Unidad I: Direccionamiento y enrutamiento IP

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 realizado 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.

1.1 Direccionamiento IP y subredes:
Máscaras de longitud fija y variable

- Identifican unívocamente un punto de acceso (interfaz) a la red. Un router o un host multi-homed tienen varias.
- Tienen un significado global en la Internet.
- Son asignadas por una autoridad central: InterNIC (Internet Network
- Information Center).
- Son números de 32 bits, expresados en notación decimal con puntos, byte a byte (p.ej. 123.3.45.77).
- Para facilidad de los usuarios, se define un mapping estático de las direcciones IP con nombres “más legibles” para las personas (DNS - Domain Name Server).

Una dirección IP es independiente de las direcciones físicas de subred

- Esquema jerárquico, constan de una parte que indica de qué red física se trata, y otra que indica la interface o punto de conexión a la red (host).

- En 1984, se agrega un tercer elemento en la jerarquía para lograr mayor flexibilidad (subnets).
- Los campos que componen la dirección son de longitudes fijas predeterminadas; actualmente se elimina esta restricción (classless addressing).
- El componente RED de la dirección IP se utiliza para ubicar la red física de destino (ruteo) y el componente HOST se utiliza para identificar la interfaz dentro de esa red física
- Las direcciones IP son identificadores en una red virtual; en última instancia deben ser mapeadas a direcciones físicas de las distintas subredes (X.25,
- Ethernet, etc.). Este proceso se denomina resolución de direcciones.
- Esquema jerárquico, constan de una parte que indica de qué red física se trata, y otra que indica la interface o punto de conexión a la red (host).
- En 1984 se agrega un tercer elemento en la jerarquía para lograr.

Mascaras de subred de tamaño variable

Las máscaras de subred de tamaño variable (variable length subnet mask, VLSM) representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP (1987) y otras como la división en subredes (1985), el enrutamiento de interdominio CIDR (1993), NAT y las direcciones ip privadas. Otra de las funciones de VLSM es descentralizar las redes y de esta forma conseguir redes más seguras y jerárquicas.

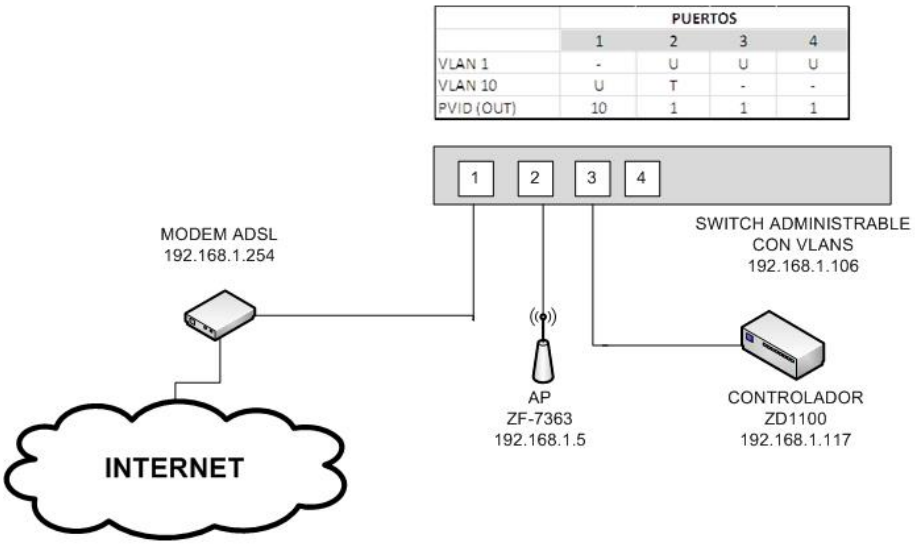
1.2 Segmentación

Tráfico, Niveles de Seguridad

En prácticamente todas las empresas y organizaciones es necesario ofrecer acceso a Internet para visitantes o invitados. Aunque es posible simplemente extender crear una WLAN (red inalámbrica) independiente para controlar el acceso, no es una buena práctica en términos de seguridad ya que aunque se

logre aislar el tráfico de esta WLAN, forzosamente tiene que salir a través del ruteador principal y consumir recursos y/o licencias del mismo.

La mejor solución a esta necesidad es utilizar VLANs (Virtual Local Area Network) para separar el tráfico completamente de los invitados y darles su propia salida a Internet. A continuación vemos el diagrama correspondiente:



No se requieren conocimientos avanzados de redes sino Esta configuración no está limitada a redes para invitados sino se puede utilizar cada vez que se desee aislar el tráfico de una red inalámbrica de las demás dentro de la red corporativa.

Las ventajas que nos ofrece esta solución, en orden de importancia son:

a) Mayor seguridad.- el tráfico de cada red inalámbrica viaja en forma aislada a través de la red LAN corporativa

b) Menor congestión.- debido a que las VLANs separan dominios de broadcast,

c) Mayor eficiencia.- los usuarios de cada red solo tendrán acceso a los dispositivos que requieren, consumiendo menos ancho de banda, licencias y ciclos de procesamiento de los demás dispositivos en la red.

1.3 Modos de conmutación de capa 2

Store-and-forward switch, cut-through switch, fragment-free switch

- ✓ *Store-and-Forward (almacenamiento y retransmisión)*

Los switches Store-and-Forward guardan cada trama en un buffer antes del intercambio de información hacia el puerto de salida. Mientras la trama está en el buffer, el switch calcula el CRC y mide el tamaño de la misma. Si el CRC falla, o el tamaño es muy pequeño o muy grande (un cuadro Ethernet tiene entre 64 bytes y 1518 bytes) la trama es descartada. Si todo se encuentra en orden es encaminada hacia el puerto de salida.

Este método asegura operaciones sin error y aumenta la confianza de la red. Pero el tiempo utilizado para guardar y chequear cada trama añade un tiempo de demora importante al procesamiento de las mismas. La demora o (delay) total es proporcional al tamaño de las tramas: cuanto mayor es la trama, mayor será la demora.

- ✓ *Cut-Through (cortar a través)*

Los Switches Cut-Through fueron diseñados para reducir esta latencia. Esos switches minimizan el delay leyendo sólo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente la encaminan.

El problema de este tipo de switch es que no detecta tramas corruptas causadas por colisiones (conocidos como runts), ni errores de CRC. Cuanto mayor sea el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar tramas corruptas.

Existe un segundo tipo de switch cut-through, los denominados fragment free, fue proyectado para eliminar este problema. El switch siempre lee los primeros 64 bytes de cada trama, asegurando que tenga por lo menos el tamaño mínimo, y evitando el encaminamiento de runts por la red.

- ✓ *Adaptative Cut-Through*

Los switches que procesan tramas en el modo adaptativo soportan tanto store-and-forward como cut-through. Cualquiera de los modos puede ser activado por el administrador de la red, o el switch puede ser lo bastante inteligente como para escoger entre los dos métodos, basado en el número de tramas con error que pasan por los puertos.

Cuando el número de tramas corruptas alcanza un cierto nivel, el switch puede cambiar del modo cut-through a store-and-forward, volviendo al modo anterior cuando la red se normalice.

Los switches cut-through son más utilizados en pequeños grupos de trabajo y pequeños departamentos. En esas aplicaciones es necesario un buen volumen de trabajo o throughput, ya que los errores potenciales de red quedan en el nivel del segmento, sin impactar la red corporativa.

Los switches store-and-forward son utilizados en redes corporativas, donde es necesario un control de errores.

- ✓ *Ethernet Switching*

En la década de 1980, cuando las empresas comenzaron a sufrir una disminución del rendimiento en sus redes, se procuraron puentes Ethernet (transparente o aprendizaje) para limitar los dominios de colisión.

En la década de 1990, los avances en las tecnologías de circuitos integrados permiten vendedores puente para mover la capa 2 de la decisión de envío Complex Instruction Set Computing (CISC) y procesadores de computación conjunto reducido de instrucciones (RISC) para circuitos integrados de aplicación específica (ASIC) y compuertas programables en campo matrices (FPGAs), reduciendo así el tiempo de manipulación de paquetes dentro del puente (es decir, la latencia) a decenas de microsegundos, así permitiendo que el puente de

manejar muchos más puertos sin una penalización de rendimiento. El término “switch Ethernet” se hizo popular.

El primer método de reenvío de paquetes de datos en la capa 2 se conoce como “store-and-forward cambio” para distinguirlo de un término acuñado en la década de 1990 por un corte a través del método de envío de paquetes.

Capa 2 Reenvío

Tanto store-and-forward y cortar a través de conmutadores de nivel 2 basan sus decisiones de envío en la dirección MAC de destino de los paquetes de datos. También aprenden las direcciones MAC mientras examinan los campos MAC de origen (SMAC) de paquetes como estaciones se comunican con otros nodos de la red.

Cuando un conmutador Ethernet de capa 2 inicia la decisión de reenvío, la serie de pasos que se somete a un cambio para determinar si se debe avanzar o descartar un paquete es lo que diferencia a la metodología de corte a través de su contraparte store-and-forward.

Mientras que un interruptor de store-and-forward realiza una decisión de envío de un paquete de datos después de haber recibido toda la estructura y comprobar su integridad, un interruptor de corte a través involucra en el proceso de expedición pronto, previo examen de la dirección MAC de destino (DMAC) de una trama entrante.

En teoría, un interruptor de corte a través de sólo recibe y examina los primeros 6 bytes de un marco, que lleva la dirección de DMAC. Sin embargo, por una serie de razones, como se muestra en este documento, de corte a través de interruptores de esperar hasta que se hayan evaluado un poco más bytes de la trama antes de decidir si enviar o descartar el paquete.

MÉTODOS DE SWITCHING

Otra gran diferencia entre bridges y switches es el método que se usa para reenviar frames.

Los bridges solo soportan un método, mientras los switches soportan tres.

Los métodos son los siguientes:

- Store and forward
- Cut-through
- Fragment free

STORE AND FORWARD

Este método es el más básico. El frame llega al switch, este lo lee completamente, lo almacena en el buffer, calcula el CRC, verifica que sea correcto y lo reenvía al puerto adecuado si es correcto. Si no es correcto, lo elimina. El switch 1900 soporta este sistema. Este es el único sistema que soporta el switch 2950.↥

CUT THROUGH

Este sistema es mucho más rápido. En cuanto el frame llega al switch (los bridges no usan este sistema), el switch lee la cabecera del frame. Obtiene de este los 8 bytes de preámbulo y la dirección MAC con 6 bytes más.

En cuanto obtiene esta información, reenvía rápidamente por el puerto adecuado.

LA desventaja de este sistema es que no provee detección de errores y puede enviar frames erróneos.

Existen algunos fabricantes que optan por un método intermedio. Se envían datos hasta que se repiten muchos errores. Entonces e cambia al método Store Forward. Cuando el número de frames erróneos baja, se vuelve al sistema Cut forward. ↥

El switch 1900 soporta este sistema, pero el 2950 no, aunque éste retransmite muchos más rápido que el 1900.

FRAGMENT FREE

Este es el sistema por defecto en los switches 1900, pero el 2950 no soporta este sistema, aunque éste retransmite muchos más rápido que el 1900.

Este método e s la mejora del Cut forward, con la única diferencia de que no lee únicamente los 14 bytes de la cabecera, sino que lee los primeros 64(mínimo tamaño para un frame Ethernet).

De esta manera reduce los frames erróneos de menos de 64 bytes.

Igualmente, este método puede retransmitir frames con CRC erróneo. Es por eso, que algunos fabricantes tienen métodos dinámicos, que saltan de método según los errores que haya. Si hay muchos errores, se escoge el sistema Store Forward. Si los errores descienden, se vuelve al método Fragment free.

1.3 Tecnologías de conmutación
LAN (VLAN, VTP), WAN (ATM, MPLS)

VLAN

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

En las redes de computadoras , una sola red de capa-2 puede ser dividido para crear múltiples dominios de difusión, que están mutuamente aislados por lo que los paquetes sólo pueden pasar entre ellos a través de uno o más enrutadores ; tal dominio se refiere como una sola red de área local virtual , Virtual LAN o VLAN.

Las VLAN también pueden ayudar a crear múltiples capas 3 redes en la misma capa 2 del conmutador. Por ejemplo, si el DHCP servidor está conectado a un interruptor que le servirá cualquier host que el interruptor que está configurado para obtener su dirección IP desde un servidor DHCP. Mediante el uso de VLANs se puede dividir fácilmente a la red de modo que algunos hosts no utilizan ese servidor DHCP y obtendrá las direcciones locales de vínculo , o de obtener una dirección de un servidor DHCP diferente. Los anfitriones también pueden utilizar un DNS del servidor si un servidor DHCP no está disponible.

Mediante el uso de VLAN, se puede controlar los patrones de tráfico y reaccionar rápidamente a las deslocalizaciones. VLAN proporcionan la flexibilidad necesaria para adaptarse a los cambios en los requisitos de red y permitir una administración simplificada.

Clasificación

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

- ✓ VLAN de nivel 2 por direcciones MAC. Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo.

- ✓ VLAN de nivel 2 por tipo de protocolo. La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC.

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

VTP

En los dispositivos Cisco, VTP (VLAN trunking protocol) se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de VLANs en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un dominio de administración VTP. Un dominio VTP para una red es un conjunto contiguo de switches unidos con enlaces trunk que tienen el mismo nombre de dominio VTP.

VTP también permite «podar» (función VTP prunning), lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces trunk.

ATM

El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

MPLS

Multi Protocol Label Switching , está reemplazando rápidamente frame relay y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.

1.4 Enrutamiento.

Estático, Dinámico (vector-distancia, estado de enlace)

Protocolo de Enrutamiento. 1.1. Definición de un Protocolo de Enrutamiento. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento usando las tablas de enrutamiento con la elección de los mejores caminos que realiza el protocolo para poder dirigir o en rutar los paquetes hacia diferentes redes. El propósito de un protocolo de enrutamiento incluye: Descubrir redes remotas. Mantener la información de enrutamiento actualizada. Escoger el mejor camino hacia las redes de destino. Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible. Su función principal es facilitar el intercambio de información, esto permite compartir información de redes remotas y agregarla automáticamente a la tabla de enrutamiento.

Los componentes de un protocolo de enrutamiento son: Estructuras de datos – tablas o bases de datos que se guardan en la memoria RAM Algoritmos – Conjunto de pasos a seguir para completar una tarea Mensajes de protocolo – Utilizado por los routers para intercambiar información, descubrir routers u otras tareas.

Enrutamiento estático

Todos ya sabemos lo que es enrutamiento, hemos visto los diferentes protocolos de enrutamiento como RIP en sus 2 versiones, EIGRP y OSPF. Los tres anteriores son protocolos que configuran el enrutamiento dinámicamente en los routers.

Rutas estaticas

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas son definidas manualmente por el administrador para que el router aprenda sobre una red remota.

Un administrador debe actualizar manualmente la entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización.

Las rutas estáticas necesitan pocos recursos del sistema, es recomendable utilizarlas cuando nuestra red esté compuesta por unos cuantos routers o que la red se conecte a internet solamente a través de un único ISP.

Ventajas del enrutamiento estático

- Poco uso del CPU, ya que no requiere ejecutar cálculos y algoritmos ante cambios en la red.
- Fácil de comprender y mantener en redes pequeñas.
- Fácil de configurar.
- Se usa para enrutamiento desde y hacia redes de conexión única.
- Requiere de menos comandos para la solución de problemas.

Razones para utilizar el enrutamiento estático

Si solamente existe una sola ruta no hay necesidad de utlizar protocolos de enrutamiento, ejemplo en redes stub.

Desventajas del enrutamiento estático

- Requiere de un configuración y mantenimiento constante por parte del administrador.
- Propenso a errores cuando se aplica en redes extensas.
- No es adecuado para redes en crecimiento rápido.
- Requiere de un conocimiento amplio de toda la red para su implementación.
- No puede aprender dinámicamente los cambios en la topología de la red.

Enrutamiento dinámico

Es un protocolo de enrutamiento para facilitar el intercambio de información de enrutamiento, es decir Con un protocolo de enrutamiento dinámico, el administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS, en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos, por lo tanto cada router conoce la red gracias a las publicaciones de las otras redes que recibe de otros routers.

- **Protocolos de enrutamiento dinámico más usados.**

RIP (Routing Information Protocol) un protocolo de enrutamiento interior por vector de distancia

IGRP (Interior Gateway Routing Protocol) el enrutamiento interior por vector de distancia desarrollado por Cisco (en desuso desde 12.2 IOS y versiones posteriores).

EIGRP (Enhanced Interior Gateway Routing Protocol) el protocolo avanzado de enrutamiento interior por vector de distancia desarrollado por Cisco.

OSPF (Open Shortest Path First): un protocolo de enrutamiento interior de estado de enlace IS-IS (Intermediate System-to-Intermediate System) un protocolo de enrutamiento interior de estado de enlace.

BGP (Border Gateway Protocol) un protocolo de enrutamiento exterior de vector de ruta.