LABORATORIO CCNA

PUNTOS QUE CUBRE EL LABORATORIO

- CONFIGURACIÓN DE RED BASICA EN LOS HOSTS
- CONFIGURACIÓN DE DISPOSITIVOS DE RED
- SUBNETING
- VLSM
- ENRUTAMIENTO ESTÀTICO
- ACCESO REMOTO SEGURO (SSH)
- CONFIGURACIÓN VLAN (TRUNK Y ACCESS)
- CONFIGURACIÓN VTP EN SWITCHES
- CONFIGURACIÓN STP EN FUNCIÓN DE LAS VLAN

Contenido

DESARROLLO DEL LABORATORIO

DISEÑO DE LA RED

El diseño simula una pequeña red empresarial, he utilizado pocos equipos para cada subred ya que quería centrarme más en la configuración de los distintos protocolos que se incluyen en el CCNA.

La red parte de la dirección 10.0.0.0/24, en la que he realizado una segmentación de la red quedándose en un /28, que admite 14 host usables debido a que tenemos una red (VLAN 10) que utiliza 10 host, las demás redes al no utilizar tantos hosts, he utilizado el VLSM para segmentar las direcciones de subred /28 y quedarme con un prefijo /29 para las redes, así no se desaprovechan direcciones de host.

En el lado del router 1 configuro las vlan para lograr conectividad entre diferentes redes virtuales, conectándolas a un SW capa 3 para así no tener que segmentar las interfaces del router, a parte configuro VTP creando el nombre de dominio en ambos switches y configurando un switch como servidor y otro como cliente.

En el otro lado que conecta con router 2 hago la misma función a excepción de configurar VTP, agrego un enlace de redundancia para enviar tráfico entre las VLANs y configuro el STP para tener un root bridge en función de la vlan por la que enviamos tráfico

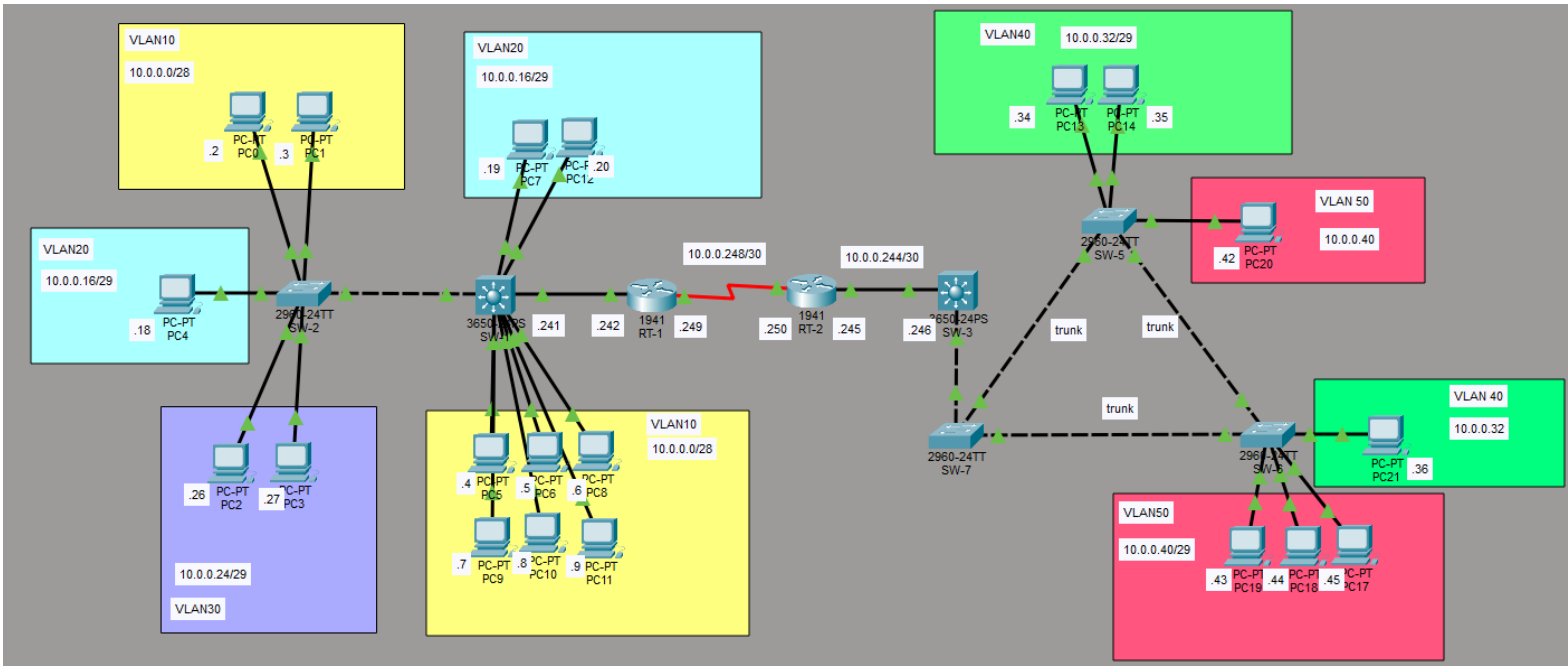


TABLA DE ENRUTAMIENTO

Red	ubicación	Máscara	Rango hosts	Broadcast	Router/Int	Gateway
10.0.0.0/28	VLAN 10	255.255.255.240	10.0.0.1-14	10.0.0.15	VLAN 10	10.0.0.1
10.0.0.16/29	VLAN 20	255.255.255.248	10.0.0.17-22	10.0.0.23	VLAN 20	10.0.0.17
10.0.0.24/29	VLAN 30	255.255.255.248	10.0.0.25-30	10.0.0.31	VLAN 30	10.0.0.25
10.0.0.32/29	VLAN 40	255.255.255.248	10.0.0.33-38	10.0.0.39	VLAN 40	10.0.0.33
10.0.0.40/29	VLAN 50	255.255.255.248	10.0.0.41-46	10.0.0.47	VLAN 50	10.0.0.41
10.0.0.240/30	PP R1-SW1	255.255.255.252	10.0.0.241-242	10.0.0.243	Gi1/0/1-Gi0/0	10.0.0.241/242
10.0.0.244/30	PP R2-SW3	255.255.255.252	10.0.0.245-246	10.0.0.247	Gi0/0-Gi1/0/1	10.0.0.245/246
10.0.0.248/30	PP R1-R2	255.255.255.252	10.0.0.249-250	10.0.0.251	Se0/1/0	10.0.0.249/250

CONFIGURACIÓN BÁSICA

CONFIGURACIÓN BÁSICA ROUTERS

Esta configuración incluye:

- Restricción en el acceso a la consola configurando una contraseña y un tiempo máximo
- Restricción en el acceso remoto creando un usuario para el ssh e indicándole al router que acceda mediante sus credenciales, también configuramos el tiempo máximo de inactividad
- Se generan las claves rsa (4096) y se configura el nombre de dominio
- Contraseñas encriptadas y bloqueo si el usuario falla el login x veces

CONSOLA Y VTY

```
banner motd ^C solo acceso autorizado ^C
!
!
!
!
line con 0
 exec-timeout 5 0
 password 7 0822455D0A160916105A5E57
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

NOMBRE DE DOMINIO Y USUARIO

```
!
no ip domain-lookup
ip domain-name cisco.com
!
.
username admin privilege 15 secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
'
```

BLOQUEO DEL LOGIN Y CONTRASEÑA DEL ENABLE

```
hostname RT-1
!
login block-for 60 attempts 3 within 60
!
!
enable secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
.
```

CONFIGURCIÓN BÁSICA SWITCHES

Esta configuración incluye:

- Restricción en el acceso a la consola configurando una contraseña y un tiempo máximo
- Restricción en el acceso remoto creando un usuario para el ssh e indicándole al switch que acceda mediante sus credenciales, también configuramos el tiempo máximo de inactividad
- Se generan las claves rsa (4096) y se configura el nombre de dominio
- Contraseñas encriptadas
- (La configuración que se muestra es de una switch multicapa en el que le activamos el enrutamiento, esto en los demás switches no se puede hacer ya que trabajan en capa 2)
- Puerta de enlace

CONSOLA Y VTY

```
line con 0
 exec-timeout 5 0
 password 7 0822455D0A160916105A5E57
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
```

NOMBRE DE DOMINIO Y USUARIO

```
username admin privilege 15 secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name ccna.com
```

ENRUTAMIENTO (SOLO SW DE CAPA 3)

```
ip routing
```

CINTRASEÑA DEL ENABLE Y HOSTNAME

```
hostname SW-1
!
!
no profinet
enable secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
```

CONFIGURACIÓN DE CONECTIVIDAD

CONFIGURACIÓN DE CONECTIVIDAD EN SWITCHES

Ya que los switches trabajan en capa 2 a excepción de la multicapa, configuramos los puertos de este como acces o trunk en función de si va a pasar por esa interfaz tráfico de más de una VLAN o no,

En el caso de que el switch sea multicapa, habilito el enrutamiento, y la interfaz que conecta con el router lo habilito como un puerto de capa 3.

SWITCH 1 (MULTICAPA)

Configuramos las distintas interfaces virtuales (de la VLAN 10 a la 30) asignándoles la ip de la puerta de enlace ya que este switch será su Gateway.

```
interface Vlan10
 description Gateway VLAN 10
 mac-address 0030.a388.9201
 ip address 10.0.0.1 255.255.255.240
!
interface Vlan20
 description Gateway VLAN 20
 mac-address 0030.a388.9202
 ip address 10.0.0.17 255.255.255.248
!
interface Vlan30
 description default gateway VLAN 30
 mac-address 0030.a388.9203
 ip address 10.0.0.25 255.255.255.248
```

Además, este switch tiene una conexión punto a punto con un router 1 que le va a permitir comunicarse con host de otras redes.

```
interface GigabitEthernet1/0/1
 no switchport
 ip address 10.0.0.241 255.255.255.252
 duplex auto
 speed auto
```

La interfaz que conecta con el SW-2 envía tráfico de 3 VLANs distintas por lo que lo configuro en trunk mode.

```
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
```

Este switch conecta directamente con equipos de distintas vlan, por lo que estos puertos se configuran en access mode con la vlan correspondiente

De la Gi1/0/3 está la VLAN 20 y de la Gi1/0/5 a la Gi1/0/10 la VLAN 10

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
```

SWITCH 2

Este switch envía y recibe tráfico de una vlan etiquetada por la Gi0/1 (trunk mode) y se lo manda a la vlan correspondiente por lo que estos puertos estarían en modo acceso.

De la Fa0/1 a la Fa0/3 se envía tráfico a la VLAN 10

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
```

En la Fa0/2 a la VLAN 20

```
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
```

De la Fa041 a la Fa0/5 se envía tráfico a la VLAN 30

```
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
```

SWITCH 3 (MULTICAPA)

Configuramos las distintas interfaces virtuales (de la VLAN 40 a la 50) asignándoles la ip de la puerta de enlace ya que este switch será su Gateway.

```
interface Vlan40
 mac-address 0030.a316.1201
 ip address 10.0.0.33 255.255.255.248
!
interface Vlan50
 mac-address 0030.a316.1202
 ip address 10.0.0.41 255.255.255.248
```

Además, este switch tiene una conexión punto a punto con un router 2 que le va a permitir comunicarse con host de otras redes.

```
interface GigabitEthernet1/0/1
 no switchport
 ip address 10.0.0.246 255.255.255.252
 duplex auto
 speed auto
```

La interfaz que conecta con el SW-7 envía tráfico de 2 VLANs distintas por lo que lo configuro en trunk mode.

```
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 40,50
 switchport mode trunk
```

SWITCH 4

Este switch envía tráfico a la puerta de enlace de las VLAN por la Gi0/1 (trunk mode), también envía tráfico de las 2 vlan por dos interfaces a los switches Gi0/2 y Fa0/24

```
interface GigabitEthernet0/1
 switchport trunk allowed vlan 40,50
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 40,50
 switchport mode trunk
```

SWITCH 5

Envía tráfico de la VLAN 40 y 50 a través de la Gi0/1 y Gi0/2

```
interface GigabitEthernet0/1
 switchport trunk allowed vlan 40,50
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 40,50
 switchport mode trunk
```

Tiene conectados directamente hosts que pertenecen a las VLAN 40 y 50.

Desde la Fa0/1 a la Fa0/2 a la VLAN 40

Fa0/3 para la VLAN 50

```
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
```

SWITCH 6

Envía tráfico de la VLAN 40 y 50 a través de la Gi0/1 y Gi0/2

```
interface GigabitEthernet0/1
 switchport trunk allowed vlan 40,50
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 40,50
 switchport mode trunk
```

Tiene conectados directamente hosts que pertenecen a las VLAN 40 y 50.

Desde la Fa0/1 a la Fa0/3 a la VLAN 50

Fa0/4 para la VLAN 40

```
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
```

CONFIGURACIÓN DE RED ROUTERS

En este caso la configuración de red es sencilla ya que hay que configurar solo dos interfaces punto a punto, una es la que conecta con la switch multicapa y la otra es la conexión punto a punto entre routers.

ROUTER 1

Interfaz Gi0/0 conexión con la switch multicapa SW1

```
interface GigabitEthernet0/0
 description Conexion LAN 10,20,30
 ip address 10.0.0.242 255.255.255.252
 duplex auto
 speed auto
```

Interfaz Serial 0/1/0 conexión punto a punto con Router 2.

```
interface Serial0/1/0
 description Conexion punto a punto con RT-2
 ip address 10.0.0.249 255.255.255.252
```

ROUTER 2

Interfaz Gi0/0 conexión con la switch multicapa SW3

```
interface GigabitEthernet0/0
 description Conexion punto a punto con SW-3
 ip address 10.0.0.245 255.255.255.252
 duplex auto
 speed auto
```

Interfaz Serial 0/1/0 conexión punto a punto con Router 1.

```
interface Serial0/1/0
 description Conexion punto a punto con RT-1
 ip address 10.0.0.250 255.255.255.252
 clock rate 2000000
```

ENRUTAMIENTO

Se realiza un enrutamiento para que un dispositivo de capa 3 conozca redes que no estén directamente conectadas a él.

ENRUTAMIENTO SW1

En este caso es sencillo ya que a las redes que no sabe llegar el switch (30,40) solo pueden tomar una ruta, que es la ip de siguiente salto del router por lo que configuramos, que cualquier red a la que no sepa llegar la switch multicapa se lo envíe al router 1 (esto lo hacemos con ip route 0.0.0 0.0.0 [ip de siguiente salto]).

```
SW-1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.0.242 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C       10.0.0.0/28 is directly connected, Vlan10
L       10.0.0.1/32 is directly connected, Vlan10
C       10.0.0.16/29 is directly connected, Vlan20
L       10.0.0.17/32 is directly connected, Vlan20
C       10.0.0.24/29 is directly connected, Vlan30
L       10.0.0.25/32 is directly connected, Vlan30
C       10.0.0.240/30 is directly connected, GigabitEthernet1/0/1
L       10.0.0.241/32 is directly connected, GigabitEthernet1/0/1
S*   0.0.0.0/0 [1/0] via 10.0.0.242
```

ENRUTAMIENTO SW3

Hacemos lo mismo que en SW1, ya que a las redes que no sabe llegar el switch (10,20,30) solo pueden tomar una ruta, que es la ip de siguiente salto del router 2 por lo que configuramos, que cualquier red a la que no sepa llegar la switch multicapa se lo envíe al router (lo hacemos con ip route 0.0.0 0.0.0 [ip de siguiente salto]).

```
SW-3(config)#do sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.0.245 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.0.0.32/29 is directly connected, Vlan40
L       10.0.0.33/32 is directly connected, Vlan40
C       10.0.0.40/29 is directly connected, Vlan50
L       10.0.0.41/32 is directly connected, Vlan50
C       10.0.0.244/30 is directly connected, GigabitEthernet1/0/1
L       10.0.0.246/32 is directly connected, GigabitEthernet1/0/1
S*   0.0.0.0/0 [1/0] via 10.0.0.245
```

ENRUTAMIENTO RT1

Cuando los paquetes de las redes que conectan al SW1 llegan al router, estas saben llegar a el por que está directamente conectado al switch, pero cuando el router tiene los paquetes no sabe que hacer con ellos porque no tiene las redes conectadas directamente, por lo que le agrego una ruta por la que enviar el trafico de las redes a las que no sabe llegar por la ip del SW1

Por otro lado, el router tiene que saber llegar a las vlan 40 y 50 que no están conectadas a el, por lo que añadimos el enrutamiento a las redes por la ip de siguiente salto del router 2.

```
RT-1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.0.241 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S       10.0.0.32/29 [1/0] via 10.0.0.250
S       10.0.0.40/29 [1/0] via 10.0.0.250
C       10.0.0.240/30 is directly connected, GigabitEthernet0/0
L       10.0.0.242/32 is directly connected, GigabitEthernet0/0
C       10.0.0.248/30 is directly connected, Serial0/1/0
L       10.0.0.249/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 10.0.0.241
```

ENRUTAMIENTO R2

En este caso pasa lo mismo que en el RT1, no sabe llegar a las VLAN de su switch conectado, por lo que las VLAN que no conoce las envía al switch capa 3.

Por otro lado, el router tiene que saber llegar a las vlan 10,20 y 30 que no están conectadas a él , por lo que añadimos el enrutamiento a las redes por la ip de siguiente salto del router 1.

```
RT-2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.0.246 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
S       10.0.0.0/28 [1/0] via 10.0.0.249
S       10.0.0.16/29 [1/0] via 10.0.0.249
S       10.0.0.24/29 [1/0] via 10.0.0.249
C       10.0.0.244/30 is directly connected, GigabitEthernet0/0
L       10.0.0.245/32 is directly connected, GigabitEthernet0/0
C       10.0.0.248/30 is directly connected, Serial0/1/0
L       10.0.0.250/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 10.0.0.246
```

SPANNING TREE PROTOCOL

En la presente topología de red se implementó el Spanning Tree Protocol (STP), utilizando su versión mejorada Rapid Spanning Tree Protocol, con el objetivo de prevenir bucles de capa 2 y mantener la redundancia entre los switches del dominio de broadcast.

La red está conformada por múltiples switches interconectados mediante enlaces troncales, que permiten el transporte de varias VLANs: VLAN 1 (Administrativa), VLAN 40 (Usuarios) y VLAN 50 (Servicios).

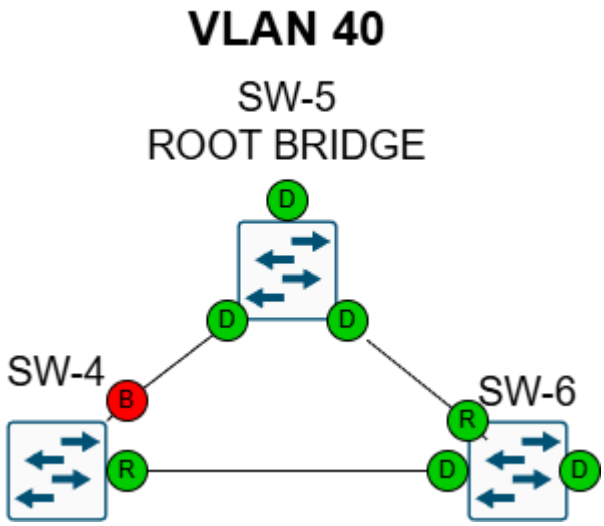
Al existir enlaces redundantes entre los switches SW-4, SW-5 y SW-6, se hace necesario el uso de STP para evitar bucles que podrían colapsar la red por tormentas de broadcast o errores de direccionamiento MAC.

Para optimizar la eficiencia y el balance de carga, se configuraron prioridades específicas por VLAN, de manera que cada switch actúe como Root Bridge de una VLAN diferente:

SW-5 es el Root Bridge para VLAN 40,

SW-6 es el Root Bridge para VLAN 50.

SPANNING TREE VLAN 40



Este seria el esquema de STP para la VLAN 40, tenemos el SW-5 como root bridge, al que le he forzado a serlo bajándole la prioridad stp a 4096, en el root bridge todos los puertos son designados.

En los demás switches se elige el root port como la mejor ruta para llegar al root bridge (con menor costo), y se bloquea el puerto con mayor costo, en mi caso fa0/24.

Comprobamos que el SW-5 esta como root bridge y tiene todos los puertos designados.

```
SW-5#sh spanning-tree vlan 40
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID     Priority    4136
              Address     000A.419D.D3C3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4136  (priority 4096 sys-id-ext 40)
              Address     000A.419D.D3C3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Desg FWD 19        128.25   P2p
```

Luego vamos al SW-6 donde el puerto Gi0/1 esta como root port ya que tiene la ruta de menor costo hasta el root bridge y los demás puertos están designados.

```
SW-6#sh spanning-tree vlan 40
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID     Priority    4136
              Address     000A.419D.D3C3
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32808  (priority 32768 sys-id-ext 40)
              Address     0004.9A27.A082
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p
```

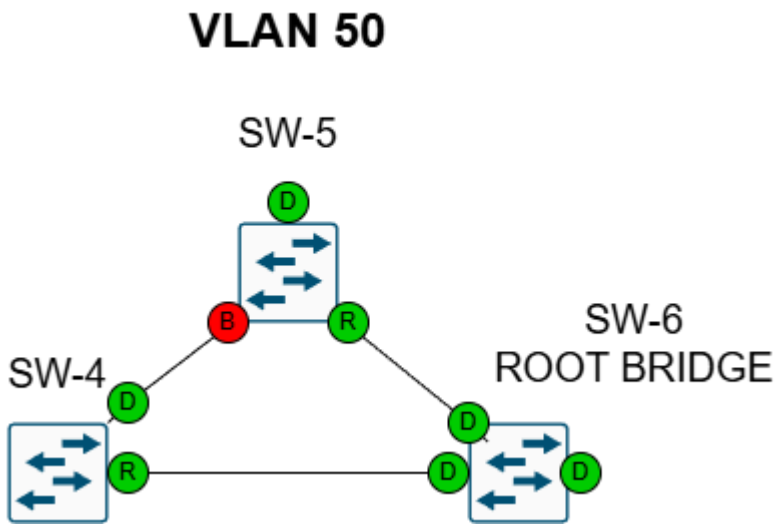
Por último, en el SW-4 vemos que tiene bloqueado el puerto fa0/24 ya que es el de mayor costo y G0/1 como root port ya que es el de menor.

```
SW-4#sh spanning-tree vlan 40
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID     Priority    4136
              Address     000A.419D.D3C3
              Cost        8
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32808  (priority 32768 sys-id-ext 40)
              Address     0001.6493.1E75
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/24           Altn BLK 19        128.24   P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

SPANNING TREE VLAN 50



Este sería el esquema de STP para la VLAN 50, tenemos el SW-6 como root bridge, al que le he forzado a serlo bajándole la prioridad stp a 4096, en el root bridge todos los puertos son designados.

En los demás switches se elije el root port como la mejor ruta para llegar al root bridge (con menor costo), y se bloquea el puerto con mayor costo, en mi caso Gi0/1 del SW5.

Comprobamos que el SW-6 está como root bridge y tiene todos los puertos designados.

```
SW-6#sh spanning-tree vlan 50
VLAN0050
  Spanning tree enabled protocol rstp
  Root ID     Priority    4146
              Address     0004.9A27.A082
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4146  (priority 4096 sys-id-ext 50)
              Address     0004.9A27.A082
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Desg FWD 4         128.25   P2p
```

Luego vamos al SW-4 donde el puerto Gi0/1 esta como root port ya que tiene la ruta de menor costo hasta el root bridge y los demás puertos están designados.

```
SW-4#sh spanning-tree vlan 50
VLAN0050
  Spanning tree enabled protocol rstp
  Root ID     Priority    4146
              Address     0004.9A27.A082
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32818  (priority 32768 sys-id-ext 50)
              Address     0001.6493.1E75
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/24           Desg FWD 19        128.24   P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Por último, en el SW-4 vemos que tiene bloqueado el puerto Gi0/1 ya que es el de mayor costo y G0/2 como root port ya que es el de menor.

```
SW-5#sh spanning-tree vlan 50
VLAN0050
  Spanning tree enabled protocol rstp
  Root ID     Priority    4146
              Address     0004.9A27.A082
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32818  (priority 32768 sys-id-ext 50)
              Address     000A.419D.D3C3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/2            Root FWD 4         128.26   P2p
Gi0/1            Altn BLK 19        128.25   P2p
```

VTP

En esta práctica se implementó el VLAN Trunking Protocol (VTP) para facilitar la administración y propagación automática de VLANs entre switches.

El SW1 se configuró como servidor VTP y el SW2 como cliente, ambos dentro del mismo dominio ccna.com.

Desde el servidor se crearon las VLANs 10, 20 y 30, que fueron replicadas automáticamente en el cliente a través de los enlaces troncales.

Gracias a esta configuración, se logró mantener una base de datos VLAN unificada, reduciendo la configuración manual y asegurando la consistencia de la red.

Comprobamos que el SW-1 trabaja en modo servidor y tiene el nombre de dominio configurado correctamente

```
SW-1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : ccna.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0002.1610.D800
Configuration last modified by 0.0.0.0 at 3-1-93 01:08:29
Local updater ID is 10.0.0.1 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 35
MD5 digest                      : 0xFC 0x64 0x34 0xF6 0x2B 0x42 0x25 0x9D
                                  0xBF 0xD8 0xA9 0xDE 0x61 0x49 0xB6 0x5B
```

Comprobamos que el SW-2 trabaja en modo cliente y tiene el nombre de dominio configurado correctamente

```
SW-2#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : ccna.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0030.F259.2200
Configuration last modified by 0.0.0.0 at 3-1-93 01:08:29

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
Configuration Revision          : 35
MD5 digest                      : 0xFC 0x64 0x34 0xF6 0x2B 0x42 0x25 0x9D
                                  0xBF 0xD8 0xA9 0xDE 0x61 0x49 0xB6 0x5B
```

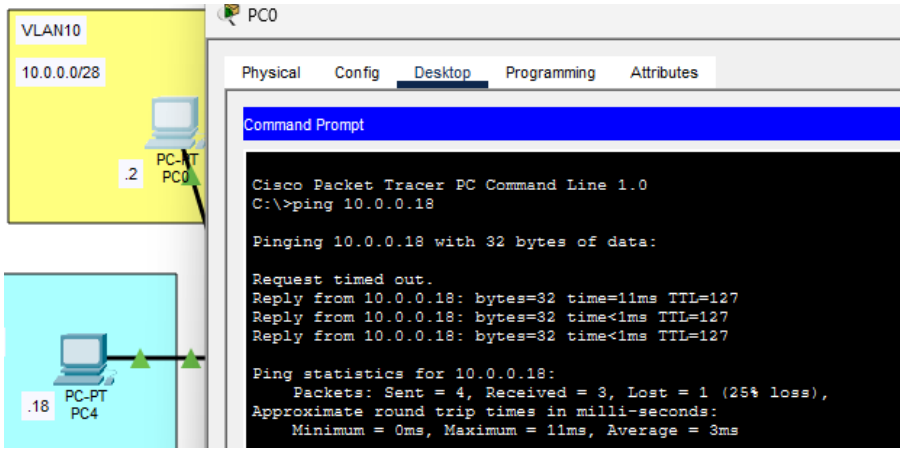
PRUEBAS

PRUEBAS CONECTIVIDAD

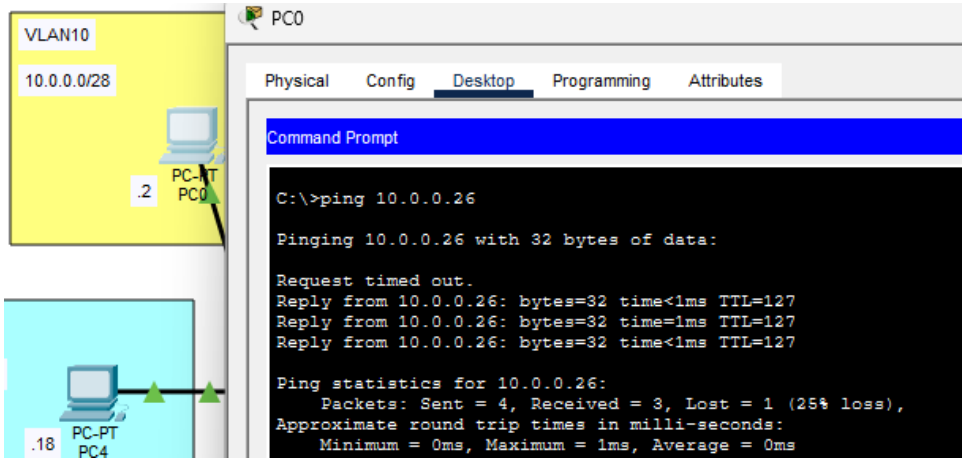
Cuando una red envía un ping a otra y obtiene respuesta, significa que la LAN a la que hace ping también sabe llegar a la red donde se envía el ping origen, por lo que, si por ejemplo se hace ping de la vlan 10 a la 40, si haces ping de la 40 a la 10 también tendrá conexión

VLAN 10

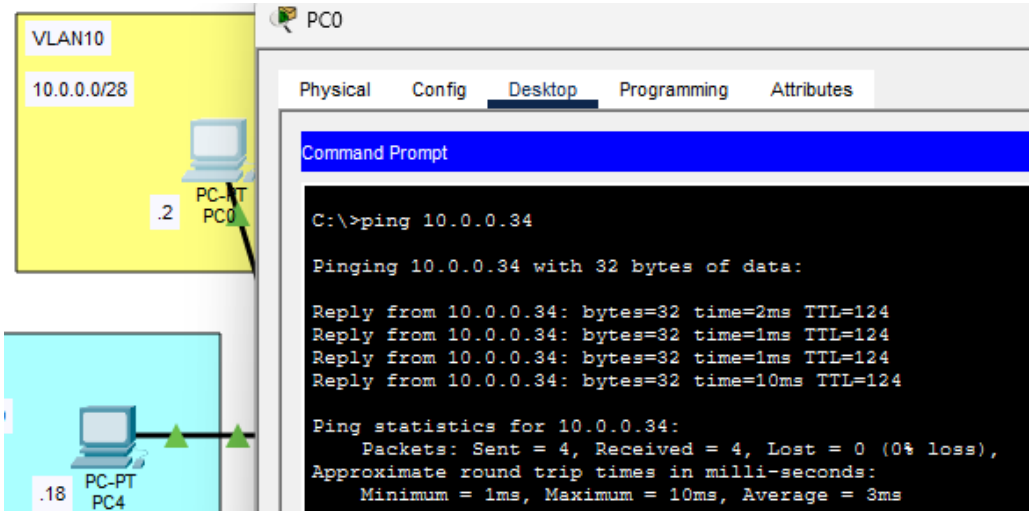
VLAN 10-20



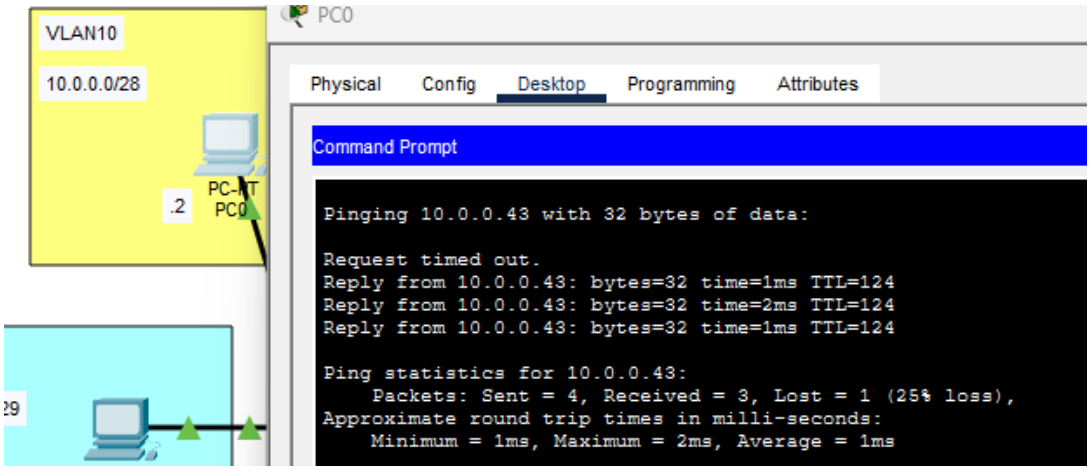
VLAN 10-30



VLAN 10-40

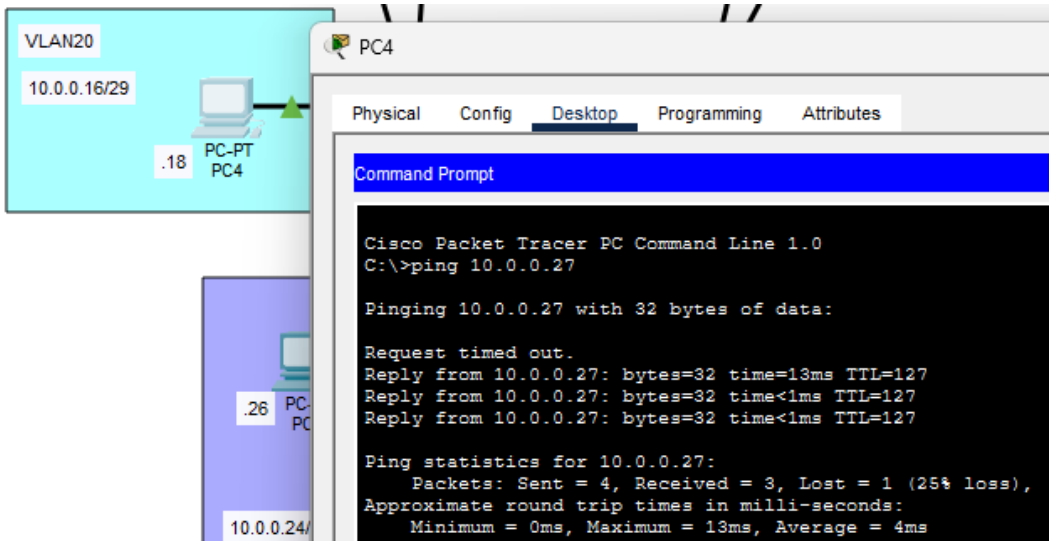


VLAN 10-50

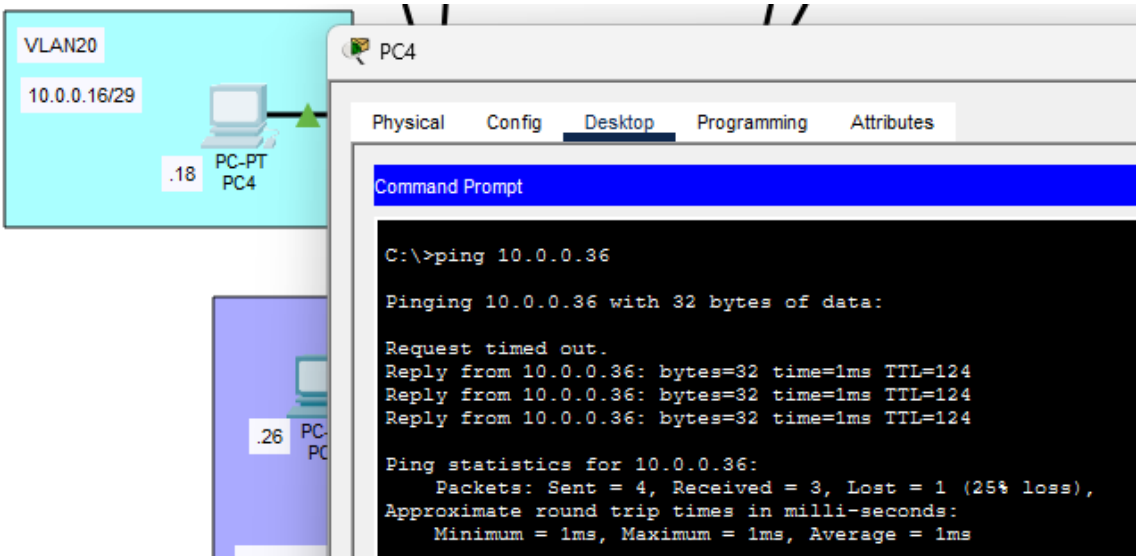


VLAN 20

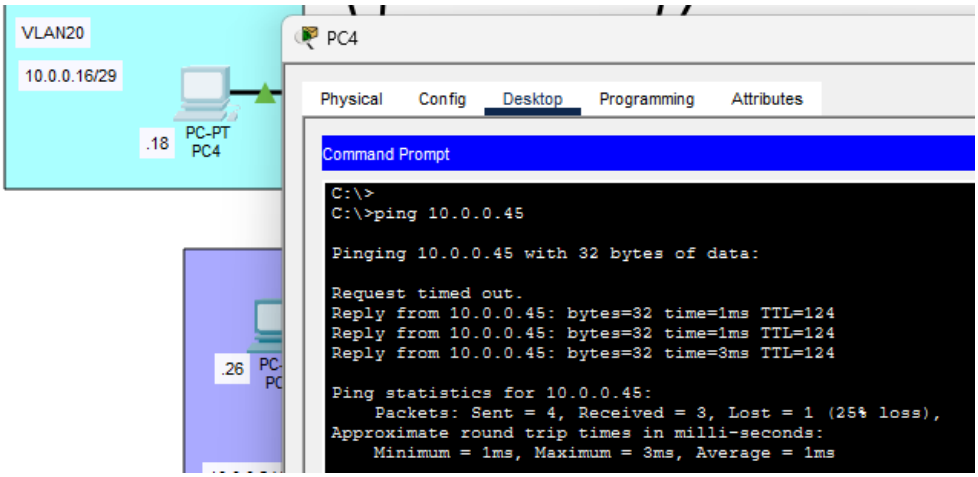
VLAN 20-30



VLAN 20-40

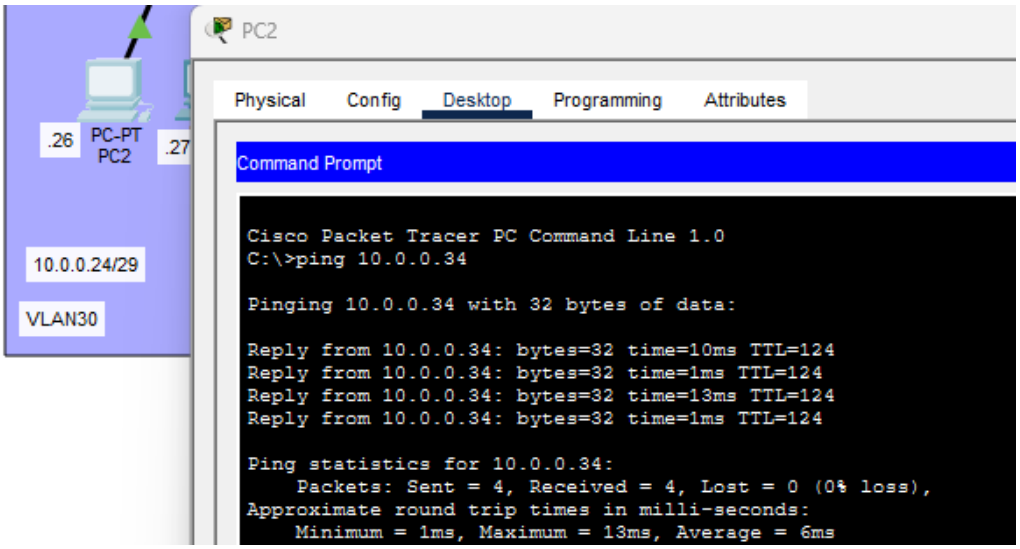


VLAN 20-50

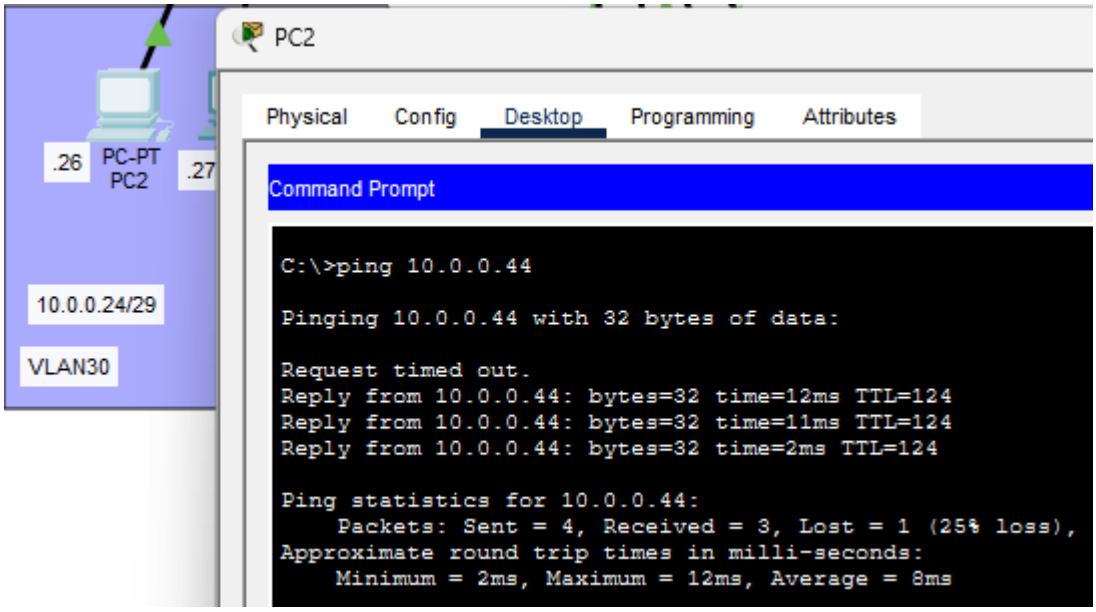


VLAN 30

VLAN 30-40

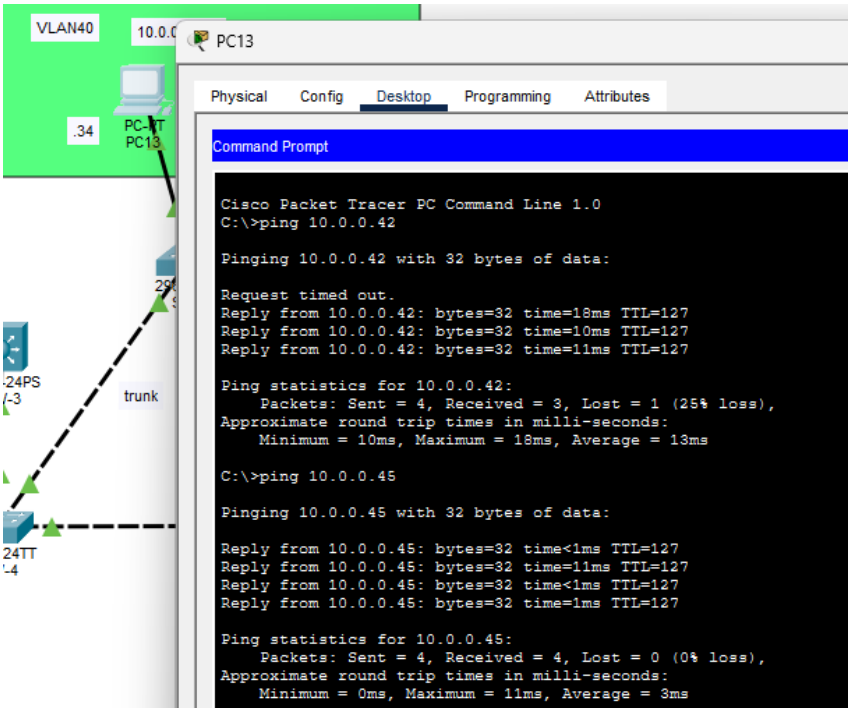


VLAN 30-50



VLAN 40

VLAN 40-50



PRUEBAS DE ACCESO REMOTO

Voy a comprobar desde 1 pc que puedo acceder remotamente (mediante ssh) a todos los dispositivos intermediarios de la red

SW1

```
C:\>ssh -l admin 10.0.0.1

Password:

 solo personal autorizado

SW-1#exit
```

SW2

```
C:\>ssh -l admin 10.0.0.10

Password:
% Login invalid


Password:

 solo personal autorizado

SW-2>exit
```

SW3

```
C:\>ssh -l admin 10.0.0.246

Password:

 solo personal autorizado

SW-3#exit
```

SW4

```
C:\>ssh -l admin 10.0.0.38

Password:

 solo personal autorizado

SW-4>exit
```

SW5

```
C:\>ssh -l admin 10.0.0.37

Password:

 solo personal autorizado

SW-5>exit
```

SW6

```
C:\>ssh -l admin 10.0.0.46

Password:

 solo personal autorizado

SW-6>exit
```

RT1

```
C:\>ssh -l admin 10.0.0.242

Password:

 solo acceso autorizado

RT-1#exit
```

RT2

```
C:\>ssh -l admin 10.0.0.250

Password:

 solo personal autorizado

RT-2#exit
```