

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
REDES DE COMPUTADORAS 2



MANUAL TÉCNICO
PRÁCTICA 1

Grupo 2	
201800476	Marvin Alexis Estrada Florian
201902781	Rodrigo Antonio Porón De León

ÍNDICE

INTRODUCCIÓN	3
IMPLEMENTACIÓN	4
Topología implementada	4
Configuración de Ip	4
Hostname y Contraseña en Switches	6
CONFIGURACIÓN DE VTP	7
ELECCIÓN DE ESCENARIO CON MEJOR CONVERGENCIA	12
PVST	13
Rapid PVST	16
Elección de escenario (Conclusión)	20
POLÍTICAS DE PUERTO COMPARTIDAS	20
Activar el port-security en todos los puertos de acceso	20
Configuración de port-security con mac-address	22

INTRODUCCIÓN

Pandora, es un colegio que se dedica a la enseñanza de niños desde la primaria hasta diversificado. Se tiene la problemática que el nuevo personal de informática, no conoce a su totalidad la funcionalidad de la red LAN del colegio, por lo cual se les brindará asesoría y configuraciones necesarias para solventar las necesidades que actualmente requieren.

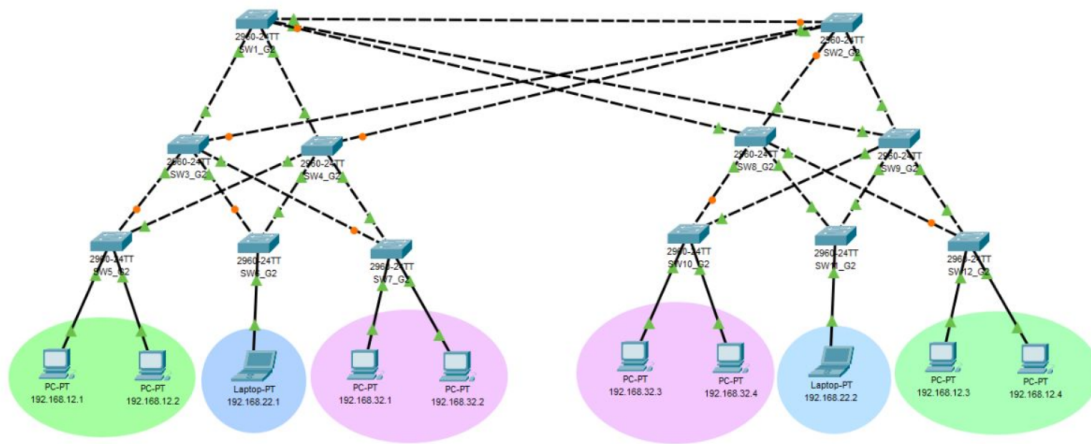
Inicialmente se llevaba un registro de direcciones IP utilizadas y un diagrama de los puertos y switches conectados, pero mientras el colegio creció, aumentaron sus switches y sus conexiones para todas las áreas y se perdió el orden. El nuevo personal de informática notó que habitualmente hay pérdidas de paquetes en las conexiones entre los departamentos y no saben por qué.

El plan del colegio, es verificar que la red se encuentre en orden y que las configuraciones que dejó el personal anterior, sean la solución más óptima y rápida para la comunicación entre sus distintos departamentos. El departamento de informática espera de la asesoría para poder implementar este sistema de la mejor manera posible.

IMPLEMENTACIÓN

Topología implementada

Se utilizó la herramienta Packet Tracer para la implementación de la topología solicitada, constando de 12 switches y 10 PC-PT, cada switch configurado con sus respectivos puertos troncales y de acceso como se detalla más adelante:



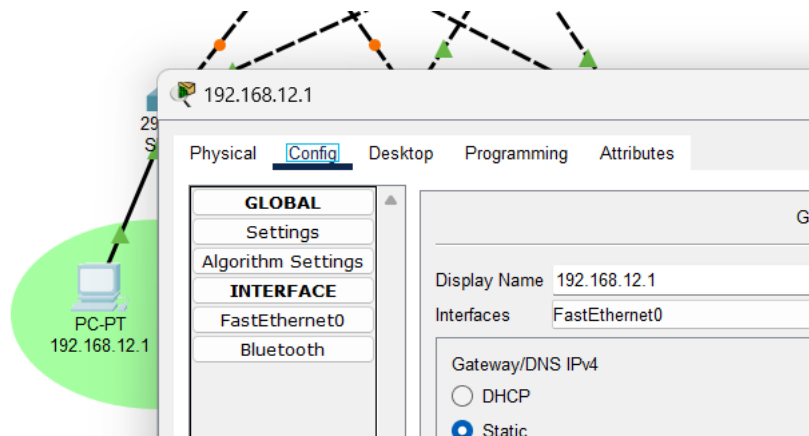
Configuración de Ip

Cada PC-PT posee una ip determinada con la siguientes direcciones de red:

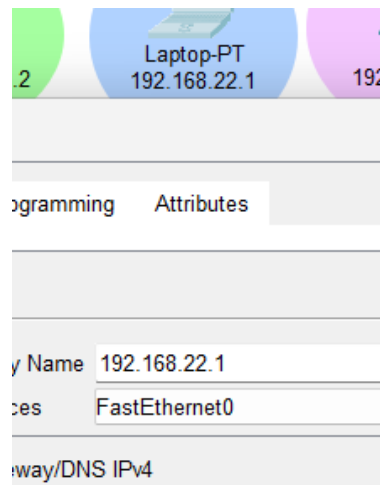
Red	Dirección
Primaria	192.168.12.0/24
Básicos	192.168.22.0/24
Diversificado	192.168.32.0/24

Por lo que se procede a configurar la respectiva Ip sobre estas, donde a continuación se muestra un ejemplo de este proceso sobre cada red solicitada:

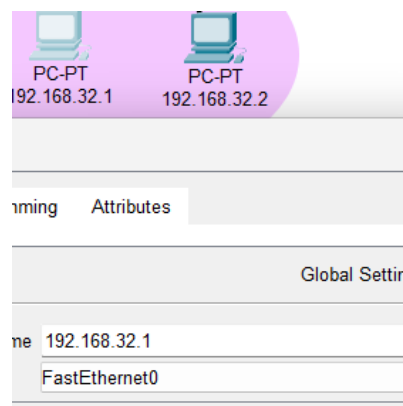
- Primaria



- Básicos

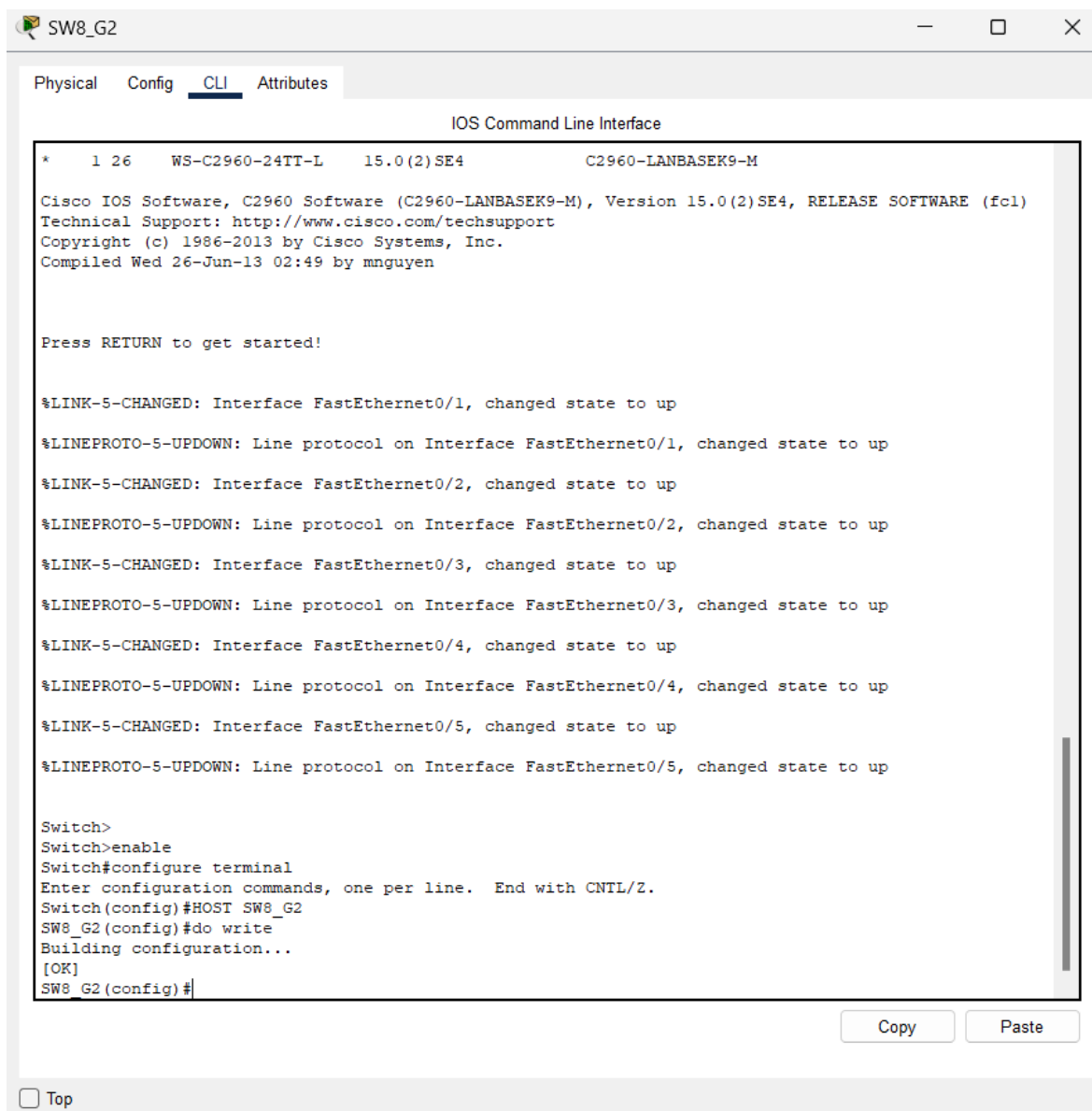


- Diversificado



Hostname y Contraseña en Switches

Como se muestra en la siguiente imagen, se tiene el comando HOST, el cual procede a cambiarle la etiqueta o nombre a un switch, esto aplicado sobre todos los switches de toda la topología:



```
*      1 26      WS-C2960-24TT-L      15.0(2)SE4      C2960-LANBASEK9-M

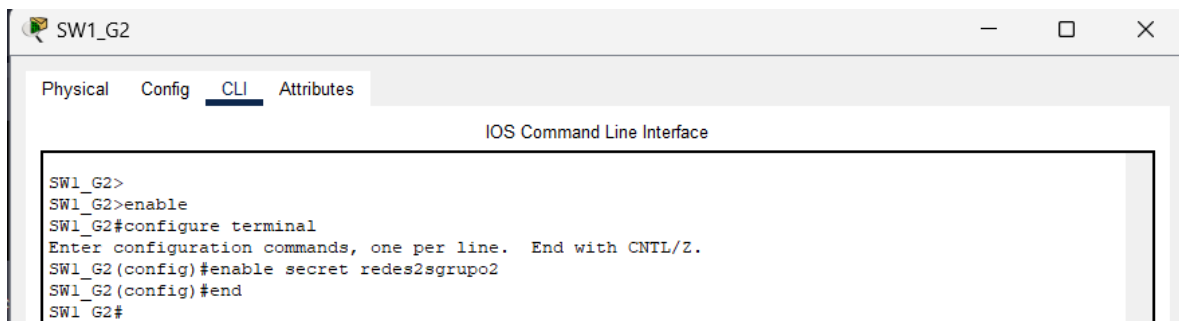
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#HOST SW8_G2
SW8_G2(config)#do write
Building configuration...
[OK]
SW8_G2(config)#
```

Se procedió a la colocación de contraseña encriptada, esto únicamente aplicado sobre el server switch SW1_G2, de la siguiente manera:



```
SW1_G2>
SW1_G2>enable
SW1_G2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1_G2(config)#enable secret redes2sgupo2
SW1_G2(config)#end
SW1_G2#
```

Por lo que para una correcta verificación de una contraseña encriptada, se observa el siguiente comando:

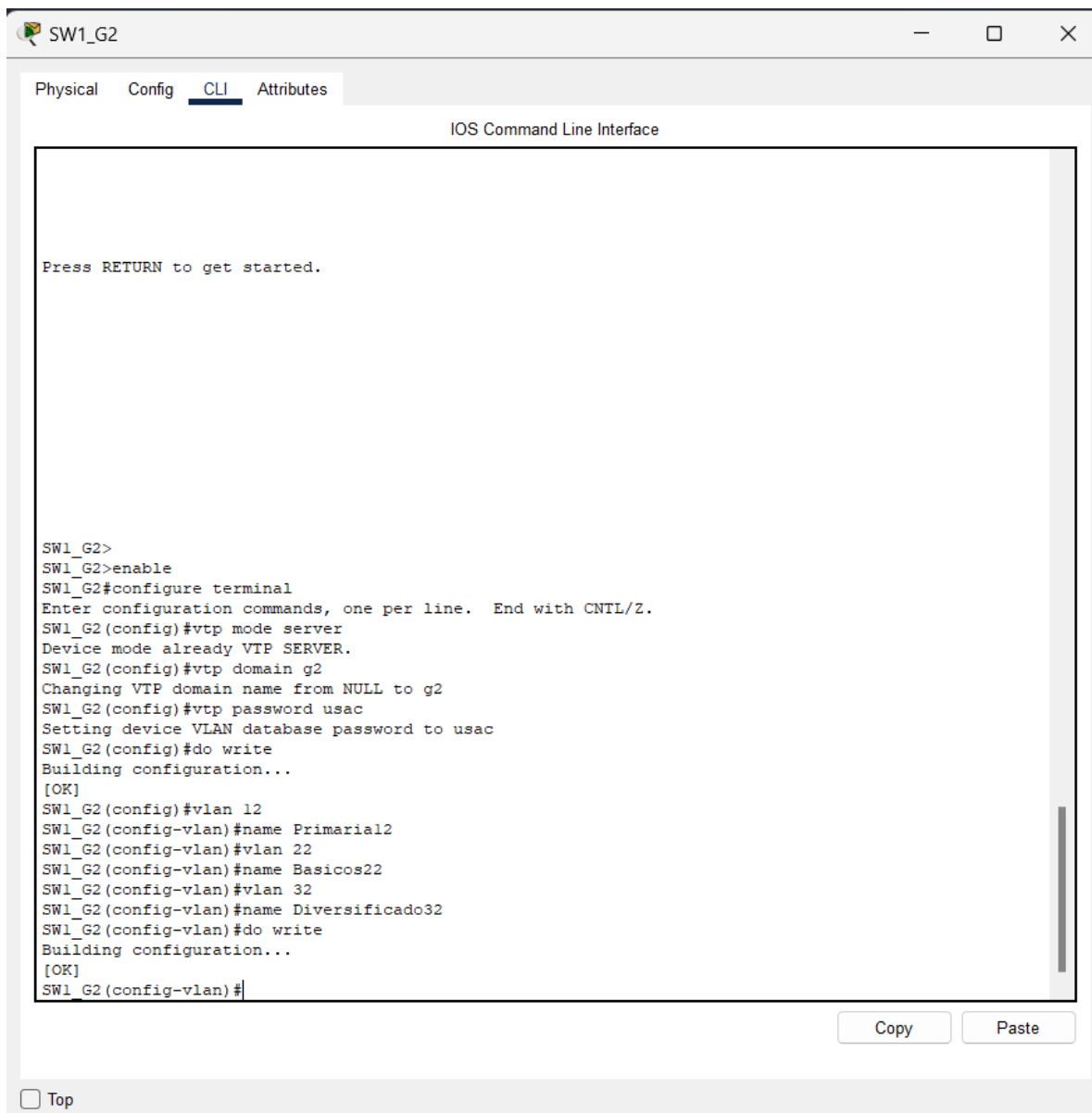
```
SW1_G2#show running-config | include enable secret
enable secret 5 $l$mERr$IMPc0kFzQ4BjnNivSgfZ0.
SW1_G2#
```

Configuración de VTP

Iniciando esta configuración se tomó como base las VLAN's solicitadas, como se muestra a continuación en la tabla:

Nombre	Número
Primaria	12
Básicos	22
Diversificado	32

Para realizar esta configuración, se seleccionó al switch SW1_G2 para ser el servidor VTP, por lo que a continuación se muestra su proceso, donde se agrega el dominio g2 y contraseña usac, para luego agregarle las VLAN's solicitadas:



Posteriormente, así como se configuró el switch server, se procedió a configurar todos los demás switches como clientes, de la siguiente forma:

The screenshot shows a web-based CLI interface for a switch named SW5_G2. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main area displays the IOS Command Line Interface. The text shows the switch is now available and prompts the user to press RETURN. The configuration session starts with 'enable', followed by 'configure terminal'. The user sets the VTP mode to client, domain to g2, and password to usac. Then, they configure interfaces Fa0/1-2 as access ports in VLAN 12. The configuration is saved with 'do write'. The session ends with 'SW5_G2(config-if-range)#'.

```
SW5_G2 con0 is now available

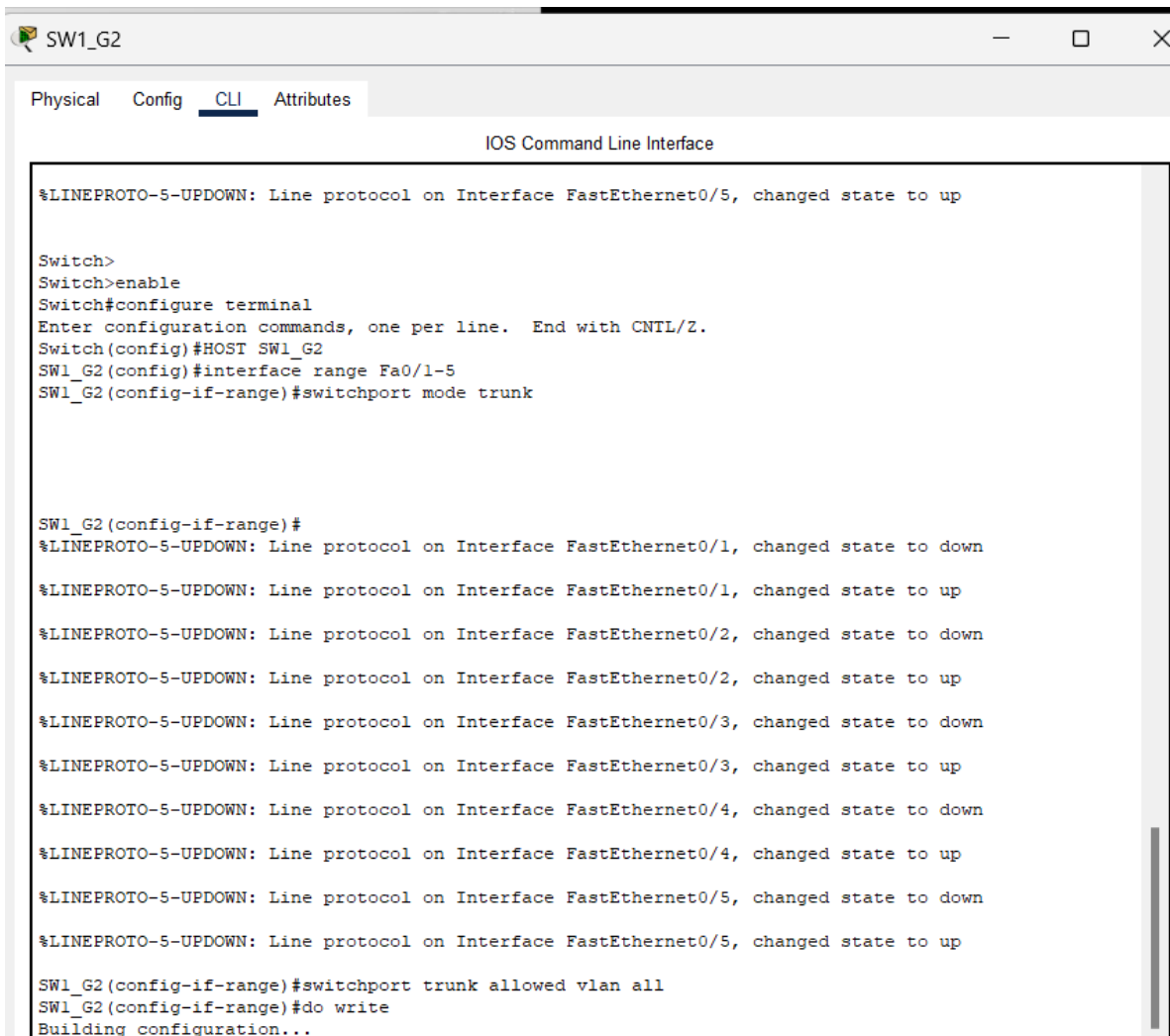
Press RETURN to get started.

SW5_G2>
SW5_G2>enable
SW5_G2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW5_G2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW5_G2(config)#vtp domain g2
Changing VTP domain name from NULL to g2
SW5_G2(config)#vtp password usac
Setting device VLAN database password to usac
SW5_G2(config)#do write
Building configuration...
[OK]
SW5_G2(config)#
SW5_G2(config)#interface range Fa0/1-2
SW5_G2(config-if-range)#switchport mode access
SW5_G2(config-if-range)#switchport access vlan 12
SW5_G2(config-if-range)#do write
Building configuration...
[OK]
SW5_G2(config-if-range)#
```

Buttons: Copy, Paste

☐ Top

Para aceptar el tráfico de paquetes de las VLAN's, se procedió a la colocación de las respectivas interfaces en modo truncal, esta configuración se aplicó a todos los switches que no tenían contacto directo con un dispositivo final:



The screenshot shows a network switch CLI window titled "SW1_G2". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The title bar also includes standard window controls (minimize, maximize, close). The main area is titled "IOS Command Line Interface" and displays the following text:

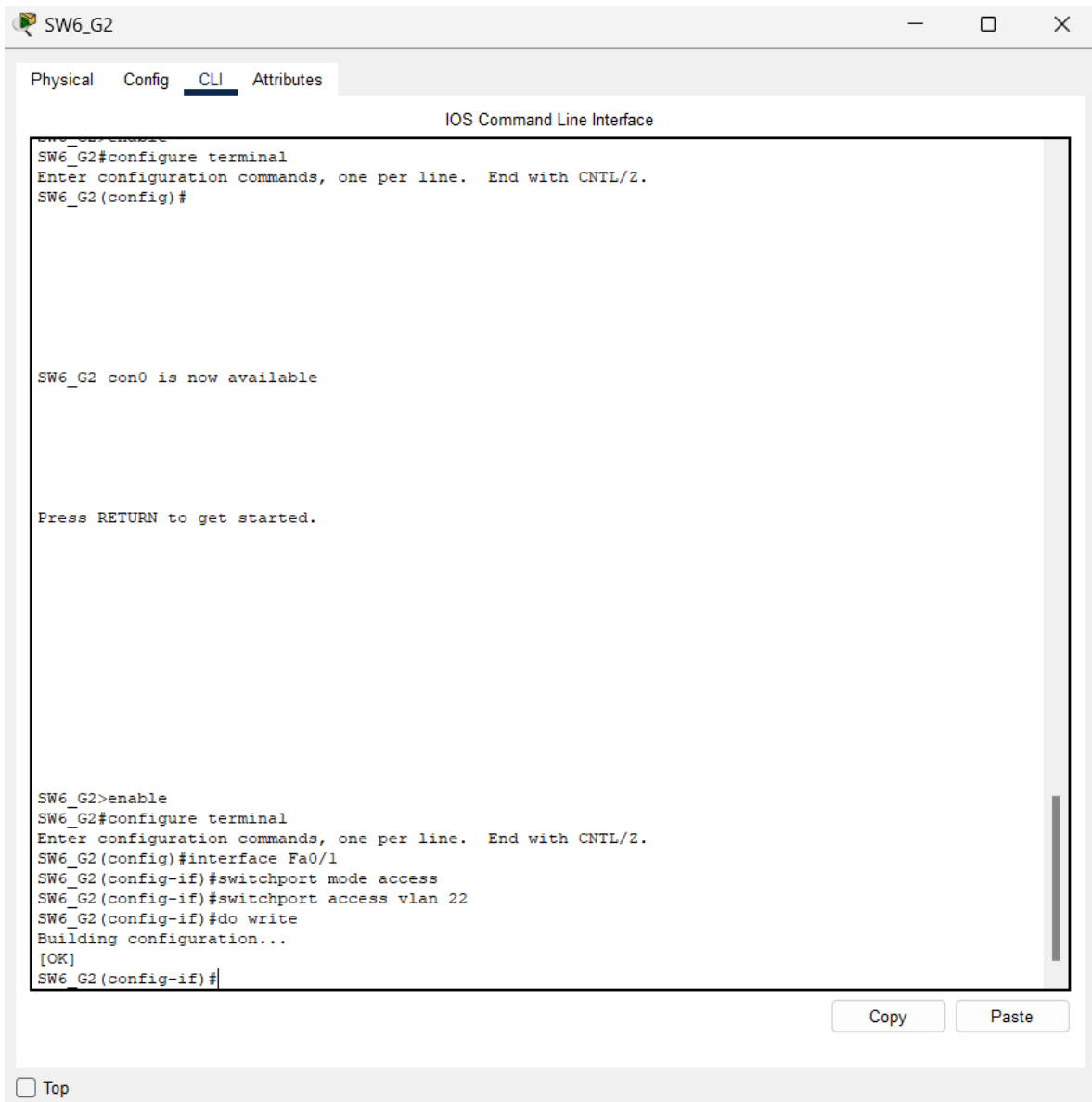
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#HOST SW1_G2
SW1_G2(config)#interface range Fa0/1-5
SW1_G2(config-if-range)#switchport mode trunk

SW1_G2(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

SW1_G2(config-if-range)#switchport trunk allowed vlan all
SW1_G2(config-if-range)#do write
Building configuration...
```

Esta configuración, al contrario del troncal, se utilizó para únicamente dejar pasar los paquetes según correspondía la vlan, por lo que en la imagen que se muestra a continuación se tiene la implementación de las interfaces en modo acceso, con contacto directo a dispositivos finales:



Por último, se tiene la prueba de envío de ping entre redes, enviandose desde 192.168.12.1 a 192.168.12.3 y 192.168.12.4, las cuales si pertenecen a su VLAN, pero 192.168.22.1 al no pertenecer a la misma, rechaza los paquetes correctamente:

```
192.168.12.1
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Reply from 192.168.12.3: bytes=32 time=1ms TTL=128
Reply from 192.168.12.3: bytes=32 time=6ms TTL=128
Reply from 192.168.12.3: bytes=32 time<1ms TTL=128
Reply from 192.168.12.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>ping 192.168.12.4

Pinging 192.168.12.4 with 32 bytes of data:

Reply from 192.168.12.4: bytes=32 time=11ms TTL=128
Reply from 192.168.12.4: bytes=32 time=6ms TTL=128
Reply from 192.168.12.4: bytes=32 time<1ms TTL=128
Reply from 192.168.12.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

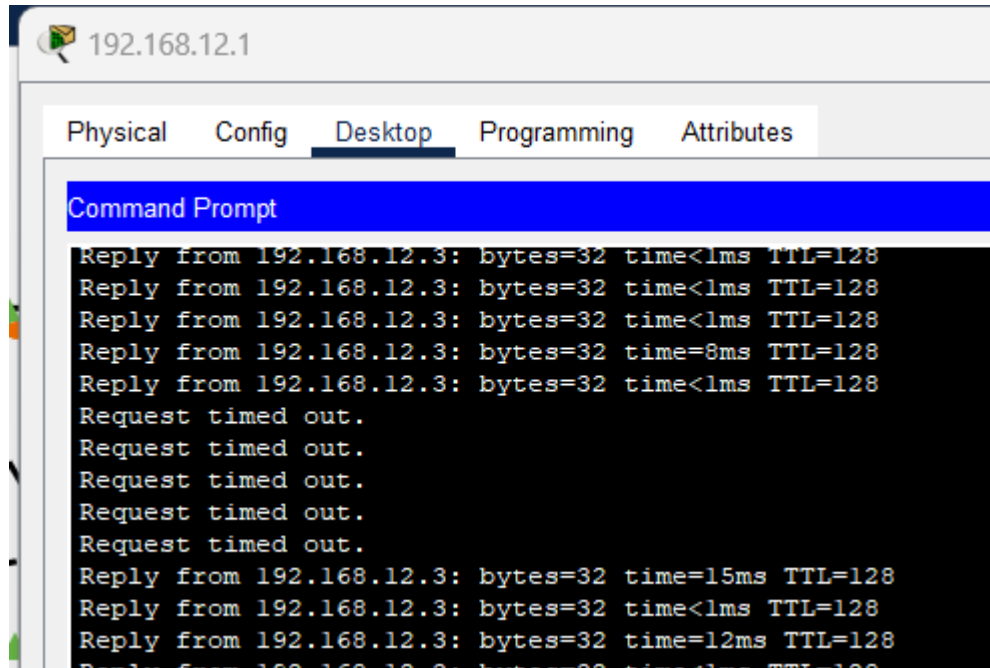
C:\>
```

Elección de escenario con mejor convergencia

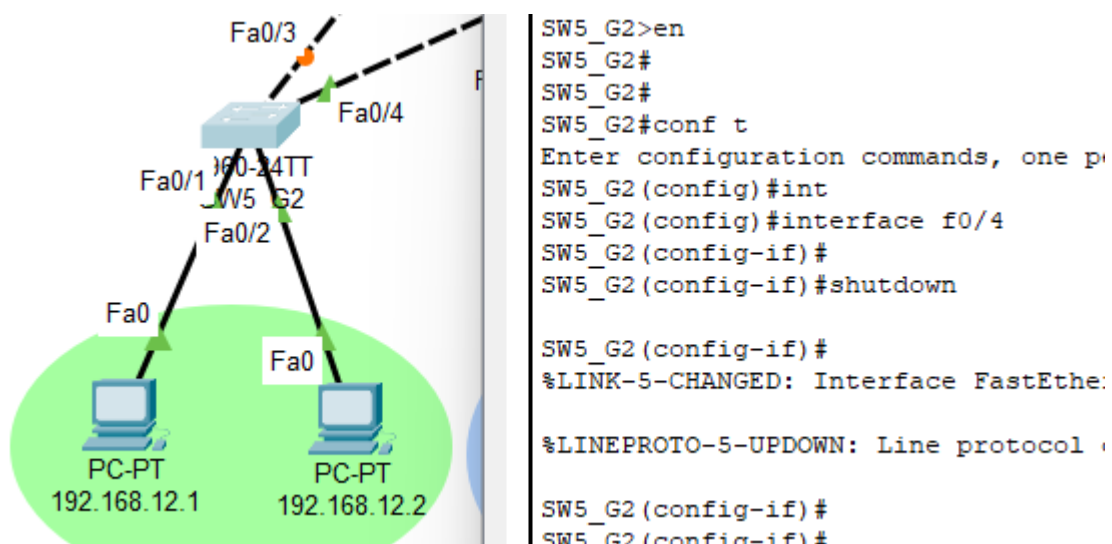
En este apartado se tiene la elección del mejor escenario de convergencia, donde se tenga el tiempo más óptimo detectado a través de las dos configuraciones solicitadas, por lo que se procedió a realizarlo de la siguiente manera:

PVST

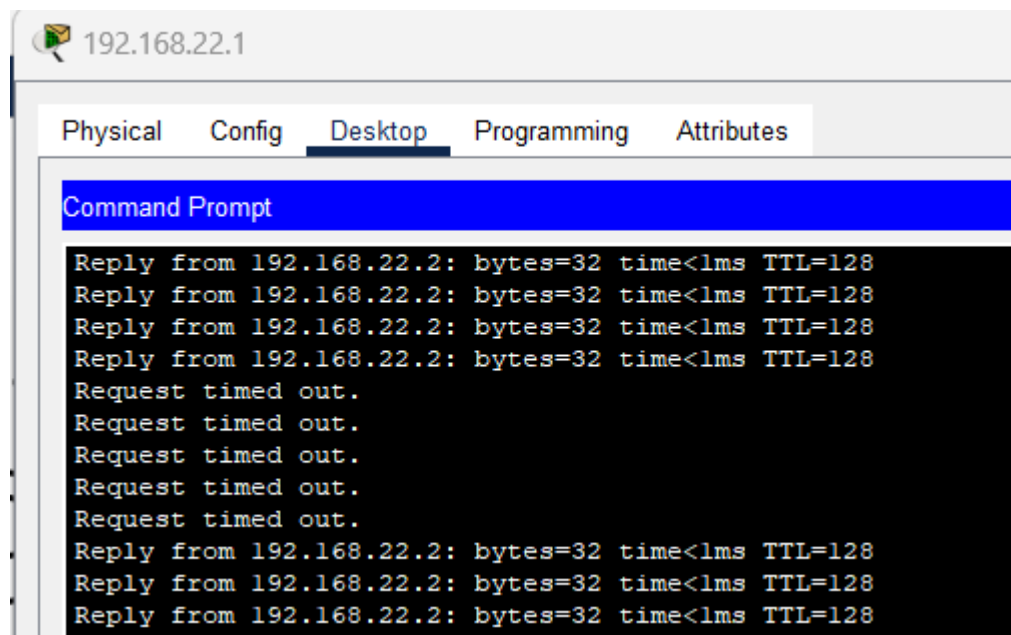
- Red Primaria



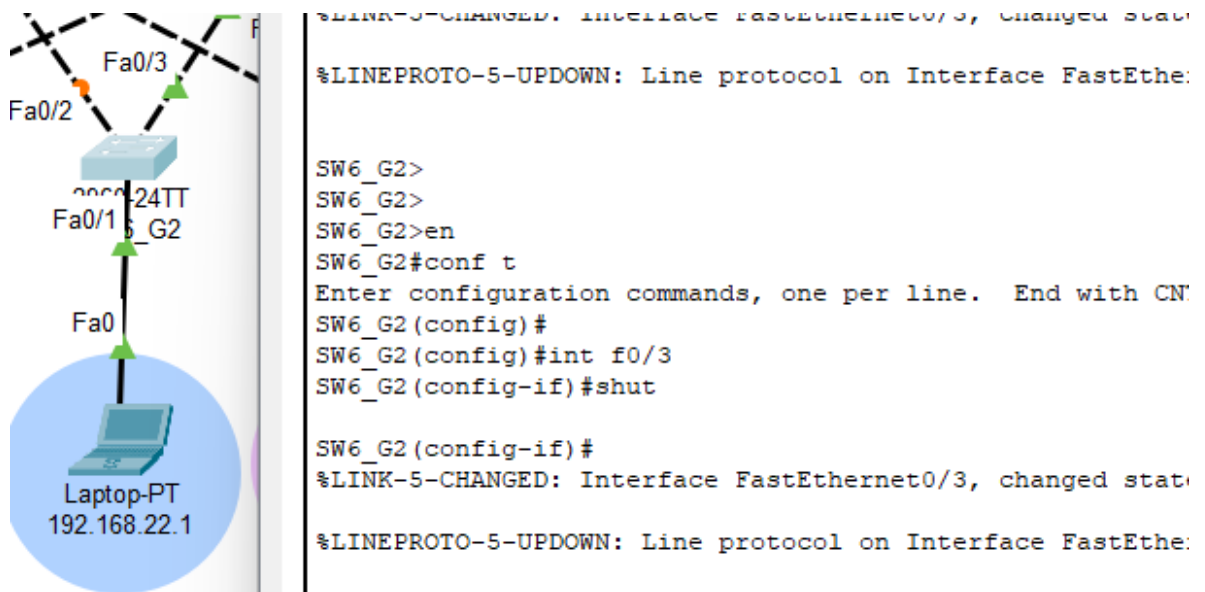
Se comenzó a hacer un ping extendido desde la PC 192.168.12.1 a la PC 192.168.12.3, se procedió a apagar el enlace que permitía la comunicación entre estas dos vlans y se observó que el tiempo de convergencia fue de 35 segundos.



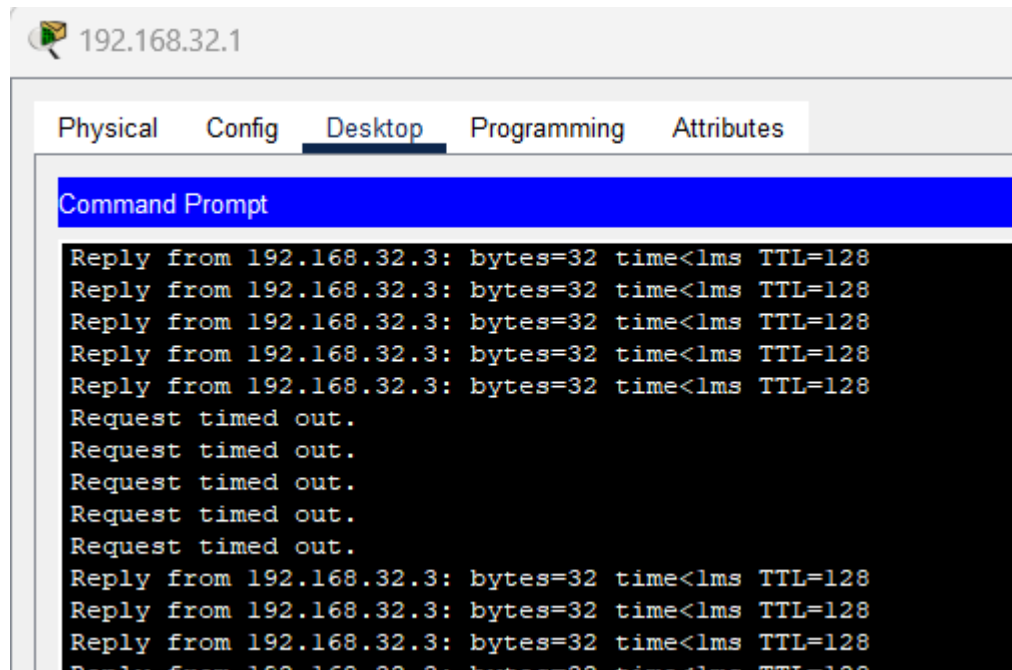
- Red Básicos



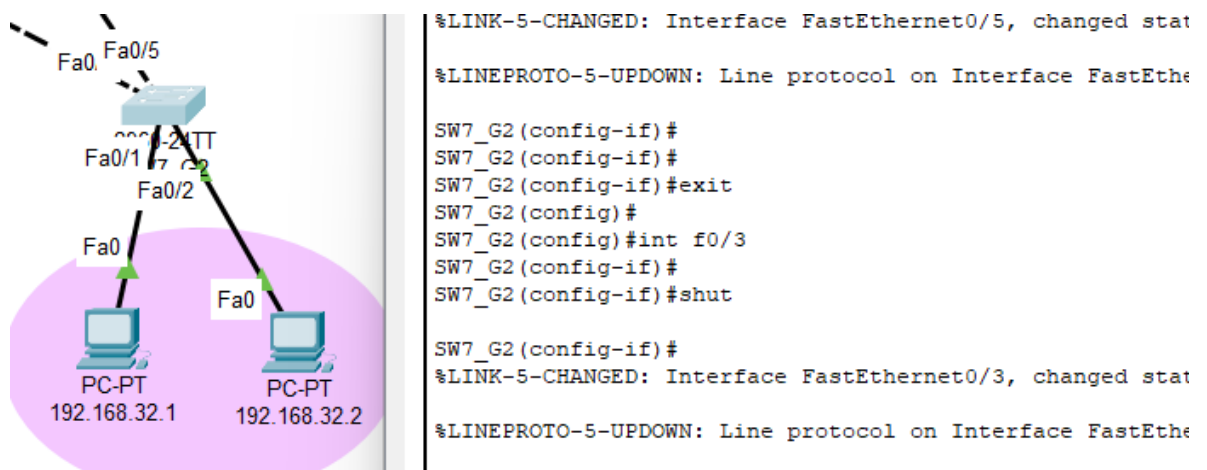
Se realizó el mismo procedimiento que en la red primaria, se hizo un ping extendido desde la PC 192.168.22.1 hacia la PC 192.168.22.2, se apagó el enlace que permitía la comunicación entre estas dos vlans y se observó que el tiempo de convergencia fue de 34 segundos.



- Red Diversificado



Al igual que en la medición de convergencias anteriores, se hizo un ping extendido desde la PC 192.168.32.1 hacia la PC 192.168.32.3, se apagó el enlace que permitía la comunicación entre estas dos vlans y se observó que el tiempo de convergencia fue de 33.20 segundos.



Rapid PVST

Rapid PVST es un protocolo que permite la convergencia de la red de manera más rápida que PVST, esto se debe a que se implementa el protocolo RSTP en cada vlan, por lo que se tiene un árbol de expansión por cada vlan.

Para hacer uso de este modo se configuró en todos los switch lo siguiente:

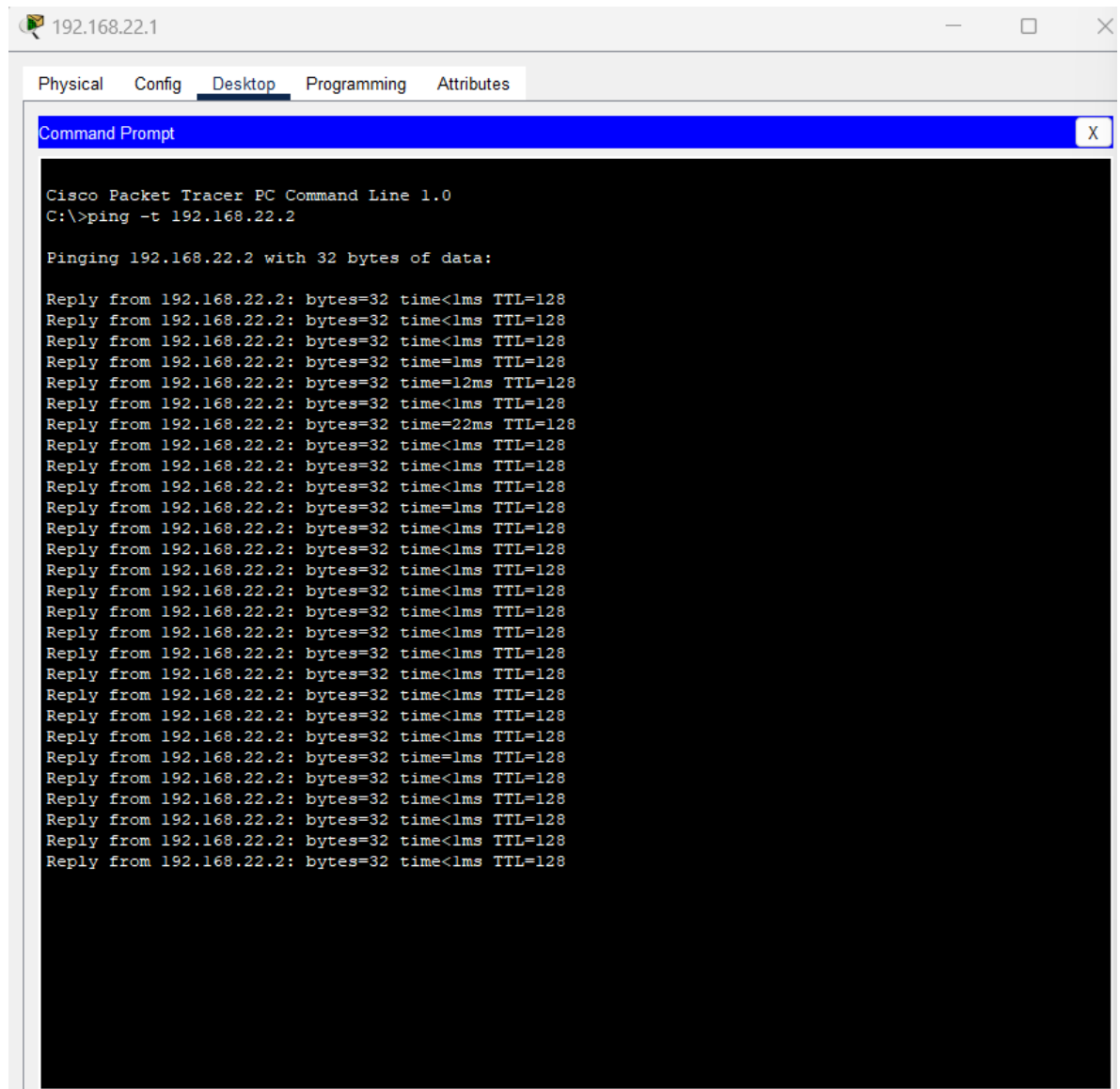
```
SW1_G2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1_G2(config)#
SW1_G2(config)#span
SW1_G2(config)#spanning-tree mode r
SW1_G2(config)#spanning-tree mode rapid-pvst
SW1_G2(config)#exit
SW1_G2#
%SYS-5-CONFIG_I: Configured from console by console
```

Lo cual es la configuración para que los switches utilicen el protocolo Rapid PVST en lugar de PVST.

Para todas las redes se realizó el mismo procedimiento que en PVST, se utilizaron los mismos hosts y se apagaron los mismos enlaces, los resultados fueron los siguientes:

- Red Primaria

Se hizo un ping extendido desde la PC 192.168.12.1 hacia la PC 192.168.12.3. La convergencia fue inmediata, no se perdió ningún paquete.



- Red Diversificado

Se hizo un ping extendido desde la PC 192.168.32.1 hacia la PC 192.168.32.3. La convergencia fue inmediata, no se perdió ningún paquete. Algo que se observó en esta red es que al momento de activar el enlace que se había apagado, se perdió un paquete.

The screenshot shows a Packet Tracer desktop environment with a window titled '192.168.32.1'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window contains the following text:

```

Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=15ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=13ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.32.3: bytes=32 time=1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128
Reply from 192.168.32.3: bytes=32 time<1ms TTL=128

```

Escenario	Protocolo Spanning-Tree	Primaria	Básicos	Diversificado
1	PVST	35s	34s	33.20s
2	Rapid PVST	0s	0s	0s

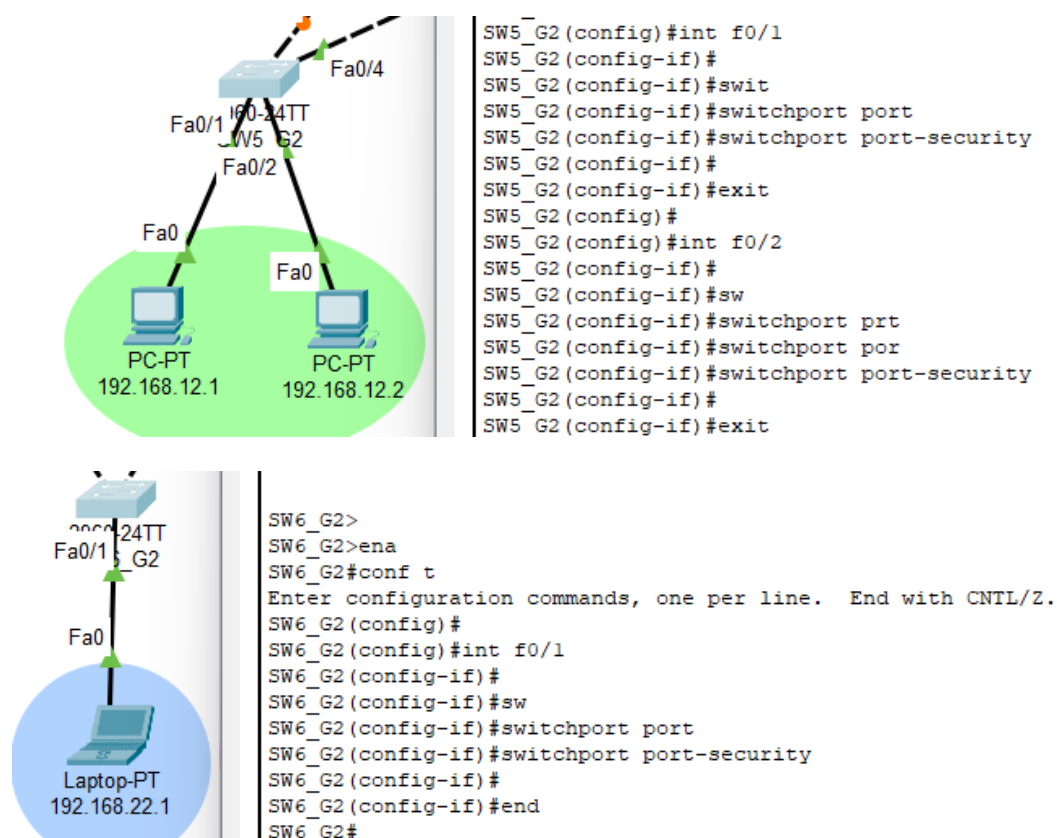
Elección de escenario (Conclusión)

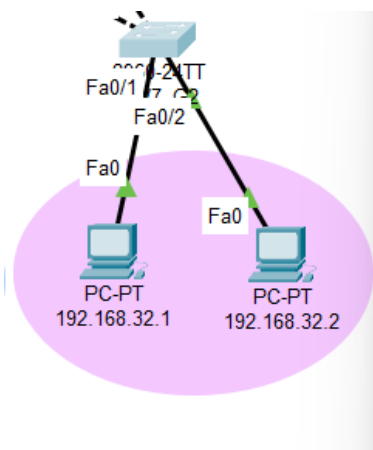
Se eligió el escenario 2, ya que la convergencia es inmediata, no se pierden paquetes y se tiene un árbol de expansión por cada vlan, lo cual permite que la red sea más eficiente. Por lo que tomando como referencia un caso de la vida real, el protocolo Rapid PVST es el más adecuado para la mayoría de las redes y en este caso, para la red que se está trabajando.

Políticas de puerto compartidas

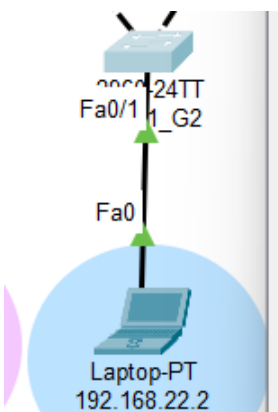
Activar el port-security en todos los puertos de acceso

El port-security es una característica que permite limitar el número de direcciones MAC que se pueden aprender en un puerto de acceso, esto con el fin de evitar ataques de tipo MAC flooding. Para activar el port-security en todos los puertos de acceso se ingresó a la interfaz fastEthernet del enlace que conecta al host y se configuró lo siguiente:



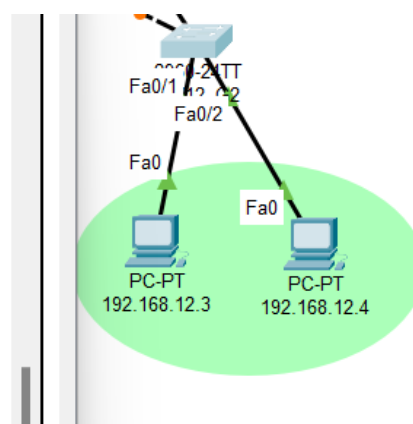


```
SW7_G2>enab
SW7_G2#conf t
Enter configuration commands, one per line. End with
SW7_G2(config)#int f0/1
SW7_G2(config-if)#
SW7_G2(config-if)#swit
SW7_G2(config-if)#switchport port
SW7_G2(config-if)#switchport port-security
SW7_G2(config-if)#
SW7_G2(config-if)#exit
SW7_G2(config)#
SW7_G2(config)#int f0/2
SW7_G2(config-if)#
SW7_G2(config-if)#swit
SW7_G2(config-if)#switchport port
SW7_G2(config-if)#switchport port-security
SW7_G2(config-if)#
SW7_G2(config-if)#end
```



```
SW11_G2>
SW11_G2>en
SW11_G2#conf t
Enter configuration commands, one per line. End with
SW11_G2(config)#
SW11_G2(config)#int f0/1
SW11_G2(config-if)#
SW11_G2(config-if)#swit
SW11_G2(config-if)#switchport por
SW11_G2(config-if)#switchport port-security
SW11_G2(config-if)#
SW11_G2(config-if)#end
SW11_G2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
SW12_G2#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
SW12_G2(config)#
SW12_G2(config)#int f0/1
SW12_G2(config-if)#swit
SW12_G2(config-if)#switchport port
SW12_G2(config-if)#switchport port-security
SW12_G2(config-if)#
SW12_G2(config-if)#exit
SW12_G2(config)#
SW12_G2(config)#int f0/2
SW12_G2(config-if)#
SW12_G2(config-if)#swit
SW12_G2(config-if)#switchport po
SW12_G2(config-if)#switchport port-security
SW12_G2(config-if)#
SW12_G2(config-if)#end
```



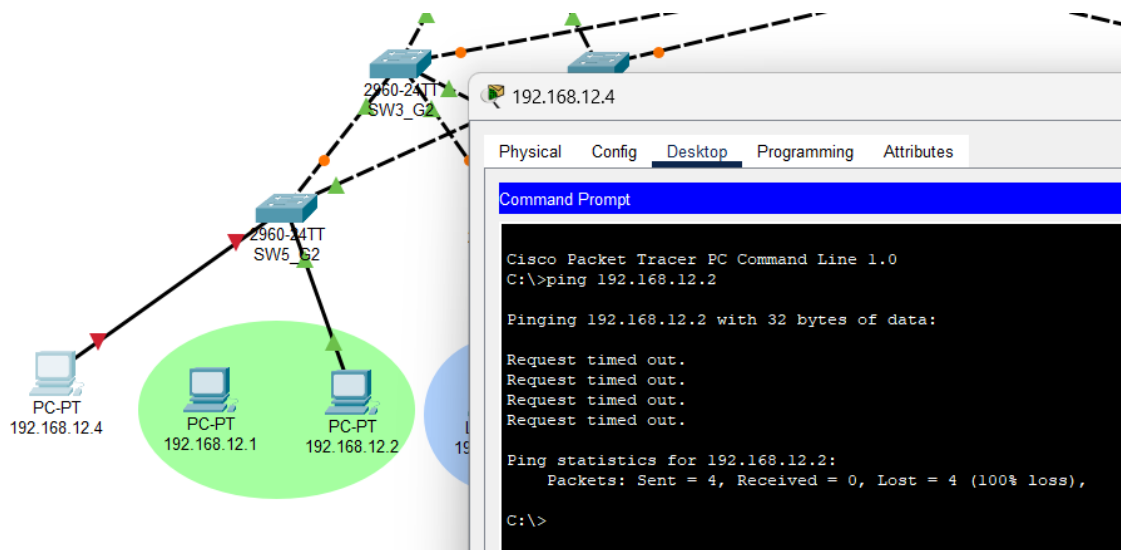
Cada imagen anterior corresponde a la configuración de cada switch que tiene un enlace hacia un host. En este caso se configuró el port-security para que solo se aprende una dirección MAC en cada puerto de acceso.

Configuración de port-security con mac-address en todos los puertos de acceso

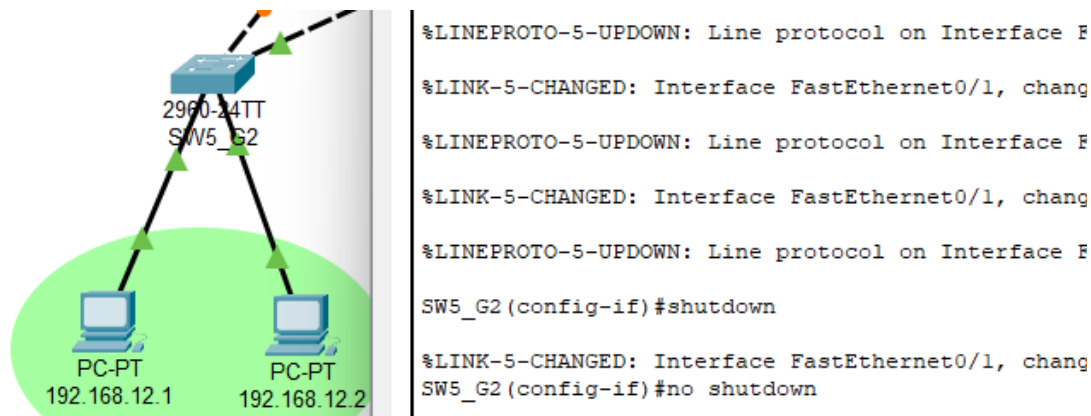
A continuación se muestra la configuración de la mac-address permitida para cada puerto con modo acceso, ingresando la correspondiente a cada PC-PT conectada a su respectiva interfaz de cada switch:

```
SW5_G2>
SW5_G2>enable
SW5_G2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW5_G2(config)#interface f0/1
SW5_G2(config-if)#switchport port-security
SW5_G2(config-if)#switchport port-security mac-address 00E0.F7EA.A0C3
SW5_G2(config-if)#do write
Building configuration...
[OK]
SW5_G2(config-if)#
```

Por lo que se procedió a realizar la conexión de otra PC-PT de la misma VLAN para la comprobación del funcionamiento del security-port, por lo que al hacer ping de 192.168.12.4 a 192.168.12.2 las solicitudes son bloqueadas y el puerto procede a apagarse:



Luego se procedió a reconectar la PC-PT correspondiente y volviendo a encender el puerto del switch, el cual se apagó por el procedimiento anterior de la siguiente forma:

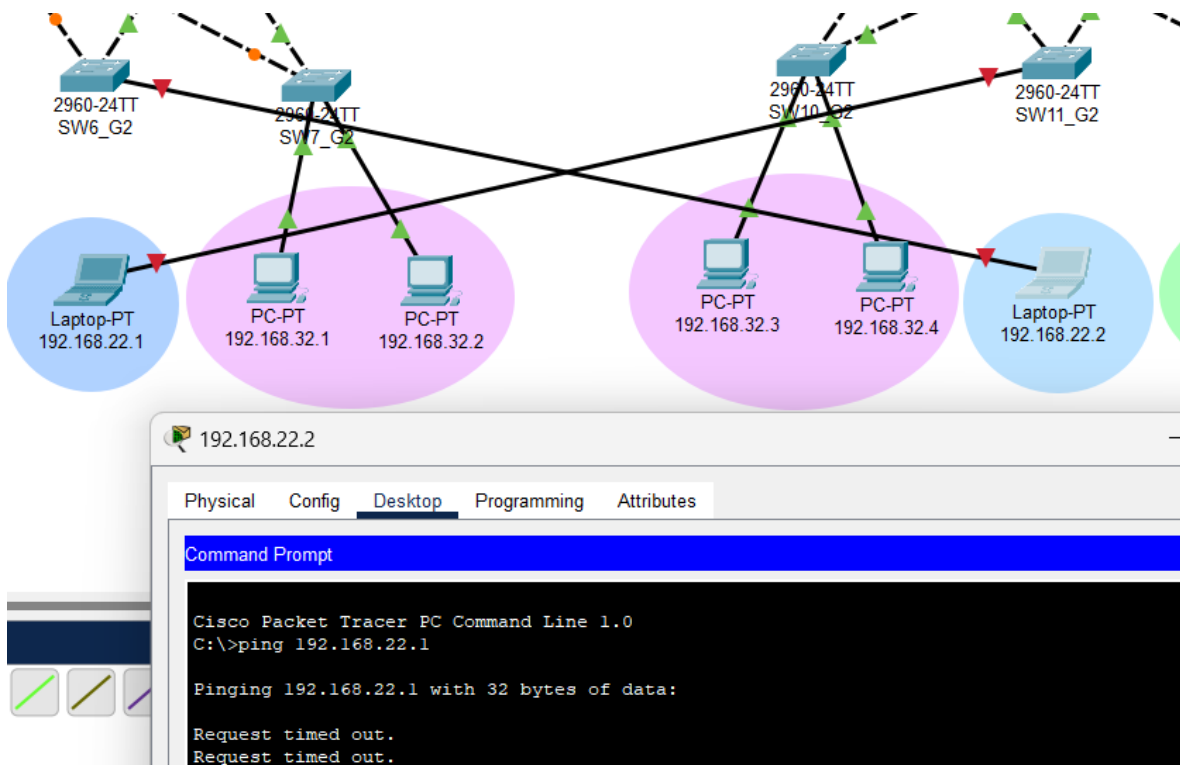


En el caso de tener un switch con dos interfaces, se muestra el detalle de cómo se configuró en su totalidad el switch con port-security, cada una con su respectiva mac-address de su PC-PT correspondiente, de la siguiente manera:

```

SW10_G2>
SW10_G2>
SW10_G2>enable
SW10_G2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW10_G2(config)#interface f0/1
SW10_G2(config-if)#switchport port-security
SW10_G2(config-if)#switchport port-security mac-address 0001.96D5.8CE2
SW10_G2(config-if)#do write
Building configuration...
[OK]
SW10_G2(config-if)#interface f0/2
SW10_G2(config-if)#switchport port-security
SW10_G2(config-if)#switchport port-security mac-address 0010.1132.7801
SW10_G2(config-if)#do write
Building configuration...
[OK]
SW10_G2(config-if)#
  
```

Se muestra un ejemplo en la red de Básicos, conectando diferentes PC-PT a cada switch, observando que los puertos se apagan y no envían los paquetes de ping enviados desde 192.168.22.1 a 192.168.22.2 y viceversa:



Por último se tiene otro ejemplo de la red de Diversificado, conectando las mismas PC-PT en su switch pero invirtiendo el puerto conectado, observando que los puertos se apagan y no envían los paquetes de ping desde 192.168.32.1 y 192.168.32.2 hacia 192.168.32.3 y 192.168.32.4 respectivamente:

