Informe - Switch

Scaravilli Sandro

6 de septiembre de 2024

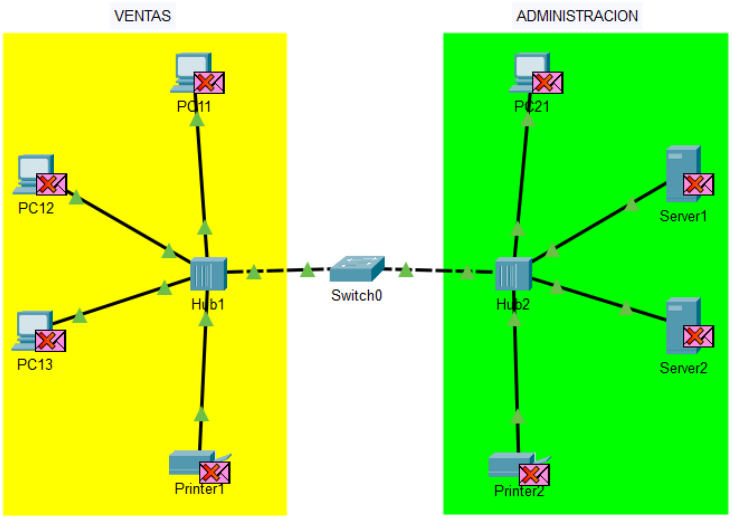
1. Switch

El **switch** es un dispositivo clave para la interconexión eficiente de dispositivos en una red local (LAN). Su función principal es recibir, procesar y reenviar datos entre los distintos nodos, optimizando el tráfico de red mediante la segmentación del ancho de banda. A diferencia de los hubs, que simplemente distribuyen la información a todos los dispositivos conectados, el switch opera de manera inteligente, enviando los datos solo al dispositivo de destino, utilizando la dirección MAC para identificar los receptores. Este comportamiento no solo mejora el rendimiento de la red, sino que también reduce colisiones y congestionamiento, garantizando una transmisión más rápida y confiable de la información.

2. Dispositivos Activos

2.1. Primer experimento

Como primer fase del escenario, se pudo comprobar que enviando dos PDU de las PCs a las Printers, agregandole un delay time a uno de los dos se producen colisiones ya que estos paquetes son enviados a todos los demas dispositivos. Sin embargo, luego de reintentar el envìo varias veces, termina siendo exitoso el envío.



2.2. Segundo experimento

En el segundo escenario, al intercambiar el hub por un switch, podemos observar que este dispositivo tiene la particularidad de que no envía la información a todos los dispositivos conectados, sino que la dirige específicamente al puerto correspondiente del destinatario. A diferencia del hub, el switch no transmite la información a todos los dispositivos en un mismo dominio de colisión, lo que ayuda a evitar colisiones.

Luego, al enviar un PDU de una PC a otra (ambas dentro del mismo dominio de difusión), buscamos generar una colisión para confirmar que el switch evita estas colisiones, ya que **segmenta** los dominios de colisión a nivel de puertos. En los switches, cada puerto opera en un dominio de colisión separado.

Finalmente, concluimos que al evitar el uso de hubs, reducimos significativamente la probabilidad de colisiones. En este caso particular, se pudo observar que el switch creó 8 dominios de colisión distintos, uno para cada puerto.

3. Protocolo ARP

El **Protocolo de Resolución de Direcciones** (ARP, por sus siglas en inglés) su propósito es permitir la comunicación dentro de redes locales que utilizan el protocolo IP. ARP se encarga de traducir las direcciones IP, que funcionan en la capa de red (Capa 3 del modelo OSI), a direcciones MAC (Media Access Control), que operan en la capa de enlace de datos (Capa 2). Este proceso es esencial para que los dispositivos en una red local puedan localizarse y comunicarse entre sí.

Cuando un dispositivo necesita enviar datos a otro dispositivo en la misma red, debe conocer su dirección MAC, ya que esta es utilizada para el direccionamiento físico dentro de la red. ARP facilita esta tarea solicitando la dirección MAC correspondiente a una dirección IP mediante mensajes ARP Request y ARP Reply. Sin este mecanismo, los dispositivos no podrían intercambiar datos en redes de área local de manera eficiente.

3.1. Practica

Los switches operan dentro de un único dominio de difusión, lo que significa que reenvían tramas de difusión a todos los dispositivos conectados a sus puertos. Cuando un dispositivo envía una trama de difusión, como una solicitud ARP, el switch reconoce que debe reenviar esta trama a todos los demás dispositivos en la red utilizando una dirección especial llamada **MAC de broadcast** (FF:FF:FF:FF:FF). De esta manera, el switch garantiza que el mensaje ARP llegue a todos los nodos dentro de ese dominio de difusión. Por lo tanto, el rol principal de los switches es gestionar el tráfico dentro de un dominio de difusión. En este escenario, podemos decir que existe un solo dominio de difusión controlado por el switch. Dentro del modo simulacion dentro de Simulation Panel editamos los filtros para que aparezcan solo la informacion de ARP.

Dispositivo	MAC Addres
PC11	0004.9AED.E15B
PC12	000D.BD96.B915
PC13	0010.114D.79D9
Printer1	0001.6394.A11E
PC21	0001.96DA.9132
Server1	00E0.F9A9.3157
Server2	0000.0C11.2106
Printer2	00D0.FFED.0B5A

A nivel Ethernet
Destination Address: FFFF.FFFF.FFFF (broadcast)
Source Address: 0004.9AED.E15B (PC11)
Type: 0x0806 (ARP)

A nivel ARP
Hardware Type: FFFF.FFFF.FFFF (broadcast)
Protocol Type: 0004.9AED.E15B (PC11)
Hardware Lenght: 0x06 bytes (MAC)
Protocol Lenght: 0x04 bytes (IP)
Opcode: 0x0001 (Request)
Source MAC: 0004.9AED.E15B (PC11)
Source IP: 192.168.1.11 (PC11)
Target MAC: 0000.0000.0000 (unknow)
Target IP: 192.168.1.12 (PC12)

Ventajas de las entradas ARP estáticas
Evitan el tráfico de difusión (broadcast): Elimina la necesidad de enviar paquetes ARP Request de difusión para obtener las direcciones MAC. Esto mejora la eficiencia al reducir el número de paquetes de broadcast en la red, especialmente en redes grandes.
Protección contra ataques ARP Spoofing: Al tener entradas estáticas ARP, se mitiga el riesgo de ataques de suplantación ARP, en los que un atacante envía respuestas ARP falsas para interceptar el tráfico.
Mejora en el rendimiento de la red: Menos tráfico innecesario significa que el ancho de banda puede ser utilizado para otros propósitos más importantes.

Desventajas de las entradas ARP estáticas
Gestión manual: Cada dirección IP y MAC debe ser introducida manualmente, lo que puede ser tedioso en redes grandes y propenso a errores humanos.
Falta de flexibilidad: Si un dispositivo cambia de dirección IP o MAC, las entradas estáticas se vuelven obsoletas y deben actualizarse manualmente, lo que genera mantenimiento adicional.
No es escalable: En redes grandes con muchos dispositivos, administrar las entradas ARP estáticas puede convertirse en un desafío logístico.

Comandos en linux
Agregar una entrada estática ARP
sudo arp -s [IP ADDRESS] [MAC ADDRESS]

Eliminar una entrada ARP
sudo arp -d [IP ADDRESS]

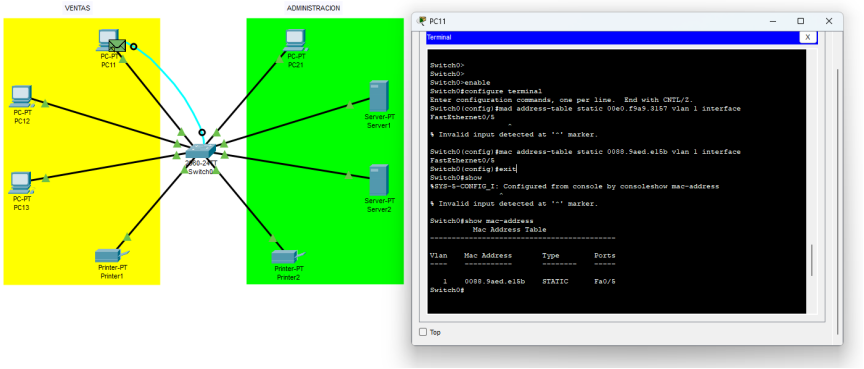
Comandos en Windows
Agregar una entrada estática ARP
netsh interface ipv4 add neighbors "[INTERFACE]"[IP ADDRESS] [MAC ADDRESS]

Eliminar una entrada ARP
netsh interface ipv4 delete neighbors "[INTERFACE]"[IP ADDRESS]

4. Switch learning

En resumen, **Switch Learning** es el proceso mediante el cual un switch construye su tabla MAC aprendiendo dinámicamente las direcciones de los dispositivos conectados. Los switchs aprende de los broadcast y generan una tabla llamada FIB con estos datos. El switch inspecciona la trama que recibe y extrae la dirección MAC de origen. Luego, almacena esta dirección MAC junto con el puerto donde fue recibida en una tabla llamada**FIB** (Forwarding Information Base).

A continuacion se muestra como se conecto el cable de consola de la PC 11 al Switch, luego se abrio la terminal y dentro se configuro manualmente el switch adiriendo la MAC addres del Server1.



Info extra: Cisco maneja 3 niveles de configuracion, en la RAM, en la Terminal y en la flash. Esto es por si cometo algun error grave asi puedo restaurar a previas configuraciones sin necesidad de tener que acceder fisicamente al dispositivo.

https://github.com/Sandrosca/LaTeX