**Router**

****

**Figura Router**

Es un dispositivo o, en algunos casos, software en un computador, que determina el próximo punto (generalmente dirección lógica) en la red al cual debe ser enviado un paquete para llegar a su destino. El router trabaja en la capa de red, debe estar conectado al menos a dos redes para decir a cuál de ellas enviar cada paquete que le llega, basándose en el conocimiento que tenga de las redes a las que está conectado y la defragmentación de cada trama recibida. Un router crea o mantiene una tabla de las rutas disponibles y sus condiciones, luego usa esta información de distancia y costo en un algoritmo de enrutamiento para determinar la mejor ruta por la cual evitar los paquetes que le llegan. Los routers poseen generalmente varios puertos los cuales son usados para configuración y para transmisión de datos. Normalmente un router posee al menos un puerto Ethernet (o cualquier otro estipulado por las normas IEEE, ej. Token Ring ), un puerto serial y un puerto de Consola o Administración. Los puertos Ethernet en los routers son usados para conectar redes de área local, LAN, con el fin de que los hosts conectados a esta red puedan llegasr a otros puntos ubicados en diferentes redes a la de él, sea: pasando a otro puerto Ethernet, a algunos puertos seriales o a otro.

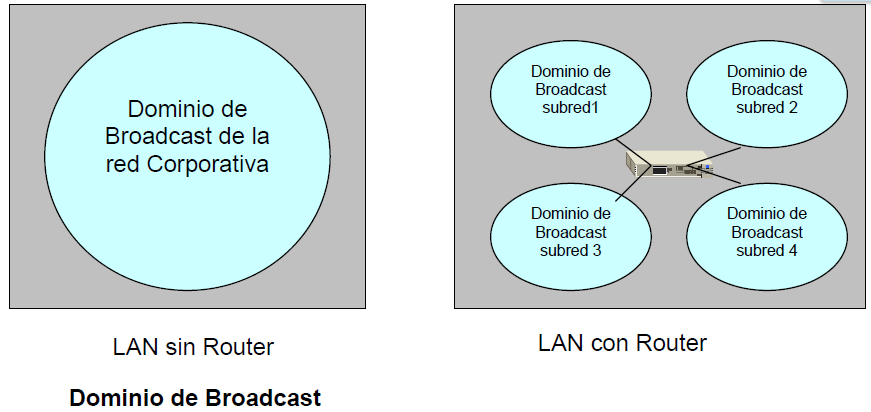
**Tipos de routers**

Los tipos principales de routers son:

**Estático:** Los routers estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.

**Dinámico:** Los routers dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración.

Son más sofisticados que los routers estáticos, examinan la información de otros routers y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

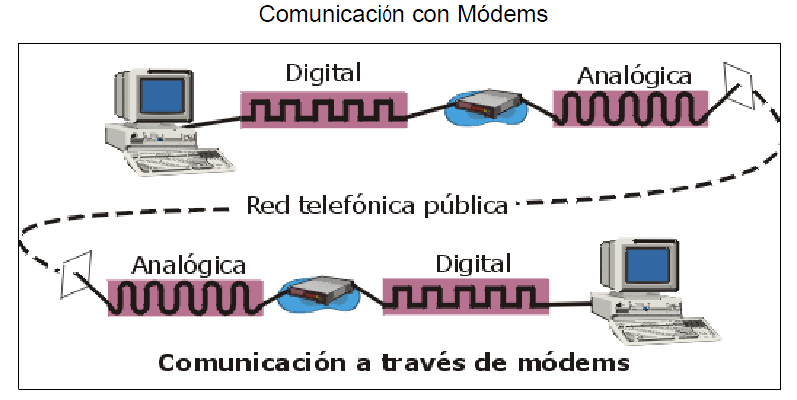


**EL MODEM**

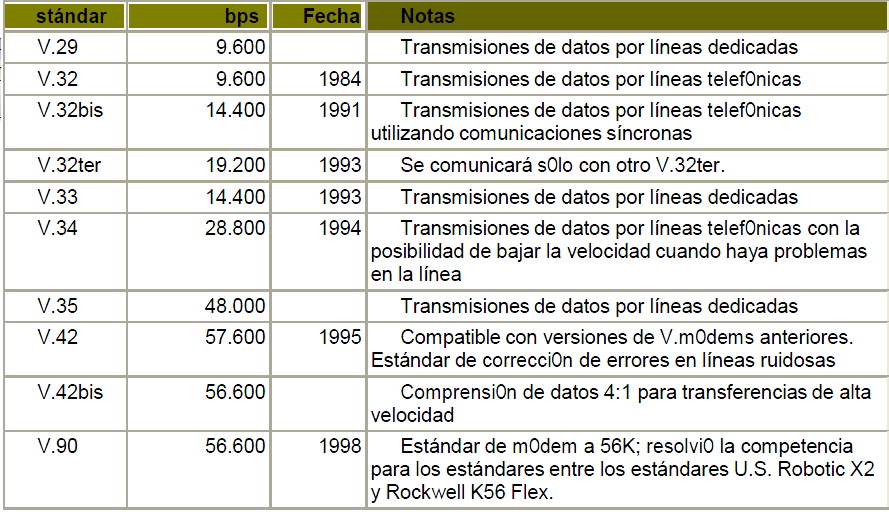
 

Es un dispositivo de comunicación más básico de conectividad entre redes, también se utilizan junto a otros dispositivos para conectar pequeñas LAN en una gran red de área extensa (WAN). Permite a los equipos comunicarse a través de una línea telefónica, un MODEM aceptará la señal análoga de la red o línea de transmisión y la convertirá en una cadena de bits.

El modem pertenece a la capa de enlace de datos del modelo OSI debido a que solamente se encarga de enlazar hacía varias redes.



Los módems se conocen como equipamiento de comunicaciones de datos (ECD) y comparten las siguientes características: Una interfaz de comunicación serie (RS 232). Una interfaz de línea telefónica RJ-11 (enchufe telefónico de cuatro hilos). Están disponibles tanto módems externos como internos. Un modem interno se instala en una ranura de expansión del equipo al igual que otra tarjeta. Un modem externo es una pequeña caja que se conecta al equipo a través un cable serie (RS-232) desde el puerto serie del equipo hasta la conexión del cable en el modem.



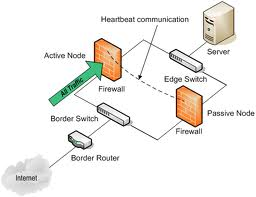
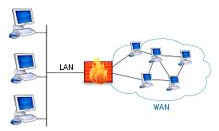
**Firewall**



Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la 143 comunicación es entrante o saliente y dependiendo de su direcciOn puede permitirla o no. De este modo un firewall puede permitir desde una red local hacia Internet servicios de Web, correo y FTP, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la Web, (si es que poseemos un servidor Web y queremos que accesible desde Internet).

Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local. Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Tipos de Firewall

Firewall de Capa de Red o de Filtrado de Paquetes: Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Firewall de Capa de Aplicación: Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder. Un firewall a nivel 7 de tráfico HTTP suele denominarse Proxy, y permite que los computadores de una organización entren a Internet de una forma controlada.

Firewall Personal: Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

CONCENTRADOR



Un concentrador es un dispositivo que permite centralizar el cableado de una red.

También conocido con el nombre de hub. Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Existen 3 clases.

**Pasivo:** No necesita energía eléctrica.

**Activo**: Necesita alimentación.

**Inteligente:** También llamados smart hubs, son hubs activos que incluyen microprocesador.

El concentrador envía información a ordenadores que no están interesados.

A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

• Este tráfico añadido genera más probabilidades de colisión.

• Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

• Un concentrador funciona a la velocidad del dispositivo más lento de la red.

Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mbps le trasmitiera a otro de 10 Mbps, se perdería del mensaje.

• En el caso del ADSL los routers suelen funcionar a 10 Mbps, si lo conectamos a nuestra red casera, toda la red funcionará a 10 Mbps, aunque nuestras tarjetas sean 10/100 Mbps

Un concentrador es un dispositivo simple, esto influye en dos características:

1. El precio es barato.

2. Un concentrador casi no añade ningún retardo a los mensajes.

Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los Sniffer.

**Switches**

****

Un Conmutador (ver figura ) es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

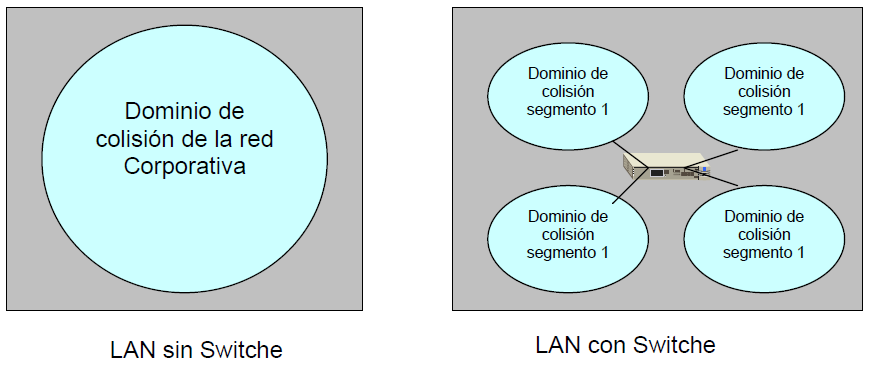
Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Área

Network- Red de Área Local).

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC.

Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones

MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.



**Tipos de Switches**

Los switches se pueden clasificar de manera muy general en dos tipos:

**Switche tipo CORE:** Estos Switches son utilizados en el centro de la red, donde los anchos de banda que se manejan no son tan elevados, su capacidad plena es limitada, así como su velocidad por puertos, normalmente este tipo de Switche es capa 2 y su costo es relativamente bajo.

**Switche Tipo EDGE:** Estos Switches son utilizados en las fronteras de la red donde los anchos de banda que se manejan son bastante elevados, debido a que en esta parte convergen todos los paquetes de los usuarios, la capacidad plena de este tipo de Switche es alta, así como su velocidad por puertos, normalmente este tipo de Switche es capa 3 o superior (hasta capa 7) y su costo es relativamente alto.

**Puentes (Bridges)**

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

Así, varias redes físicas pueden combinarse para formar una sola red lógica, construyendo cada una un segmento de red (Ver figura 2.12). Teniendo en cuenta que ambas redes deben manejar el mismo protocolo de establecimiento de red.



La tabla de direcciones MAC, son detectadas en cada segmento a que está conectado el puente. Cuando ésta detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred o segmento.

Por ejemplo, se tienen dos PC, el equipo A y el Equipo B, cada uno en un segmento de red. Entonces, el equipo A manda un paquete al equipo B. El equipo

B, recibe el paquete y sólo los de este segmento la pueden detectar y mirar. El resto del equipo A, no ve la trama que se envió. Sería lo mismo del Equipo B al A.

Los Puentes, los podemos clasificar en dos categorías:

- **Local**: Si proporciona una conexión directa entre múltiples segmentos de LAN situados en la misma área.

- **Remoto**: Si lo hace para las situadas en áreas distintas.

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, lo que tiene como resultado la transmisión infinita de datagramas de una red a otra. Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

**GateWays (Pasarelas RTC/IP):** Es un elemento esencial en la mayoría de las redes pues su misión es la de enlace zar la red VoIP con la red analógica o RDSI.

Se puede considerar al Gateway Como una caja que por un lado tiene un interface LAN y por el otro cualquiera de las siguientes Interfaces:

- FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.

- FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.

- E&M. Para conexión específica a centralitas.

- BRI. Acceso básico RDSI (2B+D)

- PRI. Acceso primario RDSI (30B+D)

- G703/G.704. (E&M digital) Conexión específica a centralitas a 2 Mbps.

**GateKeeper:** Es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es de gestión y control de los recursos de la red, de manera que no se produzca situaciones de saturación de la misma.

**MCU (Unidades de Audio Conferencia Multiple):** Permiten administrar los servicios de Audioconferencia simultaneos de la red asignando prioridad al servicio.

repetidores,