1. El acceso a las redes WAN

Las redes WAN no suelen conectar directamente nodos, sino que interconectan redes. Lo específico de ellas es que las líneas que suelen utilizar son públicas y los protocolos de comunicación que requieren tener en cuenta la seguridad de un modo especial.

1.1. Protocolos de acceso remoto

A. Protocolo PPP

PPP (Point to Point Protocol , protocolo punto a punto)

Se utiliza para referirse a un conjunto de protocolos que permiten el acceso remoto para el intercambio de tramas y autenticaciones en un entorno de red de múltiples fabricantes.

Un cliente PPP puede efectuar llamadas y, por tanto, establecer conexiones a cualquier servidor que cumpla las especificaciones PPP.

Aunque tradicionalmente PPP ha sido utilizado en conexiones sobre líneas serie, por ejemplo: para marcar por módem y realizar una conexión a Internet, existe una versión en la que se encapsula PPP sobre una capa Ethernet denominada PPPoE *(PPP over Ethernet)*, ampliamente utilizada para proveer conexiones de banda ancha añadiendo a Ethernet las ventajas que PPP ofrece como autenticación, cifrado y compresión de datos.

B. Protocolo SLIP

SLIP (*Serial Line Internet Protocol*, protocolo Internet para línea serie) es un protocolo estándar utilizado desde hace tiempo en sistemas UNIX que permite la conexión remota a través de líneas serie utilizando el protocolo

C. El protocolo de tunelización PPTP

PPTP (*Point to Point Transport Protocol*, protocolo de transporte punto a punto) es un protocolo que encapsula los paquetes procedentes de las redes de área local de modo que se hacen transparentes a los procedimientos de red utilizados en las redes de transporte de datos.

Encapsulación de protocolo: encapsular un protocolo A dentro de otro B es ponerle cabeceras de protocolo B a cada paquete de datos del protocolo A. El sinonimo es “Tunelización

1.2. Servicios de acceso remoto

El servicio de acceso remoto *(RAS, Remote Access Service)* conecta equipos remotos, posiblemente móviles, con redes corporativas, es decir, permite las conexiones de equipos distantes de la red de área local, habilitando los mismos servicios para estos usuarios remotos que los que poseen los usuarios presentados localmente. Por tanto, RAS es un encaminador software multiprotocolo con capacidad de autenticación y encriptación de los datos transmitidos.

2. El encaminador

Los encaminadores, enrutadores o routers son dispositivos software o hardware que se pueden configurar para encaminar paquetes entre sus distintos puertos de red utilizando la dirección lógica correspondiente a la Internet (subred), por ejemplo, su dirección IP.

2.1. Características generales

- Interpretan las direcciones lógicas de capa 3, en vez de las direcciones MAC de capa de enlace, como hacen los puentes o los conmutadores.
- Son capaces de cambiar el formato de la trama, ya que operan en un nivel superior a la misma.
- Poseen un elevado nivel de inteligencia y pueden manejar distintos protocolos previamente establecidos.
- Proporcionan seguridad a la red puesto que se pueden configurar para restringir los accesos a esta mediante filtrado.
- Reducen la congestión de la red aislando el tráfico y los dominios de colisión en las distintas subredes que interconectan. Por ejemplo, un router TCP/IP puede filtrar los

A. Tipos de encaminadores

Según su ubicación en la red :

-Router de interior : se utiliza en área local

-Router de exterior : Se utilizan en el núcleo de internet

-Router de borde o frontera : Se usan para interconectar una LAN a Internet a través del proveedor de servicios de internet

Según el tipo de algoritmo de encaminamiento :

-Algoritmos de encaminamiento estático : Requieren que la tabla de encaminamiento sea programada por el administrador de red . Carecen de capacidad para aprender la topología de la red por sí mismos

-Algoritmos de encaminamiento adaptativo : Son capaces de aprender por si mismos la topología de la red.

B. Protocolos de encaminamiento

Un protocolo de encaminamiento es aquel que utiliza un router para calcular el **mejor camino** (*best path*, en la terminología profesional)

El **coste de una ruta** *(route cost)* es un valor numérico que representa cuán bueno es el camino que la representa: a menor coste, mejor camino.

Protocolos de enrutamiento basados en el vector-distancia :

Un protocolo de encaminamiento basado en un vector-distancia es aquel que determina cuál es el mejor camino calculando la **distancia al destino.**

- RIP o RIPv1

- RIPv2

- BGP

Protocolos de enrutamiento basados en el estado del enlace :

Un protocolo de encaminamiento basado en el estado del enlace *(link-state)* es aquel que le permite a un router crearse un mapa de la red para que él mismo pueda determinar el mejor camino a un destino por sí mismo examinando el mapa que se ha construido.

- OSFP

- IS-IS

2.2. Configuración del enrutamiento

Cada nodo de una red IP debe tener configurados sus parámetros de red. Desde el punto de vista del enrutamiento, el parámetro más significativo es la puerta por defecto.

A. Rutas de protocolo IP :

Una **ruta** es la dirección IP de un nodo (router) que tiene suficiente inteligencia electrónica (algoritmos de encaminamiento) para saber qué hacer con un paquete IP que ha recibido de un nodo de la red con objeto de que llegue a su destino,

B. Configuración de la tabla de rutas :

- **Destino de red.** Es el nombre de la red que se pretende alcanzar.
- **Máscara de red.** Define la máscara de red de destino. La máscara de red junto con el destino de red definen el conjunto de nodos de red a los que se dirige la ruta.
- **Puerta de acceso o puerta de enlace.** Es la dirección IP del router (*gateway* o puerta de acceso en la terminología de la arquitectura IP), que debe ser capaz de resolver los paquetes que se dirijan a ese destino de red. Cuando la puerta de enlace coincide con la propia red local es señal de que el destino se alcanza inmediatamente por alguna de las interfaces de red local.
- **Interfaz.** Es la dirección IP o, en ciertos casos, el nombre de la interfaz de red que la posee por el que se deben enviar los paquetes de datos para alcanzar la puerta de enlace.
- **Métrica.** Es un parámetro que define una medida del coste telemático que supone enviar el paquete a la red destinataria a través de la puerta de acceso.

2.3. Interconexión de encaminadores

Es evidente que el enrutador corporativo no puede tener una interfaz de red por cada posible red de destino, por lo que no sería capaz de resolver el destino de la mayor parte de los paquetes.

Para solucionar esto, los enrutadores se configuran estableciendo relaciones de unos con otros.

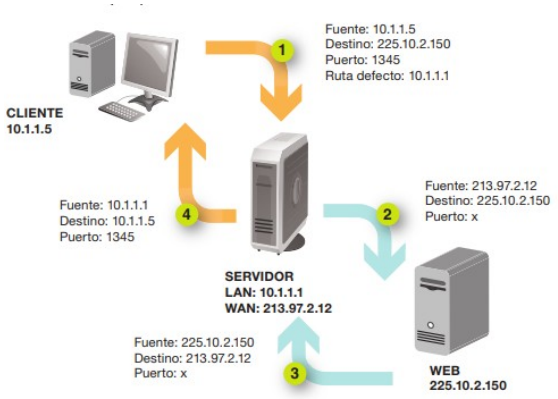
2.4. Enmascaramiento IP

El enmascaramiento IP *(IP Masquerading)* es una función de red de algunos sistemas operativos actuales que permiten la conexión de otros miembros de la red a Internet a través de la conexión que ya posee la máquina que soporta el enmascaramiento.

La función de IP Masquerading también la realiza el protocolo NAT (Network Address Traslatio)

Entre las ventajas que aporta la tecnología NAT se encuentran:

- Ahorro de direcciones IPv4 públicas, que están prácticamente agotadas.
- Mejoras en la seguridad de la LAN al hacer ocultas las direcciones IP privadas al exterior.
- Permite a los administradores de red desarrollar su propio sistema de direccionamiento IP interno.



3. El cortafuegos

3.1. Características generales

El cortafuegos se encarga de limitar los accesos en ambas direcciones , haciendo invisible la red de área local desde el exterior o restringiendo los accesos desde dentro hacia afuera

Hay cortafuegos que operan en muy distintos niveles de la arquitectura OSI. Así, un cortafuegos que opere en niveles bajos será más fácilmente configurable pero menos flexible.

En la actualidad los cortafuegos operan en las capas superiores

Traducción de direcciones NAT. Consiste en que las direcciones IP utilizadas por los hosts de la Intranet solo tienen validez dentro de la propia red de área local.

3.2. Zonas desmilitarizadas

Una zona desmilitarizada es una red local que se ubica entre la red interna de una organización y una red externa. Y protege la red de área local interna contra el tráfico no confiable.

El cortafuegos que hacer frontera entre la DMZ , la LAN e internet debe establecer tres tipos de políticas de comunicación diferenciadas entre ellas :

a) **Políticas de relación LAN con Internet.** Estas directivas configuran el acceso de los usuarios de la LAN a Internet, por ejemplo, con servicios como navegación.

b) **Políticas de relación LAN con la DMZ.** Aquí se configurará cómo los usuarios de la LAN pueden acceder a los servicios provistos por los servidores ubicados en la DMZ.

También aquí debe configurarse cómo los servidores DMZ pueden acceder a los servicios de la LAN

c) **Políticas de relación DMZ con Internet.** Aquí se configura cómo los usuarios de Internet (supuestamente anónimos) acceden a los servicios publicados por los servidores de la DMZ.

4. Servidores proxy

4.1. Características generales

Un servidor proxy de un servicio es un intermediario de red entre el cliente que solicita el servicio y el servidor que lo brinda. El cliente solicita el servicio al proxy, quien a su vez gestiona la petición en su propio nombre al servidor de destino.

El servidor proxy más común es webproxy (servidor proxy web o simplemente proxy), que permite a una red interna navegar por Internet mediante una única conexión a Internet.

Un servidor proxy enmascara las direcciones IP internas de la red de área local, sustituyéndolas al poner los paquetes en Internet por la suya propia, dirección real y única en el ámbito de Internet.

Hay que configurar el navegador y el proxy , en el navegador la configuración básicamente es la dirección o nombre del proxy que atenderá nuestras peticiones y los puertos que atenderán nuestras peticiones en función de las aplicaciones.