APUNTES DE TELECOMUNICACIONES II

ÍNDICE

I. INTERCONECTIVIDAD.

1. NIC (tarjeta de red)

Tarjeta de red o NIC (Network Interface Card), es un dispositivo electrónico que permite a un ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom etc). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, etc.), pero, actualmente el más común es del tipo Ethernet utilizando un interfaz o conector RJ45.

Las tarjetas de red Ethernet pueden variar en función de la velocidad de transmisión, normalmente 10 Mbps o 10/100 Mbps. Actualmente se están empezando a utilizar las de 1000 Mbps. Otro tipo de adaptador muy extendido hasta hace poco era el que usaba conector BNC.

La tarjeta de Red es la que permite la comunicacion y el intercambio de información entre una o mas computadoras conectadas en una Red.

Tarjeta de Red PCI de 10 Mbps

Convierte la información de Paralelo a Serie y de Serie a paralelo, es decir sin una Tarjeta de Red no tenemos Red!!!.

Cada tarjeta de red tiene un numero identificativo único de 48 bits, en hexadecimal llamado MAC (no confundir con Apple Macintosh). Estas direcciones hardware únicas son administradas por el Institute of Electronic and Electrical Engineers (IEEE). Los tres primeros octetos del numero MAC identifican a proveedores específicos y son designados por la IEEE.

Se le denomina también **NIC** a un sólo chip de la tarjeta de red, este chip se encarga de servir como interface de Ethernet entre el medio físico (por ejemplo un cable coaxial) y el equipo (por ejemplo un PC).

Es un chip usado en computadoras o periféricos tales como las tarjetas de red, impresoras de red o sistemas embebidos para conectar dos o más dispositivos entre sí a través de algún medio, ya sean conexión inalámbrica (vía aire), cable UTP, cable coaxial, fibra óptica, etc.

Velocidad de conexión

Debe utilizarse una NIC de Ethernet con un concentrador o conmutador Ethernet, y debe utilizarse una NIC de Fast Ethernet con un concentrador o conmutador Fast Ethernet.

Si conecta su PC a un dispositivo dual speed que admite ambos valores, 10 y 100Mbps, puede utilizar una NIC de 10Mbps o una NIC de 100Mbps. Un puerto en un dispositivo dual speed ajusta su velocidad automáticamente para que coincida con la velocidad más alta admitida por ambos extremos de la conexión. Por ejemplo, si la NIC soporta solamente 10Mbps, el puerto del concentrador dual speed que está conectado a dicha NIC pasará a ser un puerto de 10Mbps. Si la NIC soporta 100Mbps, la velocidad del puerto del concentrador será de 100Mbps.

De un modo semejante, si tiene una NIC 10/100, podrá conectarla al concentrador Ethernet de 10Mbps o al concentrador Fast Ethernet de 100Mbps. La NIC 10/100 ajustará su velocidad para que coincida con la velocidad más alta soportada por ambos extremos de la conexión.

Nota: Los dispositivos dual speed se conocen también como dispositivos auto negociadores, autosensores o 10/100.

Tipo de conexión

Si está instalando una red que utiliza cables de par trenzado, necesitará una NIC con un conector RJ-45.

Conectores ISA y PCI

Hay dos tipos comunes de conectores de NIC para PC:

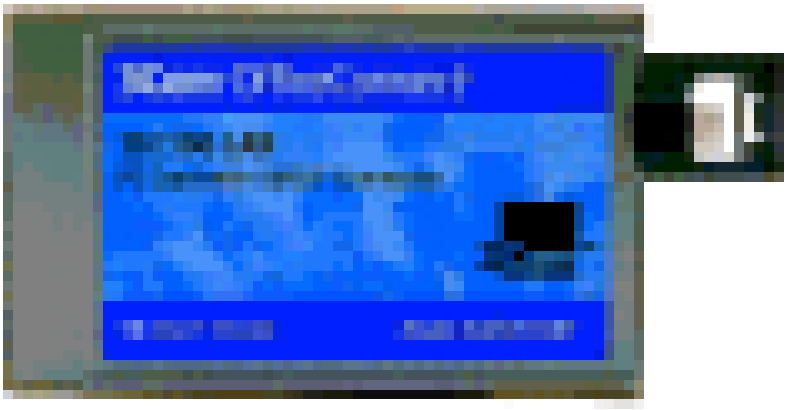
- Los zócalos ISA (Arquitectura de normas industriales) miden unos 14cm de largo.

- Los zócalos PCI (Interconexión de componente periférico) se utilizan en todos los PC Pentium de sobremesa. Los zócalos PCI tienen un mayor rendimiento que la ISA. Los zócalos PCI miden unos cm. de longitud.

Consulte la guía del usuario de su PC para averiguar qué tipo de conector hay disponible en su PC.

NIC especializadas

En algunos casos, es posible que necesite utilizar NIC especializadas. Por ejemplo, si su ordenador es un portátil, necesitará utilizar una tarjeta PCMCIA.



Cuando elija una tarjeta PCMCIA, deberá considerar lo siguiente:

- La velocidad de su concentrador, conmutador o servidor de impresora - Ethernet (10Mbps) o Fast Ethernet (100Mbps).

- El tipo de conexión que necesita - RJ-45 para par trenzado o BNC para cable coaxial.

Si tiene un puerto USB, podría considerar utilizar la Interfaz de red USB (USB Network Interface).

2. Tranceiver

Es un microchip (tranceiver) que transmite y recibe en la frecuencia de 2.45 GHz que esta disponible en todo el mundo (con algunas variaciones de ancho de banda en diferentes países). Además de los datos, están disponibles tres canales de voz.

Los datos se pueden intercambiar a velocidades de hasta 1 megabit por segundo (se esperan 2 megabits por segundo en la Segunda Generación de esta Tecnología). Un esquema de “frequency hop” (saltos de frecuencia) permite a los dispositivos comunicarse inclusive en áreas donde existe una gran interferencia electromagnética. Además de que se provee de esquemas de encriptación y verificación.

Bluetooth ha sido diseñado para operar en un ambiente multiusuario. Los dispositivos pueden habilitarse para que se comuniquen entre sí e intercambiar datos de una forma transparente al usuario. Hasta ocho usuarios o dispositivos pueden formar lo que se conoce como una “piconet” y hasta diez “piconets” pueden coexistir en la misma área de cobertura. Dado que cada enlace es codificado y protegido contra interferencia y pérdida de enlace, Bluetooth puede considerarse como una red inalámbrica de corto alcance segura.

Es tan amplia la gama de aplicaciones que pueden darse con Bluetooth, estos son algunos de los escenarios para los futuros productos que estén usando esta tecnología:

- Automatización en el hogar.

- Comercio electrónico.

- Control Industrial.

- Industria Automotriz.

- Sistemas de Vigilancia.

- Control de Acceso.

- Y muchos mas…

Dentro de los principales productos comerciales que tendrán Bluetooth podemos listar:

- Periféricos Inalámbricos (teclado, mouse, monitores, etc.).

- Accesorios como Diademas, Audífonos, etc.

- Cámaras.

- Módulo Integrado en Laptops.

- Módulo Integrado en Teléfonos celulares.

- Módulo Integrado en Computadoras de bolsillo.

Puntos de acceso: Puente universal hacia otras redes.

3. Repetidor

Dispositivo hardware encargado de amplificar o regenerar la señal entre dos segmentos de una red homogénea que se interconectan ampliando su cobertura. El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios.
Opera en el nivel físico del modelo de referencia OSI.

Un **amplificador** es un dispositivo que magnifica lo que pasa a su través.

La relación que existe entre la entrada y la salida del amplificador (normalmente expresada en función de la frecuencia[1] de la señal de entrada) se le denomina función de transferencia del amplificador y a su magnitud ganancia. Como su amplificación depende de la frecuencia, se les suele hacer funcionar en un determinado rango de frecuencias, normalmente donde la amplificación es constante o lineal.
El tipo más común de amplificadores son los amplificadores electrónicos, usados en casi todos los aparatos electrónicos, como radios, televisiones, ordenadores, equipos de comunicación, instrumentos musicales, etc.

El componente clave de estos amplificadores es el elemento activo, que puede ser un tubo de vacío o un transistor (normalmente BJT, aunque también se emplean MOSFET[2]). La función del BJT es la de amplificar la corriente eléctrica que haya en su base un determinado valor en el colector y en el emisor. El valor de amplificación depende del tipo de transistor y del diseño del circuito (valores de los componentes, configuración en base común, colector común, etc.).

Con transistores se pueden hacer dispositivos más complejos que también cumplan la función de amplificar, como los amplificadores operacionales, y éstos a su vez otros como los amplificadores de instrumentación.

---

[1] En física el término **frecuencia** se utiliza para indicar la velocidad de repetición de cualquier fenómeno periódico. Se define como el número de veces que se repite un fenómeno en la unidad de tiempo.
La unidad de medida es el hercio (Hz), en honor al físico alemán Heinrich Rudolf Hertz, donde 1 Hz es un evento que tiene lugar una vez por segundo.

[2] **MOSFET** son las siglas de **Metal Oxide Semiconductor Field Effect Transistor**.
Se trata de un dispositivo electrónico de control con aplicaciones en amplificadores de audio (etapa de potencia) aparecidos en la década de 1980.
Como cualquier amplificador su misión es aumentar el nivel de la señal, en este caso, actuando sobre su amplitud. Como su nombre indica, crean un efecto de campo gracias a la unión de un semiconductor formado por la pareja metal-oxido.
Desde su aparición son muy usados, porque aseguran una distorsión más baja, al controlar el desprendimiento térmico que se produce durante el procesado de la señal.

Otro tipo de amplificadores electrónicos son los diseñados específicamente para audio, en ellos se suelen preferir las válvulas de vacío a los transistores por sus mejores características sonoras. Estos amplificadores para audio son los preamplificadores y las etapas de potencia

4. Concentrador

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 de forma que todos los puntos tienen acceso a los datos. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

Pasivo: No necesita energía eléctrica.

Activo: Necesita alimentación.

Inteligente: o *smart hubs* son *hubs* activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de la capa física.

5. Puente

Un **puente** o **bridge** es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) 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.

6. Gateway

Gateway puede referirse a:

- Una puerta de enlace, un nodo en una red informática que sirve de punto de acceso a otra red.
- Una pasarela, un dispositivo dedicado a intercomunicar sistemas de protocolos incompatibles.

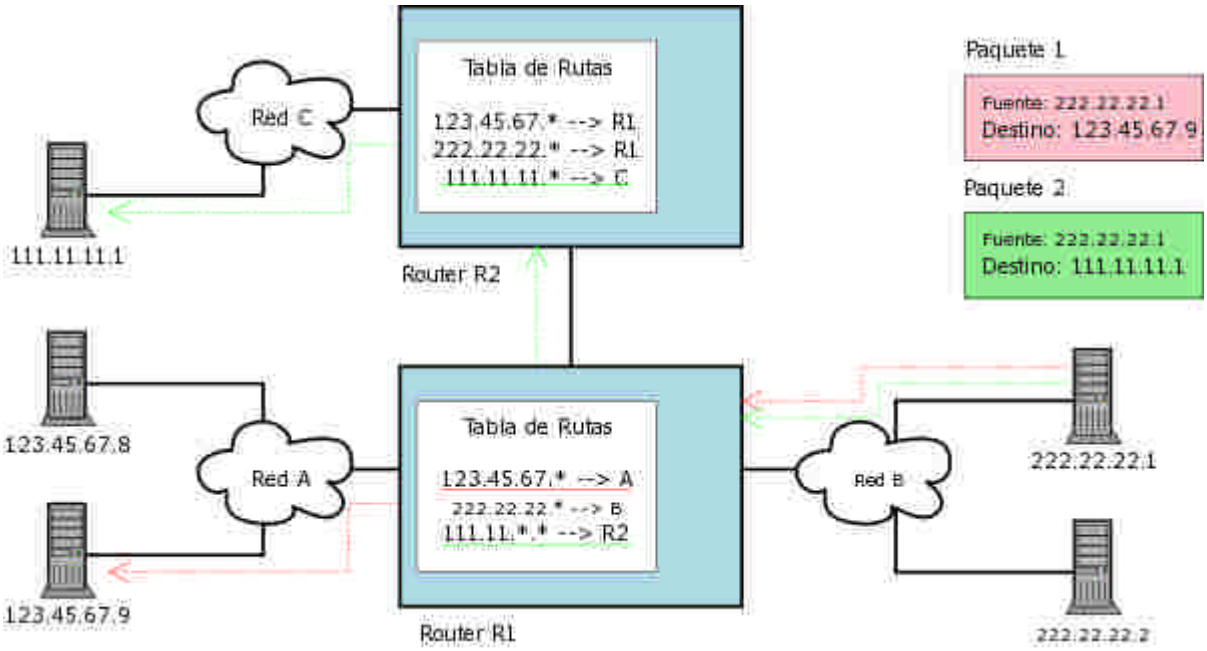
Un gateway o **puerta de enlace** es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading, usada muy a menudo para dar acceso a Internet a los equipos de una LAN

compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Ejemplo de puerta de enlace: 192.168.100.1

7. Ruteador

El **router** (**enrutador** o **encaminador**) es un dispositivo hardware o software de interconexión de redes de ordenadores / computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.



En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.

Los **broadcast**, o difusiones, se producen cuando una fuente envía datos a todos los dispositivos de una red. En el caso del protocolo IP, una dirección de broadcast es una dirección compuesta exclusivamente por números unos (1) en el campo del host.

Los protocolos de enrutamiento son aquellos protocolos que utilizan los routers o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cual es la ruta mas adecuada en cada momento para enviar un paquete. Los protocolos mas usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica. Aunque no es estrictamente necesario que un router haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

Existe la posibilidad de no utilizar equipos dedicados, opción que puede ser la más adecuada para redes locales o redes con un tráfico limitado, y usar software que implemente los protocolos de red antes mencionados. Para dar funcionalidad de router a un PC con los sistemas operativos GNU/Linux o BSD es suficiente con añadirle al menos dos interfaces de red y activar el soporte de enrutamiento en el kernel.

8. Switch

Un **switch** (en castellano "interruptor" o "conmutador") es un dispositivo de interconexión de redes de ordenadores / computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconection*). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas[3] en la red.

Un switch en el centro de una red en estrella.

Los switches se utilizan cuando se desea conectar múltiples redes. Al igual que los bridges, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs (*Local Area Network*- Red de Área Local)

9. Híbridos

[3] Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el ordenador receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ordenador destino.
La estructura de un datagrama es: cabecera y datos.
Protocolos basados en datagramas: IPX, UDP.

II. INTEROPERABILIDAD EN REDES

1. Interconexión

1.1. Redes LAN

Local Area Network (en inglés «Red de Área Local»), más comúnmente referida por su acrónimo **LAN**, se refiere a las redes locales de ordenadores.

La LAN más antigua y popular, ARCnet, fue lanzada en 1977 por Datapoint y fue originalmente diseñada para compartir múltiples discos de almacenamiento Datapoint 2200. Como todas las LANs antiguas, ARCnet era originalmente específica según cada vendedor. Los esfuerzos de estandarización por parte del IEEE resultaron en la serie IEEE 802. Actualmente hay dos tecnologías comunes de cableado para LAN, Ethernet y Token Ring. Tecnologías sin cables también existen y son convenientes para usuarios de equipos móviles.

Conectores BNC (Coaxial) y RJ45 de una tarjeta de Red

1.2. Redes MAN

Entre las LAN y WAN se encuentran las **MAN** o **Redes de área metropolitana**. Esta es una red que cubre una ciudad completa, pero utiliza la tecnología desarrollada para la LAN. Las redes de televisión por cable (CATV), son ejemplos de MAN analógicas para el caso de distribución de televisión.

La MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los proveedores de sistemas de comunicación por microondas o medios ópticos.

1.3. Redes WAN

WAN es un acrónimo de **Wide Area Network** que en inglés significa red de área amplia. Un ejemplo de este tipo de redes sería la misma Internet o cualquier red en que no esté en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Opera en la capa física y de enlace del modelo de referencia OSI.
A nivel de alcance, esta red abarca desde unos 100km (País) hasta llegar incluso a 1000km (Continente).

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

Hoy en día, Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las redes privadas virtuales (VPN) que utilizan cifrado y otras técnicas para hacer esa red dedicada aumentan.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes **WAN** pueden usar sistemas de comunicación vía satélite o de radio. Fue la aparición de los portátiles y los PDA´s la que trajo el concepto de redes inalámbricas.

Características:

-Posee máquinas dedicadas a la ejecución de programas de usuario (hosts)
-Una subred, donde conectan varios hosts.
-División entre líneas de transmisión y elementos de conmutación (enrutadores)
-Usualmente los routers son computadores de las subredes que componen la WAN.

Topologías de los routers en una red de área amplia (WAN):

-Estrella
-Anillo
-Árbol
-Completa
-Intersección de anillos
-Irregular

1.4. Conexiones Remotas

2. Dispositivos de Interconexión

2.1. Ruteadores

2.1.1 Métodos de Ruteo

2.1.1.1. Por saltos mínimos

Los árboles de ruta de acceso más corta también se conocen como árboles *basados en el origen*, lo que significa que las rutas de reenvío se basan en la ruta de unidifusión al origen más corta. Esto es lo que se quiere dar a entender cuando se dice que los árboles de origen se consideran los árboles de ruta de acceso más corta desde la perspectiva de las tablas de enrutamiento de unidifusión. Si la métrica de enrutamiento se basa en cuentas de saltos, las ramas de los árboles de ruta de acceso más corta de multidifusión representan los **saltos mínimos**. Si la métrica simboliza retraso, las ramas representan el retraso mínimo.

Para cada origen de multidifusión, hay un árbol de multidifusión correspondiente que conecta directamente el origen con todos los receptores. Una vez construido el árbol para el origen y para el grupo asociado, todo el tráfico a los miembros del grupo circula por este árbol. Los árboles de ruta de acceso más corta tienen una entrada (S, G) con una lista de interfaces salientes, donde S es la dirección de origen y G el grupo de multidifusión. Como ejemplos de otros protocolos que utilizan este tipo de árboles se pueden destacar DVMRP y MOSPF, que son protocolos de modo denso. La figura 2 muestra un ejemplo de un árbol de ruta de acceso más corta.

Figura 2 Ejemplo de un árbol de ruta de acceso más corta

En el ejemplo, el árbol de ruta de acceso más corta para el origen 1 se encuentra, a través de la interfaz I0, en el enrutador 1, a pesar de que halla una ruta alternativa a través de la combinación de los enrutadores 1 y 3. El árbol de ruta de acceso más corta para el origen 2 se genera a través de la interfaz I3, a pesar de que, una vez más, exista una ruta alternativa pero más larga. En este ejemplo la métrica representa cuentas de saltos.

2.1.1.2. Por tipo de servicio

OSPF[4] dispone de cinco tipos de servicio, los mismos que se utilizan en IPv4. El tipo de servicio se define en el campo TOS (*Type Of Service*) del paquete, y determina el significado del coste de los enlaces (o métrica). Veamos a continuación una breve descripción de cada tipo de servicio:

[4] El protocolo RIP basado en vectores de distancias fue reemplazado en 1979 por un protocolo basado en el estado de los enlaces. En 1988, la *Internet Engineering Task Force* (grupo de trabajo de ingeniería en Internet) comenzó a trabajar en un sucesor más sofisticado que llegaría a convertirse en estándar en 1990. Ese sucesor fue el protocolo OSPF (*Open Shortest Path First*, abrir primero la trayectoria más corta).

1. Normal (TOS 0): Es la métrica que se emplea por defecto, asignada por el administrador para satisfacer necesidades generales, y que es comprendida por todos los enrutadores.

2. Minimizar coste monetario (TOS 2): Métrica empleada si se puede asignar coste monetario al uso de la red.

3. Maximizar fiabilidad (TOS 4): Métrica basada en la historia reciente de fallos en la red o en tasas de paquetes erróneos.

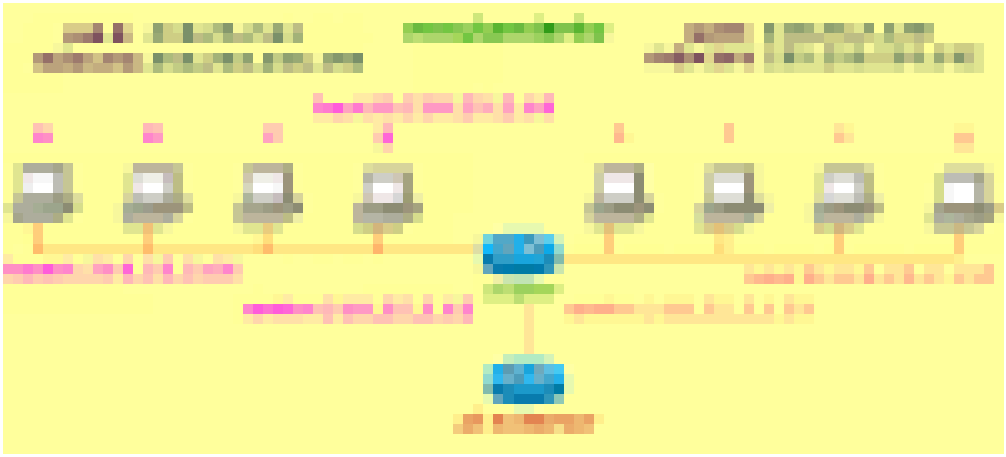
4. Maximizar caudal (TOS 8): Esta métrica debe configurarse previamente basándose en la capacidad de cada enlace. Una magnitud muy utilizada es la duración de un bit en nanosegundos.

5. Minimizar retardo (TOS 16): Medida del retardo para un salto en particular, basada en el retardo de propagación y en el retardo en los buffers.

Para proporcionar estos cinco tipos de servicio, OSPF mantiene cinco grafos de topología distintos y sus correspondientes tablas de encaminamiento. Los datagramas IP suelen incorporan un campo TOS. Según el valor de este campo, cada enrutador consulta la tabla de encaminamiento apropiada para encaminar el datagrama. Si el datagrama no incluye el campo TOS entonces se usa la tabla correspondiente a la métrica por defecto (TOS 0).

2.1.1.3. Ruteo Directo

Partamos para la explicación que sigue de una red dividida en dos subredes (210.25.2.64 y 210.25.2.128), enlazadas mediante un sólo router (210.25.2.65 en A y 210.25.2.129 en B), que además es el gateway por defecto, es decir, el encargado de sacar fuera de la red padre las tramas externas.



Cuando el host A se quiere comunicar con otro, lo primero que hace es consultar su tabla ARP, para ver si tiene en la misma la entrada que le de la equivalencia IP-MAC del host destino. Si es así, construye sus tramas completas y las envía al medio, esperando que el destinatario las reciba directamente. Si no encuentra la

entrada correspondiente en la tabla, lanza una petición ARP query, de tipo bradcast, esperando que el host destino le devuelva su dirección física.

Si el host destino es el D, que se encuentra en la misma subred, responderá a la petición ARP con su MAC o recogerá directamente las tramas a él destinadas. Este direccionamiento se conoce con el nombra de **enrutamiento directo**. En este proceso, el router recoge las tramas y hace una operación AND con la dirección IP destino que en ellas figura y con las máscara de subred de la red del host que ha enviado los datos:

210.25.2.69 AND 255.255.255.192 = 210.25.2.64

Con lo que "sabe" que el host destino se encuentra en la misma subred que el origen de datos, dejando pasar las tramas sin intervenir.

2.1.1.4. Ruteo Indirecto

Ahora bien, tomando el mismo ejemplo del punto anterior, si el host destino fuera en H, que no se encuentra en la misma subred, el router, al hacer la operación AND lógica obtendrá:

210.25.2.132 AND 255.255.255.192 = 210.25.2.128

Con lo que "sabe" que el host destino no se encuentra en la misma subred que el host A. Entonces, recoge él mismo las tramas enviadas por A y las pasa a la subred de H, con lo que se puede realizar la entrega. En este caso nos encontramos con un **enrutamiento indirecto interno**.

Un último caso se producirá cuando el host A quiera enviar datos a un host externo a las subredes que une el router. Éste, al hacer la operación AND lógica, descubre que las tramas no van a ningún host de las subredes que une, por lo que cambia la dirección MAC de las mismas por la suya propia de la subred a la que pertenece al host origen, y dejendo la dirección IP del host destino, sacando los datos entonces al exterior de las subredes, enviándolas al router externo que créa que puede proseguir mejor el enrutamiento. En este caso hablamos de **enrutamiento indirecto externo**. Los routers poséen sus correspondientes tablas de enrutamiento dinámicas, que son las que van a fijar el router externo al que se envían las tramas.
Las tramas así enviadas van viajando por diferentes routers, hasta llegar a la red/subred destino. Cuando el host que recibe las tramas responde al origen, los datos viajan en sentido opuesto (aunque no tienen porqué hacerlo por el mismo camino), y al llegar de nuevo al router de nuestras subredes, las tramas tendrán como dirección física la del router, y como dirección lógica la del host A. Entonces el router vuelve a hacer la operación lógica AND entre la dirección IP de las tramas y las de las diferentes subredes que une, obteniendo la subred a la que pertenece el host A, con lo que le envía los datos a éste, finalizando el proceso.

Es decir, en el enrutamiento indirecto externo el router funciona como un intermediario, lo mismo que los diferentes routers que van enrutando las tramas

hasta el destino, usando para ello sus propias direcciones MAC, que van cambiando, permaneciendo siempre fijas las IP de los host destino.

2.1.2 Protocolos

2.1.2.1. RIP

RIP son las siglas de **R**outing **I**nformation **P**rotocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o **IGP** (**I**nternet **G**ateway **P**rotocol) utilizado por los **routers** (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RIP se desarrolló en 1970 en los Laboratorios Xerox como parte de otro protocolo de enrutamiento. Su popularidad se debe a que fue distribuido con el UNIX de la Universidad de Berkeley.

En la actualidad existen tres versiones diferentes de RIP.

- **RIPv1**: No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058.

- **RIPv2**: Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada mediante MD5. Su especificación está recogida en el RFC 1723-2453.
- **RIPng**: RIP para IPv6. Su especificación está recogida en el RFC 2080.

Funcionamiento RIP

RIP utiliza UDP para enviar sus mensajes y el puerto 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. Esta distancia se denomina métrica. En RIPv1 la métrica es estática y vale 1, en cambio se puede modificar su valor en RIPv2

RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

Tipos de mensajes RIP

Los mensajes RIP pueden ser de dos tipos.

- **Petición**: Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.
- **Respuesta**: mensajes con la actualización de las tablas de enrutamiento. Existen tres tipos:
    - Mensajes *ordinarios*: Se envían cada 30 segundos. Para indicar que en enlace y la ruta siguen activos.
    - Mensajes enviados como *respuesta* a mensajes de petición.
    - Mensajes enviados cuando *cambia algún coste*. Sólo se envían las rutas que han cambiado.

Formato de los mensajes RIP

Los mensajes tienen una cabecera que incluye el tipo de mensaje y la versión del protocolo RIP, y un máximo de 25 entradas RIP de 20 bytes.

Las entradas en RIPv1 contienen la dirección IP de la red de destino y la métrica.

Las entradas en RIPv2 contienen la dirección IP de la red, su máscara, el siguiente enrutador y la métrica. La autentificación utiliza la primera entrada RIP..

2.1.2.2. IGRP/EIGRP

EIGRP es un protocolo de encaminamiento híbrido, propietario de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP. EIGRP al igual que IGRP usa el siguiente calculo de metrica:

Métrica= [K1 * ancho de banda + ((K2 * ancho de bande)/(256-carga))+ (K3 * retardo)]*[K5/(confiabilidad + K4)]

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

EIGRP guarda las rutas que se aprenden de maneras específicas. Las rutas reciben un estado específico y se pueden rotular para proporcionar información adicional de utilidad.

EIGRP mantiene las siguientes tres tablas:

- **Tabla de vecinos**

  Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

- **Tabla de topología**

  La tabla de topología se compone de todas las tablas de enrutamiento EIGRP en el sistema autónomo. DUAL toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino. EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de DUAL se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red. La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

- **Tabla de enrutamiento**

  La tabla de enrutamiento EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología. Los routers EIGRP mantienen una tabla de enrutamiento por cada protocolo de red.

A continuación se muestran los campos que conforman la tabla de enrutamiento:

- **Distancia factible (FD):** Ésta es la métrica calculada más baja hacia cada destino. Por ejemplo, la distancia factible a 32.0.0.0 es 2195456.

- **Origen de la ruta:** Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el enrutamiento basado en políticas. Por ejemplo, el origen de la ruta a 32.0.0.0 es 200.10.10.10 a 200.10.10.10.

- **Distancia informada (RD):** La distancia informada (RD) de la ruta es la distancia informada por un vecino adyacente hacia un destino específico. Por ejemplo, la distancia informada a 32.0.0.0 es 2195456 tal como lo indica (90/2195456).

- **Información de interfaz:** La interfaz a través de la cual se puede alcanzar el destino.

- **Estado de ruta:** El estado de una ruta. Una ruta se puede identificar como pasiva, lo que significa que la ruta es estable y está lista para usar, o activa, lo que significa que la ruta se encuentra en el proceso de recálculo por parte de DUAL.

Protocolos que utiliza EIGRP

Uno de los Protocolos que utiliza EIGRP es el *Protocolo de Transporte Confiable* (RTP, no confundir con el *Real-time Transport Protocol*), que es un protocolo de capa de transporte que garantiza la entrega ordenada de paquetes EIGRP a todos los vecinos. En una red IP, los hosts usan TCP para secuenciar los paquetes y asegurarse de que se entreguen de manera oportuna. Sin embargo, EIGRP es independiente de los protocolos. Esto significa que no se basa en TCP/IP para intercambiar información de enrutamiento de la forma en que lo hacen RIP, IGRP y OSPF. Para mantenerse independiente de IP, EIGRP usa RTP como su protocolo de capa de transporte propietario para garantizar la entrega de información de enrutamiento. EIGRP puede hacer una llamada a RTP para que proporcione un servicio confiable o no confiable, según lo requiera la situación. Por ejemplo, los paquetes *hello* no requieren el gasto de la entrega confiable porque se envían con frecuencia y se deben mantener pequeños. La entrega confiable de otra información de enrutamiento puede realmente acelerar la convergencia porque entonces los routers EIGRP no tienen que esperar a que un temporizador expire antes de retransmitir. Con RTP, EIGRP puede realizar envíos en multicast y en unicast a diferentes pares de forma simultánea. Esto maximiza la eficiencia.

El núcleo de EIGRP es DUAL, que es el motor de cálculo de rutas de EIGRP. El nombre completo de esta tecnología es máquina de estado finito DUAL (FSM). Una FSM es una máquina de algoritmos, no un dispositivo mecánico con piezas que se mueven. Las FSM definen un conjunto de los posibles estados de algo, los acontecimientos que provocan esos estados y los eventos que resultan de estos estados. Los diseñadores usan las FSM para describir de qué manera un dispositivo, programa de computador o algoritmo de enrutamiento reaccionará ante un conjunto de eventos de entrada. La FSM DUAL contiene toda la lógica que se utiliza para calcular y comparar rutas en una red EIGRP.

DUAL rastrea todas las rutas publicadas por los vecinos. Se comparan mediante la métrica compuesta de cada ruta. DUAL también garantiza que cada ruta esté libre de bucles. DUAL inserta las rutas de menor costo en la tabla de enrutamiento. Estas rutas principales se denominan rutas del sucesor. Una copia de las rutas del

sucesor también se coloca en la tabla de enrutamiento. EIGRP mantiene información importante de ruta y topología a disposición en una tabla de vecinos y una tabla de topología. Estas tablas proporcionan información detallada de las rutas a DUAL en caso de problemas en la red. DUAL usa la información de estas tablas para seleccionar rápidamente las rutas alternativas. Si un enlace se desactiva, DUAL busca una ruta alternativa, o sucesor factible, en la tabla de topología.

Una de las mejores características de EIGRP es su diseño modular. Se ha demostrado que los diseños modulares o en capas son los más escalables y adaptables. EIRGP logra la compatibilidad con los protocolos enrutados, como IP, IPX y AppleTalk, mediante los PDM. En teoría, EIGRP puede agregar PDM para adaptarse fácilmente a los protocolos enrutados nuevos o revisados como IPv6. Cada PDM es responsable de todas las funciones relacionadas con su protocolo enrutado específico.

El módulo IP-EIGRP es responsable de las siguientes funciones:

- Enviar y recibir paquetes EIGRP que contengan datos IP
- Avisar a DUAL una vez que se recibe la nueva información de enrutamiento IP
- Mantener de los resultados de las decisiones de enrutamiento DUAL en la tabla de enrutamiento IP
- Redistribuir la información de enrutamiento que se aprendió de otros protocolos de enrutamiento capacitados para IP

Configuración del protocolo

Como se trata de un protocolo propietario que sólo es implementado en los routeres de *Cisco* es posible detallar aquí la forma de realizar una configuración básica de EIGRP.

1. Use lo siguiente para habilitar EIGRP y definir el sistema autónomo:

```
router(config)#router eigrp autonomous-system-number
```

El número de sistema autónomo se usa para identificar todos los routers que pertenecen a la internetwork. Este valor debe coincidir para todos los routers dentro de la internetwork.

2. Indique cuáles son las redes que pertenecen al sistema autónomo EIGRP en el router local mediante el siguiente comando:

```
router(config-router)#network network-number
```

Network-number es el número de red que determina cuáles son las interfaces del router que participan en EIGRP y cuáles son las redes publicadas por el router. El comando network configura sólo las redes conectadas. Por ejemplo, la red 3.1.0.0, que se encuentra en el extremo izquierdo de la Figura principal, no se encuentra

directamente conectada al router A. Como consecuencia, esa red no forma parte de la configuración del Router A.

3. Al configurar los enlaces seriales mediante EIGRP, es importante configurar el valor del ancho de banda en la interfaz. Si el ancho de banda de estas interfaces no se modifica, EIGRP supone el ancho de banda por defecto en el enlace en lugar del verdadero ancho de banda. Si el enlace es más lento, es posible que el router no pueda convergir, que se pierdan las actualizaciones de enrutamiento o se produzca una selección de rutas por debajo de la óptima. Para establecer el ancho de banda para la interfaz, aplique la siguiente sintaxis:

```
router(config-if)#bandwidth kilobits
```

Sólo el proceso de enrutamiento utiliza el comando bandwidth y es necesario configurar el comando para que coincida con la velocidad de línea de la interfaz.

4. Cisco también recomienda agregar el siguiente comando a todas las configuraciones EIGRP:

```
router(config-router)#eigrp log-neighbor-changes
```

Este comando habilita el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas.

2.1.2.3. OSPF

Open Shortest Path First (frecuentemente abreviado **OSPF**) es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa *cost* como su medida de métrica. Además, construye una base de datos enlace-estado identica en todos los encaminadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en redes grandes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural a RIP, es VLSM o *sin clases* desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que también soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas. Una red OSPF se puede descomponer en red más pequeñas. Hay una área especial llamada **área backbone** que forma la parte central de la red y donde hay otras áreas conectadas a ella. Las rutas entre diferentes areas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los encaminadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. Los encaminadores eligen a un **encaminador designado'** ***(DR) y un*** **encaminador designado secundario** (BDR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el IP protocolo 89.

Tipos de área

Una red OSPF está dividida en áreas. Estas áreas son grupos lógicos de encaminadores cuya información se puede resumir para el resto de la red. Se pueden definir diferentes tipos de aŕeas "especiales":

Área Backbone

El área backbone (o área cero) forma el núcleo de una red OSPF. Todas las demás áreas y las rutas interiores de las aŕeas están conectadas a un encaminador conectado a una área backbone.

Área de segmento

Un área de segmente es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron distribuidas en OSPF en otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Área de no-segmento

También conocidas como NSSA, una área de no-segmento es un tipo de área de segmento que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

2.1.2.4. BGP

El **BGP** o **Border Gateway Protocol** es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo mas utilizado para redes con intencion de configurar un EGP *(external gateway protocol)*
La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como Sistema Autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).

Introducción a BGP (Border Gateway Protocol)

El protocolo BGP se ha constituido como el principal protocolo de encaminamiento externo utilizado en Internet. Prácticamente todo el tráfico que fluye entre unos ISPs (Internet Service Provider) y otros es encaminado a través de BGP. La versión actual, BGP-4, se encuentra descrita en las RFC 1771 [1] y 1772 [2]. Con el fin de reducir el tamaño de las tablas de encaminamiento y de facilitar su gestión, Internet se encuentra dividido en sistemas autónomos (AS). Un sistema autónomo es un conjunto de redes administradas por una misma organización que tiene definida una única política de encaminamiento [3]. Esta política de encaminamiento decide las rutas admitidas desde los sistemas autónomos vecinos y las rutas que se envían hacia estos sistemas autónomos. En su interior, el AS utiliza un protocolo interno de encaminamiento como, por ejemplo, OSPF. El protocolo BGP un protocolo de encaminamiento entre sistemas autónomos. Cada sistema autónomo en Internet tiene un identificador (ASN) formado por 16 bits, lo que permitiría hasta 65536 sistemas autónomos teóricos diferentes, si bien el rango de 64512 a 65535 se encuentra reservado para uso privado. Las tablas de encaminamiento de BGP-4 almacenan rutas para alcanzar redes, más concretamente prefijos de cierto número de bits. Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo. El principal motivo para almacenar la ruta completa es la detección y eliminación de bucles (loops), esto es, que los paquetes se reenvíen de forma infinita entre unos mismos sistemas autónomos (A-B-C-A-B-C-A...) sin alcanzar nunca el destino o, dicho de otra manera, que los mismos paquetes pasen varias veces por un mismo sistema autónomo. Según el número de conexiones con otros sistemas autónomos y las políticas definidas, un sistema autónomo puede ser de diferentes tipos. El más sencillo (denominado stub AS) tiene una única conexión con otro AS, que será normalmente su ISP. Por este sistema autónomo únicamente circula tráfico local. Si el AS tuviese más de una conexión a otros sistemas, por motivos de redundancia generalmente, se denominaría multihomed. El tráfico que circula dentro del AS seguiría siendo local. Por último, un sistema autónomo de tránsito es un sistema con varias conexiones, el cual reenvía tráfico de una conexión a otra. Por supuesto, los sistemas autónomos pueden decidir y de hecho así lo hacen los tipos de tráfico que transportan, mediante el establecimiento de políticas. 2 Aspectos de seguridad Supongamos una organización A que utiliza BGP para conexión redundante con dos ISPs. Esta organización se ha registrado como sistema autónomo y dispone por tanto de un ASN, el 60500, por ejemplo. Además, en este sistema autónomo, la organización utiliza la red de su propiedad 200.10.4.0/23. El sistema BGP anuncia el prefijo 200.10.4.0/23 a los dos routers vecinos (uno por cada ISP). Y cada ISP propaga las rutas hacia el exterior de forma que el resto de routers BGP de Internet serán informados de la mejor ruta para alcanzar la red 200.10.4.0/23. Hasta aquí todo parece correcto, aunque desde el punto de vista de la seguridad nos podemos formular algunas preguntas [9]: ¿realmente el prefijo 200.10.0/23 pertenece a la organización A? ¿el router que dialoga con los routers vecinos de los ISPs es el que la organización A ha instalado y no es un suplantador que inyecte información maliciosa? ¿la ruta que utiliza un usuario final para conectarse a un servidor de la

organización A es realmente la correcta y no ha sido modificada durante su propagación para redirigir el tráfico hacia un sistema autónomo comprometido B? Realmente BGP-4 no tiene forma de garantizar la respuesta a estas preguntas. Los ataques de suplantación de prefijos, sistemas autónomos o routers pueden realizarse con relativa facilidad y tener repercusiones a nivel de Internet. Necesitamos mecanismos de autentificación que nos garanticen que cada elemento del sistema es quien dice ser. BGP tiene otras carencias de seguridad como la falta de control temporal en sus mensajes. Sin este control, un atacante situado entre dos routers BGP vecinos podría capturar tráfico BGP (un mensaje UPDATE que elimine cierta ruta por ejemplo) y reproducirlo en un instante futuro. Además, al estar BGP basado en TCP, hereda todos sus fallos de seguridad. Los routers vecinos mantienen establecida una conexión TCP permanentemente (sesión BGP). En caso de que esta conexión se interrumpa, el router vecino asumirá que el enlace se ha desconectado o el router del otro extremo ha dejado de funcionar, por lo que eliminará automáticamente todas las rutas afectadas. Un ataque conocido es la inyección de segmentos TCP con el bit de RST activado [6]. El router que recibe un RST considera que el otro extremo le solicita un cierre de conexión y cierra automáticamente la sesión. La consecuencia para la organización A que comentamos en el ejemplo anterior sería que su red quedaría inaccesible, puesto que se eliminarían todas las ruta hacia su red. 3 Soluciones parciales Ante este abanico de problemas de seguridad, los administradores pueden tomar en la actualidad ciertas medidas; sin embargo, como veremos, se trata de medidas que reducen tan sólo una parte de los problemas y, realmente, lo que buscamos son soluciones globales de seguridad en BGP. Mediante la utilización de reglas de filtrado podemos definir las rutas que aceptaremos y aquellas que anunciaremos. Un ISP debería filtrar todas las rutas que procedan de una organización final diferentes a las correspondientes a sus prefijos registrados. Una organización final deberá ajustar sus filtros para no anunciar rutas de otros sistemas autónomos (para no hacer tránsito). Los filtros siempre han existido en BGP y son ciertamente potentes, pero su configuración pormenorizada puede resultar compleja y no se descartan errores por parte del administrador. La seguridad en BGP no sólo debe cubrir ataques intencionados sino también errores de configuración por parte del administrador. Estos últimos son en la actualidad más numerosos que los primeros y deben ser tenidos en cuenta en las políticas de seguridad. Con el fin de evitar la suplantación de routers vecinos, una opción es la utilización de contraseñas en los extremos de la sesión. Sin embargo, esta solución acarrea dificultades añadidas: ¿cómo distribuir la contraseña? Si la enviamos de forma no segura por Internet podría ser interceptada. Pero no sólo eso: ¿cada cuánto tiempo se cambia la contraseña? ¿deben ponerse de acuerdo los administradores vecinos para realizar el cambio justo en el mismo instante? Como vemos, genera demasiados inconvenientes operacionales. Por otro lado, una contraseña utilizada únicamente al inicio de una sesión BGP no impide que se pueda interceptar una conexión ya validada y suplantar a uno de los dos extremos. Desde luego, podemos asegurar el canal completo entre dos routers vecinos ya sea mediante una línea dedicada o bien mediante la utilización de IPSec u otras tecnologías. Aunque esto no haría nada contra la propagación de rutas inválidas que hayan sido inyectadas en algún tramo anterior. Un método para garantizar que las rutas propagadas por un router

tienen su origen en un sistema autónomo propietario de los prefijos anunciados es mediante la utilización de registros de enrutamiento como RADB [7]. El router puede consultar un registro para verificar que cada ruta tiene un origen válido y no está propagando rutas falsas. Esta opción no impide que se pueda modificar una ruta que debería ir del sistema autónomo 1 al 2 y hacerla pasar por un sistema autónomo malicioso, 3, entre ambos. 4 S-BGP Entre las soluciones propuestas más completas para dotar de seguridad a BGP se destaca S-BGP (Secure BGP), desarrollado por BBN y promovido por NSA y DARPA. Su objetivo es dotar de autenticidad, integridad y autorizaciones a los mensajes BGP. Su último borrador data de enero de 2003 [4]. S-BGP está formado por tres elementos: o o Certificados digitales. Se utilizan dos PKIs, una para autentificar los prefijos IP y otra para los sistemas autónomos. Los autores proponen que las autoridades de certificación se correspondan con los actuales organismos de gestión de direcciones IP y números de sistemas autónomos (ICANN, RIRs como RIPE o ARIN, etc.) o o Attestations.(atestaciones) Mediante este término se denominan las autorizaciones emitidas que, según se explica más adelante, pueden ser de dos tipos: de direcciones y de rutas. o o IPSec. Su misión es aportar autenticidad e integridad en los enlaces entre dos routers. No se considera la confidencialidad puesto que no es necesaria para la difusión de rutas. En los siguientes apartados se estudian cada uno de los elementos mencionados. 4.1 Certificados digitales Se utilizan dos PKIs basadas en certificados X.509v3, una para direcciones y otra para sistemas autónomos. El motivo de establecer dos PKIs es porque las entidades que asignan prefijos de red y las que asignan sistemas autónomos podrían ser distintas. Esto es, una organización podría recibir de una entidad sus prefijos de red y de otra distinta, su número de sistema autónomo. La estructura de cada PKI está encabezada por el ICANN como propietario de todo el espacio de direcciones IP y de números de sistemas autónomos, el cual va delegando en distintos entidades intermedias hasta llegar al ISP u organización final. 4.1.1 PKI para la asignación de direcciones La primera PKI es para la asignación de direcciones. Está formada por certificados que asocian un conjunto de prefijos como propiedad de una organización. Al contrario que un certificado tradicional que se utiliza para probar la identidad de su propietario, estos certificados prueban la pertenencia de un conjunto de prefijos de red. Para este fin los autores consideran la utilización de un atributo X.509 pero lo descartan por no estar soportado suficientemente, a favor de una extensión privada v3 al certificado de clave pública [4]. 4.1.2 PKI para la asignación de sistemas autónomos y routers asociados La segunda PKI es para la asignación de sistemas autónomos y routers asociados. Los certificados almacenados en esta PKI pueden ser de tres tipos: o o Certificado emitido por un registro (o el ICANN) a una organización que contiene su número de sistema autónomo y la clave pública de la organización. Prueba la propiedad de un sistema autónomo. Se firma con la clave privada del registro. o o Certificado emitido por una organización (ISP) que contiene su número de sistema autónomo y su clave pública. Se firma con la clave privada de la organización. o o Certificado emitido por una organización (ISP) que identifica a su router BGP, mediante su nombre DNS, un identificador, un número de sistema autónomo y la clave pública del router. Prueba que un router pertenece al sistema autónomo de una organización. Se firma con la clave privada de la organización. El objetivo de esta PKI es probar que

un sistema autónomo dado y un router pertenecen a cierta organización. Los routers intermedios utilizarán los certificados de las PKIs para asegurar la autenticidad de la información contenida en las rutas recibidas. 4.2 Attestations Un attestation es un documento digital que emite una entidad para autorizar cierto comportamiento a un objeto. Se definen dos tipos de attestations: de direcciones y de rutas, los cuales se difunden mediante mecanismos diferentes. 4.2.1 Attestations de direcciones Los attestations de direcciones (AA) son emitidos (firmados) por una organización para que un sistema autónomo de su propiedad pueda anunciar unos prefijos. Mediante la clave pública contenida en el correspondiente certificado de direcciones, un router intermedio puede verificar la validez de un AA. El certificado es la prueba de la pertenencia de un prefijo a una organización y el AA, la autorización para que ese prefijo se pueda anunciar. Debido a que los attestations de direcciones apenas se modifican, se prefiere su almacenamiento en un repositorio externo, en lugar de enviarlos en los propios mensajes BGP. Cada vez que un router intermedio recibe una ruta contenida en un mensaje BGP de tipo UPDATE, verifica la pertenencia de los prefijos anunciados a una organización. Para ello necesitará consultar el certificado de la organización. 4.2.2 Attestations de rutas Los attestations de rutas (RA) son firmados por un router S-BGP para autorizar al siguiente router vecino a propagar una ruta. El objetivo aquí es asegurar la cadena de routers, de forma que no pueda alterarse la ruta en tránsito para incluir un sistema autónomo intermedio no autorizado. A diferencia del anterior tipo de attestation, los RA son muy cambiantes, por lo que se envían en el propio mensaje UPDATE, utilizando para ello un nuevo atributo. Este nuevo atributo se ha definido de tipo opcional y transitivo para que aquellos sistemas BGP intermedios que no soporten S-BGP, puedan no interpretarlo pero sí se lo pasen al siguiente sistema BGP. Cada sistema BGP añade un RA al mensaje UPDATE antes de pasarlo al siguiente sistema autónomo. De esta manera, el router BGP que recibe el mensaje debe verificar cada uno de los RA recibidos, lo que le permitirá validar toda la cadena de saltos entre cada sistema autónomo y el siguiente. Para ello necesitará garantizar la validez de los RA, consultando los respectivos certificados de routers BGP. 4.3 IPSec Finalmente, el último elemento de S-BGP es IPSec. Su misión es asegurar las sesiones BGP entre dos routers vecinos proporcionando integridad y autenticidad. Se utilizan los componentes ESP e IKE de IPSec. S-BGP no garantiza la confidencialidad, por lo que se configura IPSec para no hacer encriptación en los mensajes BGP. Realmente, la encriptación no es necesaria puesto que las rutas son públicas y además ni siquiera sería aconsejable puesto que supondría una carga extra de proceso el cifrado y descifrado de mensajes. Una ventaja adicional de IPSec es que, al funcionar en la capa de red, subsana las vulnerabilidades de TCP explicadas anteriormente. Los segmentos TCP enviados fuera de una conexión IPSec a un host no se llegan siquiera a procesar, por lo que BGP deja de verse afectado por el envío de segmentos RST falsos, inundaciones de SYN u otras deficiencias inherentes a TCP. 5 Implementación de S-BGP La puesta en funcionamiento de S-BGP en Internet es compleja. Por un lado, requiere la colaboración de las entidades de registro para hacerse cargo de los procedimientos asociados a una PKI: emisión de certificados, revocación de los mismos, mantenimiento y publicación de listas de revocación (CRL), etc. Esto requiere nueva infraestructura en equipos y personal,

así como una cuidada política de seguridad, por parte no sólo del ICANN sino del resto de autoridades de registro delegadas incluyendo ISPs. En caso de que la colaboración de estas entidades supusiera un grave impedimento, se podría estudiar la fórmula para utilizar autoridades de certificación independientes, aunque esta posibilidad no está contemplada por los autores y supondría replantear todas las especificaciones. Por parte de las organizaciones se requiere la actualización de sus routers BGP, no sólo de software sino también de hardware. La ampliación de hardware es necesaria puesto que S-BGP requiere que los routers almacenen certificados digitales (mayor memoria) y tengan potencia suficiente para la realización de funciones criptográficas (mayor capacidad de proceso). Una posibilidad para no tener que cambiar los costosos routers BGP es anexarles un PC que les proporcione memoria adicional e incluso, CPU. Los certificados, CRLs y attestations de direcciones se almacenan de forma externa en un repositorio. Los routers sin embargo requieren estos elementos para validar las rutas. Esto nos lleva a un problema operacional, que no queda claramente resuelto por los autores, de cómo se inicializa un router para comenzar a funcionar estando el repositorio hospedado en otra red, si para validar las rutas requiere certificados y para tener certificados requiere rutas. Quizás sea necesaria una inicialización con certificados instalados offline, aunque su almacenamiento es problemático puesto que los certificados tienen una fecha de caducidad y además podrían ser revocados en cualquier momento. Por otro lado, podemos pensar en el mayor ancho de banda ocupado por los UPDATE de S-BGP, los cuales transmiten además ahora los attestations de rutas. Se requiere también mayor capacidad de proceso y de memoria para el almacenamiento de certificados, como hemos comentado anteriormente. Sin embargo, los autores demuestran estadísticamente [4] que estos incrementos de ancho de banda, proceso y memoria no son significativos. Las actualizaciones de software y hardware resultan costosas para las organizaciones, las cuales no ven una mejora inmediata que puedan repercutir a sus clientes. Probablemente sean necesarios varios ataques al protocolo BGP antes de que las organizaciones afectadas consideren la necesidad de asegurar sus sistemas. 6 Trabajos relacionados con S-BGP La RFC 2385 describe TCP/MD5 [5], una extensión a TCP para incluir firmas MD5 en sus mensajes. La utilización de TCP/MD5 en los segmentos TCP intercambiados entre dos pares BGP proporciona integridad y autentificación en los mensajes BGP. Sin embargo, no resuelve otros problemas de BGP como la validación de las rutas anunciadas. El principal problema de TCP/MD5 es la distribución de las claves entre los pares BGP, lo que en la práctica provoca que se utilice un “secreto compartido” entre ambos extremos (clave simétrica) y que ésta no se modifique tan periódicamente como sería recomendable. Una alternativa a S-BGP es soBGP (Secure Origen BGP) [6][7]. Utiliza certificados digitales y un nuevo tipo de mensaje BGP denominado “Security Message”. Valida el origen de las rutas anunciadas pero no considera ataques que alteren los saltos intermedios de una ruta. 7 Conclusiones El correcto funcionamiento de BGP es crucial para el funcionamiento de Internet. De BGP depende que cuando un host envíe un paquete a otro host situado en un sistema autónomo diferente, éste llegue correctamente a su destino. Los ataques al protocolo BGP no son frecuentes en la actualidad, aunque podrían popularizarse en un futuro poniendo contra las cuerdas a toda la infraestructura de Internet,

desviando rutas y dejando redes inaccesibles. Sin embargo, no sólo se deben considerar los ataques al protocolo, sino también los fallos de configuración por parte de los administradores. El objetivo de la seguridad en BGP es que un ataque a un sistema autónomo o fallo de configuración no se propague al resto de Internet y se mantenga local. S-BGP son unas extensiones de seguridad que proporcionan integridad, autenticidad y autorizaciones a BGP. Sus elementos constituyentes son: PKI para la asignación de direcciones, PKI para la asignación de sistemas autónomos y routers asociados, attestations de direcciones, attestations de rutas e IPSec. El sostenimiento de las PKIs se asigna a las mismas entidades responsables de la asignación de direcciones IP y sistemas autónomos (ICANN y registros delegados). Cada vez que un router BGP recibe una ruta, verifica que la cadena de saltos entre sistemas autónomos anteriores esté autorizada, así como que los prefijos y sistema autónomo inicial de la ruta sea válido. Para ello necesita consultar los certificados digitales. La función de IPSec es asegurar los canales entre pares de routers. S-BGP constituye unas extensiones complejas que requieren la colaboración de numerosas organizaciones, las cuales deben realizar inversiones para actualizar sus routers. Si comparamos S-BGP con otras soluciones, como soBGP, encontramos que es el protocolo que cubre el mayor número de posibles ataques, a costa de un aumento en complejidad, infraestructura y procesamiento. La seguridad tiene siempre un coste, aunque su implantación no debe ser excesivamente compleja puesto que no sería práctico [8]. Queda por determinar el compromiso entre el grado de seguridad necesario y factores como complejidad, rendimiento y costes. Aunque no cubra el 100% de las vulnerabilidades conocidas, otra solución podría ser finalmente puesta en marcha si abarca las principales vulnerabilidades pero con un coste considerablemente menor.

2.2. Protocolos Ruteables

2.2.1 IP

El **Protocolo de Internet** (**IP**, de sus siglas en inglés *Internet Protocol*) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

Tecnologías y protocolos de red

Nivel de aplicación	FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, *etcétera*
Nivel de presentación	ASN.1, MIME, SSL/TLS, XML, *etcétera*
Nivel de sesión	NetBIOS, SIP, *etcétera*
Nivel de transporte	SCTP, SPX, TCP, UDP, *etcétera*
Nivel de red	AppleTalk, **IP**, IPX, NetBEUI, X.25, *etcétera*
Nivel de enlace	ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi, *etcétera*
Nivel físico	Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232, *etcétera*

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del *mejor esfuerzo* (*best effort*), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, esta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU[5]) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de como estén de congestianadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (switches) y los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y

---

[5] La **unidad máxima de transferencia** (*Maximum Transfer Unit* - **MTU**) es un término informático que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.
Ejemplos de MTU:Ethernet: 1500 bytes, ATM (AAL5): 8190 bytes, FDDI: 4470 bytes y PPP: 576 bytes
Los datos pueden recorrer varios tipos de redes mediante distintos protocolos antes de llegar a su destino, por lo tanto para que un paquete llegue sin fragmentación, este ha de ser menor o igual que el mínimo MTU de los protocolos de redes que lo transporten.

destino de 128 bits, muchas mas direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La version 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

Direccionamiento IP y enrutamiento

Quizás los aspectos más complejos de IP son el direccionamiento y el enrutamiento. El direccionamiento se refiere a la forma como se asigna una dirección IP y como se dividen y se agrupan subredes de equipos.

El enrutamiento consiste en encontrar un camino que conecte una red con otra y aunque es llevado a cabo por todos los equipos, es llevado a cabo principalmente por enrutadores que no son más que computadores especializados en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos...

2.2.2 IPX

Siglas de *Internetwork Packet Exchange* (Intercambio de paquetes interred).

Protocolo de nivel de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

Intercambio de paquetes interredes. Protocolo de comunicaciones NetWare que se utiliza para encaminar mensajes de un nodo a otro. Los paquetes IPX incluyen direcciones de redes y pueden enviarse de una red a otra. Ocasionalmente, un paquete IPX puede perderse cuando cruza redes, de esta manera el IPX no garantiza la entrega de un mensaje completo. La aplicación tiene que proveer ese control o debe utilizarse el protocolo SPX de NetWare. IPX provee servicios en estratos 3 y 4 del modelo OSI (capas de red y transporte). Actualmente este protocolo esta en desuso y solo se utiliza para juegos en red antiguos

2.2.3 Aplle-table

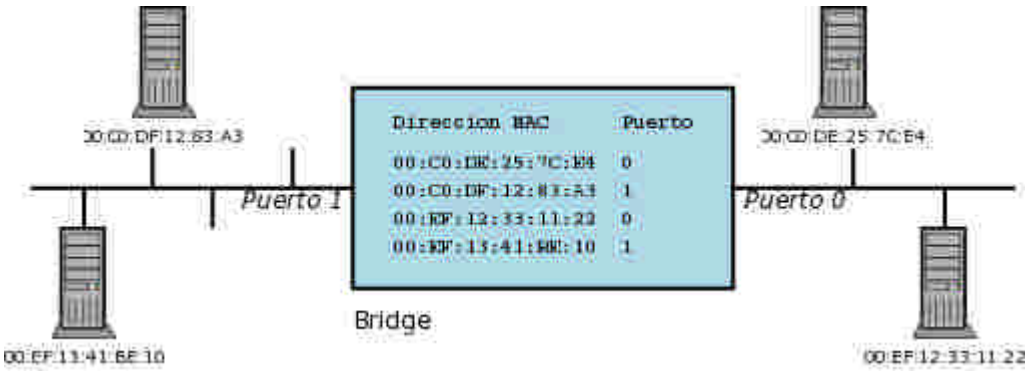
2.3. Bridges

Un bridge conecta dos redes como una sola red usando el mismo protocolo de establecimiento de red.

Funciona a través de una tabla de direcciones MAC[6] detectadas en cada segmento a que esta conectado. Cuando detecta que un nodo de uno de los segmentos está

[6] En redes de computadoras **Media Access Control address** cuyo acrónimo es **MAC** es un identificador físico -un número, único en el mundo, de 48 bits- almacenado en fábrica dentro de una tarjeta de red o una interface usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de internet. Las direcciones MAC son asignadas por el IEEE y son utilizadas en varias tecnologías incluyendo:

intentando transmitir datos a un nodo del otro, el bridge copia el *frame* para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.



Ejemplo de 2 redes interconectadas por un bridge.

La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier *frame* con cualquier destino para todos los otros nodos conectados, en cambio el primer sólo pasa los *frames* pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Para hacer el *bridging* o interconexión de más de 2 redes, se utilizan los switches.

2.4. Switches

Interconexión de switches y bridges

Los bridges y 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.

- Ethernet
- Token Ring
- 802.11 redes inalámbricas (WIFI).
- ATM

MAC opera en el nivel 2 de OSI, el cual se encarga de enviar paquetes ARP para verificar qué número (expresado en hexadecimal) tiene impreso en la tarjeta. La información recibida se almacena en una tabla para futuros envios de información, o sea que en redes LAN bastante grandes, para enviar información más rapidamente.

2.4.1 Características

2.4.2 Modos de operación

Introducción al funcionamiento de los conmutadores

Conexiones en un switch Ethernet

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.

Bucles de red e inundaciones de tráfico

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallos.

Conmutadores de nivel 3

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiples redes de nivel 2 (ver VLANs) y encaminar los paquetes

(de nivel 3) entre las redes, realizado por tanto las funciones de encaminamiento o routing (ver router).

2.4.3 VLAN' S

VLAN es el acrónimo de Virtual Local Area Network o Virtual LAN.

Este concepto surge con la aparición de los conmutadores (ver switch) de nivel 3 o superior, que aglutinan tanto las funciones de conmutación (nivel 2 Capa_de_enlace_de_datos) como las funciones de enrutado (nivel 3 Capa_de_red). Consiste en cada una de las redes de área local (LAN) creadas en los conmutadores, de forma que el tráfico de las distintas redes dentro del mismo switch no se mezcla entre ellas gracias a los mecanismos de enrutado.

También se dice que son "dominios de broadcast" (ver router) dado que el tráfico de broadcast a nivel 2 no se difunde entre las diferentes VLANs sino que se queda limitado al conjunto de puertos (físicos o virtuales) que pertenecen a cada una de las VLANs.

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador (VER hub) Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo con-centrador o segmento de la red. Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast"

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub.

Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, logramos, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar puentes y encaminadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, podemos mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

Tecnología:

Existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de bridging, y conmutación de segmentos con funciones de bridging/routing.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, sólo la última, con funciones de bridge/router, ofrece todos las ventajas a las VLAN.

1. Conmutadores de puertos.

Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se

diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignadas y reasignadas a diferentes grupos de trabajo o redes virtuales.

Podemos definir a los conmutadores de puertos como "software patch panels", y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo; sin embargo, tienen graves limitaciones.

Dado que están diseñados como dispositivos compartiendo un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador, y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos, padecen de conectividad con el resto de la red. Al segmentar sus propios backplanes, no proporcionan conectividad integrada entre sus propios backplanes, y por tanto están "separados" de la comunicación con el resto de la red. Para ello requieren un bridge/router externo. Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red.

Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, y por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

2. Conmutadores de segmentos con bridging:

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Para ello, se emplean los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos, para proporcionar conectividad entre varios segmentos a la "velocidad del cable" o velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane, sino grupos lógicos de nodos que pueden ser conectados a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, mediante comandos software se puede reconfigurar y modificar la estructura de la VLAN, con la ventaja añadida del ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de

grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red precisan de routers (encaminadores), con las consecuencias de las que ya hemos hablado en el caso anterior respecto del coste y la reconfiguración de la red.

3. Conmutadores de segmentos con bridging/routing:

Son la solución evidente tras la atenta lectura de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además, con funciones añadidas de routing (encaminamiento), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de red.

Además, sus funciones de routing facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales, podemos crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndonos así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de routing, la comunicación con el resto de la red se puede realizar de dos modos diferentes: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLAN’s.

Prestaciones de las VLAN:

Los dispositivos con funciones VLAN nos ofrecen unas prestaciones de "valor añadido", suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN.

Al igual que en el caso de los grupos de trabajo "físicos", las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast. Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física. Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica.

Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.

Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes.
Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que nos permiten determinar con gran precisión las características del tráfico y de la seguridad que deseamos en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

Aplicaciones y productos:

Vamos a intentar esquematizar los puntos en que las redes virtuales pueden beneficiar a las redes actuales:

1. Movilidad:

2. Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo. Dominios lógicos:

3. Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos. Control y conservación del ancho de banda:

4. Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros. Conectividad:

5. Los modelos con funciones de routing nos permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos. Seguridad:

6. Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad. Protección de la inversión:

Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.

El primer suministrador de conmutadores con soporte VLAN fue ALANTEC (familia de concentradores / conmutadores multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones VLAN: Bytex (concentrador inteligente 7700), Cabletron (ESX-MIM), Chipcom (OnLine), Lannet (MultiNet Hub), Synoptics (Lattis System 5000), UB (Hub Access/One) y 3Com (LinkBuilder).

Resumiendo:

Con los procesos de reingeniería de empresas y de downsizing, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes.

Las redes virtuales combinan mayores anchos de banda, facilidades de configuración y potencial de crecimiento, lo que ayudará a que se conviertan en un standard en los entornos corporativos.

En la actualidad, las implementaciones de tecnologías de redes virtuales no son interoperativos entre diferentes productos de diversos fabricantes.

Muchos de estos fabricantes intentan buscar soluciones adecuadas para lograr dicha interoperatividad, y por ello, una gran ventaja de las soluciones basadas en software es que podrán ser adaptadas a las normalizaciones que tendrán lugar en un futuro cercano. Algunas soluciones basadas en hardware habrán de quedarse atrás en este sentido.

Otro punto a destacar es que la tecnología ATM prevé, como parte importante de sus protocolos, grandes facilidades para las redes virtuales, lo que sin duda equivaldrá a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas VLAN.

El futuro es claro respecto de este punto: Las características VLAN formarán parte, en breve, de todos los equipos que se precien de querer ser competitivos.

3. Servicios de Voz y Video

III. INTEGRIDAD

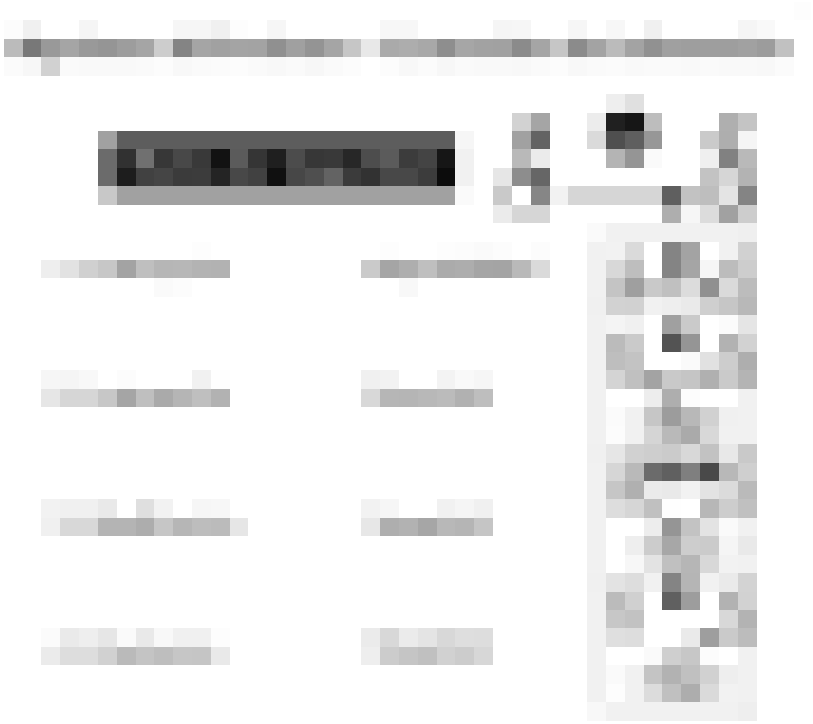
1. Definición en redes

Una de las mejores definiciones sobre la naturaleza de una red es la de identificarla como un sistema de comunicaciones entre computadoras. Como tal, consta de un soporte físico que abarca cableado y placas adicionales en las computadoras, y un conjunto de programas que forma el sistema operativo de red.

La diferencia sustancial entre un sistema basado en una minicomputadora o gran computadora (mainframe) y una red es la distribución de la capacidad de procesamiento . En el primer caso, se tiene un poderoso procesador central, también denominado "host", y terminales "bobas" que funcionan como entrada y salida de datos pero son incapaces de procesar información o de funcionar por cuenta propia. En el segundo caso, los miembros de la red son computadoras que trabajan por cuenta propia salvo cuando necesitan un recurso accesible por red.

2. Conceptos Generales de

Cuando se piensa establecer una estrategia de seguridad, la pregunta que se realiza, en primera instancia, es: ¿en qué baso mi estrategia?. La respuesta a esta pregunta es bien simple. El algoritmo Productor/Consumidor.



En este algoritmo, hay dos grandes entidades: una que es la encargada de producir la información; la otra entidad es el consumidor de esta información y otra, llamada precisamente “otros”. Entre el productor y el consumidor, se define una relación que tiene como objetivo una transferencia de “algo” entre ambos, sin otra cosa que

intervenga en el proceso. Si esto se logra llevar a cabo y se mantiene a lo largo del tiempo, se estará en presencia de un sistema seguro.

En la realidad, existen entidades y/o eventos que provocan alteraciones a este modelo. El estudio de la seguridad, en pocas palabras, se basa en la determinación, análisis y soluciones de las alteraciones a este modelo**.**

En una observación y planteamiento del modelo, determinamos que sólo existen cuatro tipos de alteraciones en la relación producción-consumidor (ver el gráfico del algoritmo) Antes de pasar a explicar estos casos, habrá que definir el concepto de "recurso".

Recurso, está definido como "bienes, medios de subsistencia". Esta es una definición muy general. De todas maneras, resulta conveniente para nuestra tarea. Podemos mencionar como recurso a cualquier cosa, ya sean bienes específicos o que permitan la subsistencia de la organización como tal.

Debido a ello, es que podemos diferenciar claramente tres tipos de recursos:

- Físicos
- Lógicos
- Servicios.

Los recursos físicos son, por ejemplo, las impresoras, los servidores de archivos, los routers, etc.

Los recursos lógicos son, por ejemplo, las bases de datos de las cuales sacamos la información que permite trabajar en la organización.

Los servicios son, por ejemplo, el servicio de correo electrónico, de página WEB, etc.

Todas las acciones correctivas que se lleven a cabo con el fin de respetar el modelo estarán orientadas a atacar uno de los cuatro casos. Explicaremos y daremos ejemplos de cada uno de ellos.

2.1. Protección

En el cual se pone en riesgo la privacidad de los datos.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos sobre cuentas en el banco	Se ha puesto un dispositivo que permite monitorear los paquetes en la red y sacar información de ellos.	Conseguir datos privados sobre montos de cuentas corrientes.

Servicio	Correo electrónico	Se ha implantado un programa que duplica los mensajes (mails) que salen de una sección y los envía a una dirección.	Leer información

2.2. Interrupción

Este caso afecta la disponibilidad del recurso (tener en cuenta la definición de recurso: físico, lógico y servicio).

Por ejemplo:

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Alguien dio de baja el servidor (por algún método)	No poder enviar Mail
Físico	Impresora	Falta de alimentación eléctrica.	No imprime

2.3. Modificación

Afecta directamente la integridad de los datos que le llegan al consumidor.

Recurso Afectado	Nombre	Causa	Efecto
Lógico	Base de datos de pagos en cuentas corrientes	Se ha implantado un programa que redondea en menos los pagos y carga éstos redondeos a una cuenta corriente	Incrementar el crédito de una cuenta corriente sobre la base del redondeo realizado en los pagos
Servicio	Servidor de página WEB	Alguien logró ingresar como WEBMASTER y ha cambiado los contenidos de la página	Los datos mostrados en la página no son los reales

2.4. Fabricación

En éste, la información que recibe el consumidor es directamente falaz.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos de deudores	Se ha generado una base de datos falsa, la que ante el pedido de informes, responde ella con sus datos	Hacer pasar a los deudores como que no lo son
Servicio	Servidor WEB	Alguien se ha apropiado del password del WEBMASTER y, modificando el direccionamiento, logra que se cargue otra página WEB	Redireccionar la página WEB hacia otro sitio

2.5. Control de acceso

Este servicio se utiliza para evitar el uso no autorizado de recursos.

2.6. Disponibilidad

3. Protocolos de seguridad

Un escenario típico consiste de un número de *principales*, tales como individuos, compañías, computadoras, lectores de tarjetas magnéticas, los cuales se comunican usando una variedad de canales (teléfono, correo electrónico, radio . . .) o dispositivos físicos (tarjetas bancarias, pasajes, cédulas . . .).

Un *protocolo de seguridad* define las reglas que gobiernan estas comunicaciones, diseñadas para que el sistema pueda soportar ataques de carácter malicioso.

Protegerse contra todos los ataques posibles es generalmente muy costoso, por lo cual los protocolos son diseñados bajo ciertas premisas con respecto a los riesgos a los cuales el sistema está expuesto. La evaluación de un protocolo por lo tanto envuelve dos preguntas básicas: ¿Es el modelo de riesgo realista? ¿El protocolo puede controlar ese nivel de riesgo?

Un *protocolo* es una serie de pasos, que involucra a dos o mas principales, diseñado para realizar una tarea particular.

1. Todos los principales deben conocer los pasos del protocolo de antemano.

2. Todos deben estar de acuerdo en seguir el protocolo.

3. El protocolo no admite ambigüedades.

4. El protocolo debe ser completo – define qué hacer en cualquier circunstancia posible.

5. No debe ser posible hacer más (o aprender más) que lo que el protocolo define.

Un *protocolo criptográfico* es un protocolo que usa funciones criptograficas en algunos o todos los pasos.

Taxonomía de Protocolos

Los protocolos pueden ser clasificados en base a su modo de funcionamiento en:

Protocolos arbitrados: Aquellos en los que es necesaria la participación de un tercero para garantizar la seguridad del sistema. *Ejemplo:* método de compra y venta usando un notario.

Los protocolos arbitrados pueden ser ineficientes, o incluso vulnerables a ataques contra el árbitro.

Protocolos adjudicados: Son protocolos que tienen dos partes, una parte no-arbitrada y una arbitrada. El subprotocolo arbitrado se activa solo en caso de disputa.

Protocolos auto-reforzados o autoadjudicados: No se requiere de un arbitro para garantizar el protocolo. Se puede abortar la secuencia de pasos en cualquier momento, dejando sin efecto las acciones tomadas. No todas las situaciones son apropiadas para este tipo.

Los **ataques** contra protocolos pueden ser *activos* o *pasivos*.

Si el adversario es uno de los participantes, se trata de una **trampa**. *Ejemplo:* Acordando una Clave de Sesión.

Las *claves de sesión* buscan reducir la oportunidad de ataques, usando una clave nueva cada vez que se abre una nueva sesión de intercambio de mensajes.

Evidentemente la clave no puede ser transmitida en claro sobre el canal. Entonces, necesitamos un *protocolo inicial* para acordar una nueva clave (aleatoria) para cada sesión. El protocolo inicial también tiene que ser seguro. Una posibilidad podría ser usar claves públicas para el protocolo inicial (en general son demasiado ineficientes para la sesión misma).

El protocolo **Needham-Schroeder** es la versión formal del anterior.

4. Permisos

5. Sistemas de respaldo

IV. SEGURIDAD

1. Importancia de la Seguridad en Redes

Los orígenes de la seguridad de redes datan de finales de los años 60 y 70 cuando aparecen procedimientos de seguridad física . El disponer del procesamiento y su interfaz de ingreso en un área físicamente segura, nos garantizaba un medio seguro. Posteriormente, el entorno de computación cambió drásticamente durante los años 80 y a principios de los 90, aparecieron nuevos retos significativos para la seguridad de las redes necesarios de controlar. Comienza el proceso de interconexión de las distintas redes locales y el uso creciente de Internet complica aún más las vulnerabilidades de las redes.

A finales de los años 90, los proveedores de software comercial, en nuestro medio por ejemplo la empresa Orion penetraron en el mercado aún incipiente de la seguridad de redes y tomaron posesión del sector, con productos puntuales que proporcionaban soluciones de firewall, encriptación, antivirus y otras actividades de gestión de riesgos de seguridad a la información.

Según la *International Data Corporation* (IDC), en la Unión Europea, el mercado de los productos de seguridad como ser: los programas informáticos de seguridad para Internet, el mercado de la seguridad de las comunicaciones electrónicas y el mercado de la seguridad para las tecnologías de la información han registrado un crecimiento sustancial a lo largo de los últimos años y se estima que crecerá aún mas para el 2004.

Para la National Security Agency, la seguridad *es una condición que resulta del establecimiento y mantenimiento de medidas protectivas que aseguran un estado de inviolabilidad de acciones o influencias hostiles*. Luego, la seguridad de las redes puede entenderse como aquello que *describe todos los aspectos de protección a un acceso no autorizado de la información sensible almacenada en un computador o que fluye a través de una red de computadoras*. Esto incluye, la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

La intrusión o el acceso no autorizado a redes de computadores se realiza habitualmente de forma malintencionada para copiar, modificar o destruir datos violando los principios de autenticidad, integridad, disponibilidad o no repudio de la información.

En general los problemas de seguridad en redes tienen que ver con malas configuraciones, deficientes contraseñas o vulnerabilidades en la función de una red de datos cual es la de transmitir y recibir información desde y a lugares remotos

utilizando recursos de hardware y software que son susceptibles de ser interceptados por intrusos.

Estudios internacionales sobre el mercado de seguridad en redes, señalan que esta tecnología se convertirá probablemente en un factor clave del desarrollo de la sociedad de la información a medida que las aplicaciones de las redes desempeñen un papel fundamental en la vida económica y social. Se estima que la demanda de profesionales en seguridad de redes irá en aumento.

2. Funciones de Seguridad

2.1. Análisis de Riesgo

La autenticación suele realizarse mediante una contraseña, aún cuando sería más lógico - si bien los costos resultan todavía altos para la mayoría de sistemas - que se pudiera combinar con características biométricas del usuario para impedir la suplantación. Entre éstas pueden estar: la realización de la firma con reconocimiento automático por ordenador, el análisis del fondo de ojo, la huella digital u otras.

Al margen de la seguridad, nos parece que el mayor riesgo, aún teniendo un entorno muy seguro, es que la Informática y la Tecnología de la Información en general no cubran las necesidades de la entidad; o que no estén alineadas con las finalidades de la organización.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples.

El primer paso es conocerlos y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido y debiera crearnos una situación de desasosiego.

Dado que las medidas tienen un costo, a veces, los funcionarios se preguntan cuál es el riesgo máximo que podría soportar su organización. La respuesta no es fácil porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto de la información, y del impacto que su no disponibilidad pudiera tener en la entidad. Si nos basamos en el impacto nunca debería aceptarse un riesgo que pudiera llegar a poner en peligro la propia continuidad de la entidad, pero este listón es demasiado alto.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente - normalmente de poco impacto pero frecuencia muy alta - y otros, como por ejemplo: el acceso indebido a los datos (a veces a través de redes), · la cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible"), los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior), la variación no autorizada de programas, su copia indebida, y tantos otros, persiguiendo el propio beneficio o causar un daño, a veces por venganza.

Otra figura es la del “hacker”, que intenta acceder a los sistemas sobre todo para demostrar (a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección que se hayan establecido.

Alguien podría preguntarse por qué no se citan los virus, cuando han tenido tanta incidencia. Afortunadamente, este riesgo es menor en la actualidad comparando con años atrás. Existe, de todas maneras, un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Un riesgo adicional es que los virus pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil - no nos atrevemos a decir que imposible- por las características y la complejidad de los grandes equipos y debido a las características de diseño de sus sistemas operativos.

En definitiva, las amenazas hechas realidad pueden llegar a afectar los datos, en las personas, en los programas, en los equipos, en la red y algunas veces, simultáneamente en varios de ellos, como puede ser un incendio.

Podríamos hacernos una pregunta realmente difícil: ¿qué es lo más crítico que debería protegerse? La respuesta de la mayoría, probablemente, sería que las personas resultan el punto más crítico y el valor de una vida humana no se puede comparar con las computadoras, las aplicaciones o los datos de cualquier entidad. Ahora bien, por otra parte, podemos determinar que los datos son aún más críticos si nos centramos en la continuidad de la entidad.

Como consecuencia de cualquier incidencia, se pueden producir unas pérdidas que pueden ser no sólo directas (comúnmente que son cubiertas por los seguros) más fácilmente, sino también indirectas, como la no recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

2.2. Servicios de Seguridad

El documento de ISO que describe el Modelo de Referencia OSI, presenta en su Parte 2 una *Arquitectura de Seguridad*. Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes **servicios de seguridad**:

2.2.1 Autenticación de las Comunicaciones

Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación. Puede ser de dos tipos:

- **Con prueba de origen**. Cuando el destinatario tiene prueba del origen de los datos.
- **Con prueba de entrega**. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

2.2.2 Autenticación de los Datos

Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

El mecanismo de integridad de datos soporta el servicio de integridad de datos.

2.2.3 Control de Acceso

Autentica las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el enviante está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

2.2.4 Garantía de la privacidad de los datos

Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

2.2.5 Análisis de flujo del tráfico

2.2.6 Garantía de la Integridad de los datos

Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta

cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una infomración suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

El mecanismo de integridad de datos soporta el servicio de integridad de datos.

2.2.7 Reconocimiento del Receptor y/o Transmisor

Existen dos grados en el mecanismo de autenticación:

- **Autentificación simple**. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
- **Autentificación fuerte.** Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado.

Un certificado es un documento firmado por una Autoridad de Certificación, válido dunte el período de tiempo indicado, que asocia una clave pública a un usuario.

El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par, el cual es un servicio que corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra.

BIBLIOGRAFÍA BÁSICA

1. BLACK, ULISES*, REDES DE COMPUTADORES: PROTOCOLOS, NORMAS E INTERFACES,* 2ª. ED ,ESPAÑA, ALFA OMEGA-RAMA, 2002.
2. CABALLERO, JOSÉ MANUEL, *REDES DE BANDA ANCHA,* ESPAÑA, ALFA OMEGA-RAMA, 2002.
3. CARBALLAR, JOSÉ A., *EL LIBRO DE LAS COMUNICACIONES DEL PC,* ESPAÑA, ALFA OMEGA-RAMA, 2002.
4. CASTRO, MANUEL, *SISTEMAS BÁSICOS DE COMUNICACIONES,* ESPAÑA, ALFA OMEGA-RAMA, 2002.
5. COMMER, DOUGLAS E., *EL LIBRO DE INTERNET, TODO LO QUE USTED NECESITA SABER ACERCA DE REDES DE COMPUTADORAS Y COMO FUNCIONAN,* 2ª. EDICIÓN, MÉXICO, PRENTICE HALL HISPANOAMERICANA, 1998, 344 PP.
6. GALLO, MICHAEL A., *COMUNICACIÓN ENTRE COMPUTADORAS Y TECNOLOGÍA DE REDES*, MÉXICO, THOMSON, 2002, 632 PP.
7. GUIJARRO, LUIS, *REDES ATM. PRINCIPIOS DE INTERCONEXIÓN Y SU APLICACIÓN*, ESPAÑA, ALFA OMEGA-RAMA, 2002.
8. OPPLIGER, ROLF*, SISTEMAS DE AUTENTIFICACIÓN PARA SEGURIDAD EN REDES*, ESPAÑA, ALFA OMEGA-RAMA, 2002.
9. PALMER, MICHELL J., *REDES DE COMPUTADORAS, UNA GUÍA PRÁCTICA,* MÉXICO, THOMSON, 2001, 482 PP.
10. RAYA, JOSÉ LUIS*, TCP/IP EN WINDOWS NT SERVER,* MÉXICO, ALFA OMEGA-RAMA, 2002.
11. RAYA, JOSÉ LUIS, *REDES LOCALES Y TCP/IP,* ESPAÑA, ALFA OMEGA-RAMA, 2002.
12. STALLINGS, WILLIAM, *COMUNICACIÓN Y REDES DE COMPUTADORAS*, 6ª. EDICIÓN, MÉXICO, PRENTICE HALL, 2000, 840 PP.
13. TANNENBAUM, ANDREW S., *REDES DE COMPUTADORAS,* 3A. EDICIÓN, MÉXICO, PRENTICE HALL HISPANOAMERICANA, 1997, 784 PP.

SITIOS EN INTERNET

- http://es.wikipedia.org/wiki/Portada, La enciclopedia libre. 11/Dic/05, Wikipedia.
- http://moncayo.unizar.es/ccuz/proced.nsf/0/512e3a141f024ee0c125690600475d5f?OpenDocument, Generalidades tarjeta de red. 11/Dic/05, Unizar.
- http://www.ericsson.com.mx/wireless/products/mobsys/tdma/bluetooth_descripcion.shtml, Productos con ciertas especificaciones para avanzados servicios digitales e inalambricos,11/Dic/05, Ericsson.
- http://www.geocities.com/CapeCanaveral/2566/seguri/sie7.htm, Los servicios de seguridad, 11/Dic/05, Geocities.
- http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf, manual de seguridad, 11/Dic/05.
- http://www.hardings.cl/docencia/cc51c/apuntes/capa_red.pdf, comunicación de datos, 12/Dic/05

- http://www.htmlweb.net/redes/subredes/subredes_2.html, Enrutamiento en subredes por Luciano Moreno, 17/Ene/06, HTMLWEB diseño web, programación
- http://www.info-ab.uclm.es/descargas/thecnicalreports/ DIAB-01-02-16/diab-01-02-16.pdf, University of Castilla, 18/·Enero/06
- http://www.microsoft.com/latam/technet/articulos/windows2k/pimsm2/default.asp , Protocolo de enrutamiento de multidifusión,18/Enero/06, Microsoft.
- http://sipan.inictel.gob.pe/users/hherrera/defredes.htm, Definición de redes, 18/Enero/06.
- http://www.umsanet.edu.bo/docentes/rgallardo/publicaciones/LA%20IMPORTANCIA%20DE%20LA%20SEGURIDAD%20EN%20REDES.PDF, La importancia de la seguridad en redes, 18/Enero/06, Lic. Ramiro Gallardo Portanda.
- http://www.ldc.usb.ve/~poc/Seguridad/protocolos.pdf, Protocolos de seguridad, 18/Enero/06.