Topologías de Red

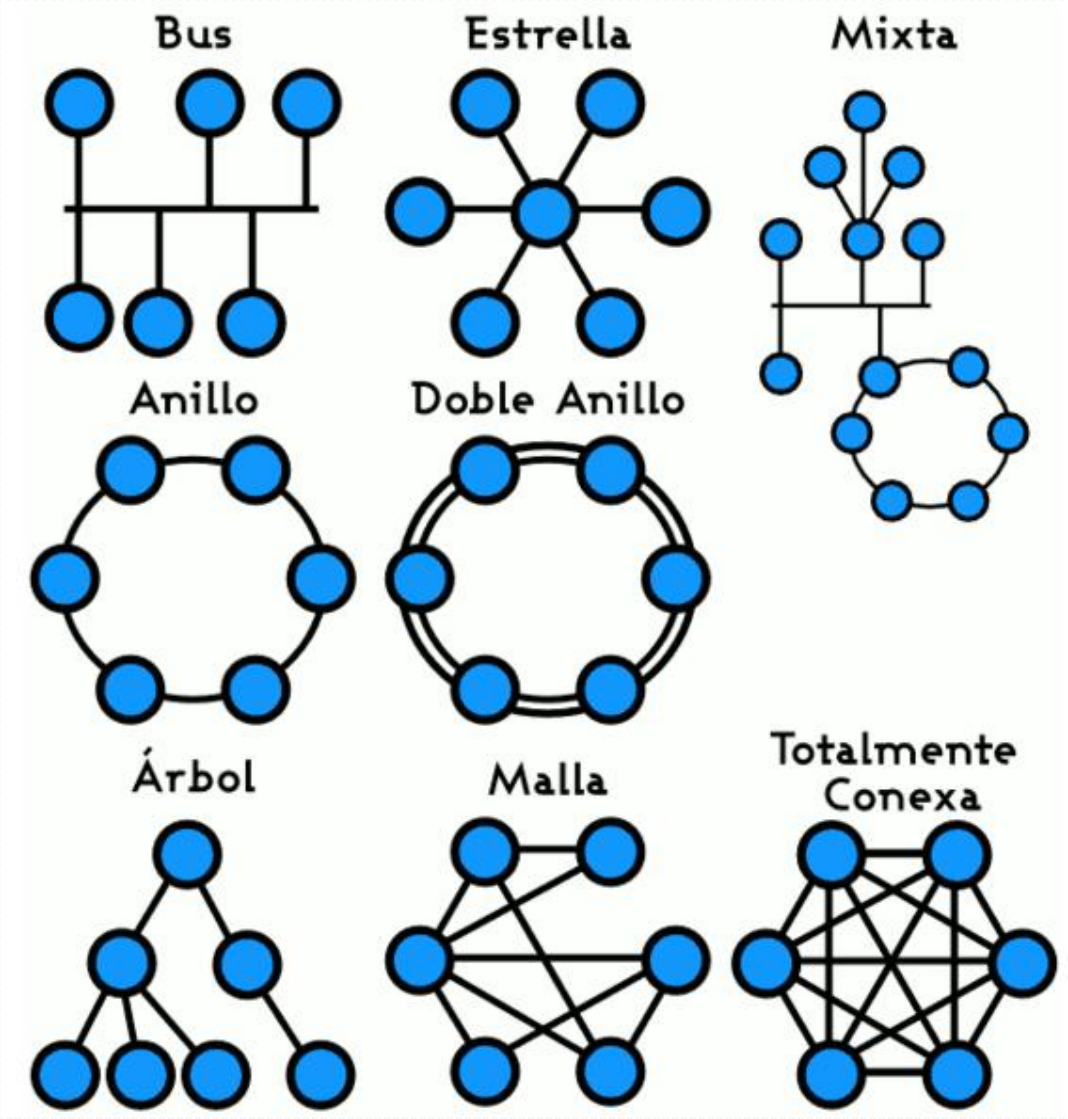
Topologías de Red

En esta lección usted aprenderá sobre las diferentes formas de configurar su red física, hacer una descripción en profundidad de las tecnologías de red de área ancha, y aprender cómo cambiar lógicamente su red física mediante VPN y VLAN.

- Topología de la red general
- Red Topologías físicas - Bus Lineal
- Red Topologías físicas - Estrella
- Red Topologías físicas - Anillo
- Red Topologías físicas - Malla
- Red Topologías físicas - Hibrida
- Conmutación de circuitos y conmutación de paquetes
- POTS, PSTN, T1/E1, T3/E3 y ISDN
- SONET y SDH
- Frame Relay y ATM
- MPLS, DSL, módem por cable, satélite y PON
- Sin hilos
- Protocolos de túnel
- VLANs

¿Qué es Topología?

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los *hosts* acceden a los medios para enviar datos. Las topologías más comúnmente usadas son las siguientes:


Bus
Estrella
Mixta
Anillo
Doble Anillo
Árbol
Malla
Totalmente Conexa

Topologías Físicas

•Una **topología de bus circular** usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
•La **topología de anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
•La **topología en estrella** conecta todos los cables con un punto central de concentración.
•Una **topología en estrella extendida** conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
•Una **topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los HUBs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
•La **topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. En esta topología, cada host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.
•La **topología de árbol** tiene varias terminales conectadas de forma que la red se ramifica desde un servidor base.

Topologías Lógicas

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

•La **topología broadcast** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.

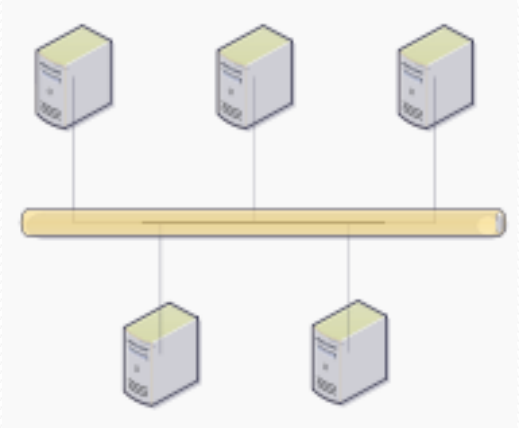
•La **topología transmisión de tokens** controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

Red Topologías físicas – Bus Lineal

Una **red en bus** es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

Los 2 extremos de los cables se determinan con una resistencia de acople denominada *terminador red*, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus por medio de un acople de impedancias.

Es la tercera de las topologías principales. Las estaciones están conectadas por un único segmento de cable. A diferencia de una red en anillo, el bus es pasivo, no se produce generación de señales en cada nodo o router.



Ventajas

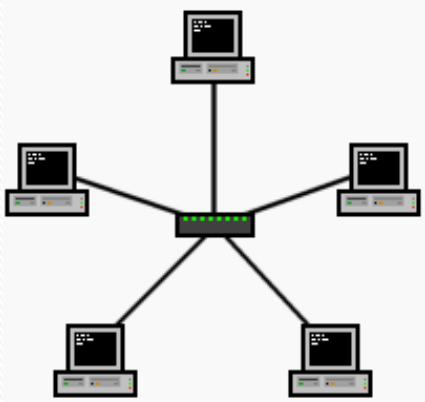
- Facilidad de implementación y crecimiento.
- Simplicidad en la arquitectura.

Desventajas

- Hay un límite de equipos dependiendo de la calidad de la señal.
- Puede producirse degradación de la señal.
- Complejidad de reconfiguración y aislamiento de fallos.
- Limitación de las longitudes físicas del canal.
- Un problema en el canal usualmente degrada toda la red.
- El desempeño se disminuye a medida que la red crece.
- El canal requiere ser correctamente cerrado (caminos cerrados).
- Altas pérdidas en la transmisión debido a colisiones entre mensajes.
- Es una red que ocupa mucho espacio.

Red Topologías físicas – Estrella

Una **red en estrella** es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central *activo* que normalmente tiene los medios para prevenir problemas relacionados con el eco.
Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes de usuarios.



Ventajas

❖Si una computadora se desconecta o se rompe el cable solo queda fuera de la red aquel equipo.
❖Posee un Sistema que permite agregar nuevos equipos fácilmente.
❖Reconfiguración Rápida.
❖Fácil de prevenir daños y/o conflictos.
❖Centralización de la red.
❖Esta red es de costo económico.

Desventajas

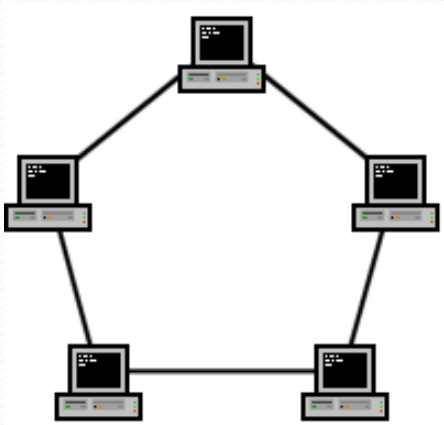
❖Si el Hub (repetidor) o switch central falla, toda la red deja de transmitir.
❖Es costosa, ya que requiere más cable que las topologías bus o anillo.
❖El cable viaja por separado del concentrador a cada computadora.

Red Topologías físicas – Anillo

Una **red en anillo** es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

En un anillo doble (Token Ring), dos anillos permiten que los datos se envíen en ambas direcciones (Token passing). Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.



Ventajas

- El sistema provee un acceso equitativo para todas las computadoras.
- El rendimiento no decae cuando muchos usuarios utilizan la red.
- Arquitectura muy sólida.

Desventajas

- Longitudes de canales
- El canal usualmente se degradará a medida que la red crece.
- Difícil de diagnosticar y reparar los problemas.
- Si una estación o el canal falla, las restantes quedan incomunicadas (Circuito unidireccional).

Red Topologías físicas – Malla

La **topología de red mallada** es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

Funcionamiento

Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).
Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.
Es una opción aplicable a las redes sin hilos (wireless), a las redes cableadas (wired) y a la interacción del software de los nodos.
Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. Por ello cobran mayor importancia en el uso de redes inalámbricas (por la no necesidad de cableado) a pesar de los inconvenientes propios de las redes sin hilos.
En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida.
Una red de malla extiende con eficacia una red, compartiendo el acceso a una infraestructura de mayor porte.

Ventajas

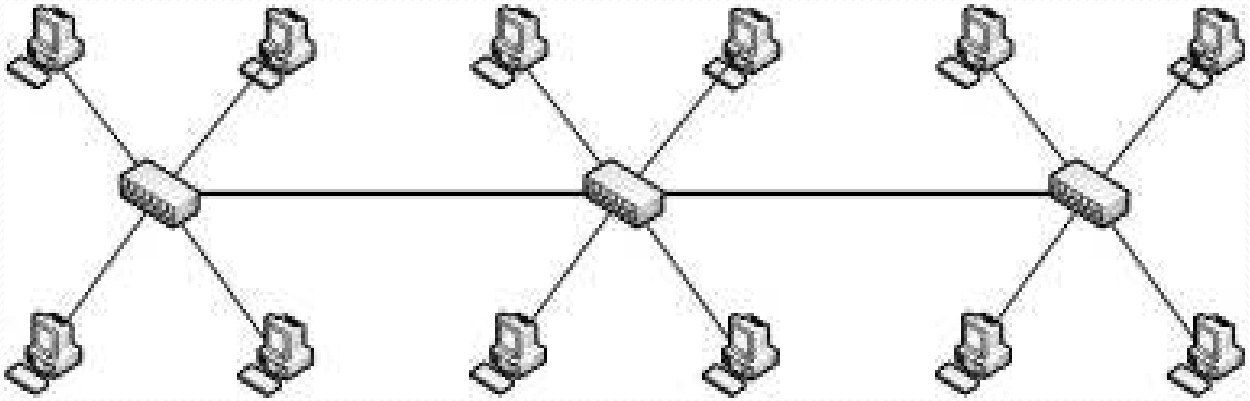
- Es posible llevar los mensajes de un nodo a otro por diferentes caminos.
- No puede existir absolutamente ninguna interrupción en las comunicaciones.
- Cada servidor tiene sus propias comunicaciones con todos los demás servidores.
- Si falla un cable el otro se hará cargo del tráfico.
- No requiere un nodo o servidor central lo que reduce el mantenimiento.
- Si un nodo desaparece o falla no afecta en absoluto a los demás nodos.
- Si desaparece no afecta tanto a los nodos de redes.

Desventajas

- El costo de la red puede aumentar en los casos en los que se implemente de forma alámbrica, la topología de red y las características de la misma implican el uso de más recursos.
- En el caso de implementar una red en malla para atención de emergencias en ciudades con densidad poblacional de más de 5000 habitantes por kilómetro cuadrado, la disponibilidad del ancho de banda puede verse afectada por la cantidad de usuarios que hacen uso de la red simultáneamente; para entregar un ancho de banda que garantice la tasa de datos en demanda y, que en particular, garantice las comunicaciones entre organismos de rescate, es necesario instalar más puntos de acceso, por tanto, se incrementan los costos de implementación y puesta en marcha.

Red Topologías físicas - Hibrido

• Diferentes tipos de topologías se pueden utilizar juntos para formar una topología híbrida.



Tecnologías WAN

• **Conmutación de Circuitos**

- Una ruta de conexión física se establece entre el origen y el destino típicamente a través de una serie de circuitos.

• **Conmutación de Paquetes**

- Los datos se dividen en paquetes que luego cada uno tomar una ruta independiente separada para el destino, en donde se vuelven a montar de nuevo en datos.

Tecnologías WAN

• POTS - Plain Old Telephone Service

• PSTN - Red Telefónica Pública Conmutada

• T1 / E1 - Un T1 es una línea digital alquilada consta de 24 Canales de 64K proporciona una velocidad de transferencia de hasta 1,544 Mbps. Un E1 es la versión europea con 30 canales que proporciona hasta 2.048 Mbps.

• T3/E3 - El T3 es básicamente 28 líneas T1 (672 canales) que proporcionan una velocidad de transferencia de hasta 44,736 Mbps. El E3 tiene 512 canales que ofrecen hasta 34.368 Mbps.

Tecnologías WAN

• RDSI - Red Digital de Servicios Integrados

-BRI: Interfaz de velocidad básica utiliza 64K 2 canales B para transmitir datos y 16 K 1 D-canal para transmitir información de control.

- PRI: Interfaz de velocidad primaria utiliza 23 canales B de 64 KB para datos y un canal D de 64 K para transmitir información de control, proporcionando esencialmente el mismo rendimiento como una línea T1.

Tecnologías WAN

• SONET / OC-x - Red óptica síncrona

SONET es una tecnología de red diseñado para transportar grandes volúmenes de tráfico en las relativamente largas distancias a través de cables de fibra óptica.

--Los tipos de datos de una red SONET se dividen en OC-niveles (Niveles de portador Opticos):

OC-1 = 51.84 Mbps OC-48 = 2.488 Gbps

-OC-3 = 155.52 Mbps OC-192 = 10 Gbps

-OC-12 = 622.08 Mbps OC-256 = 13,271 Gbps

-OC-24 = 1.244 Gbps OC-768 = 40 Gbps

Tecnologías WAN

• Frame Relay

- Una WAN donde todos los nodos están conectados a través de una nube de conmutación de paquetes.

Usted paga un precio base para un acuerdo sobre la CIR (Tasa de Información Comprometida) y luego pagar adicional por sólo el ancho de banda efectivamente utilizado.

• Cajero automático - Modo de transferencia asíncrono

- Red Avanzada de conmutación de paquetes utilizando paquetes de longitud fija (53 bytes).

- Proporciona velocidades de datos de hasta 622 Mbps.

• **MPLS** - Conmutación de etiquetas multiprotocolo

-MPLS es una técnica, no un servicio y es conocido por muchos nombres diferentes.

-Su concepto primario es el uso del etiquetado.

• **DSL** - Digital Subscriber Line (Línea de abonado digital)

Proporciona conexiones de alta velocidad a Internet utilizando los cables telefónicos de cobre convencionales.

Tipos de DSL:
ADSL - Línea de abonado digital asimétrica permite POTS y los datos a ser transmitidos simultáneamente.

SDSL - Línea de abonado digital simétrica no puede compartir la transmisión de datos con POTS.

VDSL - Línea de Muy Alta Velocidad de abonado digital permite el acceso al ancho de banda máximo disponible en una línea telefónica estándar (13 - 55 Mbps).

Tecnologías WAN

• **Cable Modem**

-Proporciona conexiones de alta velocidad a Internet mediante una conexión de cable de banda ancha.

• **Satélite**

- Proporciona conexiones de alta velocidad a Internet utilizando la comunicación vía satélite.
- Normalmente se utiliza donde DSL y por cable a Internet no están disponibles.

• **Wireless**

- Se utiliza principalmente por los usuarios móviles.
- Siempre a través de puntos de acceso WiFI o a través de la red de telefonía celular.

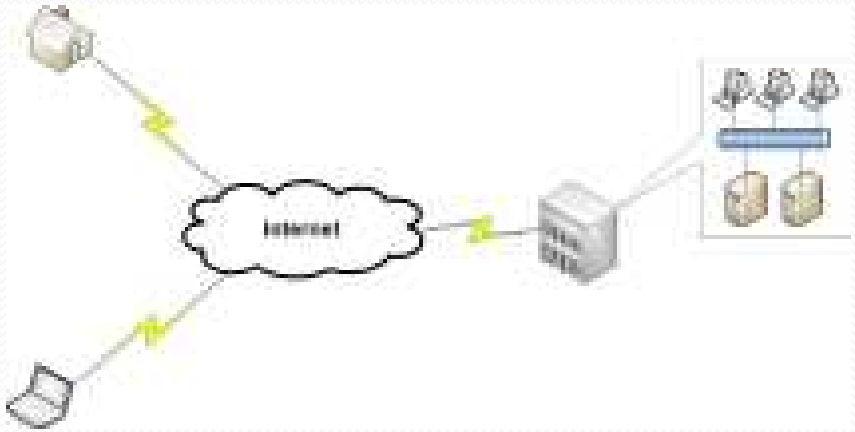
¿Qué es una VPN?

• VPN significa Red Privada Virtual

• Las VPN permiten a los usuarios que viajan a conectar a la red local cuando no están en la oficina.

• Los usuarios conectarse remotamente a un servidor VPN a través de una conexión de Internet estándar.

• Las conexiones VPN están aseguradas mediante el uso de protocolos de túnel.



Una **red privada virtual**, **RPV**, o **VPN** de las siglas en inglés de ***Virtual Private Network***, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada.
Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad de toda la comunicación:
Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza *funciones de Hash*. Los algoritmos de hash más comunes son los *Message Digest* (MD2 y MD5) y el *Secure Hash Algorithm* (SHA).
Confidencialidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como *Data Encryption Standard* (DES), Triple DES (3DES) y *Advanced Encryption Standard* (AES).
No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.

Requerimientos Básicos

❖Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

❖Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.

❖Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

❖Nuevo algoritmo de seguridad SEAL.

Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto
Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto
Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o *tunneling*.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

Implementaciones

El protocolo estándar *de facto* es el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Fortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link,Mikrotik, etc.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.

En ambos casos se pueden utilizar soluciones de firewall ('cortafuegos' o 'barrera de fuego', en castellano), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

Tipos de Conexión

Conexión de Acceso Remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN Router a Router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

¿Qué es una VLAN?

VLAN siglas de Virtual LAN (Red de Área Local).

Hay dos formas de ver una VLAN:

1. Un segmento físico dividido lógicamente en 2 o más segmentos.
2. Múltiples segmentos físicos que actúan como un segmento lógico.

Una **VLAN** (acrónimo de *virtual LAN*, «**red de área local virtual**») es un método de crear redes lógicamente independientes dentro de una misma red física.[1] Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

Clasificación

Aunque las más habituales son las **VLANs basadas en puertos** (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

VLAN de nivel 1 (por puerto). También conocida como “port switching”. Se especifica qué puertos del switch pertenencen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLANs si el usuario se mueve físicamente. Es la más común y la que se explica en profundidad en este artículo.

VLAN de nivel 2 por direcciones MAC. Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

VLAN de nivel 2 por tipo de protocolo. La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...

VLAN de nivel 3 por direcciones de subred (subred virtual). La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLANs.

VLAN de niveles superiores. Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día..