LABORATORIO CCNA

Puntos que cubre este 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)

Contenido

TOPOLOGÍA DE LA RED

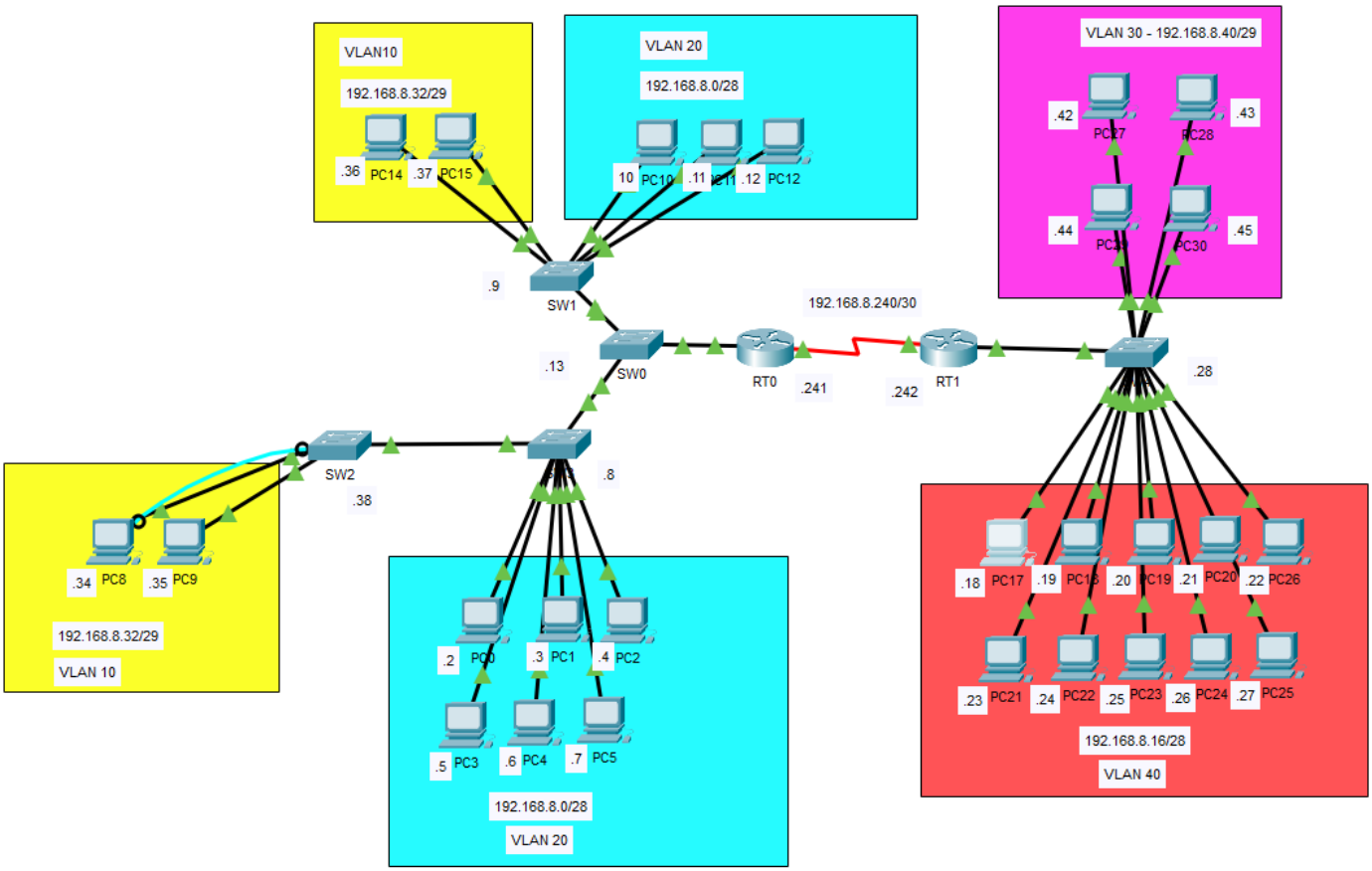
La dirección de red parte de la dirección 192.168.8.0/24 la que he segmentado en redes de 14 direcciones asignables por lo que la dirección se quedaría en 192.168.8.0/28.

He ajustado cada dirección de red a la cantidad de equipos que tiene cada una de ellas utilizando VLSM, a continuación, mostraré la tabla de enrutamiento:

Red / VLAN	Ubicación	Máscara	Rango de Hosts	Broadcast	Router / Int	Gateway
192.168.8.0/28	VLAN 20	255.255.255.240	192.168.8.1 – 192.168.8.14	192.168.8.15	R0 G0/0.20	192.168.8.1
192.168.8.16/28	VLAN 40	255.255.255.240	192.168.8.17 – 192.168.8.30	192.168.8.31	R1 G0/0	192.168.8.17
192.168.8.32/29	VLAN 10	255.255.255.248	192.168.8.33 – 192.168.8.38	192.168.8.39	R0 G0/0.10	192.168.8.33
192.168.8.40/29	VLAN 30	255.255.255.248	192.168.8.41 – 192.168.8.46	192.168.8.47	R1 G0/0.30	192.168.8.41
192.168.8.240/30	Enlace punto a punto entre Router0 y Router1	255.255.255.252	192.168.8.241 – 192.168.8.242	192.168.8.243	S/0/1/0	192.168.8.241 (R0) / 192.168.8.242 (R1)

La topología implementada corresponde a un laboratorio de redes basado en segmentación por VLAN y enrutamiento con VLSM, diseñado para simular una red empresarial a pequeña escala.

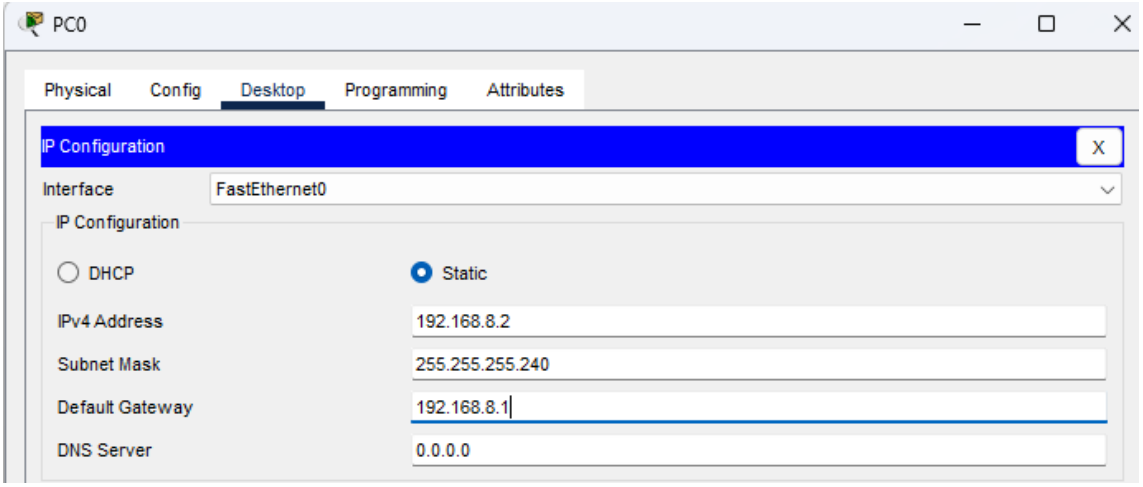
La infraestructura está compuesta por dos routers (RT0 y RT1), conectados entre sí mediante un enlace punto a punto /30, y varios switches de acceso y distribución que interconectan a los diferentes segmentos de usuarios.



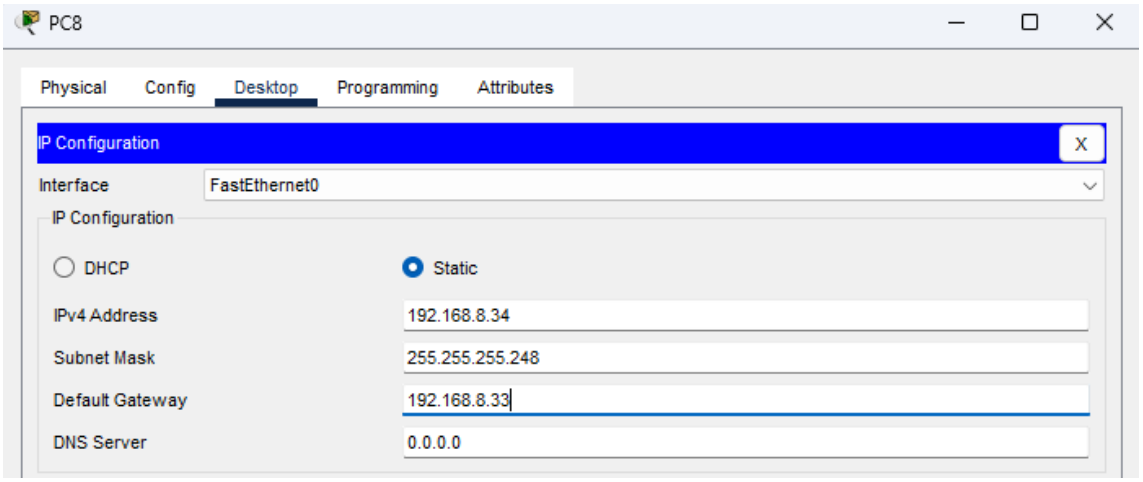
CONFIGURACIÓN BÁSICA EN LOS HOSTS

Esta configuración consiste en agregar una dirección ip correspondiente a la red en la que está situado cada dispositivo host, en la documentación mostraré la configuración de un solo dispositivo en cada red ya que es la misma configuración en todos.

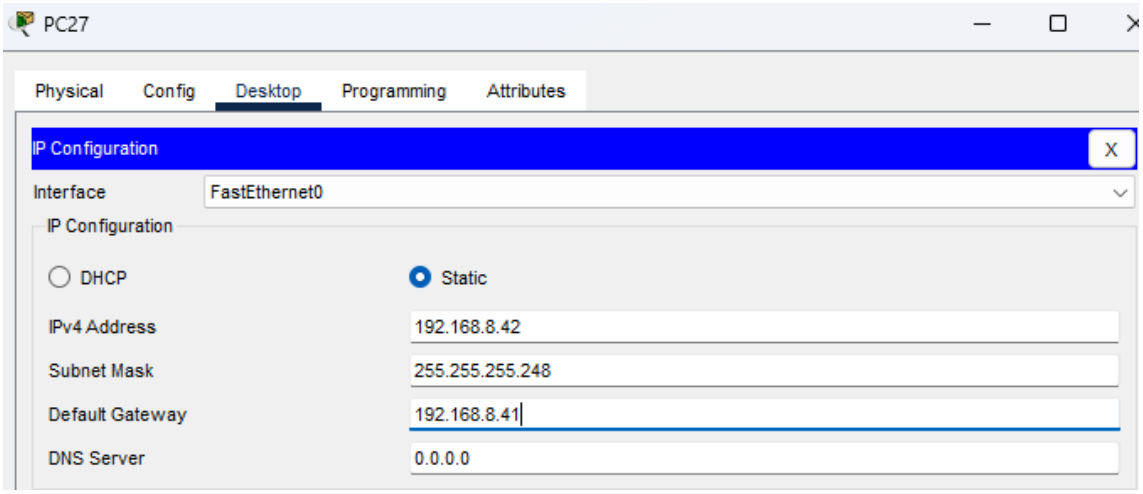
PC0 VLAN 20



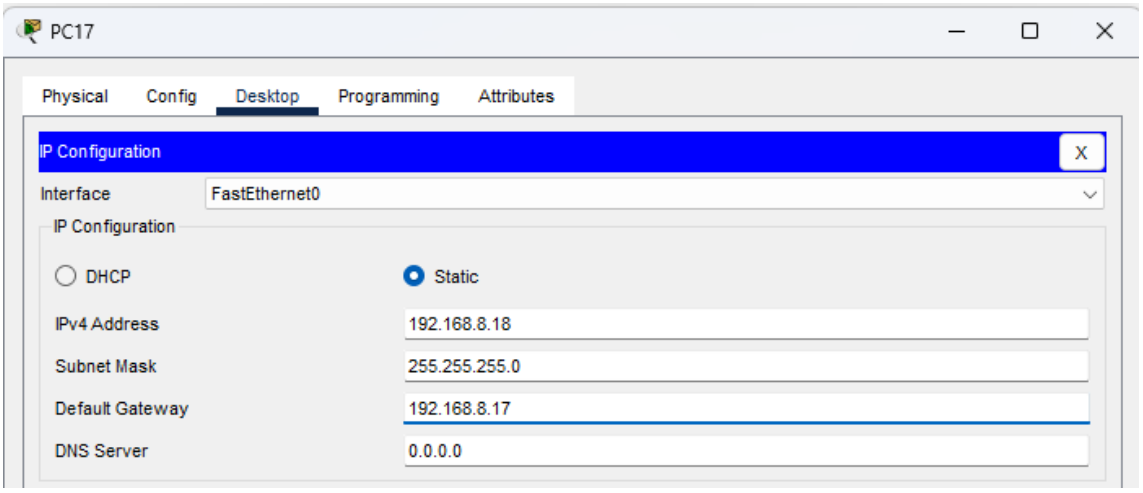
PC8 VLAN 10



PC27 VLAN 30



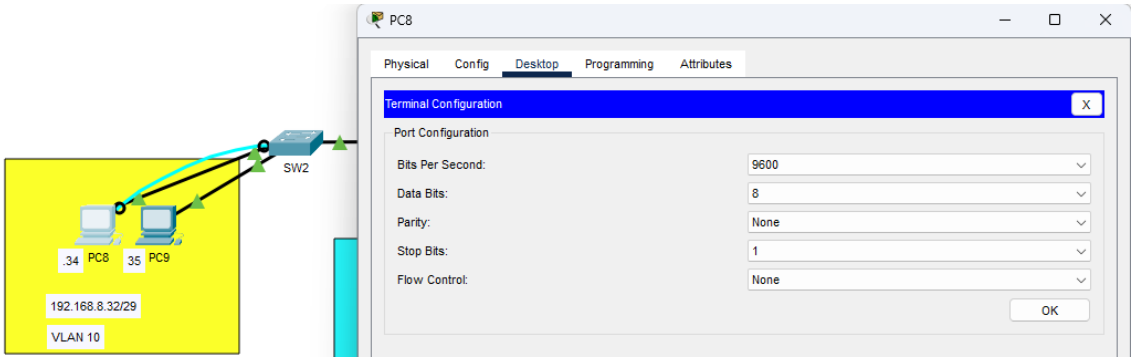
PC17 VLAN 40



CONFIGURACIÓN BÁSICA SWITCHES Y ACCESSO REMOTO

He configurado todos los switches para añadiéndoles contraseñas, una puerta de enlace y acceso remoto seguro, en todos los switches realizo la misma configuración, excepto la puerta de enlace que cada switch tendrá la de la interfaz de el router correspondiente, por lo que mostraré la configuración de un solo switch, pero la puerta de enlace que he configurado en todos.

Accedo al switch correspondiente mediante una conexión con un host de consola



Habilito una contraseña cifrada, creo un usuario para el acceso mediante SSH y configuro un nombre de dominio para generar el par de claves RSA.

```
SW2#show run
Building configuration...

Current configuration : 1416 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW2
!
enable secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
!
!
!
ip domain-name cisco.com
!
username dani secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
!
!
!
```

Configuro la línea de consola para que cuando se entre por consola al switch se pida al usuario se identifique y si está más de 5 minutos inactivo para que cierre la sesión

Configuro la línea VTY para permitir el acceso remoto pidiendo un usuario que es el que hemos generado anteriormente y capando el servicio telnet

Añado una puerta de enlace al switch

```
ip default-gateway 192.168.8.33
!
banner motd ^C solo personal autorizado ^C
!
!
!
line con 0
 password 7 0822455D0A160916105A5E57
 logging synchronous
 login
 exec-timeout 5 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```

CONFIGURACIÓN BÁSICA ROUTERS Y ACCESSO REMOTO

La configuración básica de los routers es bastante similar a la de los switches, se configura la línea de consola con contraseña y tiempo excedido, se configura la línea VTY con un usuario y contraseña que creamos.

La configuración que añadimos en routers que no añadimos en el switch es la capacidad de establecer una norma de caracteres mínimos para crear una contraseña y además establecemos una norma de sacar al usuario del inicio de sesión si falla la contraseña x veces en x segundos.

La configuración que muestro a continuación es la general del RT-0 (hostname, RSA keys, domain name, login block y service password encryption)

```
hostname RT0
!
login block-for 30 attempts 3 within 60
!
!
enable secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$zU/OhmPOrIxrk68Sj4Mzz/
!
!
license udi pid CISCO1941/K9 sn FTX1524ZX1Q-
!
!
!
!
!
!
!
!
!
ip domain-name cisco.com
```

Aparte de esta configuración general configuro la línea de consola y la de acceso remoto para gestionar el acceso mediante contraseña y controlar la inactividad.

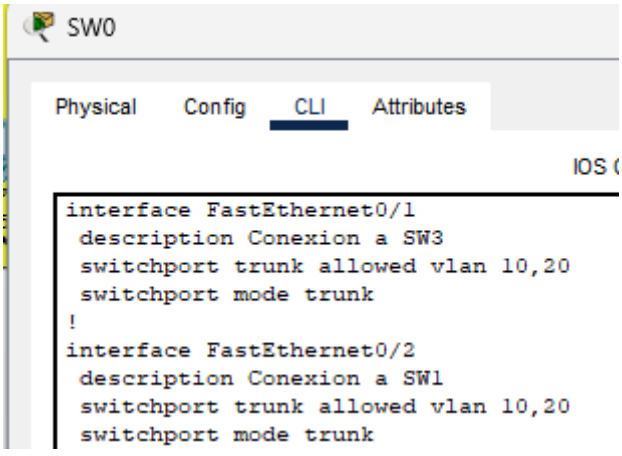
```
banner motd ^C solo personal autorizado ^C
!
!
!
!
line con 0
 exec-timeout 5 0
 password 7 0822455D0A160916105A5E57
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
line vty 5 15
 exec-timeout 5 0
 login local
 transport input ssh
```

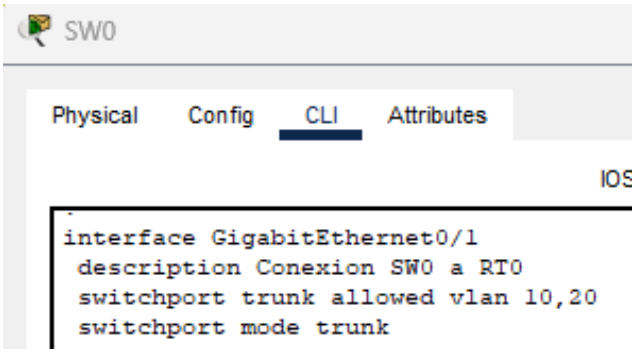
CONFIGURACIÓN CONECTIVIDAD A VLAN SW0

Este switch conecta desde la interfaz G 0/1 al router 1 llevando hasta el tráfico de las VLAN 10 y 20 que le envían los switches SW1 (FA 0/2) y SW3 (FA 0/1).

Teniendo en cuenta que tiene que recoger el tráfico de las dos interfaces que se conectan al switch y cada una de ellas envían el tráfico por la vlan 10 y la vlan 20, tanto FA 0/1 como FA 0/2 se tienen que configurar como switchport mode trunk admitiendo las vlan 10 y 20.

En la interfaz G 0/1 igual que en las demás, envía al router tráfico de las dos VLANS por lo que configuramos el puerto en trunk mode.



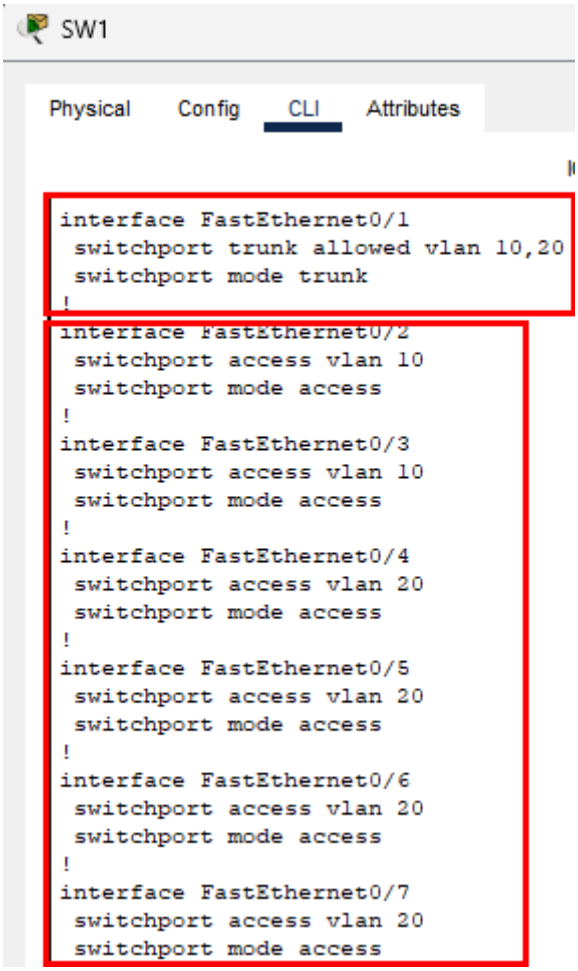


CONFIGURACIÓN CONECTIVIDAD A VLAN SW1

Este switch tiene conexión directa a los equipos, desde la Fa 0/2 a la Fa 0/3 están conectados los equipos que se encuentran en la vlan 10, y desde la Fa 0/4 a la Fa 0/7 se conectan los dispositivos de la vlan 20.

Por lo que cada puerto se configura de modo acceso, permitiendo el tráfico a la vlan correspondiente.

El puerto Fa 0/1 se conecta directamente al SW0 por lo que el puerto tiene que estar en trunk mode ya que envía tráfico de la vlan 10 y la vlan 20

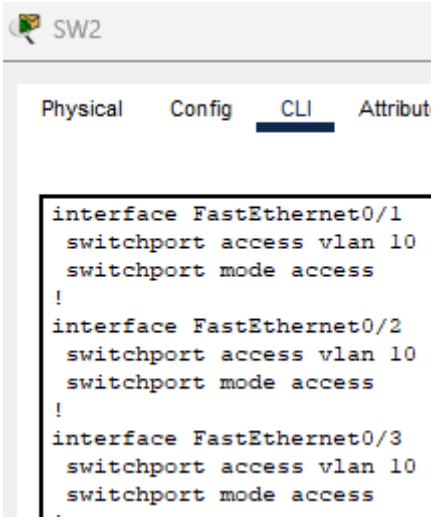


CONFIGURACIÓN CONECTIVIDAD A VLAN SW2

Conecta al SW3 enviando el tráfico de la VLAN10 y a su vez conecta a los dispositivos de dicha VLAN.

Usa los puertos Fa 0/2 y Fa 0/3 para conectar los hosts, como solo enviamos tráfico de 1 sola VLAN configuramos dichos puertos como mode Access vlan 10

El puerto Fa 0/3 envía tráfico de la VLAN 10 por lo que al solo enviar información de una sola VLAN se configura en Access mode vlan 10

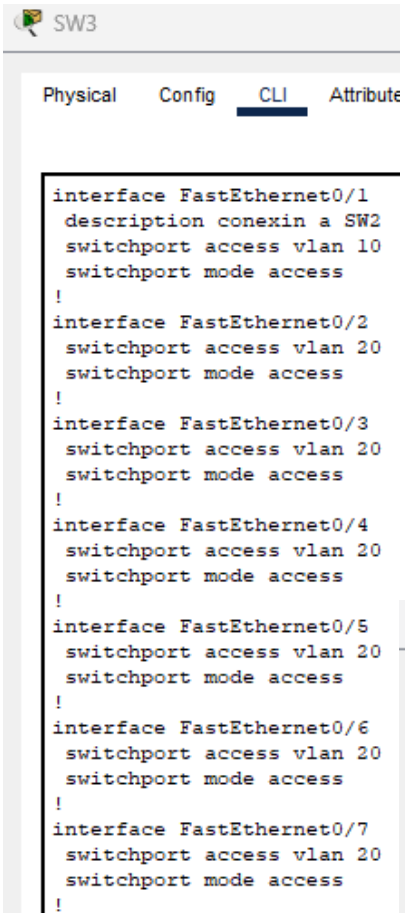


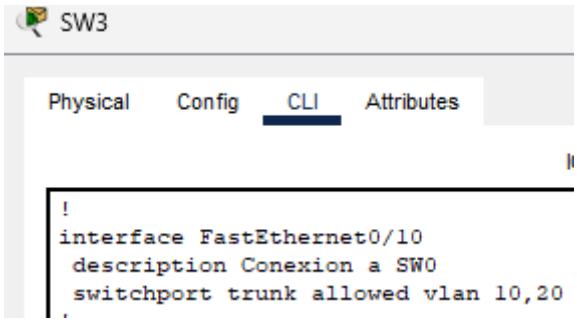
CONFIGURACIÓN CONECTIVIDAD A VLAN SW3

Este switch conecta directamente a los dispositivos de la VLAN 20 y directamente al SW 0 para enviar el tráfico de la VLAN 20 y 10

Entra las interfaces Fa 0/1 y la Fa 0/7 conectan a los hosts de la VLAN20 por lo que este rango lo configuramos en Access mode

La interfaz Fa 0/10 conecta al SW 0 enviando tráfico de las 2 VLAN por lo que lo configuramos en trunk mode.





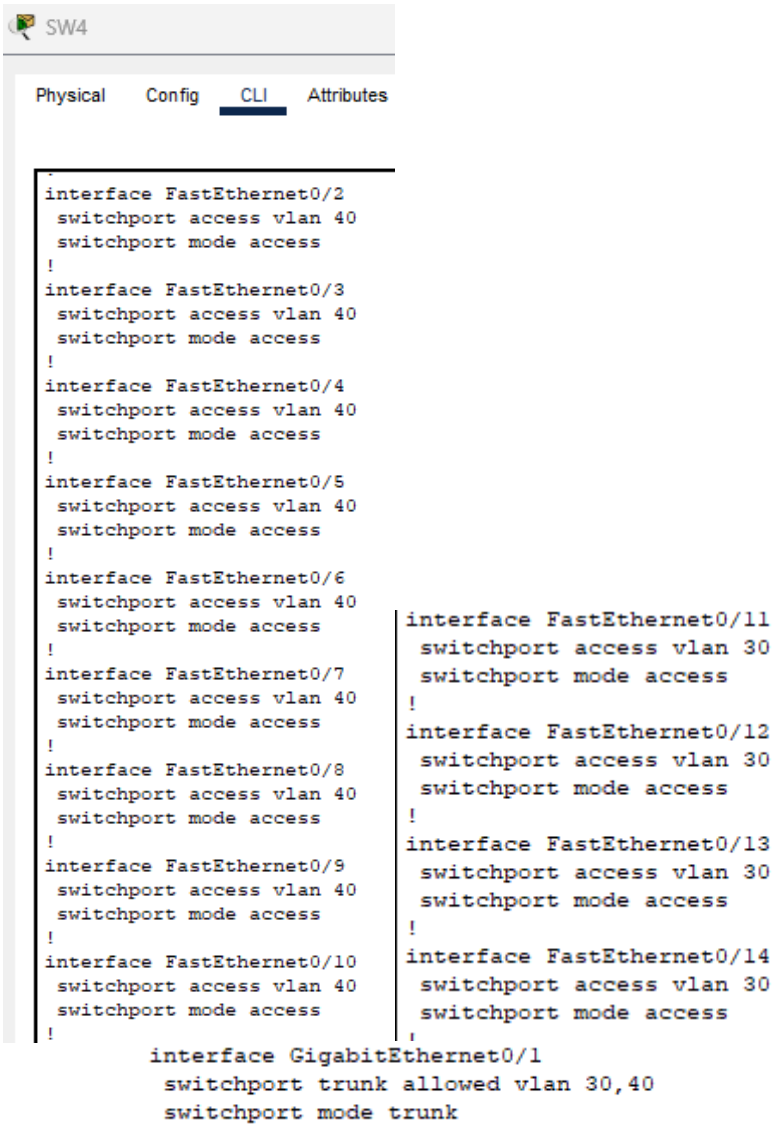
CONFIGURACIÓN CONECTIVIDAD A VLAN SW4

Este switch lleva el tráfico de las VLAN 30 y 40 hacia el router 1 por la interfaz G 0/1y por las demás interfaces envían el tráfico a los dispositivos de su LAN correspondiente

La interfaz G 0/1 conecta al R1 y le envía tráfico de las VLAN 30 y de la 40 por la que configuramos el puerto en trunk mode permitiendo las vlan 30 y 40

El rango de interfaces Fa 0/11 – Fa 0/14 conecta a los dispositivos que pertenecen a la VLAN10 y estos puertos los configuramos en Access mode VLAN 30

El rango de interfaces Fa 0/2 – Fa 0/13 conecta a los dispositivos que pertenecen a la VLAN20 y estos puertos los configuramos en Access mode VLAN 40



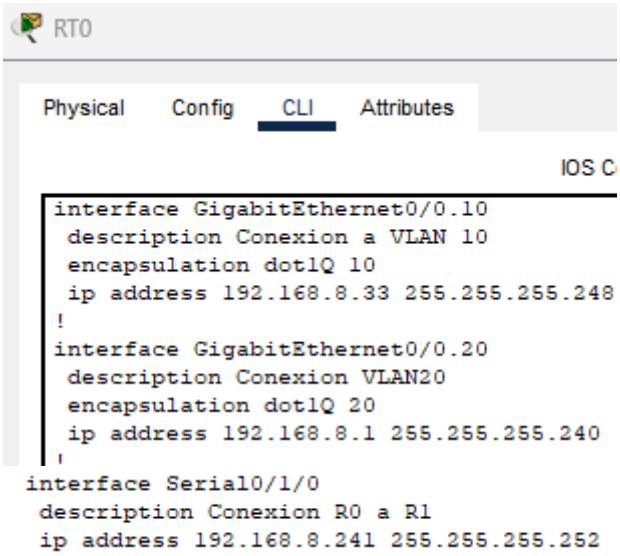
CONFIGURACIÓN CONECTIVIDAD ROUTER 0

El router 1 tiene 3 direcciones de red conectadas a él directamente:

192.168.8.240/29 por la interfaz Serial 0/1/0: Esta interfaz conecta con el router 1 y tiene la dirección ip de 192.168.8.241/30, utilizo esta conexión para más adelante enrutar para conocer las VLAN 30 y VLAN 40.

192.168.8.0/28 por la subinterfaz Gigabitethernet 0/0.20: Esta subinterfaz está configurada encapsulando el tráfico de la VLAN 20 con la ip 192.168.8.1/28

192.168.8.32/29 por la subinterfaz Gigabitethernet 0/0.10: Esta subinterfaz está configurada encapsulando el tráfico de la VLAN 10 con la ip 192.168.8.33/29

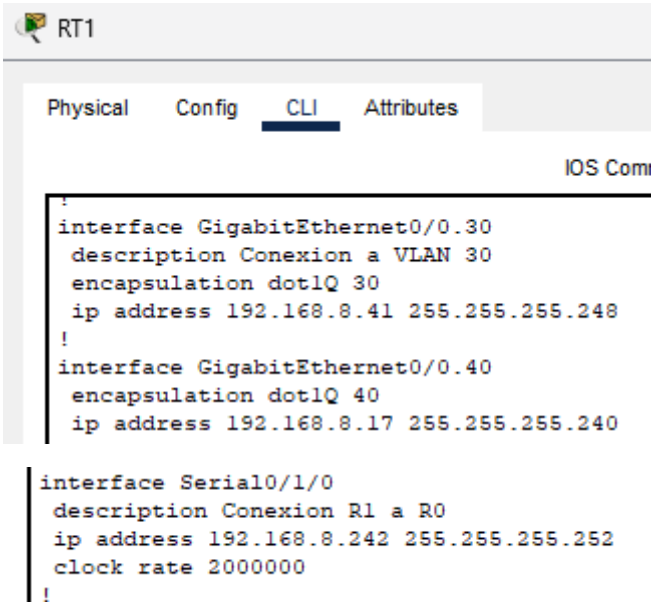


CONFIGURACIÓN CONECTIVIDAD ROUTER 1

192.168.8.240/29 por la interfaz Serial 0/1/0: Esta interfaz conecta con el router 0 y tiene la dirección ip de 192.168.8.242/30, utilizo esta conexión para más adelante enrutar para conocer las VLAN 10 y VLAN 20.

192.168.8.16/28 por la subinterfaz Gigabitethernet 0/0.40: Esta subinterfaz está configurada encapsulando el tráfico de la VLAN 40 con la ip 192.168.8.17/28

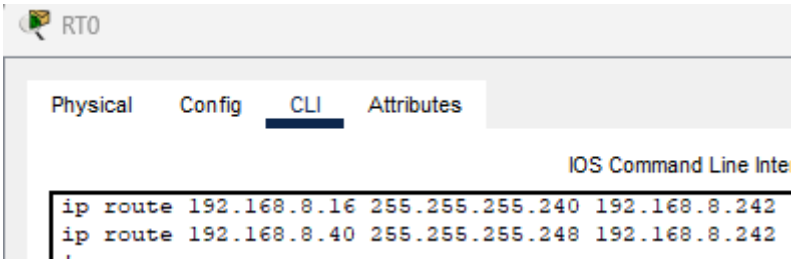
192.168.8.40/29 por la subinterfaz Gigabitethernet 0/0.30: Esta subinterfaz está configurada encapsulando el tráfico de la VLAN 30 con la ip 192.168.8.41/29



ENRUTAMIENTO ESTÁTICO R0

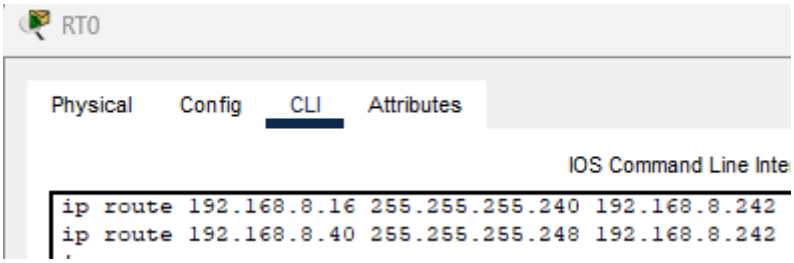
Para tener conectividad con redes que no están directamente conectadas al router lo podemos hacer mediante enrutamiento estático o dinámico, en mi caso lo hare con rutas estáticas.

R0 no tiene conexión directa con las VLAN 30 y VLAN 40 pero puede conocerlas creando una ruta estática mediante la ip de siguiente salto del router 1 que en su caso seria 192.168.8.242



ENRUTAMIENTO ESTÁTICO R1

R1 no tiene conexión directa con las VLAN 10 y VLAN 20 pero puede conocerlas creando una ruta estática mediante la ip de siguiente salto del router 1 que en su caso seria 192.168.8.242

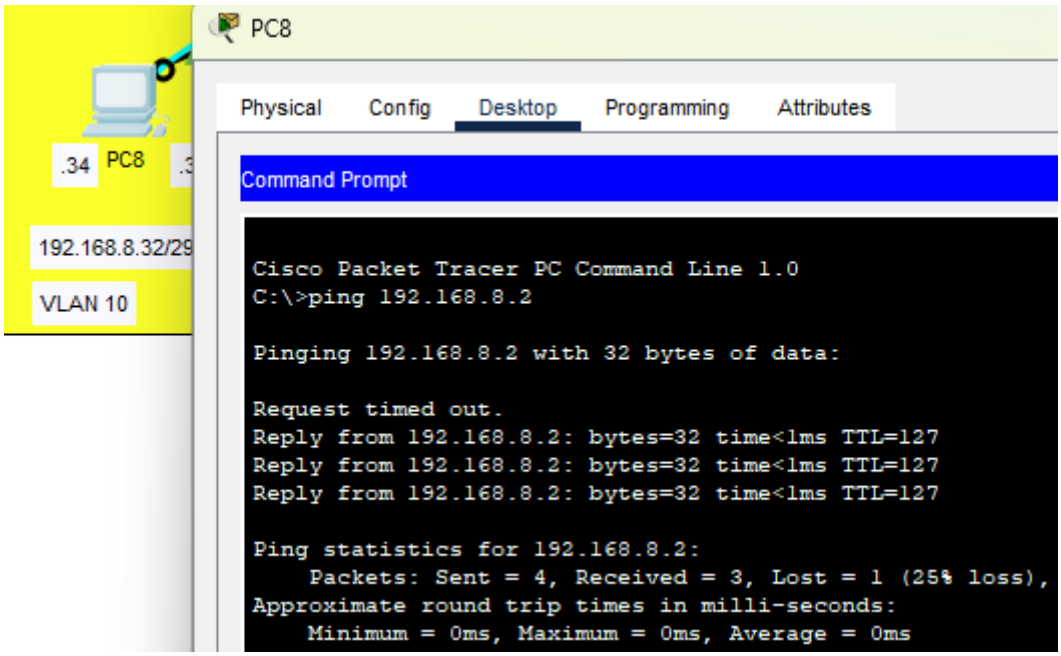


CONECTIVIDAD DE LA RED

Una vez ya hemos enrutado y realizado toda la configuración correspondiente cualquier dispositivo de la red se puede comunicar con todos.

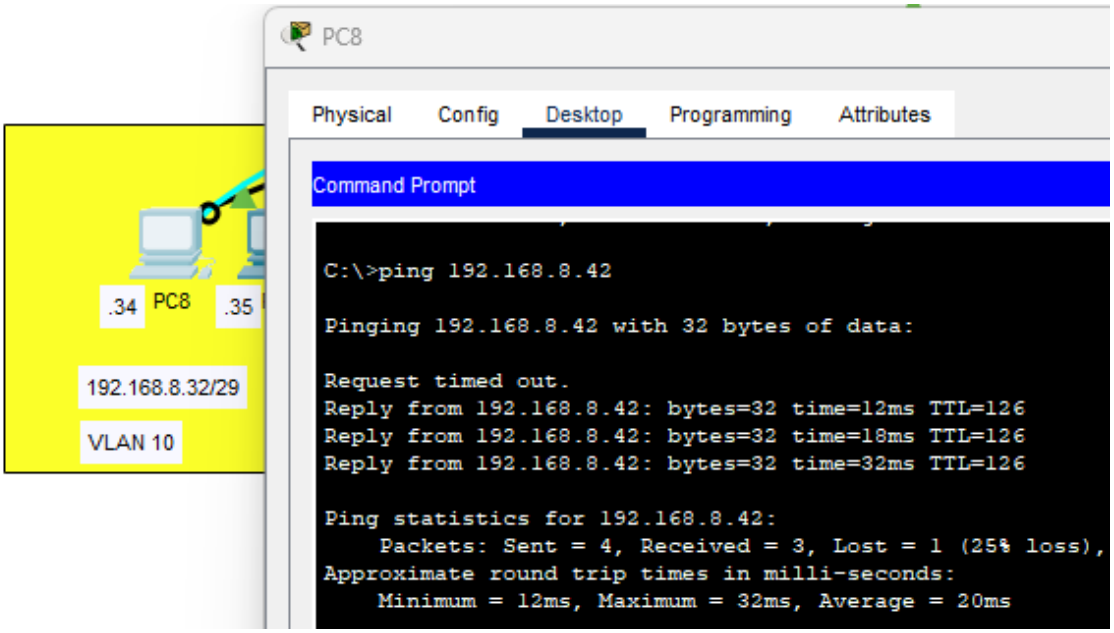
Conectividad LAN 10 – LAN 20

Hacemos ping desde un pc que pertenezca a la VLAN 10 a cualquier otro que pertenezca a la 20 y comprobamos conectividad.



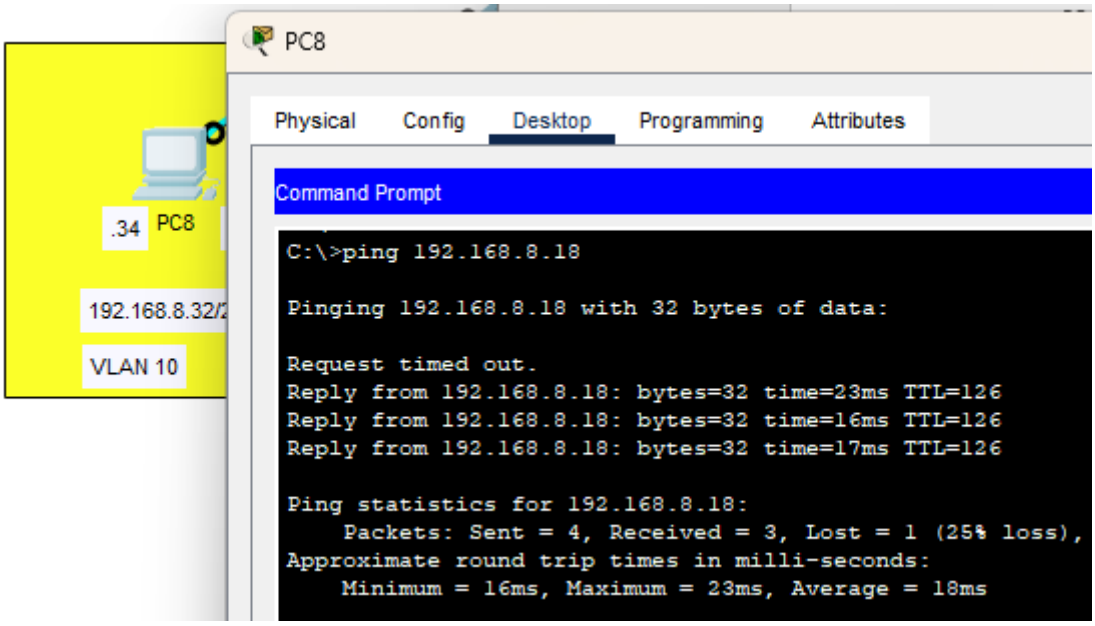
Conectividad LAN 10 – LAN 30

Hacemos ping desde un pc que pertenezca a la VLAN 10 a cualquier otro que pertenezca a la 30 y comprobamos conectividad.



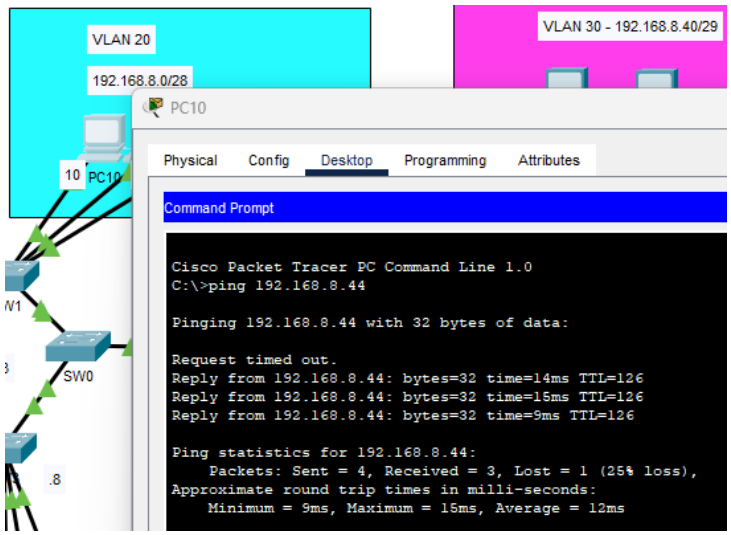
Conectividad LAN 10 – LAN 40

Hacemos ping desde un pc que pertenezca a la VLAN 10 a cualquier otro que pertenezca a la 30 y comprobamos conectividad.



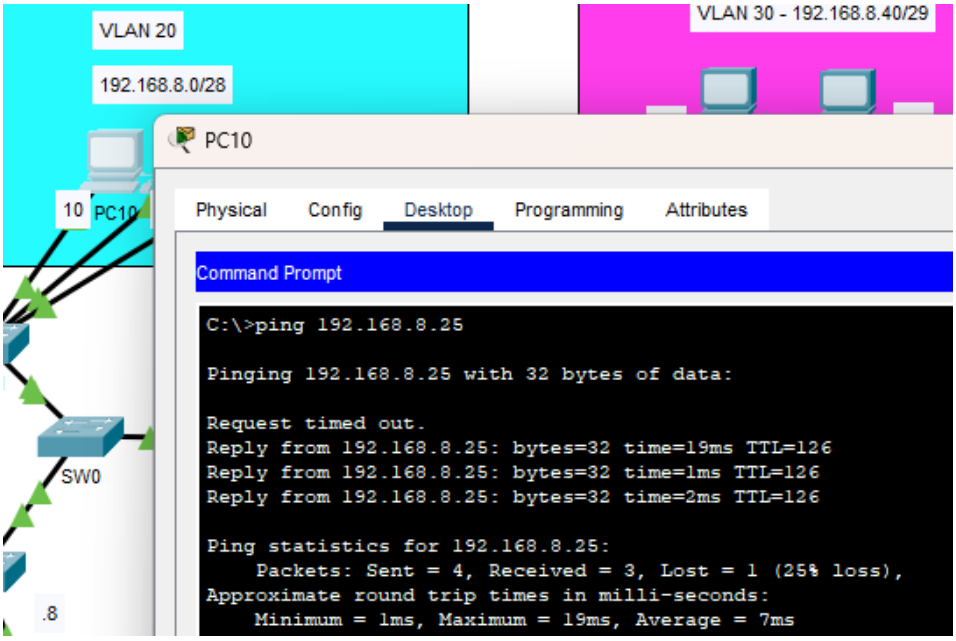
Conectividad LAN 20 – LAN 30

Hacemos ping desde un pc que pertenezca a la VLAN 20 a cualquier otro que pertenezca a la 30 y comprobamos conectividad.



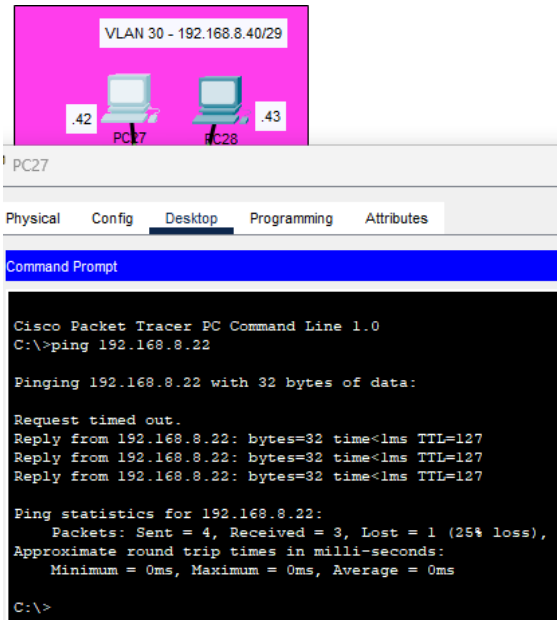
Conectividad LAN 20 – LAN 40

Hacemos ping desde un pc que pertenezca a la VLAN 20 a cualquier otro que pertenezca a la 40 y comprobamos conectividad.



Conectividad LAN 30 – LAN 40

Hacemos ping desde un pc que pertenezca a la VLAN 30 a cualquier otro que pertenezca a la 40 y comprobamos conectividad.



ACCESO REMOTO SEGURO

En la configuración inicial de Routers y switches se realizó la configuración de SSH.

Todas las redes tienen conectividad entre ellas y los switches tienen una ip asignada en la VLAN, por lo que se pueden administrar remotamente desde cualquier PC, debido a que todos los dispositivos tienen la misma configuración enseñare una captura de que se puede acceder a uno, por lo cual accederíamos de la misma forma a los demás.