LABORATORIO 4

VLANs y Trunking

Objetivos del laboratorio

- Entender la finalidad y ventajas de usar **VLANs.**
- Crear VLANs en switches Cisco y asignar **puertos de acceso.**
- Configurar un **enlace troncal** (trunk) entre switches usando **802.1Q.**
- Configurar **Router-on-a-Stick** (ROAS) para enrutamiento **inter-VLANs.**
- Verificar y **resolver problemas** básicos (comandos show).
- Aplicar **buenas prácticas** de seguridad básicas para VLANs y trunks.

Conceptos básicos

¿Qué es una VLAN?

Una **VLAN** es una división lógica de una red de capa 2 que agrupa puertos de un switch en dominios de broadcast independientes. Con VLANs se separa el tráfico por función, por seguridad o por departamento sin necesidad de hardware físico adicional. Ej.: VLAN 10 para RH, VLAN 20 para Ventas, etc.

Ventajas: segmentación del tráfico, mejora de seguridad, eficiencia en el uso del ancho de banda y gestión más ordenada.

Puertos de acceso y puertos trunk

- **Puerto de acceso (access port):** es un puerto asociado a una sola VLAN, es decir, un host conectado a este puerto pertenece a esa VLAN y envía tramas sin etiqueta (untagged).
- **Puerto troncal (trunk port):** es un puerto que transporta tráfico de múltiples VLANs entre switches, o hacia routers, las tramas de distintas VLANs viajan etiquetadas (tagged) con 802.1Q. El puerto trunk tiene una VLAN nativa (native) cuyas tramas se envían sin etiqueta.

802.1Q y etiquetado (tagging)

El estándar **802.1Q** inserta una etiqueta en la trama Ethernet para identificar la VLAN de origen. Es el método más usado para trunking de VLANs en redes Cisco.

Enrutamiento inter-VLANs

Las VLANs separan dominios de broadcast. Para que hosts en distintas VLANs se comuniquen, se necesita enrutamiento. Para esto, existen dos opciones:

Router-on-a-Stick (ROAS)

Un router (o firewall) con subinterfaces 802.1Q en una única interfaz física se conecta a un switch mediante un puerto trunk y realiza el enrutamiento.

Switch Virtual Interface (SVI)

En switches capa 3 se crean interfaces VLANs, se les asigna una IP y se habilita el routing en el switch.

Comandos básicos

A continuación se muestran los comandos más usados para crear VLANs, asignar puertos y configurar puertos trunks. Cada bloque de comandos incluye una explicación de cada línea.

1) Crear una VLAN en el switch y asignarle un nombre

Comandos:

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
```

Explicación:

- `configure terminal` — entra al modo de configuración global.
- `vlan 10` — crea la VLAN con ID 10 (o entra a su contexto si ya existe).
- `name HR` — asigna un nombre descriptivo a la VLAN.
- `exit` — sale del submodo VLAN.

Comando de verificación:

```
Switch# show vlan brief
```

Muestra todas las VLANs configuradas y los puertos asociados.

2) Configurar un puerto de acceso y asignarlo a una VLAN

Comandos:

```
Switch# configure terminal
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# description PC-HR
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Explicación:

- `interface FastEthernet0/2` — selecciona la interfaz física del switch a configurar.
- `switchport mode access` — fuerza al puerto a operar como un puerto de acceso.
- `switchport access vlan 10` — asigna ese puerto a la VLAN 10.
- `description PC-HR` — etiqueta administrativa (o comentario) para identificar el puerto.
- `no shutdown` — asegura que el puerto esté administrativamente activo.
- `exit` — vuelve al modo de configuración global.

Verificación:

```
Switch# show interfaces FastEthernet0/2 switchport
```

Muestra el modo del puerto y la VLAN asignada.

3) Configurar un puerto como trunk (802.1Q)

Comandos:

Ejemplo: enlace entre SW1 (Fa0/24) y SW2 (Fa0/24)

```
Switch(config)# interface FastEthernet0/24
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,99
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Explicación:

- `interface FastEthernet0/24` — selecciona la interfaz física a configurar como puerto troncal (trunk).
- `switchport trunk encapsulation dot1q` — establece 802.1Q como protocolo de encapsulación.
    - **Nota:** en switches modernos 802.1Q es el único protocolo de encapsulación disponible y este comando puede no ser necesario, o devolver error, en ese caso omitirlo.
- `switchport mode trunk` — configura el puerto en modo troncal (trunk port: transporta múltiples VLANs).
- `switchport trunk allowed vlan 10,20,99` — limita qué VLANs se permiten en el trunk (buena práctica: permitir sólo las VLANs necesarias).
- `switchport trunk native vlan 99` — define la VLAN nativa (las tramas sin etiqueta pertenecerán a la VLAN 99). Usar una VLAN nativa no utilizada para tráfico de usuarios, para mayor seguridad.
- `no shutdown` — asegura que la interfaz esté activada.

Verificación:

```
Switch# show interfaces trunk
```

Muestra todos los puertos trunks activos y las VLANs que están siendo transportadas a través de el.

4) Deshabilitar negociación DTP y forzar trunk

Comando:

```
Switch(config)# interface FastEthernet0/24
Switch(config-if)# switchport nonegotiate
```

Explicación:

- `switchport nonegotiate` — evita que el puerto envíe (y acepte) mensajes **DTP (Dynamic Trunking Protocol)**. Esto es una medida de seguridad (se impide que un puerto negocie accidentalmente, y de manera automática, un trunk con un dispositivo no previsto).

Buenas prácticas: configurar ambos extremos del enlace con `switchport mode trunk` y `switchport nonegotiate` para evitar negociación automática.

5) Crear una SVI en un switch capa 3

Comandos:

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip routing
```

Explicación:

- `interface vlan 10` — selecciona (o crea si no existe) la interfaz virtual VLAN 10 (SVI).
- `ip address` — asigna una dirección IP a la SVI.
- `no shutdown` — habilita la SVI.
- `ip routing` — habilita el enrutamiento en el switch (comando sólo disponible en switches de capa 3).

Verificación:

```
Switch# show ip interface brief
```

Se verá la SVI Vlan 10 con su IP y estado `up/up` si hay puertos en esa VLAN.

6) Configuración de Router-on-a-Stick

Escenario: un router conectado por trunk a un switch. En el router se crean subinterfaces para cada VLAN.

Comandos en el router:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface GigabitEthernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

Explicación:

- `interface GigabitEthernet0/0.10` — crea una subinterface para VLAN 10 sobre la interfaz física G0/0.
- `encapsulation dot1Q 10` — configura 802.1Q y especifica que esta subinterface maneja la VLAN con ID 10.
- `ip address` — asigna la dirección IP 192.168.10.1/24 a la subinterface G0/0.10 del router, la cuál será usada como puerta de enlace de los hosts de la VLAN 10.
- Se repite para VLAN 20 en subinterface G0/0.20.

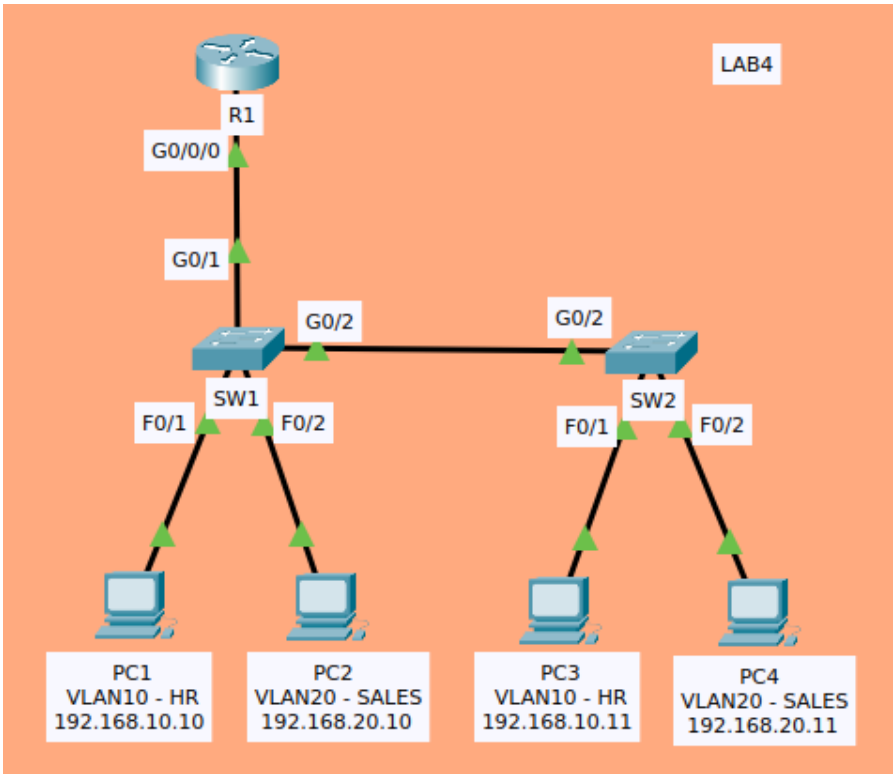
Nota: la interfaz física del router hacia el switch debe estar conectada a un puerto trunk en el switch que transporte las VLANs 10 y 20.

Laboratorio en Packet Tracer

Objetivos del laboratorio

Crear dos VLANs (10 y 20), asignar PCs a cada VLAN a través de dos switches interconectados mediante un puerto trunk, y permitir la comunicación inter-VLAN mediante un Router (ROAS). Verificar con comandos show y ping.

Topología



Direccionamiento:

- VLAN 10 (HR): red 192.168.10.0/24
    - Router subinterface: 192.168.10.1
    - PCs: 192.168.10.10, 192.168.10.11
- VLAN 20 (SALES): red 192.168.20.0/24
    - Router subinterface: 192.168.20.1
    - PCs: 192.168.20.10, 192.168.20.11
- VLAN nativa: VLAN 99 (no usada por hosts).

Actividades

1) Asignar nombres (hostname) a los dispositivos de red.

2) Crear las VLANs necesarias en ambos switches.

3) Asignar los puertos de acceso a las VLANs según corresponda.

4) Configurar puertos troncales entre el Router y los Switches.

5) Configurar Router-on-a-Stick (ROAS) en el Router.

6) Realizar verificación de conectividad entre PCs de diferentes VLANs.

Resolución del laboratorio

1) Asignar hostname a los dispositivos

SW1:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)#
```

SW2:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW2
SW2(config)#
```

R1:

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

2) Crear VLANs en ambos switches

En SW1:

```
SW1(config)# vlan 10
SW1(config-vlan)# name HR
SW1(config-vlan)# exit
SW1(config)# vlan 20
SW1(config-vlan)# name SALES
SW1(config-vlan)# exit
SW1(config)# vlan 99
SW1(config-vlan)# name NATIVE
SW1(config-vlan)# exit
```

En SW2:

```
SW2(config)# vlan 10
SW2(config-vlan)# name HR
SW2(config-vlan)# exit
SW2(config)# vlan 20
SW2(config-vlan)# name SALES
SW2(config-vlan)# exit
SW2(config)# vlan 99
SW2(config-vlan)# name NATIVE
SW2(config-vlan)# exit
```

3) Asignar puertos acceso a las VLANs

En SW1:

```
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# interface FastEthernet0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

En SW2:

```
SW2(config)# interface FastEthernet0/1
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 10
SW2(config-if)# no shutdown
SW2(config-if)# exit
SW2(config)# interface FastEthernet0/2
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 20
SW2(config-if)# no shutdown
SW2(config-if)# exit
```

4) Configurar trunks entre R1, SW1 y SW2

En SW1:

```
SW1(config)# interface GigabitEthernet0/1
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 99
SW1(config-if)# switchport trunk allowed vlan 10,20,99
SW1(config-if)# switchport nonegotiate
SW1(config-if)# no shutdown
SW1(config-if)# exit
SW1(config)# interface GigabitEthernet0/2
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 99
SW1(config-if)# switchport trunk allowed vlan 10,20,99
SW1(config-if)# switchport nonegotiate
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

En SW2:

```
SW2(config)# interface GigabitEthernet0/2
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport trunk native vlan 99
SW2(config-if)# switchport trunk allowed vlan 10,20,99
SW2(config-if)# switchport nonegotiate
SW2(config-if)# no shutdown
SW2(config-if)# exit
```

Verificar trunks (SW1):

```
SW1#show interfaces trunk
Port        Mode         Encapsulation   Status     Native vlan
Gig0/1      on           802.1q          trunking   99
Gig0/2      on           802.1q          trunking   99
Port        Vlans allowed on trunk
Gig0/1      10,20,99
Gig0/2      10,20,99
Port        Vlans allowed and active in management domain
Gig0/1      10,20,99
Gig0/2      10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,99
Gig0/2      10,20,99
SW1#show vlan brief
VLAN  Name             Status     Ports
---- ---------------- --------- -------------------------------
1     default          active     Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                  Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                  Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                  Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                  Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                  Fa0/23, Fa0/24, Gig0/1
10    HR               active     Fa0/1
20    SALES            active     Fa0/2
99    NATIVE           active
```

5) Configurar ROAS en R1

En R1:

```
R1(config)# interface GigabitEthernet0/0/0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/0/0.99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# exit
```

Nota: las subinterfaces permiten que un solo enlace físico hacia el switch sirva múltiples VLANs, el router realiza el enrutamiento entre ambas subinterfaces.

6) Verificaciones

Desde PC1 a PC3 (misma VLAN):

```
PC1:\> ping 192.168.10.11
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Desde PC1 a PC4 (debe responder si el ROAS en R1 está correctamente configurado):

```
PC1:\> ping 192.168.20.11
Reply from 192.168.20.11: bytes=32 time<1ms TTL=127
Reply from 192.168.20.11: bytes=32 time<1ms TTL=127
Reply from 192.168.20.11: bytes=32 time=1ms TTL=127
Reply from 192.168.20.11: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

En switches usar:

```
Switch# show vlan brief
Switch# show interfaces status
Switch# show mac address-table
Switch# show interfaces trunk
```

En router usar:

```
Router# show ip interface brief
Router# show running-config
```

Buenas prácticas y seguridad

- **Limitar VLANs permitidas en trunks** (`switchport trunk allowed vlan`) para minimizar exposición.
- **Desactivar la negociación automática de trunk** (`switchport nonegotiate`) y establecer ambos extremos en `switchport mode trunk`.
- **Evitar usar la VLAN 1** para tráfico de usuario o gestión.
- **Usar una VLAN nativa no utilizada para tráfico** (ej.: VLAN 99) para reducir riesgos con tramas sin etiqueta.
- **Documentar la asignación de VLANs** (mapa de puertos, descripción en interfaces, etc.).
- **Seguridad física**: restringir acceso a los switches y puertos de consola.
- Cambiar contraseñas por defecto y usar enable secret y SSH para administración remota.

Errores comunes y soluciones rápidas

- **Puerto trunk no sube:** verificar switchport mode trunk en ambos extremos y no shutdown.
- **Ping inter-VLAN falla:** verificar IP del gateway, subinterfaces en el router y que el enlace entre el router y el switch sea trunk y que permita las VLANs necesarias.
- **Trunk muestra VLANs inesperadas:** usar `switchport trunk allowed vlan` para limitar las VLANs.

Repaso de conceptos importantes

- **VLAN: limita el dominio de broadcast,** permite segmentar la red sin cambiar cableado físico.
- **Puerto de acceso (access port):** conecta un host a una única VLAN.
- **Puerto troncal (trunk port):** enlace que transporta múltiples VLANs entre switches/routers.
- **802.1Q:** protocolo estándar de etiquetado usado en trunks.
- **Router-on-a-Stick** y **SVI** son las dos formas habituales de enrutamiento inter-VLANs.
- **Seguridad en trunks:** limitar VLANs, desactivar DTP y usar VLAN nativa no utilizada.

Conclusión

La capacidad de crear VLANs y configurar trunks es una de las habilidades fundamentales para diseñar y operar redes LANs modernas. Con VLANs se logra segmentación, mejor gestión del tráfico y una base para políticas de seguridad. En este laboratorio abordó teoría y se practicó la configuración en un escenario realista. Con éste dominio, se podrá avanzar a temas como seguridad por VLAN (ACLs), VTP, STP y optimización de trunking en redes más grandes.

Es esencial que, además de configurar, se adopten buenas prácticas: limitar VLANs en trunks, deshabilitar la negociación automática, evitar usar la VLAN 1 para tráfico de usuario y documentar todas las asignaciones.