CLASE 13 - 21

VLAN:

- cada dominio de broadcast será una VLAN, creando una VLAN se crea un nuevo dominio de broadcast.
- se asigna cada puerto del switch.
  VLAN001: Fa0/1 y Fa0/2
  VLAN002: Fa0/3 y Fa0/4.

- Beneficios: seguridad, reducción costos y mejor desempeño.
- VLAN: es una LAN virtual, división lógica de la red de capa 2, se pueden crear multiples divisiones y estas coexistir. Cada VLAN es un dominio de broadcast y generalmente con su propia IP. Están aislados entre sí y los paquetes solo pasan entre ellas a través de un router.

VLAN nativa y 802.1q tagging:

- tagging se utiliza para transmitir correctamente varias tramas de VLAN a través de un enlace troncal para esto el switch etiquetará la trama para identificar la VLAN a la que pertenece, usando el protocolo IEEE.802.1q, este define la estructura del encabezado de etiquetado agregado al marco. Luego el switch agregará una etiqueta de VLAN a las tramas antes de colocarlas en el enlace troncal y eliminará las etiquetas antes de re-enviar las tramas a través de un puerto no troncal, etiquetada correctamente, la trama puede atravesar cualquier numero de switches a traves de enlaces troncales y aún pueden reenviarse dentro de la VLAN correcta en el destino.

Routing entre VLANS:

- Router por puerto: cada puerto del switch en modo acceso conectado a cada puerta del router, (el router tiene en cada puerto una subred o VLAN).
- Router on a stick: consiste en crear una subinterfaz en una sola interfaz física de un router. Una sola interfaz para enrutar los paquetes de varias VLAN que viajan a través del puerto trunk de un switch conectado a esa interface.

Internetworking:

¿Se puede hacer crecer una red con switches?

→ **Problemas con el uso de switch:**

- es necesario evitar los bucles con STP
- Las tablas CAM de cada switch deberan contener las direcciones MAC de todos los equipos en la red. no escala.
- Las direcciones MAC no permiten organizar los hosts por zona. direccionamiento NO jerarquico.

→ **conmutación de paquetes:** esto quiere decir que los paquetes se almacenan completamente antes de re-enviarlos, la direccion de cual es el sgte router es basada en la direccion IP de destino.

Protocolo IPV4:

- reto de paquetes a través de la red.
- realiza el mejor esfuerzo para la distribucion de paquetes., pueden ser entregados fuera de orden, recuperar paquetes perdidos y la re-secuenciación se encargan capas superiores.
- Protocolo ~~es~~ orientado a no conexion, fragmenta paquetes de ser necesario.
- **fragmentacion:** un router fragmenta un datagrama si la longitud es demasiado grande para la siguiente red. Cada fragmento necesita un identificador unico para el datagrama mas un identificador para la posicion dentro del datagrama.
  En el campo posición del fragmento proporciona la posicion inicial del fragmento dentro del datagrama en incremento de 8 bytes (campo de 13 bits), el campo de longitud de encabezado proporciona la longitud total en bytes (campo de 16 bits).

Direccionamiento IPV4:

→ tiene un largo de 32 bits.

→ se escribe en notacion decimal de cuatro puntos representada por 4 octetos de 4 bytes.

Ej: 172.16.254.1 (cuatro puntos)
2.886.794.753 (decimal)
0xAC10FE01 (hexadecimal).

172.16.254.1

10101100 00010000 11111110 00000001

8 bits.

32 bits (4 bytes).

→ poseen estructura jerarquica.
→ La direccion puede identificar a un host o una subred o red.
→ Clases de direccionamiento IPV4:
• Cada uno de los cuatro octetos puede tener numeros decimales desde el 0 al 256.
• direcciones clase A:
→ primer octeto comienza siempre con un 0 binario, y es el ID de la red y los otros tres octetos restantes son los ID del host.
• direcciones clase B:
→ primer octeto comienza siempre con un 10 binario, y el primer y segundo octeto son el ID de red y los dos restantes son los ID de host.
• direcciones clase C:
→ primer octeto comienza siempre con un 110 binario, y el primer, segundo y tercero octeto son el ID de red y el cuarto octeto es el ID de host.

Direcciones Privadas y Publicas:
• Direcciones IP publicas: son visibles a todo internet. un nodo con IP publica es accesible desde cualquier otro nodo conectado a internet.
• Direcciones IP privadas: son visibles unicamente por otros nodos de su propia red o de otras redes privadas interconectadas por router.

Mascara de red:
• conversion binario a decimal:
BINARIO = 1101 → $2^3 \cdot 1 + 2^2 \cdot 1 + 2^1 \cdot 0 + 2^0 \cdot 1 = 8 + 4 + 0 + 1 = 13$ decimal.
• conversion decimal a binario:
decimal: 124 → binario: 1111100
124/2 = 62 → 0
62/2 = 31 → 0
31/2 = 15 → 1
15/2 = 7 → 1
7/2 = 3 → 1
3/2 = 1 → 1
1/2 = 0 → 1

- Los routers al igual que los switch tienen tablas con la ubicacion del host destino, pero a diferencia de los switch, el router almacena la direccion de subred de cada destino. Por lo tanto, cuando un router recibe un paquete, inspecciona la direccion IP de destino y revisa a que subred pertenece y busca en su tabla por cual interfaz esta conectada la subred de destino.

Ej: ¿Como sabe el router a que subred de destino pertenece una direccion IP?

- mascara de subred
- IP origen: 200.1.20.45 , IP destino: 150.15.8.99
- cuando el paquete llega al router B, este analiza su tabla de ruteo

entonces teniendo.

destino: 150.15.8.99.
mascara: 255.255.255.0.

Pasando a binario

destino: 10010110.00001111.00001000.01100011
mascara: 11111111.11111111.11111111.00000000
operacion AND. 0-0=0 / 0-1=0 / 1-0=0 / 1-1=1

10010110.00001111.00001000.00000000

red destino: 150.15.8.0

Ej: ¿Calcule la subred a la que pertenece 215.45.87.12/20?

Primero: direccion IP: 215.45.87.12
mascara: /20 → 255.255.240.0.

Luego pasamos ambos a binarios.

direccion: 11010111.00101101.01010111.00001100
mascara: 11111111.11111111.11110000.00000000

Para calcular la direccion de red realizamos un AND entre ambas. obteniendo como resultado.

= 11010111.00101101.01010000.00000000

subred = 215.45.80.0

Técnicas de división de red (subnetting):

→ Nace de los siguientes problemas, imposibilidad de conmutar paquetes entre routers basado en la dirección IP de destino; el tamaño de una red puede ser demasiado grande para formar un solo dominio de broadcast. (2)

Problema 1:

conmutar paquetes a través de los routers a través de routers usando la dirección IP de destino es ineficiente, ya que no se puede tener una tabla de ruteo donde estén las direcciones IP de todos los host del mundo, para esto se necesita realizar una agrupación de los host basado en las direcciones IP de cada uno de ellos, esta agrupación está basada en un concepto de subred:

Subred: grupo de host que comparten el mismo dominio de broadcast, la misma dirección de subred, el mismo default gateway, están conectados por uno o más switch, pero dos host en la misma subred, no pueden estar separados por un router.

Lógicamente, son todas las direcciones IP que comparten el mismo identificador de red.

Problema 2:

La división por clase permite agrupar las direcciones IP en subredes y solucionó el problema 1. El problema ahora es que cada subred, al menos la clase A y B, son demasiado grandes para ser administradas, para solucionar esto, se divide una red en redes más pequeñas.

división por mascara de red fija:

Por obtener n subredes se deben reservar $(\log_2(n)$ de la porción de host ID.

Ej: si se tiene la dirección clase C 201.50.41.0, se solicita que esta red sea dividida en 4 subredes.

$(\log_2(4)$ es igual a 2 bits. Por lo tanto, se deben tomar 2 bits de la porción de hosts. Por ende, la parte de host, ya no tiene 8 sino que 6 bits.

La capacidad de cada subred es de 62 hosts:

$$n\text{subredes} = 2^{\text{bits de subred}} = 2^2 = \text{subredes } 4$$

$$n\text{ host por subred} = 2^{\text{bits de subred}} - 2 = 2^6 - 2 = 62 \text{ host por subred.}$$

división por mascara de red variable: VLSM:

La longitud de la mascara de subred varía según la cantidad de bits que se toman prestado para una subred específica, es decir, permite dividir un espacio de red en partes desiguales.

- Las formulas para calcular la cantidad de host por subred y la cantidad de subredes que se crean son validos para VLSM. La diferencia es que la division de subredes se puede hacer varias veces.

Ej: se tienen 5 clientes, 3 tienen 60 hosts y 2 tienen 25 hosts.
C1: 60 hosts ; C2: 60 hosts ; C3: 60 hosts ; C4 = 25 hosts ; C5: 25 hosts.
usando C: 201.50.41.0/24 ¿Como dividiria la red?
R: La C: 201.50.41.0/24 tiene 256 direcciones disp / 254 utilizables para host.
Por ende para 60 hosts, necesitamos al menos 64 direcciones / 64 utiles, por ende usamos la mascara /26. → 255.255.255.192
Para 25 host, usamos mascara /27 que tiene 32 direcciones / 30 disponibles → 255.255.255.224.
Luego se asignan los rangos de direcciones para cada cliente.

- Cliente 1: 60 hosts.
  subred: 201.50.41.0/26 / tamaño necesario: 64 direcciones.
  rango IPs: 201.50.41.0 - 201.50.41.63 → 64 direcciones, una menos que la normal
  (restar uno al mayor)
  host utilizables: 201.50.41.1 a 201.50.41.62.
  (sumar 1 al 1°)
  (marca en la sgte direccion del cliente 1)

- Cliente 2: 60 host. (aumentamos en 64 por las direcciones)
  subred: 201.50.41.64 | 26.
  rango IPs: 201.50.41.64 - 201.50.41.127 → 63 direcciones, una menos que la normal.
  host utilizables: 201.50.41.65 - 201.50.41.126
  (marca en la sgte direccion del cliente 2.)

- Cliente 3: 60 host.
  subred: 201.50.41.128/26.
  rango IPs: 201.50.41.128 - 201.50.41.191 → 63 direcciones.
  host utilizables: 201.50.41.129 - 201.50.41.190. → +1 / -1.

- Cliente 4: 25 host (parte de la siguiente.) } 32 direcciones / 27.
  subred: 201.50.41.192 /27.
  rango IP: 201.50.41.192 - 201.50.41.223 → 31 direcciones
  host utilizables: 201.50.41.193 - 201.50.41.222

- Cliente 5: (parte del siguiente.)
  subred: 201.50.41.224/27
  rango IP: 201.50.41.224 - 201.50.41.255 / utilizables: 201.50.41.225 - 201.50.41.254

- Para calcular la dirección broadcast.
  → conocer la dirección de red y la máscara.
  (dirección de red, se obtiene aplicando un AND entre la IP de unitio y la máscara de subred)
  → Para calcular la dirección de broadcast aplica un OR entre la dirección de red y el complemento de la mascadra de subred.

  Ej: red: 201.90.41.0/26
  máscara: /26 → 255.255.255.192
  ↳ binario → 11111111.11111111.11111111.11000000
  red (binaria) → 11001001.00110010.00101001.00000000
  complemento máscara (invertir los bits / cambiar 1 a 0 y 0 a 1)
  complemento máscara: 00000000.00000000.00000000.00111111
  Por ende se hace un OR
  OR → 11001001.00110010.00101001.00000000
  00000000.00000000.00000000.00111111
  11001001.00110010.00101001.00111111
  resultado: 201.90.41.63.

PROTOCOLO DHCP: protocolo de configuración dinamica de host y funcionamiento
→ Protocolo que proporciona direccionamiento IP automatico y otra información a los clientes: dirección IP, mascara de subred, dirección de puerta de enlace predeterminada y dirección del servidor DNS
→ Utiliza 3 metodos:
1. Asignación manual: asignación una dirección IP a una maquina determinada.
2. Asignación automatica: asigna automaticamente una dirección IPV4 estatica de forma permanente a un dispositivo.
3. Asignacion dinamica: asigna una dirección IPV4 de un grupo de direcciones durante un periodo de tiempo limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.

NAT: Network Address Translation (NAT)

→ Permite al dispositivo con una dirección IPV4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet.

→ Terminología:

- red interna: es el conjunto de redes sujetas a traducción.
- red externa: se refiere a todas las otras redes.
- NAT incluye 4 tipos de direccionamiento: local interna, global interna, local externa, global externa.
  - → dirección interna: dirección del dispositivo que se traduce por medio de NAT.
  - → " externa: dirección del dispositivo de destino.
  - → " local: cualquier dirección que aparece en la porción interna de la red.
  - → " global: cualquier dirección que aparece en la porción externa de la red.

→ Tipos de NAT:

- NAT estática: consiste en una asignación uno a uno entre direcciones locales y globales. La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.
- NAT dinámico: utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita el acceso a una red externa, se le asigna una dirección IPV4 pública disponible del conjunto.
- PAT (Port Address Translation): asigna varias direcciones IPV4 privadas a una dirección IPV4 pública o a algunas direcciones

Beneficios NAT:

→ conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets

→ aumenta la flexibilidad de las conexiones a la red pública.

→ proporciona seguridad a la red.

Desventaja NAT:

→ deteriora el rendimiento.

→ pérdida del direccionamiento de extremo a extremo.

→ impedimento de inicio de sesiones TCP en la red externa.

Enrutamiento (Routing):

- En capa 2, la decisión para entregar un frame, esta basada exclusivamente en la dirección MAC de destino.
- En capa 3, el puerto de destino o el siguiente router a quien enviar el mensaje esta basado en la red a la que pertenece el destino.

→ corresponde a la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad, es efectuado por los routers.

→ 2 formas de enrutamiento.

- forma estatica: las tablas son configuradas por el administrador de red, ideal para redes mas pequeñas. Encaminamiento asociado a un punto unico de salida definido y no hay conocimiento de otras redes remotas.
- forma dinamica: basado en un protocolo de ruteo encargado de completar las tablas de ruteo de los routers. La selección de la ruta esta basada en la subred de destino. todos los protocolos de enrutamiento dinamico cumplen una serie de pasos relativamente similares para poder completar, mantener y modificar las tablas de rutas en los routers.
  1. cuando las tablas de ruteo estan vacias, los routers comienzan a enviar sus redes.
  2. cuando todos ya tienen sus tablas con la info de la red, se dice que el protocolo de ruteo ha convergido.
  3. Luego de converger, comienza el envio y recepción de mensaje de mantenimiento y modificacion frente a algún cambio de topología.
  4. Los router deben comunicarse con sus pares utilizando el mismo protocolo de ruteo.

Protocolos enrutamiento dinamico:

- Interior Gateway Protocols (IGP):
  RIP: Routing Information Protocol.
  IGRP: Interior Gateway Routing Protocol.
  OSPF: Open Shortest Path First
- Exterior Gateway Protocols (EGP):
  BGP: Border Gateway Protocol.

Enrutamiento por vector de distancia:

- utiliza el algoritmo de Bellman-Ford para calcular rutas.
- El protocolo requiere que un router informe a sus vecinos de los cambios en la topología periodicamente y en algunos casos cuando se detecta un cambio en la topología de red.
- se basa en calcular la dirección y la distancia hasta cualquier enlace en la red.

RIP: Routing Information Protocol:

- su algoritmo de encaminamiento esta basado en el vector de distancia, ya que calcula la metrica o ruta mas corta posible hasta el destino a partir del numero de "saltos" o equipos intermedios que los paquetes IP deben atravesar.
- max saltos = 15. si llega a 16 es una ruta inalcanzable.
- modo de operación:

cuando RIP inicia, envia un mensaje a cada uno de sus vecinos pidiendo una copia de la tabla de encaminamiento del vecino. Los routers vecinos devuelven una copia de sus tablas de encaminamiento. Cuando RIP esta activo envia cada 30s su talda de encaminamiento a todos los vecinos por broadcast, si RIP descubre que una metrica ha cambiado, la difunde por broadcast a los demas routers. cuando recibe el mensaje RIP lo comobora y la tabla local se actualiza.

- tipos de mensaje:

→ peticion: enviados por algún router recientemente iniciado que solicita información de los routers vecinos.

→ respuesta. mensajes con la actualización de las tablas de encaminamiento

- temporizadores (Timers).

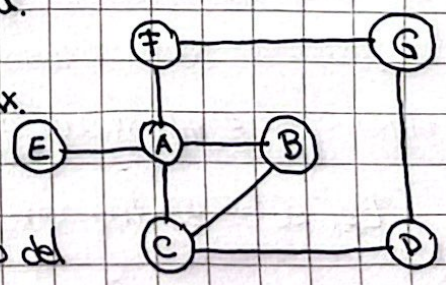
→ temporizadores periodicos: controla la publicacion de los mensajes de actualización regulares.

→ temporizadores de caducidad: establece cuanto tiempo puede estar una ruta en la tabla de ruteo sin ser actualizada

→ temporizador de colección de basura: controla el tiempo que pasa entre que una ruta es invalidada y el tiempo que pasa hasta que se elimina la entrada de la tabla de ruteo.

- Count-to-infinity (Problema).

¿Que ocurre si el link entre A y E falla? Cuenta infinita.



solución:

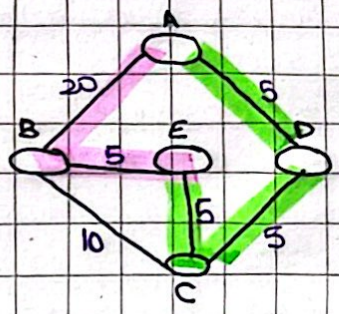
- Limitar el numero de saltos. RIP lo limita a 16 saltos max.
- split horizon: no se envian actualizaciones al vecino de cual las aprendieron.
- Poisoning Reverse, si se envia actualización al nodo del cual se aprendieron pero con valor INF.

- todas afectan al rendimiento y a la escalabilidad de la red.

Enrutamiento por estado de Enlace:

→ Dijkstra, permite encontrar la ruta mas corta entre 2 nodos de un grafo.
→ grafo compuesto por nodos y aristas.
→ La ruta mas corta no se refiere a la ruta con menos cantidad de saltos.
→ Para este caso, el graf estara compuesto por routers (nodos) y enlaces (aristas).
→ el protocolo de enrutamiento de enlace se encarga de darle un peso o costo a cada arista basado en parametros como ancho de banda, latencia, etc.
→ Ej: se quiere saber cual es la ruta mas corta entre router A y el router E.

R: Camino 1:
ABE = con costo 25.
Camino 2:
ADCE = con costo 15



→ Proceso de enrutamiento de enlace:

1. Cada R obtiene inf. de sus propios enlaces y sus propias redes conectadas directamente.
2. Cada R es responsable de saludar a sus vecinos en redes conectadas directamente.
3. Cada R crea un paquete Link-state (LSP) que incluye el estado de cada enlace directamente conectado.

Ej: R1; Red Ethernet 10.1.0.0/16, Costo: 2.
R1 → R2, red serial punto-a-punto, 10.2.0.0/16, costo 20. } LSP

4. Cada R satura a todos los vecinos con el LSP. Estos vecinos almacenan todos los LSP recibidos en una base de datos.
5. Cada R utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino.

→ Open Shortest Path First (OSPF)

- protocolo de enrutamiento de estado por enlace, tipo de protocolo de puerta de enlace interna (IGP), que fue diseñado para escalar y admitir redes mas extensas.
- utiliza Dijstra para encontrar la ruta mas corta entre nodos y utiliza como metrica el ancho de banda del enlace para encontrar la ruta mas corta enhe el origen y el destino.
- utiliza el paquete de saludo o el temporizador Keep-alive para mantener los estados de los routers adyacentes.
- usa el ancho de banda del enlace como el costo ⟹ $costo = \frac{10^8}{BW}$

- utiliza paquetes de estado de enlace (LSP) para establecer y mantener adyacencias de vecinos, así como para intercambiar actualizaciones de routing.
- Tablas OSPF:
  - → tablas vecinos: contiene los routers conectados directamente a diferentes interfaces de un enrutador.
  - → tabla topológica: contiene todas las rutas posibles a diferentes enrutadores en la red.
  - → tabla de ruteo: se usa para encontrar la mejor ruta posible a cualquier enrutador de la red.
- OSPF Multi-area: se utiliza para dividir redes OSPF grandes; un OSPF de diversas áreas se implementa con una jerarquía de área de dos capas.
  - → área de red troncal (de tránsito) y área común (no de red troncal).

Exterior Gateway Protocol: (EGP):

→ cada dominio es un dominio administrativo que opera con políticas uniformes de ruteo, independiente de otros dominios, por esto, se les llama Sistemas Autonomos (SA).

→ sistema autonomo: grupo de redes de direcciones IP que son gestionadas por uno o mas operadores de red que poseen una clara y unica política de ruteo, tienen un numero asociado que se usa como identificador en el intercambio de info de extremo a extremo
- se agrupan en tres categorías:
  1. AS stub: se conecta unicamente con un sistema autónomo
  2. AS de tránsito: se conecta con varios sistemas autónomos y además permite que se comuniquen entre ellos
  3. AS multihomed: se conecta con varios sistemas autonomos, pero no soporta el trafico de transito entre ellos.

BGP: Border Gateway Protocol:

→ protocolo de enrutamiento de internet, basado en el concepto de Path Vector.

→ los vecinos se llaman Peers, I BGP peers (dentro del mismo AS), eBGP (conectan con diferentes AS)

→ cuando los peers forman un vecindario, comparten su tabla de ruta completa.

→ BGP envía un open message para iniciar sesion con un peer, envia Keep-alive msg cada 60s para ver que esten arriba, envia update message para intercambiar info de rutas entre peers y puede mandar notification msg en caso de error fatal.