red.

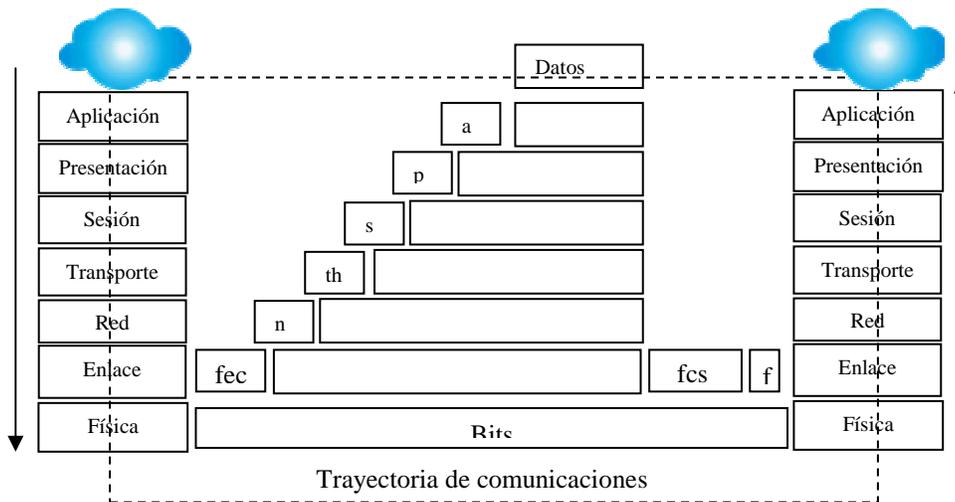


Figura 15: Flujo de datos sobre TCP/IP

Con referencia a las figuras 14 y 15, se puede decir que un mensaje o stream originado en la capa de aplicación (FTP, por ejemplo) da lugar a unidades de datos en la capa de presentación, las que se encapsulan en paquetes TCP en la capa 4 (transporte), los cuales son a su vez encapsulados en datagramas IP en la capa 3 (red) y estos son

El figura 18 se muestra el formato del frame IEEE 802.3, y en la figura 19 el frame IEEE 802.5.

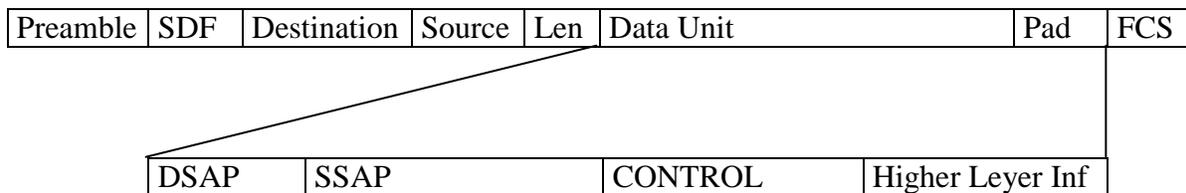


Figura 18: Formato Frame IEEE 802.3

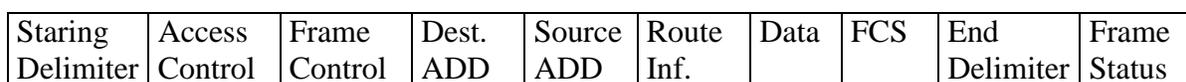


Figura 19: Formato del Frame IEEE 802.5

El protocolo de acceso físico definido para las redes Ethernet e IEEE 802.3 se denomina CSMA/CD (Carrier Sense Multiple Access/Colision Detect) y consiste en lo esencial, en que antes de transmitir un nodo verifica que no hay ningún otro transmitiendo. Cuando esto se ha verificado comienza a transmitir. Si durante la transmisión detecta que otro nodo también está transmitiendo aborta su propia transmisión y espera un tiempo aleatorio para retransmitir. El otro nodo hará lo mismo, y como las probabilidades indican que los tiempos serán diferentes, habrá uno que transmita primero.

El protocolo de acceso al medio en redes IEEE 802.5 (Token-Ring) se denomina Token-Passing. Básicamente éste consiste en un mensaje o “Token” que los nodos están haciendo circular constantemente entre ellos, en este mensaje que se pasa de un nodo a otro se insertan los paquetes que los nodos se transfieren entre sí, en forma análoga a como se transportaría carga entre estaciones que estuvieran conectadas por una línea ferroviaria circular.

Al nivel físico, los objetos transmitidos son sólo bits, los dispositivos que operan a este nivel no están al tanto del contenido de los mensajes ni de los protocolos empleados por los agentes que operan en los niveles superiores. Los agentes que actúan a nivel de enlace arman y desensamblan frames, sin preocuparse tampoco de los protocolos usados en los niveles superiores. De esta forma, es como se pueden soportan las comunicaciones TCP/IP sobre cualquiera de estos estándares físicos y de enlaces.

Como se puede apreciar, los encabezados o headers contienen información referente al nodo que emite el frame (source address) y destinatario (destination address). Estas direcciones, denominadas MAC o físicas, identifican sin error ni duplicidad a cada nodo de una red (mundialmente no existen dos MAC iguales). La información MAC es utilizada en la trayectoria o paso de los paquetes LAN a través de la red o para enrutarlos entre redes.

El Protocolo Internet (*Internet Protocol - IP*)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP

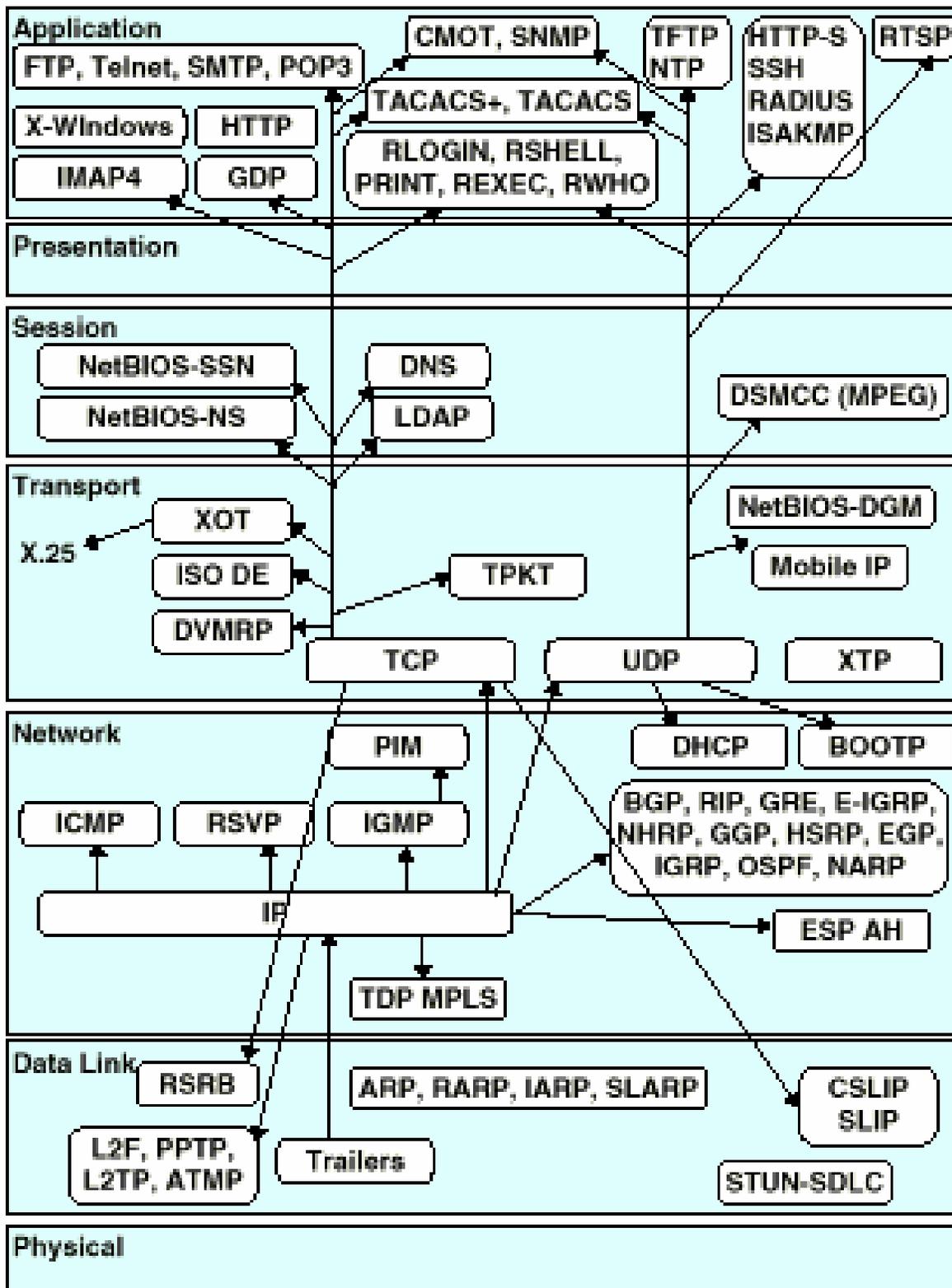
Las características de este protocolo son:

- NO ORIENTADO A CONEXIÓN
- Transmisión en unidades denominadas **datagramas**.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

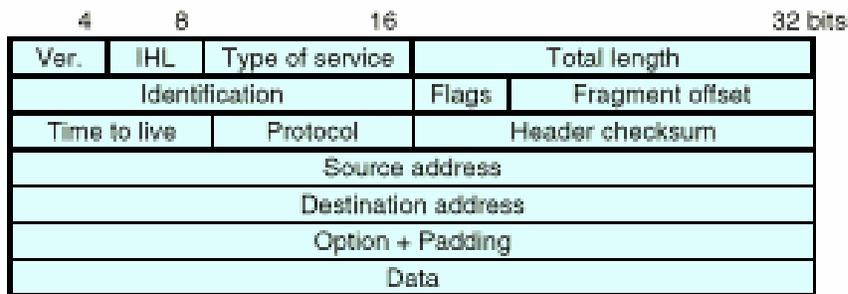
La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

En cuanto al ruteo (encaminamiento) este puede ser:

- Paso a paso a todos los nodos
- Mediante tablas de rutas estáticas o dinámicas



TCP/IP en Relación al Modelo OSI



Estructura del Heather IP

Ver. (Versión)

El campo versión indica el formato del Internet Heather

IHL (Internet Heather Length)

Largo del Internet Heather en palabras de 32 bits, apuntada a el principio de la data. El mínimo valor admitido es 5.

Type of Service (Tipo de Servicio)

Indica la calidad de servicio deseado, las redes pueden ofrecer servicios referidos por prioridades, significando que ellas solo aceptan tráfico dependiendo ciertas prioridades definidas en el heather IP en momentos de alto tráfico. Existen tres filosofias de definir prioridades, delay (retardo), reliability (calidad) y throughput (flujo).

Bit 0-2	Prioridad
111	Network Control
110	Internet Network Control
101	Critic/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority
000	Routine
Bit 3	Dealy
0	Normal Delay
1	Low Delay
Bit 4	Troughput
0	Normal Throughput
1	High Troughput
Bit 5	Reliability
0	Normal Reliability
1	High Reliability
Bit 6-7	Reserved for future use

Total Lenght (Largo Total)

Largo del datagrama medido en Bytes, incluyendo el Heather IP y la Data.. Este campo permite un largo máximo de 65.535 Bytes, de todos modos datagramas de esta

envergadura son impracticables para la mayoría de las redes y sus hosts. Todo host esta habilitado para recibir datagramas de mas de 576 Bytes.

Identification (Identificación)

Valor de identificación enviado por el host transmisor para el reensamble de los datagramas en destino.

Flags (Banderas)

3 Bits, control.

Bit 0: Reservado y debe ser cero

Bit 1: 0 Fragmentación

1 Sin fragmentación

Bit 3: 0 Ultimo fragmento

1 Mas fragmentos

Fragment Offset (Delta de cabecera de fragmento)

13 Bits, indica donde comienza el fragmento en el datagrama, el Fragment Offset es medido en unidades de 8 Bytes (64 Bits), el primer fragmento posee offset cero.

Time to Live (Tiempo de Vida).

Indica el máximo tiempo de vida que posee el datagrama en el sistema interred, si este campo posee el valor cero el datagrama será destruido, este campo es modificado y procesado a través de la red y es medido en segundos.

Protocol (Protocolo)

Indica el protocolo del siguiente nivel usado en la porción de data del datagrama.

Heather Checksum (Chequeo del Encabesado)

Chequeo del Heather solamente, mientras algunos campos del heather cambian. Por ejemplo el TTL es recalculado al paso por cada nodo de la red.

Source Address/Destination Address (Dirección Fuente/Dirección Destino)

32 Bits cada una. Una distinción se efectúa entre Nombres, Direcciones y Rutas. Un nombre indica un objeto a resolver (obtener dirección de objeto), una dirección indica la ubicación del objeto, una ruta indica como llegar al objeto.

Options (Opciones)

Este campo puede y no puede aparecer en los datagramas, a pesar de ser implementado en todo host o gateway. Este campo es variable en su largo, pueden haber cero opciones o más opciones. Existen dos formatos para una opción:

Un solo octeto de tipo de opción

Dos octetos, uno para el tipo de opción y otro para el largo de la opción.

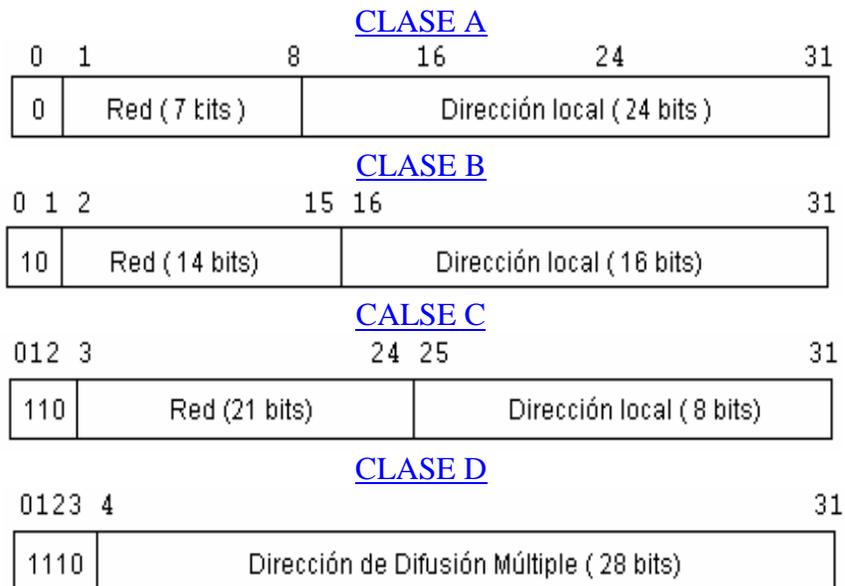
Data (Datos)

Datos IP o información de heathers de protocolos de niveles superiores.

Direccionamiento IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro) aparecen en la figura:



Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid)) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de **Clase A** corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

Las direcciones de **Clase B** sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.

Las direcciones de **Clase C** tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de **Clase D** se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Cabe decir que, las direcciones de **clase E** (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser **red.local.local.local** para **Clase A** hasta **red.red.red.local** para **clase C**.

A partir de una dirección IP, una red puede determinar si los datos se enviarán a través de una compuerta (GTW, ROUTER). Obviamente, si la dirección de la red es la misma que la dirección actual (enrutamiento a un dispositivo de red local, llamado *host directo*), se evitará la compuerta; pero todas las demás direcciones de red se enrutarán a una compuerta para que salgan de la red local. La compuerta que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento can base en la dirección IP de los datos y una tabla interna que contiene la información de enrutamiento.

Otra de las ventajas que ofrece el direccionamiento IP es el uso de **direcciones de difusión** (*broadcast addresses*), que hacen referencia a todos los host de la misma red. Según el estándar, cualquier dirección local (hostid) compuesta toda por 1s está reservada para difusión (broadcast). Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando a 1s toda la dirección local o de anfitrión (hostid), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

Ejemplos prácticos:

EJEMPLO I:

Consideremos la siguiente dirección IP en binario:

11001100.00001000.00000000.10101010 (204.8.0.170)

La dirección de la máscara (MASK) es en binario:

11111111.11111111.11100000.00000000 (255.255.255.0)

Según lo visto anteriormente, para hallar la dirección de SubRED (SubNet) tomamos la IP y considerando que todo lo que tenga 1s en la máscara se queda como esta en la IP, y todo lo que tenga 0s en la máscara se pone a 0 en la IP. Entonces, la dirección de SubRed es:

11001100.00001000.00000000.00000000 (204.8.0.0)

EJEMPLO II:

Sea la dirección IP en binario:

00001001.01000011.00100110.00000000 (9.67.38.0)

Cuya máscara de red es:

11111111.11111111.11111111.11000000 (255.255.255.192)

Siguiendo el criterio anterior, tenemos que la dirección de SubNet es:

00001001.01000011.00100110.00000000 (9.67.38.0)

En la dirección de la máscara de red, los últimos 6 bits han quedado a 0. Estos bits son los que definen las máquinas de la SubRed ($2^6=64$). De estas 64 máquinas quitamos la última de ellas (será para el Broadcast). Por tanto tendremos:

9.67.38.0	SubNet Address
9.67.38.1	(1ª máquina de la SubRed)
9.67.38.2	(2ª máquina de la SubRed)
.....	
9.67.38.62	(última máquina de la SubRed)
9.67.38.63	BROADCAST

EJEMPLO III:

Sea la dir.IP la **201.222.5.121**, la dirección de máscara **255.255.255.248**, entonces, haciendo los correspondientes cálculos en binario tenemos que:

201.222.5.121 (IP address)
 255.255.255.248 (NET MASK)
 201.222.5.120 (SubNet addr.)

En la dirección de máscara, el 248 es 0111000, por tanto los últimos 3 bits a 0 son destinados para las máquinas de red ($2^3=8$), por tanto habrá 6 máquinas:

201.222.5.120	SubNet address
201.222.5.121	1ª máquina de la SubNet
201.222.5.122	2ª máquina de la SubNet
.....	
201.222.5.126	última máquina de la SubNet
201.222.5.127	BROADCAST

EJEMPLO IV:

15.16.193.6	(IP addr.)
255.255.248.0	(Net MASK), el SubNet addr. Será :
15.16.192.0	y como en la máscara de red 248.0 es 11111000.00000000
	tendremos por tanto $2^{11}=2048$, lo que implica que tenemos 2046 máquinas en la SubRed:
15.16.192.0	SubNet address
15.16.192.1	1ª máquina de la SubRed
15.16.192.2	2ª máquina de la SubRed
.....	
15.16.199.254	última máquina de la SubRed
15.16.199.255	BROADCAST

Direcciones de Red y Difusión

La mayor ventaja de la codificación de información de red en las direcciones de red en IP tiene una ventaja importante: hacer posible que exista un ruteo eficiente. Otra ventaja es que las direcciones de red IP se pueden referir tanto a redes como a anfitriones (hosts). Por regla, nunca se asigna un campo hostID igual a 0 a un anfitrión individual. En vez de eso, una dirección IP con campo hostID a 0 se utiliza para referirse a la red en sí misma. En resumen:

Las direcciones IP se pueden utilizar para referirse a redes así como a anfitriones individuales. Por regla, una dirección que tiene todos los bits del campo hostID a 0, se reserva para referirse a la red en sí misma.

Otra ventaja significativa del esquema de direccionamiento IP es que éste incluye una dirección de difusión (BROADCAST) que se refiere a todos los anfitriones de la red. De acuerdo con el estándar, cualquier campo hostID consistente solamente en 1s, esta reservado para la difusión (BROADCAST). Esto permite que un sistema remoto envíe un sólo paquete que será públicamente difundido en la red especificada.

Resumen de las Reglas Especiales de Direccionamiento:

En la práctica, el IP utiliza sólo unas cuantas combinaciones de ceros ("está") o unos ("toda"). Las posibilidades son las siguientes:

TODOS 0 - Éste anfitrión permitido solamente en el arranque del sistema, pero nunca es una dirección válida de destino.

TODOS 0 | ANFITRIÓN - Anfitrión en ésta RED (solo para arranque, no como dir. válida)

TODOS 1 - Difusión limitada (red local) (Nunca es una dirección válida de origen)

RED | TODOS 1 - Difusión dirigida para RED

127 | NADA (a menudo 1) - LOOPBACK (nunca de be aparecer en una red)

Como se menciona arriba, la utilización de todos los ceros para la red sólo está permitida durante el procedimiento de iniciación de la maquina. Permite que una máquina se comunique temporalmente. Una vez que la máquina "aprende" su red y dir. IP correctas, no debe utilizar la red 0.

Protocolos de Ruteo (nivel IP)

A dos routers dentro de un sistema autónomo se les denomina "interiores" con respecto a otro.

¿Cómo pueden los routers en un sistema autónomo aprender acerca de redes dentro del sistema y redes externas?

En redes como InterNet que tienen varias rutas físicas, los administradores por lo general seleccionan una de ellas como ruta primaria. Los ruteadores interiores normalmente se comunican con otros, intercambian información de accesibilidad a red o información de ruteo de red, a partir de la cual la accesibilidad se puede deducir.

A diferencia de esto, en la comunicación de un router exterior no se ha desarrollado un solo protocolo que se utilice con los sistemas autónomos.

Protocolo de Información de Ruteo (RIP)

Uno de los I.G.P. (Interior Gateway Protocol) más ampliamente utilizados es el RIP, también conocido con el nombre de un programa que lo implementa (el routeD o Route Daemon), deriva de un protocolo de igual nombre implementado por Xerox.

El protocolo RIP es consecuencia directa de la implantación del ruteo de vector-distancia para redes locales. En principio, divide las máquinas participantes en activas o pasivas (silenciosas). Los routers activos anuncian sus rutas a los otros; las máquinas pasivas listan y actualizan sus rutas con base a estos anuncios. Sólo un router puede correr RIP en modo activo de modo que un anfitrión deberá correr el RIP en modo pasivo.

Un router con RIP en activo difunde un mensaje cada 30 segundos, éste mensaje contiene información tomada de la base de datos de ruteo actualizada. Cada mensaje consiste en pares, donde cada par contiene una dirección IP y un entero que representa la distancia hacia esta red (el IP address).

El RIP por tanto hace uso de un vector de distancias, con una métrica por número de saltos donde se considera que 16 saltos o más es infinito. De esta manera, el número de saltos (hops number) o el contador de saltos (hop count) a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de routers que un datagrama encontrará a lo largo de su trayectoria. Por tanto lo que se hace es utilizar el conteo de saltos para calcular la trayectoria óptima (aunque esto no siempre produce resultados buenos).

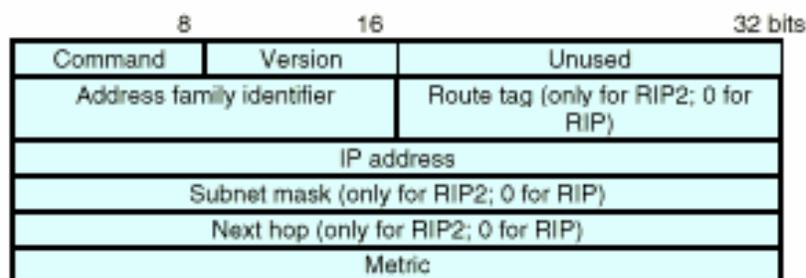
Para prevenir que dos routers oscilen entre dos o más trayectorias de costos iguales, RIP especifica que se deben conservar las rutas existentes hasta que aparezca una ruta nueva con un costo estrictamente menor.

Si falla el primer router que anuncia la ruta RIP especifica que todas las escuchas deben asociar un tiempo límite a las rutas que aprenden por medio de RIP. Cuando un router instala una ruta en su tabla, inicia un temporizador para tal ruta. Este tiempo debe iniciarse cada vez que el router recibe otro mensaje RIP anunciando la ruta. La ruta queda invalidada si transcurren 180 segundos sin que el router haya recibido un anuncio nuevamente.

RIP debe manejar tres tipos de errores ocasionados por los algoritmos subyacentes. En primer lugar, dado que el algoritmo no especifica detección de ciclos de ruteo, RIP debe asumir que los participantes son confiables o deberá tomar precauciones para prevenir los ciclos. En segundo lugar, para prevenir inestabilidades, RIP debe utilizar un valor bajo para la distancia máxima posible (RIP utiliza 16 saltos como medida máxima). Esto implica que

para una red como Internet, los administradores deben dividirla en secciones o utilizar un protocolo alternativo. En tercer y último lugar, el algoritmo vector-distancia empleado por RIP crea un problema de convergencia lenta o conteo al infinito, problema en el cual aparecerán inconsistencias, debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red. Seleccionando un infinito pequeño (16) se ayuda a limitar la convergencia lenta, pero NO se elimina.

RIP está basado en UDP, cada host que use RIP como protocolo de ruteo envía y recibe datagramas en el puerto UDP 520, el formato del datagrama RIP se muestra a continuación.



Estructura del Paquete RIP

La porción del paquete RIP desde Address Family ID hasta la Métrica puede aparecer hasta 25 veces.

Command (Comando)

Este campo especifica el propósito del datagrama.

1=> Request (requerimiento), petición para que el sistema envíe su tabla de rutas o parte de ella.

2=> Respons (respuesta), mensaje que contiene toda o parte de la tabla de rutas. Este mensaje puede ser la respuesta a un request o bien un upgrade de tablas de ruteo.

3=> Traceon, los mensajes que contenga este comando serán ignorado. Este comando esta obsoleto.

4=> Traceoff, idem Traceon

5=> Reserved, usado por Sun Microsistem para sus propios requerimientos.

Versión

El número de versión de RIP, los datagramas son procesados según la versión según se lista a continuación.

0=> Todo datagrama que posea versión cero será ignorado

1=> Los datagramas con versión 1 son procesados.

2=> Especifica un mensaje RIP de autenticación.

>2 => Todos los datagramas con versión mayor que uno son procesados.

Address Family Identifier (Identificador de tipo de familia de direcciones)

Especifica que tipo de direcciones son enviadas en el datagrama. Esto es clave dado que RIP rutea diferentes tipos de protocolos. En el caso específico de IP este campo toma el valor 2.

Route Tag

Se asigna a rutas especiales que se deben mantener y publicar, este campo define la filosofía a tomar en cuenta para separar datagramas RIP locales de datagramas RIP externos.

IP Address

Dirección IP del destino

Subnet Mask

Valor aplicado a la dirección IP para separar e identificar Host – Net

Next Hop

Dirección IP del próximo salto dentro de la ruta que debe seguir el paquete para llegar a destino

Metric

Representa el costo total de llevar el datagrama desde el host hasta el destino, este valor representa la suma de los costos de pasar por cada nodo de red hasta llegar al destino definido por el host origen.

Solución al problema de la convergencia lenta:

Es posible resolver el problema de la convergencia lenta mediante una técnica conocida como actualización de horizonte separado (split horizon update). Cuando se utilizan horizontes separados, un router registra la interfaz por la que ha recibido una ruta particular y no difunde la información acerca de la ruta de regreso sobre la misma interfaz. Con esto evitamos que la información "negativa" no sea difundida con rapidez.

Una de las técnicas finales para resolver el problema de la convergencia lenta se conoce como Poison Reverse. Una vez que una conexión desaparece, el router anuncia la conexión conservando la entrada de información por varios periodos de actualización e incluye un costo infinito en la difusión. Para hacer el Poison Reverse más efectivo, se debe combinar con las Triggered Updates (actualizaciones activadas) que obligan al router a que envíe una difusión inmediatamente al recibir "malas noticias", en lugar de esperar el próximo periodo de difusión. Al enviar una actualización inmediatamente, un router minimiza el tiempo en que es vulnerable por recibir "buenas noticias".

Protocolo SPF abierto (OSPF)

El algoritmo de propagación de rutas abierto (OSPF) propone los siguientes objetivos:

- Tecnología de estado de enlaces
- Soporta tipos de servicio (los administradores pueden instalar múltiples rutas hacia un destino, uno por cada tipo de servicio).
- Proporciona un balance de cargas entre rutas de igual peso (Si un administrador especifica múltiples rutas hacia un destino con el mismo costo, el OSPF distribuye el tráfico entre todas las rutas de la misma manera. Nótese que el RIP calcula una sola ruta para cada destino).
- Partición en áreas.
- Propagación de modificaciones entre los enlaces.
- Localización automática de routers vecinos.
- Propagación de rutas aprendidas de fuentes externas.
- Routers designados en redes multiacceso.

PROTOSCOLOS DE RESOLUCION DE DIRECCIONES

El objetivo es diseñar un software de bajo nivel que oculte las direcciones físicas (MAC) y permita que programas de un nivel más alto trabajen sólo con direcciones IP. La transformación de direcciones se tiene que realizar en cada fase a lo largo del camino, desde la fuente original hasta el destino final. En particular, surgen dos casos. Primero, en la última fase de entrega de un paquete, éste se debe enviar a través de una red física hacia su destino final. La computadora que envía el paquete tiene que transformar la dirección IP de destino final en su dirección física (MAC). Segundo, en cualquier punto del camino, de la fuente al destino, que no sea la fase final, el paquete se debe enviar hacia un router intermedio. Por lo tanto, el transmisor tiene que transformar la dirección IP del router en una dirección física.

El problema de transformar direcciones de alto nivel en direcciones físicas se conoce como *problema de asociación de direcciones* (Address Resolution Problem). Este problema se suele resolver, normalmente, mediante tablas en cada máquina que contienen pares de direcciones, de alto nivel y físicas.

En el problema de asociación de direcciones en TCP/IP para redes con capacidad de difusión como Ethernet, se utiliza un protocolo de bajo nivel para asignar direcciones en forma dinámica y evitar así la utilización de una tabla de conversiones. Este protocolo es conocido como **Protocolo de Asociación de Direcciones (ARP - Address Resolution Protocol)**. La idea detrás de la asociación dinámica con ARP es muy sencilla: cuando un host A quiere definir la dirección IP (IPb), transmite por difusión (broadcast) un paquete especial que pide al anfitrión (host) que posee la dirección IP (IPb), que responda con su dirección física (Pb). Todos los anfitriones reciben la solicitud, incluyendo a B, pero sólo B reconoce su propia dirección IP y envía una respuesta que contiene su dirección física. Cuando A recibe la respuesta, utiliza la dirección física para enviar el paquete IP directamente a B. En resumen:

El ARP permite que un anfitrión encuentre la dirección física de otro anfitrión dentro de la misma red física con sólo proporcionar la dirección IP de su objetivo.

La información se guarda luego en una tabla ARP de orígenes y destinos.

Protocolo de Asociación de Direcciones por Réplica (RARP):

Una máquina sin disco utiliza un protocolo TCP/IP para internet llamado RARP (Protocolo Inverso de Asociación de Direcciones) o Reverse Address Resolution Protocol, a fin de obtener su dirección IP desde un servidor.

En el arranque del sistema, una máquina de estas características (sin HDD permanente) debe contactar con un servidor para encontrar su dirección IP antes de que se pueda comunicar por medio del TCP/IP. El protocolo RARP utiliza el direccionamiento físico de red para obtener la dirección IP de la máquina. El mecanismo RARP proporciona la dirección hardware física de la máquina de destino para identificar de manera única el procesador y transmite por difusión la solicitud RARP. Los servidores en la red reciben el mensaje, buscan la transformación en una tabla (de manera presumible en su almacenamiento secundario) y responden al transmisor. Una vez que la máquina obtiene su dirección IP, la guarda en memoria y no vuelve a utilizar RARP hasta que se inicia de nuevo.

MENSAJES DE ERROR Y CONTROL en IP (ICMP)

Como hemos visto anteriormente, el Protocolo Internet (IP) proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada router direcciona datagramas. Si un router no puede, por ejemplo, rutear o entregar un datagrama, o si el router detecta una condición anormal que afecta su capacidad para direccionarlo (v.q., congestión de la red), necesita informar a la fuente original para que evite o corrija el problema.

Para permitir que los routers de una red reporten los errores o proporcionen información sobre circunstancias inesperadas, se agregó a la familia TCP/IP un mecanismo de mensajes de propósito especial, el *Protocolo de Mensajes de Control Internet (ICMP)*. El ICMP permite que los routers envíen mensajes de error o de control hacia otros routers o anfitriones, proporcionando una comunicación entre el software de IP en una máquina y el mismo software en otra.

Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

Formato de los mensajes ICMP:

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (TIPO) de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo CODE (CODIGO), de 8 bits, que proporciona más información sobre el tipo de mensaje, y un campo CHECKSUM (SUMA DE VERIFICACIÓN), de 16 bits. Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.

La razón de regresar más que el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa qué protocolo(s) y qué programas de aplicación son responsables del datagrama.

El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos incluyen:

<u>CAMPO TYPE</u>	<u>Tipo de Mensaje ICMP</u>
0	Respuesta de ECO
3	Destino inaccesible
4	Disminución de origen (source quench - datagrama eliminado por congestión)
5	Redireccionar (cambiar una ruta)
8	Solicitud de ECO
11	Tiempo excedido para un datagrama
12	Problema de parámetros de un datagrama
13	Solicitud de TIMESTAMP
14	Respuesta de TIMESTAMP
15	Solicitud de Información (obsoleto)
16	Respuesta de Información (obsoleto)
17	Solicitud de Máscara de dirección
18	Respuesta de máscara de dirección

Una de las herramientas de depuración más utilizadas incluye los mensajes ICMP de *echo request (8)* y *echo reply (0)*. En la mayoría de los sistemas, el comando que llama al usuario para enviar solicitudes de eco ICMP se conoce como **ping**.

Protocolo de Datagrama de Usuario (UDP)

La mayoría de los Sistemas Operativos actuales soportan multiprogramación. Puede parecer natural decir que un proceso es el destino final de un mensaje. Sin embargo, especificar que un proceso en particular en una máquina en particular es el destino final para un datagrama es un poco confuso. Primero, por que los procesos se crean y se destruyen dinámicamente, los transmisores rara vez saben lo suficiente para identificar un proceso en otra máquina. Segundo, nos gustaría poder reemplazar los procesos que reciben datagramas, sin tener que informar a todos los transmisores (v.q. reiniciar la máquina puede cambiar todos los PID de los procesos). Tercero, necesitamos identificar los destinos de las funciones que implantan sin conocer el proceso que implanta la función (v.q. permitir que un transmisor contacte un servidor de ficheros sin saber qué proceso en la máquina de destino implanta la función de FS).

En vez de pensar en un proceso como destino final, imaginaremos que cada máquina contiene un grupo de puntos abstractos de destino, llamados *puertos de protocolo*. Cada puerto de protocolo se identifica por medio de un número entero positivo. Para comunicarse con un puerto externo, un transmisor necesita saber tanto la dirección IP de la máquina de destino como el número de puerto de protocolo del destino dentro de la máquina.

El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. En resumen:

El UDP proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de la computadora anfitrión.

Formato de los mensajes UDP:

Cada mensaje UDP se conoce como *datagrama de usuario*. Conceptualmente, un datagrama de usuario consiste en dos partes: un encabezado UDP y un área de datos UDP. El encabezado se divide en cuatro campos de 16 bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

Protocolo de Control de Transmisión (TCP) **Servicio de Transporte de Flujo Confiable**

En las secciones anteriores hemos visto el servicio de entrega de paquetes sin conexión y no confiable, que forma la base para toda comunicación en InterNet, así como el protocolo IP que lo define.

Ahora veremos el segundo servicio más importante y mejor conocido a nivel de red, la entrega de flujo confiable (Reliable Stream Transport), así como el Protocolo de Control de Transmisión (TCP) que lo define.

En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga de la red,...). Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de propósito general para estos casos.

La interfaz entre los programas de aplicación y la entrega confiable (es, decir, las características del TCP) se caracterizan por cinco funciones:

Servicio Orientado a Conexión: El servicio de entrega de flujo en la máquina destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en la máquina origen.

Conexión de Circuito Virtual: Durante la transferencia, el software de protocolo en las dos máquinas continúa comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo (v.q. falla el hardware de red), ambas máquinas detectarán la falla y la reportarán a los programas apropiados de aplicación. Se utiliza el término *circuito virtual* para describir dichas conexiones porque aunque los programas de aplicación visualizan la conexión como un circuito dedicado de hardware, la confiabilidad que se proporciona depende del servicio de entrega de flujo.

Transferencia con Memoria Intermedia: Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente bytes de datos al software de protocolo. Cuando se transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueden ser tan pequeñas como un byte. En el extremo receptor, el software de protocolo entrega bytes del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y se verifican. El software de protocolo puede dividir el flujo en paquetes, independientemente de las piezas que transfiera el programa de aplicación. Para hacer eficiente la transferencia y minimizar el tráfico de red, las implantaciones por lo general recolectan datos suficientes de un flujo para llenar un datagrama razonablemente largo antes de enviarlo. Por lo tanto, inclusive si el programa de aplicación genera el flujo un byte a la vez, la transferencia a través de la red puede ser sumamente eficiente. De forma similar, si el programa de aplicación genera bloques de datos muy largos, el software de protocolo puede dividir cada bloque en partes más pequeñas para su transmisión. Para

aplicaciones en las que los datos de deben entregar aunque no se llene una memoria intermedia, el servicio de flujo proporciona un mecanismo de *empuje* o *push* que las aplicaciones utilizan para forzar una transferencia. En el extremo transmisor, el push obliga al software de protocolo a transferir todos los datos generados sin tener que esperar a que se llene una memoria intermedia. Sin embargo, la función de push sólo garantiza que los datos se transferirán, por tanto, aún cuando la entrega es forzada, el software de protocolo puede dividir el flujo en formas inesperadas (v.q. el transmisor puede reducirlo en caso de congestión).

Flujo no estructurado: Posibilidad de enviar información de control junto a datos.

Conexión Full Duplex: Se permite la transferencia concurrente en ambas direcciones. Desde el punto de vista de un proceso de aplicación, una conexión full duplex permite la existencia de dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente. Esto ofrece una ventaja: el software subyacente de protocolo puede enviar datagramas de información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga REDUCE EL TRAFICO en la red.

La “Contradicción”: Hemos visto que el servicio de entrega de flujo confiable garantiza la entrega de los datos enviados de una máquina a otra sin pérdida o duplicación. Surge ahora la pregunta contradictoria “del millón”: *¿Cómo puede el software subyacente de protocolo proporcionar una transferencia confiable si el sistema subyacente de comunicación sólo ofrece una entrega NO confiable de paquetes?*

La respuesta es complicada, pero la mayor parte de los protocolos confiables utilizan una técnica fundamental conocida como *acuse de recibo positivo con retransmisión*. La técnica requiere que un receptor se comunique con el origen y le envíe un mensaje de acuse de recibo (**ACK**) conforme recibe los datos (ver los primeros temas para una descripción más detallada). El transmisor guarda un registro de cada paquete que envía y espera un ACK antes de enviar el siguiente paquete. El transmisor también arranca un temporizador cuando envía un paquete y lo retransmite si dicho temporizador expira antes de que llegue un ACK.

El problema final de la confiabilidad surge cuando un sistema subyacente de entrega de paquetes los duplica. Los duplicados también pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión prematura. Para evitar la confusión causada por ACKs retrasados o duplicados, los protocolos de acuses de recibo positivos envían los números de secuencia dentro de los ACKs, para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

Pero, como casi todo en esta vida es un problema tras otro, el TCP no iba a ser menos; uno de los problemas que acarrea lo anterior es que un protocolo simple de acuses de recibo positivos ocupa una cantidad sustancial de ancho de banda de red debido a que debe retrasar el envío de un nuevo paquete hasta que reciba un ACK del paquete anterior.

La solución está en otra técnica conocida como *ventana deslizante*, que es una forma más compleja de acuse de recibo positivo y retransmisión. Los protocolos de ventana deslizante utilizan el ancho de banda de red de mejor forma al permitir que el transmisor envíe varios paquetes sin esperar el ACK (remitirse a capítulos anteriores para una descripción de éste método).

Puertos, conexiones y puntos extremos.

Al igual que el UDP, el TCP reside sobre el IP en el esquema de estratificación por capas de protocolos. El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el demultiplexado del tráfico TCP entrante entre los programas de aplicación. Así mismo, al igual que el UDP, el TCP utiliza números de *puerto de protocolo* para identificar el destino final dentro de una máquina. Cada puerto tiene asignado un número entero pequeño utilizado para identificarlo.

Para comprender el significado de un puerto hay que pensar de cada puerto como en una cola de salida en la que el software de protocolo coloca los datagramas entrantes, aunque en realidad los puertos TCP son más complejos, ya que un número de puerto no corresponde a un sólo objeto. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos.

¿Qué es exactamente un punto extremo en TCP?

Un punto extremo es un par de números enteros (**host, puerto**), en donde *host* es la dirección IP de un anfitrión y *puerto* es el un puerto TCP en dicho anfitrión.

Las conexiones vienen definidas por dos puntos extremos, y es más: la abstracción de la conexión para TCP permite que varias conexiones compartan un punto extremo (por ejemplo, varias conexiones en los mismos puertos). Esto es posible a que el TCP identifica una conexión por medio de un par de puntos extremos, y por eso varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

El TCP combina la asignación dinámica y estática de puertos mediante un conjunto de *asignación de puertos bien conocidos* para programas llamados con frecuencia, pero la salida de la mayor parte de los números disponibles para el sistema se asigna conforme los programas lo necesitan.

La siguiente tabla muestra un ejemplo de números de puerto TCP asignados actualmente.

DECIMAL	CLAVE	CLAVE UNIX	DESCRIPCIÓN
0			Reservado
1	TCPMUX		Multiplexor TCP
5	RJE		Introducción de función remota
7	ECHO	echo	Eco
9	DISCARD	discard	Abandonar
11	USERS	systat	Usuarios activos
13	DAYTIME	daytime	Fecha, hora
15		netstat	Estado de red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de caracteres
20	FTP-DATA	ftp-data	Datos para FTP
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Conexión por terminal
25	SMTP	smtp	Protocolo de Transporte de Correo Sencillo
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	Comando whois
53	DOMAIN	nameserver	Servidor de nombre de dominio (DNS)
79	FINGER	finger	Comando finger
93	DCP		Protocolo de Control de Dispositivo
101	HOSTNAME	hostnames	Servidor de Nombre de Anfitrión NIC
103	X400	x400	Servicio de correo X400
104	X400-SND	x400-snd	Envío de correo X400

La Interface SOCKET

El Paradigma de E/S de UNIX y la E/S de la Red

En primer lugar hemos de distinguir entre los protocolos de interface y el TCP/IP, debido a que los estándares no especifican exactamente cómo es que interactúan los programas de aplicación con el software de protocolo.

A pesar de la carencia de un estándar, veremos la interface del UNIX BSD como se emplea el TCP/IP en programación. En particular, la interface *Winsock* proporciona la funcionalidad socket para MsWindows.

Veamos pues cómo empezó todo este “jaleo”:

Unix fue desarrollado y diseñado como un sistema operativo de tiempo compartido para computadoras uniprocador. Se trata, como ya es sabido, de un S.O. orientado a proceso, en el que cada programa de aplicación se ejecuta como un proceso de nivel de usuario. Derivados de los MULTICS, los primitivos sistemas de E/S de UNIX siguen un paradigma conocido como “*Open-Read-Write-Close*”: Antes de que un proceso de usuario pueda ejecutar operaciones de E/S, llama a *Open* para especificar el archivo o dispositivo que se va a utilizar (recuérdese la independencia de dispositivo de UNIX) y obtiene el

permiso. La llamada a *Open* devuelve un pequeño entero (el descriptor de archivo) que el proceso utiliza al ejecutar las operaciones de E/S en el archivo abierto. Una vez abierto un objeto, se pueden hacer las llamadas a *Read* y/o *Write*. Tanto *Read* como *Write* toman tres argumentos (descriptor de archivo, dirección del buffer y nº de bytes a transferir). Una vez completadas estas operaciones el proceso llama a *Close*.

Originalmente, todas las operaciones UNIX se agrupaban como se ha descrito anteriormente, y una de las primeras implementaciones de TCP/IP también utilizó éste paradigma. Pero el grupo que añadió los protocolos TCP/IP al BSD decidió que, como los protocolos de red eran más complejos que los dispositivos convencionales de E/S, la interacción entre los programas de usuario y los protocolos de red debía ser más compleja. En particular, la interface de protocolo debía permitir a los programadores crear un código de servidor que esperaba las conexiones pasivamente, así como también un código cliente que formara activamente las conexiones. Para manejar datagramas, se decidió abandonar este paradigma.

La abstracción de SOCKET

La base para la E/S de red en UNIX se centra en una abstracción conocida como *socket*.

El socket es la generalización del mecanismo de acceso a archivos de UNIX que proporciona un punto final para la comunicación. Al igual que con el acceso a archivos, los programas de aplicación requieren que el S.O. cree un socket cuando se necesite. El S.O. devuelve un entero que el programa de aplicación utiliza para hacer referencia al socket recientemente creado. La diferencia principal entre los descriptors de archivo y los descriptors de socket es que el sistema operativo enlaza un descriptor de archivo a un archivo o dispositivo del sistema cuando la aplicación llama a *Open*, pero puede crear sockets sin enlazarlos a direcciones de destino específicas.

Básicamente, el socket es una API en la que el servidor espera en un puerto predefinido y el cliente puede utilizar sin embargo un puerto dinámico.

EJEMPLOS:

- Creación de un socket:

resultado = socket (pf, tipo, protocolo)

El argumento PF especifica la familia de protocolo que se va utilizar con el socket (v.q. PF_INET para TCP/IP). El argumento tipo especifica el tipo de comunicación que se desea (v.q. SOCK_DGRAM para servicio de entrega de datagramas sin conexión, o SOCK_STREAM para servicio de entrega confiable de flujo).

- Envío de datos:

`write (socket, buffer, lenght)`

- Especificación de una dirección local:

`bind (socket, localaddr, addrlen)`

Inicialmente, un socket se crea sin ninguna asociación hacia direcciones locales o de destino. Para los protocolos TCP/IP, esto significa que ningún número de puerto de protocolo local se ha asignado y que ningún puerto de destino o dirección IP se ha especificado. En muchos casos, los programas de aplicación no se preocupan por las direcciones locales que utilizan, ni están dispuestos a permitir que el software de protocolo elija una para ellos. Sin embargo, los procesos del servidor que operan en un puerto “bien conocido” deben ser capaces de especificar dicho puerto para el sistema. Una vez que se ha crea un socket, el servidor utiliza una llamada del sistema BIND (enlace) para establecer una dirección local para ello. BIND tiene la forma que se ha descrito arriba.

Sistema de Nombres de Dominios (DNS)

Los protocolos descritos anteriormente utilizan enteros de 32 bits, llamados direcciones de protocolo internet (dir. IP) para identificar máquinas. Aún cuando cada dirección proporciona una representación compacta y conveniente para identificar la fuente y el destino en paquetes enviados a través de la red, los usuarios prefieren asignar a las máquinas nombres fáciles de recordar.

El DNS tiene dos aspectos conceptualmente independientes. El primero es abstracto. Especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. El segundo es concreto: especifica la implantación de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones.

Resolución de nombres

Conceptualmente, la resolución de nombres de dominio procede de arriba hacia abajo, comenzando con el servidor de nombres raíz y siguiendo luego hacia los servidores localizados en las ramas del árbol de la red.

Hay dos forma de utilizar en sistema de nombres de dominio: contactar un servidor de nombres cada vez o solicitar al sistema de servidores de nombres que realice la traducción completa. En este caso, el software cliente forma una solicitud de nombres de dominio que contiene el nombre a resolver, una declaración sobre la clase del nombre, el tipo de respuesta deseada y un código que especifica si el servidor de nombres debe traducir el nombre completamente. Se envía la solicitud a un servidor de nombre para su resolución.

Cuando un servidor de nombres de dominio recibe una solicitud, verifica si el nombre señala un subdominio sobre el cual tenga autoridad. Si es así, traduce el nombre a una dirección de acuerdo con su base de datos y anexa una respuesta a la solicitud, antes de enviarla de regreso al cliente. Si el DNS no puede resolver el nombre completamente, verifica que tipo de interacción especificó el cliente. Si el cliente solicita una traducción completa (una *resolución recursiva* en la terminología DNS), el servidor se pone en contacto con un servidor de nombres de dominio que pueda resolver el problema del nombre y devuelve la respuesta al cliente.

Si el cliente solicita una resolución no recursiva (resolución iterativa), el servidor de nombres no puede dar una respuesta. Se genera una réplica que especifica el nombre del servidor que el cliente deberá contactar la próxima vez para resolver el nombre.

Cómo encuentra un cliente un DNS para comenzar la búsqueda?

Cómo encuentra un DNS a otros DNSs que puedan responder a las solicitudes que el no puede responder?

La respuesta es sencilla: Un cliente debe saber como contactar al ultimo DNS para asegurarse de que el DNS puede alcanzar a otros, el sistema de dominio requiere que cada servidor conozca la dirección del último servidor en la raíz. Además, un servidor podría conocer la dirección de un servidor para el dominio de un nivel inmediatamente superior (llamado padre).

Los DNSs utilizan un puerto de protocolo bien conocido para toda comunicación, así, los clientes saben cómo comunicarse con un servidor una vez que conocen la dirección IP de la máquina que se conecta al servidor. No hay forma estándar que los anfitriones localicen una máquina en el entorno local, el cual corre un DNS; esto se encuentra abierto para quien diseñe el software cliente.

En algunos sistemas, la dirección de la máquina que proporciona el servicio de nombres de dominio está dentro de la frontera de los programas de aplicación en el tiempo de compilación, mientras que en otros la dirección se encuentra configurada dentro del S.O. en el arranque. En otros mas, al administrador coloca la dirección de un servidor en un archivo en almacenamiento secundario (/etc/hosts).

2.3.1 Switches y Routers

- Tecnología de SWITCH
- Tecnología de RUTEADOR
- Dónde usar Switch?
- Dónde usar un ruteador?
- Segmentando con Switches y Ruteadores
- Segmentando LANs con Switch
- Segmentando Subredes con Ruteadores
- Seleccionando un Switch o un Ruteador para Segmentar
- Diseñando Redes con Switches y Ruteadores
- Diseñando Redes para Grupos de Trabajo
- Pequeños Grupos de Trabajo

Opción #1: Solución con Ruteador

- Opción #2: Solución con Switch*
- Grupos de Trabajo Departamentales
Respecto al tráfico de Broadcast
 - El Futuro de los Switches
 - Soporte Multimedia
 - Futuro del Ruteo
 - Interfaces LAN y WAN

Tecnología de SWITCH

Un switch es un dispositivo de *propósito especial* diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

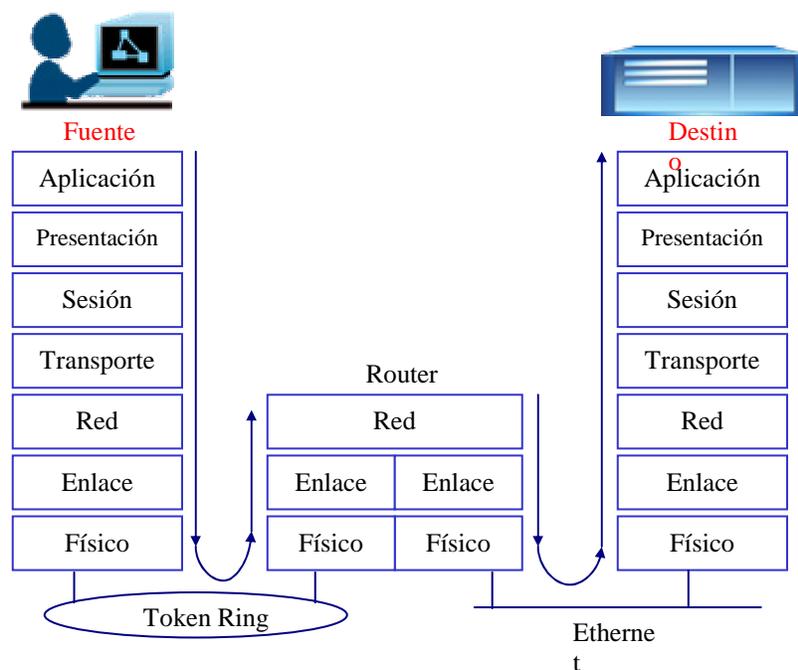


Figura: Modelo de trabajo de Switch respecto a OSI

Tecnología de RUTEADOR

Un ruteador es un dispositivo de *propósito general* diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes. El ruteador realiza dos funciones básicas:

- El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
- La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesamiento de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

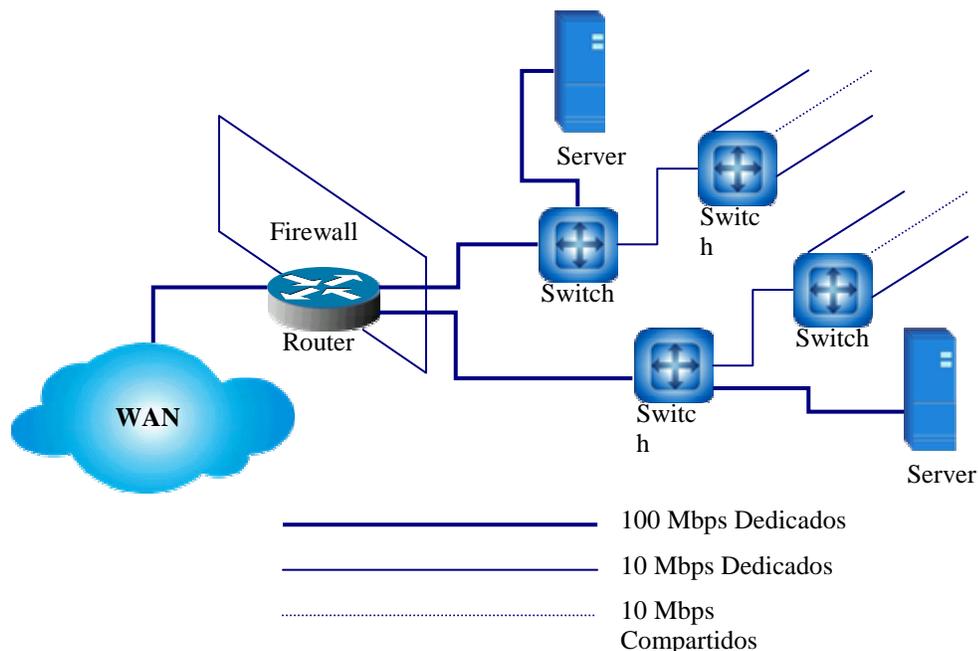


Figura: Segmentación de redes por medio de Router

Dónde usar Switch?

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente/servidor, pues los usuarios juzgan la red por la rapidez de obtener un prompt y la confiabilidad del servicio.

Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- El elevado incremento de nodos en la red.
- El continuo desarrollo de procesadores más rápidos y poderosos en estaciones de trabajo y servidores.
- La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente/servidor.
- Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

La regla tradicional 80/20 del diseño de redes, donde el 80% del tráfico en una LAN permanece local, se invierte con el uso del switch.

Los switches resuelven los problemas de anchos de banda al segmentar un dominio de colisiones de una LAN, en pequeños dominios de colisiones.

En la figura la segmentación casi elimina el concurso por el medio y da a cada estación final más ancho de banda en la LAN.

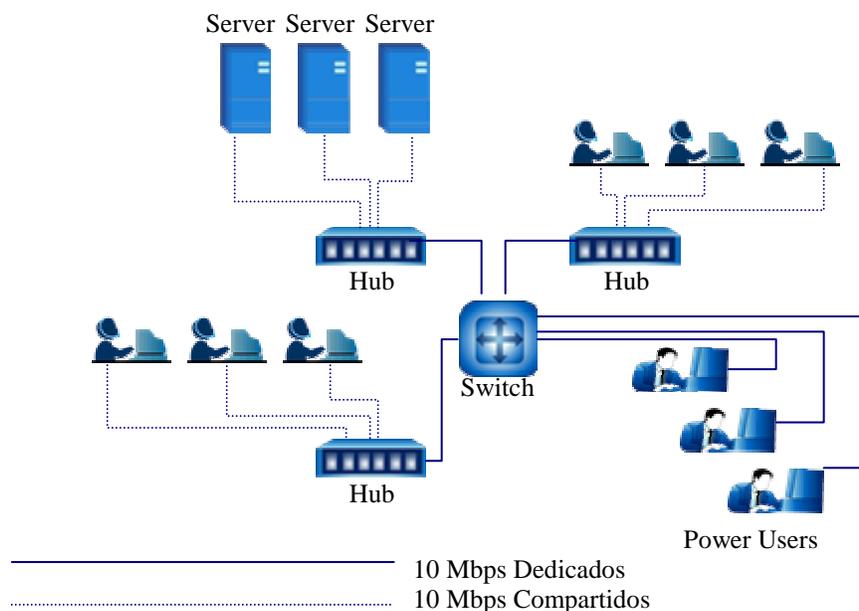


Figura: Segmentación de red por medio de switch

Dónde usar un ruteador?

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de broadcast.
- Suministrar un envío inteligente de paquetes. Y
- Soportar rutas redundantes en la red.

Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasaran a través del ruteador.

Otros importantes beneficios del ruteador son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

Segmentando con Switches y Ruteadores

Probablemente el área de mayor confusión sobre switch y ruteador, es su habilidad para segmentar la red y operar en diferentes capas del modelo OSI, permitiendo así, un tipo único de diseño de segmentación.

Segmentando LAN's con Switch

Podemos definir una LAN como un dominio de colisiones, donde el switch esta diseñado para segmentar estos dominios en dominios más pequeños. Puede ser ventajoso, pues reduce el número de estaciones a competir por el medio.

En la figura cada dominio de colisión representa un ancho de banda de 10 Mbps, mismo que es compartido por todas las estaciones dentro de cada uno de ellos. Aquí el switch incrementa dramáticamente la eficiencia, agregando 60 Mbps de ancho de banda.

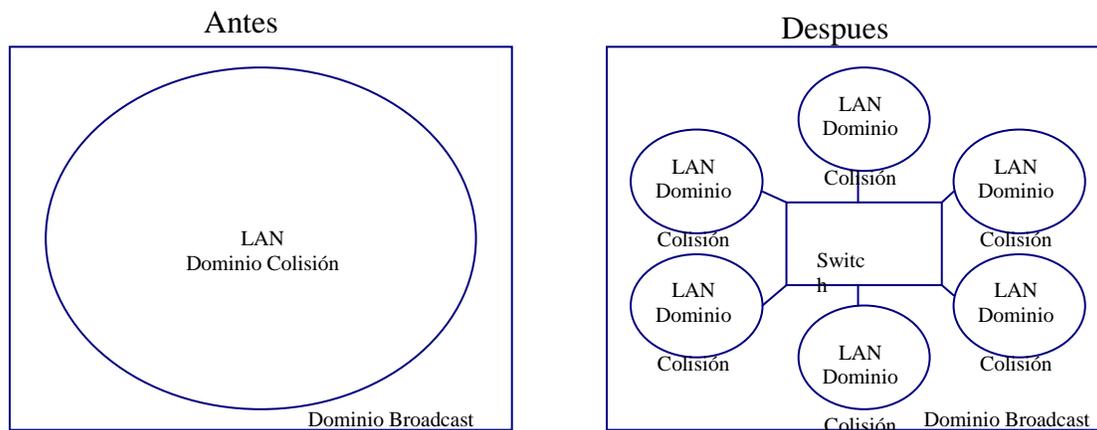


Figura: Beneficios de la segmentación con switch

Es importante notar que el tráfico originado por el broadcast en un dominio de colisiones, será reenviado a todos los demás dominios, asegurando que todas las estaciones en la red se puedan comunicar entre si.

Segmentando Subredes con Ruteadores

Una subred es un puente o un switch compuesto de dominios de broadcast con dominios individuales de colisión. Un ruteador esta diseñado para interconectar y definir los limites de los dominios de broadcast.

La figura muestra un dominio de broadcast que se segmento en dos dominios de colisiones por un switch, aquí el tráfico de broadcast originado en un dominio es reenviado al otro dominio.

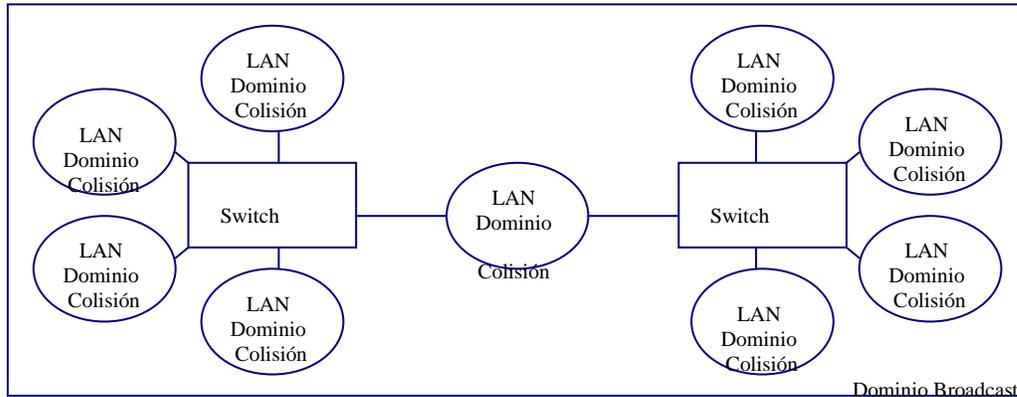


Figura: Un dominio de broadcast en dos dominios de colisión

En la siguiente figura muestra la misma red, después que fue segmentada con un ruteador en dos dominios diferentes de broadcast. En este medio el tráfico generado de broadcast no fluye a través del ruteador al otro dominio.

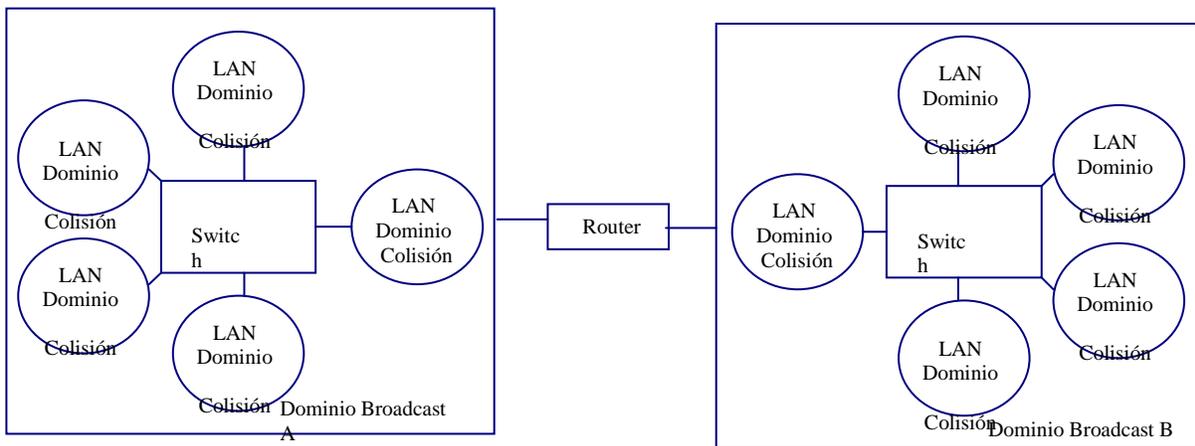


Figura: Segmentación de dominio de broadcast

Seleccionando un Switch o un Ruteador para Segmentar

Al trabajar un ruteador en la capa 3 del modelo OSI, puede también ejecutar funciones de la capa 2, es decir el ruteador crea dominios de broadcast y de colisiones separados en cada interface. Esto significa que tanto el switch como el ruteador pueden usarse para segmentar una LAN y adicionar ancho de banda.

Entonces, cual es la selección más óptima para el diseño de la red?

- Si la aplicación requiere soporte para rutas redundantes, envío inteligente de paquetes o acceder la WAN, se debe seleccionar un ruteador.
- Si la aplicación sólo requiere incrementar ancho de banda para descongestionar el tráfico, un switch probablemente es la mejor selección.

Dentro de un ambiente de grupos de trabajo, el costo interviene en la decisión de instalar un switch o un ruteador y como el switch es de propósito general tiene un bajo costo por puerto en comparación con el ruteador.

Además el diseño de la red determina cuales son otros requerimientos (redundancia, seguridad o limitar el tráfico de broadcast) que justifique el gasto extra y la complejidad de instalar un ruteador dentro de dicho ambiente.

Diseñando Redes con Switches y Ruteadores

Cuando se diseña eficientemente una red de comunicación de datos, puede ser la parte central de una organización de negocios. Pero si se diseña mal, la red puede ser un obstáculo para el éxito de la organización.

El diseño abarca todos los aspectos del sistema de comunicación, desde el nivel individual de enlace hasta el manejo global de la red, también un diseño exitoso debe fijarse dentro de los límites presupuestales de la organización.

Se mostrarán diferentes diseños de red con switches y ruteadores, sus beneficios y limitaciones en grupos de trabajo, backbone y ambiente WAN, en ellos se usa la siguiente tecnología:

Campus Backbone	Building Backbone	Server	Workgroup
FDDI	Fast Ethernet	Fast Ethernet	Ethernet
ATM	FDDI	FDDI	Fast Ethernet
	ATM	ATM	Token Ring

Figura: Tecnologías de Enlace

Estos diseños no deben ser vistos como una solución, pues cada uno de ellos tiene sus propias prioridades, topología y objetivos.

Diseñando Redes para Grupos de Trabajo

Un grupo de trabajo es una colección de usuarios finales que comparten recursos de cómputo; pueden ser grandes o pequeños, localizados en un edificio o un campus y ser permanente o un proyecto.

Pequeños Grupos de Trabajo

En la figura se ve un típico ambiente de grupos de trabajo en una red interna. Tiene los concentradores y puede crecer hasta 20, con 200 usuarios.

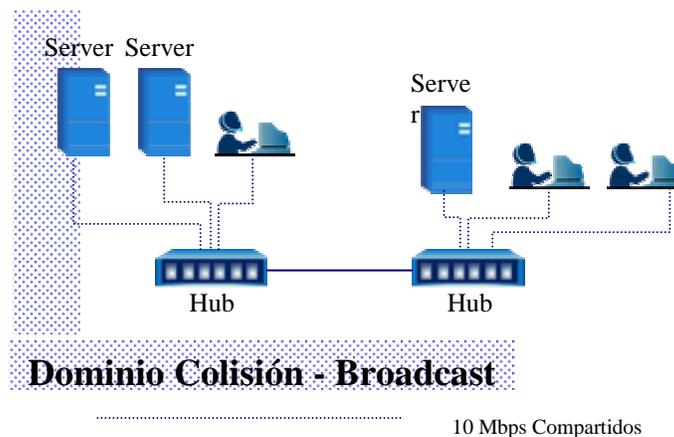
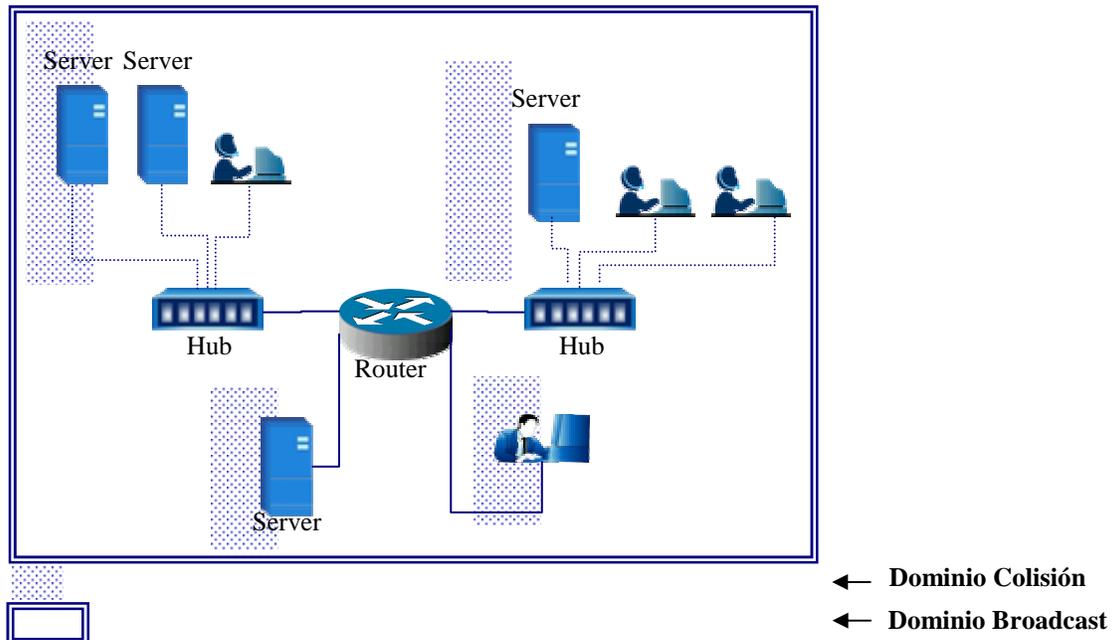


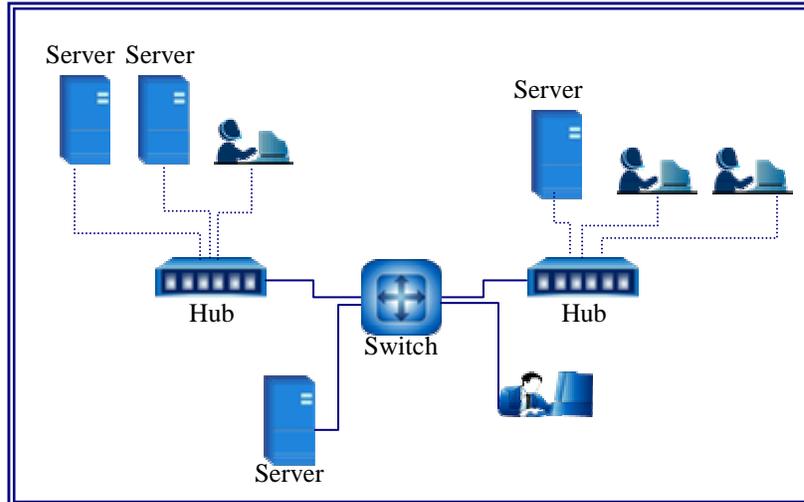
Figura: Ambiente típico de grupo de trabajo

Aquí el administrador quiere maximizar el ancho de banda de los servidores y dividir las PCs en pequeños dominios de colisiones que compartan 10 Mbps y sólo un número limitado de usuarios poderosos requerirán 10 Mbps dedicados para sus aplicaciones.

Opción #1: Solución con Ruteador**Figura: Segmentación vía router**

El ruteador es configurado con una interface dedicada de alta velocidad al servidor y un número grande de interfaces ethernet, las cuales son asignadas a cada uno de los concentradores y usuarios poderosos. Y para instalarlo, el administrador de red divide los dominios grandes de broadcast y colisiones en dominios pequeños.

La selección del ruteador no se baso en lo económico o en la tecnología. Desde una perspectiva de costo, el ruteador tiene un alto costo por puerto y un gasto a largo plazo en su manejo, mayor que el de un switch. Desde una perspectiva tecnológica el ruteador proporciona pocos paquetes de salida. Probablemente también los niveles de tráfico de broadcast no justifiquen la complejidad adicional de separarlos.

Opción #2: Solución con Switch**Figura: Segmentación vía router**

La figura muestra el mismo grupo de trabajo, pero con un switch. En este ambiente el dominio de broadcast se divide en 4 dominios de colisiones, donde los usuarios atados a dichos dominios comparten 10 Mbps. Los accesos dedicados a servidores y usuarios poderosos, eliminan la competencia por acceder el medio y el servidor local tiene una interface de alta velocidad para eliminar posibles cuellos de botella. Además de garantizar que los paquetes no se perderán por la limitación del buffer, cuando el tráfico de varios puertos sea enviado a un sólo puerto destino.

Por ejemplo, supongamos un ambiente ethernet, donde cada uno de los 5 puertos del switch es de 10 Mbps, enviando 64 paquetes hacia el servidor en un rango de 4,000 pps, la carga total por puerto será de 20,000 pps. Este valor sobre pasa al estándar ethernet de 14,880 pps, (límite por frames de 64-octetos). Este problema se elimina con una interface Fast Ethernet, donde su capacidad es hasta 148,800 pps. para frames de 64-octetos.

Si se tiene un dispositivo backbone colapsado en la central de datos de alta velocidad, se puede adicionar un segundo modulo al switch, para acomodarse a esa tecnología e ir emigrando suavemente.

Si únicamente se quiere dar hancha de banda a los grupos de trabajo, el switch es la mejor solución, pues sus ventajas son mayores a las del ruteador para este tipo de aplicaciones dado que:

- El switch ofrece mayor velocidad, al enviar su salida a todos los puertos a la vez. El rendimiento de su salida puede ser crítico, cuando el cliente y el servidor son puestos en segmentos diferentes, pues la información debe pasar por diversos dispositivos de la red interna.
- El switch da mayor rendimiento por puerto en termino de costos que un ruteador. Un switch ethernet tiene un costo aproximado de \$200 DLLS. por puerto, mientras que un ruteador ethernet tiene un costo aproximado de \$2,000 DLLS. El costo es un factor importante, pues limita la compra de dispositivos y el poder adicionar segmentos a la red.

- Un switch es más fácil de configurar, manejar y reparar que un ruteador. Cuando el número de dispositivos de la red se incrementa, generalmente es más deseable tener unos cuantos dispositivos complejos, que un gran número de dispositivos simples.

Grupos de Trabajo Departamentales

Un grupo de trabajo departamental, es un grupo compuesto de varios grupos pequeños de trabajo. La figura ilustra un típico grupo de trabajo departamental, donde los grupos de trabajo individuales son combinados con un switch que proporciona interfaces de alta velocidad -Fast ethernet, FDDI o ATM. Y todos los usuarios tienen acceso a la granja de servidores, vía una interface compartida de alta velocidad al switch departamental.

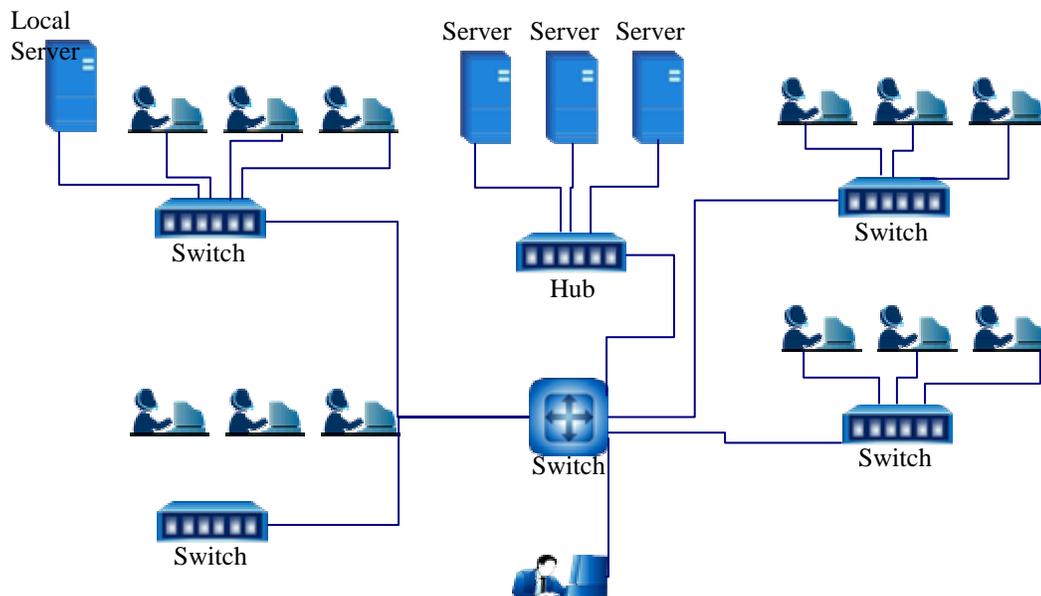


Figura: Grupos de Trabajo Departamentales

La eficiencia del switch departamental, debe ser igual a los switches individuales, ofreciendo además un rico conjunto de facilidades, versatilidad modular y una forma de migración a tecnologías de alta velocidad. En general un switch a nivel departamental es la base de los dispositivos del grupo de trabajo.

Si los usuarios necesitan más ancho de banda, selectivamente pueden reemplazar la base instalada de concentradores por switches de 10 Mbps de bajo costo.

Respecto al tráfico de Broadcast

Dado el alto rendimiento que ofrecen los switches, algunas organizaciones se interesan por los altos niveles de tráfico de broadcast y multicast. Es importante comprender que algunos protocolos como IP, generan una cantidad limitada de tráfico de broadcast, pero otros como IPX, hacen un abundante uso de tráfico de broadcast por requerimientos de RIP, SAP, GetNearestServer y similares.

El Futuro de los Switches

El precio de la tecnología del switch continua descendiendo, como resultado del desarrollo ASIC unido con la eficiencia de la manufactura y técnicas de distribución. Como el costo por puerto del switch se aproxima al de los hubs, muchos usuarios eligen el switch. La extensa disponibilidad de la tecnología de switch de bajo costo tiene implicaciones para las redes de los edificios y el backbone de campus. Habrá una demanda creciente para switches de backbone de alta densidad, con un número grande de puertos de alta velocidad, para enlazar grupos de trabajo individuales.

Eventualmente el equipo de escritorio será dedicado a enlaces de 10 Mbps, la mayoría de los servidores estarán conectados a los switch de alta velocidad y ATM se usara en enlaces internos de los edificios y al backbone de campus.

Soporte Multimedia

Nadie puede saber con certeza el futuro de las aplicaciones multimedia, como serán o como se explotarán. En un medio LAN un enlace privado de 10 Mbps provee bastante ancho de banda para soportar video comprimido para videoconferencias. Pero el ancho de banda no es bastante.

Tienen pensado poner alta prioridad al tráfico de multimedia, tal que el tráfico tradicional de datos en un camino de datos multimedia no tenga un tiempo sensitivo. En resumen, hay más preguntas concernientes a la habilidad de distribuir aplicaciones multimedia a través de la WAN.

Un buen despliegue de aplicaciones multimedia requiere que la red tenga altos niveles de funcionalidad y calidad fija en el servicio. Hay diversas innovaciones que se integran dentro de la tecnología del switch para realzar el soporte de futuras aplicaciones multimedia:

- Sobre segmentos privados ethernet 40% o 50% del ancho de banda utilizado, es considerado funcionalmente excelente, debido a los tiempos muertos de colisiones, lagunas de interframe y otros. Sobre una interface LAN privada, una tecnología tal como PACE, asegura un acceso imparcial al ancho de banda, mantiene funcionalidad fluida y crea múltiples niveles de servicio. PACE permite tiempo real, multimedia y las aplicaciones de datos tradicionales pueden coexistir. Con esta tecnología, la utilización del ancho de banda puede incrementarse hasta un 90%.
- El IGMP es un estándar IETF que permite a un host participar en un grupo de IP multicast. Ahora los switches son requeridos para enviar tráfico IP multicast sobre todas las interfaces, despojando el ancho de banda sobre esas interfaces que no

tienen miembros del grupo multicast. Switches pequeños pueden curiosear sobre mensajes IGMP para crear dinámicamente filtros para limitar el flujo de multicast en la red de switches.

Futuro del Ruteo

El ruteo es la llave para desarrollar redes internas. El desafío es integrar el switch con ruteo para que el sistema aproveche el diseño de la red. Cada uno de los grandes vendedores de ruteadores tiene investigando más de 300 millones de dólares en hora/hombre, desarrollando líneas de código para sus productos. Cada liberación de software representa un tremendo esfuerzo de ingeniería, para asegurar que el ruteador soporte la última tecnología y dirección de diseño en redes internas.

Inicialmente los switches estarán en todas las organizaciones que requieran incrementar el ancho de banda y obtener la funcionalidad que necesitan. No obstante al incrementar la complejidad de la red, los administradores necesitarán controlar el ambiente de switch, usando segmentación, redundancia, firewall y seguridad. En este punto, la disponibilidad de ruteo sofisticado esencialmente crecerá y la red se escalará en grandes redes de switches.

El usuario demandará que los vendedores de ruteadores hagan sus productos fáciles de instalar y configurar.

Interfaces LAN y WAN

En general el ruteo dentro de los edificios se está moviendo hacia un pequeño número de interfaces de alta funcionalidad para conectar switches de alta densidad en los ruteadores. Este es el verdadero modelo costo-efectividad, especialmente cuando un gran número de interfaces LAN van de velocidades baja a media.

Como el número de interfaces LAN decrementa, la venta para interfaces WAN sobre la oficina central de ruteadores es movida a dos diferentes direcciones. Algunos usuarios requerirán un incremento en el número de interfaces WAN de baja velocidad para conectar sus sitios remotos con arrendamiento de líneas y conexiones telefónicas. Otros usuarios requerirán unas cuantas interfaces físicas como FrameRelay y ISDN, proporcionando la funcionalidad de líneas dedicadas arrendadas por fracción de costo.