CONCEPTOS DE SWITCHING

REDES II

Carlos Rojas Sánchez

Licenciatura en Informática

Universidad del Mar

Contenido

Introducción

¿Qué es Switching?

El Switching o conmutación es el proceso mediante el cual los dispositivos de red (como switches) reciben, procesan y reenvían tramas hacia el destino correcto dentro de una red local (LAN).

¿Qué es una trama?

Una trama es un bloque de datos estructurado que se envía a nivel de enlace de datos (Capa 2 del modelo OSI). Contiene información de control, direcciones MAC, y los datos reales (payload).

Estructura de una trama Ethernet típica

| Preámbulo | MAC destino | MAC origen | Tipo | Datos | CRC |

- El preámbulo tiene 8 bytes, su propósito es sincronizar la comunicación.
- Dirección MAC de destino: A quién va dirigida la trama.
- Dirección MAC de origen: De quién proviene la trama.
- Tipo/Longitud: Indica el protocolo de nivel superior (por ejemplo, IPv4).
- Datos: Información que se quiere transmitir (hasta 1500 bytes en Ethernet).
- CRC (FCS): Verifica si la trama tiene errores (checksum).

Preámbulo de una trama Ethernet

- Las redes Ethernet son asincrónicas, lo que significa que los dispositivos no comparten un reloj común.
- El preámbulo ayuda a que el receptor se sincronice con la señal del emisor.
- Si no hubiera preámbulo, el receptor podría leer datos mal alineados.

Comandos ping y tracert en Windows 11

- ping - Verifica si hay respuesta - Simple (1 destino)
- tracert - Muestra la ruta hasta el destino - Avanzada (varios nodos)

Ejemplo práctico

Cuando haces ping a otro equipo:

- Se crea un paquete IP con la solicitud ICMP.
- Este paquete se inserta dentro de una trama Ethernet.
- La trama se envía al switch, que la reenvía al equipo destino según su MAC.

Reenvío de tramas en redes

El reenvío de tramas es el proceso mediante el cual un switch o un dispositivo de capa 2 decide por qué puerto enviar una trama Ethernet recibida, con base en su dirección MAC de destino.

Tipos de reenvío según la dirección destino

Unicast Conocida Reenvía por puerto específico.

Unicast Desconocida Inunda por todos los puertos.

Broadcast Inunda por todos los puertos.

Multicast Inunda por puertos registrados (o todos).

Dispositivos clave

- Switch: Dispositivo de Capa 2 que segmenta la red y envía tramas basándose en direcciones MAC.
- Bridge: Predecesor del switch; también opera en Capa 2 pero con menos puertos y capacidad.
- Hub: Dispositivo antiguo que reenvía datos a todos los puertos (sin inteligencia).

Tabla de direcciones MAC (CAM)

- Los switches aprenden y almacenan las direcciones MAC en una tabla CAM.
- Esta tabla indica a qué puerto pertenece cada dirección MAC.
- Permite enviar tramas solo al puerto correspondiente → mayor eficiencia.

Tipos de Switching

- Store-and-Forward: Almacena toda la trama, verifica errores (CRC), luego la reenvía.
- Cut-Through: Lee solo la dirección MAC de destino y la reenvía de inmediato (menor latencia).
- Fragment-Free: Reenvía la trama después de leer los primeros 64 bytes (reduce colisiones).

VLANs (Redes LAN Virtuales)

- Permiten segmentar lógicamente la red, sin importar la ubicación física de los dispositivos.
- Un switch puede tener varias VLANs, aislando el tráfico entre ellas.

Trunking y 802.1Q

- Trunk: Enlace que transporta tráfico de múltiples VLANs entre switches.
- 802.1Q: Protocolo que etiqueta las tramas con información de VLAN.

STP (Spanning Tree Protocol)

- Previene bucles de red desactivando enlaces redundantes temporalmente.
- Determina automáticamente una topología libre de bucles.

PoE (Power over Ethernet)

- Tecnología que permite alimentar eléctricamente dispositivos como cámaras o teléfonos IP a través del cable de red.

Comandos

Comandos útiles en IOS (Cisco)

```
show mac address-table
# Muestra la tabla de direcciones MAC aprendidas por el switch
show vlan brief
# Lista todas las VLAN configuradas y sus puertos asociados
show interfaces status
# Muestra el estado de todos los puertos del switch
configure terminal
# Entra al modo de configuración global
interface fastEthernet0/1
# Entra a la configuración del puerto FastEthernet 0/1
switchport mode access
# Configura el puerto como acceso (no trunk)
switchport access vlan 10
# Asigna el puerto a la VLAN 10
```

Comandos útiles en el Command Prompt del PC

```
ipconfig
# Muestra la configuración IP del PC

ping 192.168.1.1
# Verifica conectividad con la puerta de enlace

tracert 192.168.1.20
# Muestra los saltos hasta el destino

arp -a
# Muestra la tabla ARP (IP ↔ MAC)

netstat -r
# Muestra la tabla de rutas del PC

nslookup www.google.com
# Realiza una consulta DNS (requiere servidor DNS configurado)
```

Práctica 1

Escenario

- PC1 (MAC A1) envía una trama a PC2 (MAC B2) a través de un switch 2960.
- El switch aprende que A1 está en el puerto `Fa0/1`.
- Si conoce B2 en `Fa0/3`, reenvía la trama solo a ese puerto.
- Si no conoce a B2, reenvía la trama a todos los puertos excepto el de entrada.

Topología

Configuración IP en PCs

```
PC1:
IP: 192.168.1.10
Máscara: 255.255.255.0

PC2:
IP: 192.168.1.20
Máscara: 255.255.255.0
```

Comandos en el Switch

```
Switch> enable
Switch# show mac address-table
```

Modo Simulación

1. Entra al modo Simulación.
2. Envía un `ping` de PC1 a PC2.
3. Observa el comportamiento:
    - Si el switch no conoce B2: flooding.
    - Si ya aprendió B2: reenvío directo a Fa0/3.

Dominios de Switching

¿Qué son los dominios de switching?

Los dominios de switching se refieren a los ámbitos lógicos o físicos dentro de una red donde ciertas reglas de tráfico se aplican. Los dos más importantes son:

- Dominio de Colisión (Collision Domain)
- Dominio de Broadcast

Dominio de Colisión (Collision Domain)

- Es el área de una red donde los dispositivos compiten por el mismo canal de comunicación. Si dos dispositivos transmiten al mismo tiempo, ocurre una colisión.
- En redes antiguas con hubs, todos los dispositivos están en el mismo dominio de colisión.
- Un switch crea un dominio de colisión por puerto, evitando colisiones.

Dominio de Broadcast

- Es el área de la red donde un broadcast enviado por un dispositivo llega a todos los demás.
- Un broadcast es un paquete enviado a todas las direcciones (MAC FF:FF:FF:FF:FF:FF).
- Todos los dispositivos en la misma VLAN comparten el mismo dominio de broadcast.
- Routers separan dominios de broadcast.

Dominios de switching

- Los dominios de colisión se eliminan con switches (uno por puerto).
- Los dominios de broadcast se controlan con VLANs o routers.
- Entender estos dominios es clave para diseñar redes escalables y eficientes.

Práctica 2

Dominios de Switching: Conceptos Clave

- **Dominio de colisión:** Área donde pueden ocurrir colisiones. Un switch crea un dominio por puerto.
- **Dominio de broadcast:** Área donde un broadcast llega a todos. Separado por VLANs o routers.

Práctica: Dominios de Colisión

1. Conecta 4 PCs al switch 2960 en Fa0/1 a Fa0/4.
2. Asigna IPs: 192.168.1.1–192.168.1.4 /24
3. Haz ping entre pares (PC1–PC2 y PC3–PC4).
4. Observa que no hay colisiones (cada puerto es un dominio de colisión).

Práctica: VLANs para Dominios de Broadcast

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name RED1
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name RED2
Switch(config-vlan)# exit

Switch(config)# interface range fa0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config)# interface range fa0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
```

Resultados Esperados

Prueba	Resultado	Dominio
PC1 $\leftrightarrow$ PC2	Funciona	Mismo broadcast
PC3 $\leftrightarrow$ PC4	Funciona	Mismo broadcast
PC1 $\leftrightarrow$ PC3	Falla	Diferente VLAN

VLAN

Definición técnica

Una VLAN es un dominio de broadcast independiente en una red de capa 2 (modelo OSI). Esto significa que los dispositivos dentro de la misma VLAN pueden comunicarse directamente entre sí, pero no con dispositivos de otras VLAN sin la intervención de un router o un switch de capa 3.

¿Para qué sirve una VLAN?

- Segmentación de red: separa el tráfico entre diferentes departamentos o grupos (por ejemplo, administración, ventas, soporte).
- Seguridad: los dispositivos de una VLAN no pueden comunicarse con los de otra sin reglas explícitas.
- Optimización del rendimiento: reduce el tráfico innecesario de broadcast en la red.
- Flexibilidad y escalabilidad: permite mover dispositivos dentro de la red sin cambiar el cableado físico.

Tipos de VLAN

- Estáticas (por puerto): asignas manualmente cada puerto del switch a una VLAN.
- Dinámicas: se asignan automáticamente según la MAC, el usuario o el tipo de dispositivo (requiere configuración especial).

Configuración de VLANs en Cisco

1. Entrar al modo privilegiado y de configuración

```
Switch> enable
Switch# configure terminal
```

2. Crear VLANs

```
Switch(config)# vlan 10
Switch(config-vlan)# name Contabilidad
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Ventas
Switch(config-vlan)# exit
```

3. Asignar puertos a VLAN 10 (Fa0/1 - Fa0/3)

```
Switch(config)# interface range fa0/1 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
```

3. Asignar puertos a VLAN 20 (Fa0/4 - Fa0/6)

```
Switch(config)# interface range fa0/4 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
```

4. Verificar configuración

```
Switch# show vlan brief
```

5. Guardar configuración (opcional)

```
Switch# write memory
-- o --
Switch# copy running-config startup-config
```

6. Pruebas de conectividad (desde los PCs)

```
ping 192.168.X.X
```

Redes VLAN en un entorno conmutado múltiple

Cuando hablamos de Redes VLAN en un entorno conmutado múltiple, nos referimos a la implementación de VLANs en una red que involucra múltiples switches conectados entre sí, donde se busca mantener la segmentación lógica de la red a través de enlaces troncales (trunks) y asegurar la comunicación entre dispositivos de la misma VLAN en diferentes switches.

¿Qué es un entorno conmutado múltiple?

Es una red donde hay dos o más switches interconectados, y los dispositivos están distribuidos entre ellos. Para que las VLANs funcionen correctamente en este entorno, se requiere:

- Consistencia en la configuración de VLANs entre switches
- Uso de enlaces troncales entre switches
- Protocolo de encapsulación (como IEEE 802.1Q)

Troncal (Trunk)

Un enlace entre switches que puede transportar tráfico de múltiples VLANs. Este enlace está etiquetado para indicar a qué VLAN pertenece cada trama.

VLANs distribuidas

Permiten que, por ejemplo, la VLAN 10 exista tanto en el Switch A como en el Switch B. Así, los dispositivos en VLAN 10, aunque estén conectados a switches diferentes, pueden comunicarse como si estuvieran en el mismo switch.

Comandos clave para enlaces troncales entre switches

```
Switch(config)# interface fa0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
```

Práctica de VLANs con Trunk entre dos Switches

Objetivo

Configurar dos switches conectados mediante un **enlace troncal (trunk)** para permitir la comunicación entre dispositivos de la misma VLAN conectados a switches diferentes.

Topología de la red

- **Switch1** y **Switch2** conectados por Fa0/24 (trunk)
- **PC1 y PC3** en VLAN 10 (Contabilidad)
- **PC2 y PC4** en VLAN 20 (Ventas)
- PC1 y PC2 conectados a Switch1
- PC3 y PC4 conectados a Switch2

1. Crear VLANs en ambos switches

```
Switch(config)# vlan 10
Switch(config-vlan)# name Contabilidad
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Ventas
Switch(config-vlan)# exit
```

2. Asignar puertos a VLANs en Switch1

```
Switch1(config)# interface fa0/1
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10

Switch1(config)# interface fa0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 20
```

3. Asignar puertos a VLANs en Switch2

```
Switch2(config)# interface fa0/1
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 10

Switch2(config)# interface fa0/2
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
```

4. Configurar el enlace troncal (trunk)

```
Switch1(config)# interface fa0/24
Switch1(config-if)# switchport mode trunk

Switch2(config)# interface fa0/24
Switch2(config-if)# switchport mode trunk
```

5. Verificar VLANs y trunk

```
Switch# show vlan brief
Switch# show interfaces trunk
```

6. Probar conectividad entre PCs

```
Desde PC1: ping a PC3 (misma VLAN 10)
Desde PC2: ping a PC4 (misma VLAN 20)
```

Protocolo de enlace troncal dinámico

El Protocolo de Enlace Troncal Dinámico, conocido como DTP (Dynamic Trunking Protocol), es un protocolo propietario de Cisco que se utiliza para negociar automáticamente la formación de enlaces troncales (trunks) entre dos dispositivos de red (principalmente switches Cisco).

¿Qué es DTP?

DTP (Dynamic Trunking Protocol) permite que los puertos de los switches se configuren automáticamente como troncales si el otro extremo también lo permite. Es útil en redes donde se desea automatizar la configuración de enlaces troncales, pero también puede representar un riesgo de seguridad si no se controla adecuadamente.

¿Cómo funciona?

Cuando dos switches están conectados, DTP intercambia mensajes para negociar el modo de enlace (acceso o trunk). El comportamiento depende del modo configurado en cada puerto:

Modo local	Modo remoto	Resultado
dynamic auto	dynamic auto	acceso
dynamic auto	dynamic desirable	trunk
dynamic desirable	dynamic desirable	trunk
trunk	cualquier modo	trunk
access	cualquier modo	acceso

Modos posibles con switchport mode

```
Switch(config-if)# switchport mode access ←           Fijo como acceso
Switch(config-if)# switchport mode trunk ←            Fijo como trunk
Switch(config-if)# switchport mode dynamic auto ←     Espera que el otro negocie trunk
Switch(config-if)# switchport mode dynamic ←desirable Intenta negociar trunk activamente
```

Ejemplo de uso de DTP

En Switch 1

```
interface fa0/24
switchport mode dynamic desirable
```

En Switch 2

```
interface fa0/24
switchport mode dynamic auto
```

Consideraciones de seguridad

- Es recomendable deshabilitar DTP en enlaces que no deban formar trunks.
- Puedes hacerlo así:

```
interface fa0/24
switchport mode access
switchport nonegotiate
```

Enrutamiento entre VLANs

¿Qué es el enrutamiento entre VLANs?

- Permite la comunicación entre dispositivos ubicados en diferentes VLANs.
- Las VLANs son redes lógicas separadas; requieren un dispositivo de capa 3 para comunicarse.
- Se puede implementar con un **router (Router-on-a-Stick)** o un **switch de capa 3**.

Opción 1: Router-on-a-Stick

- Se usa un solo enlace físico entre el switch y el router.
- El router crea subinterfaces para cada VLAN.
- El enlace entre el router y el switch se configura como trunk.

Configuración del Router (Router-on-a-Stick)

```
interface g0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

interface g0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
```

Configuración del Switch (Router-on-a-Stick)

```
interface fa0/24
switchport mode trunk
```

Opción 2: Switch de Capa 3 (SVI)

- El propio switch realiza el enrutamiento entre VLANs.
- Se crean interfaces virtuales (SVI) para cada VLAN.
- Se activa el comando `ip routing`.

Configuración en un Switch de Capa 3

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown

interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown

ip routing
```

Requisitos para el enrutamiento entre VLANs

- VLANs configuradas correctamente en los switches.
- Enlace trunk entre el switch y el router (o entre switches).
- PCs con IPs y puerta de enlace adecuada según su VLAN.

Ejemplo de prueba de conectividad

```
Desde PC1 (VLAN 10) a PC2 (VLAN 20):
ping 192.168.20.10
```

Práctica: Enrutamiento entre VLANs

Objetivo de la práctica

Implementar el enrutamiento entre VLANs usando la técnica **Router-on-a-Stick**, permitiendo la comunicación entre PCs en diferentes VLANs a través de un router.

Topología de la red

- 1 Router (G0/0 conectado al Switch)
- 1 Switch
- 4 PCs:
  - PC1 y PC2 en VLAN 10 (192.168.10.0/24)
  - PC3 y PC4 en VLAN 20 (192.168.20.0/24)

1. Crear las VLANs en el switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Contabilidad
Switch(config)# vlan 20
Switch(config-vlan)# name Ventas
```

2. Asignar puertos del switch a las VLANs

```
Switch(config)# interface range fa0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10

Switch(config)# interface range fa0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
```

3. Configurar el puerto trunk en el switch

```
Switch(config)# interface fa0/24
Switch(config-if)# switchport mode trunk
```

4. Configurar el router (Router-on-a-Stick)

```
Router> enable
Router# configure terminal

interface g0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

interface g0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0

interface g0/0
no shutdown
```

5. Configurar IPs y puerta de enlace en los PCs

- PC1: IP 192.168.10.10, Gateway 192.168.10.1
- PC2: IP 192.168.10.11, Gateway 192.168.10.1
- PC3: IP 192.168.20.10, Gateway 192.168.20.1
- PC4: IP 192.168.20.11, Gateway 192.168.20.1

6. Verificación de configuración

```
Switch# show vlan brief
Switch# show interfaces trunk

Router# show ip interface brief
```

7. Prueba de conectividad

```
Desde PC1:
ping 192.168.10.11  (PC2 misma VLAN)
ping 192.168.20.10  (PC3 otra VLAN)

Desde PC3:
ping 192.168.20.11  (PC4 misma VLAN)
ping 192.168.10.10  (PC1 otra VLAN)
```