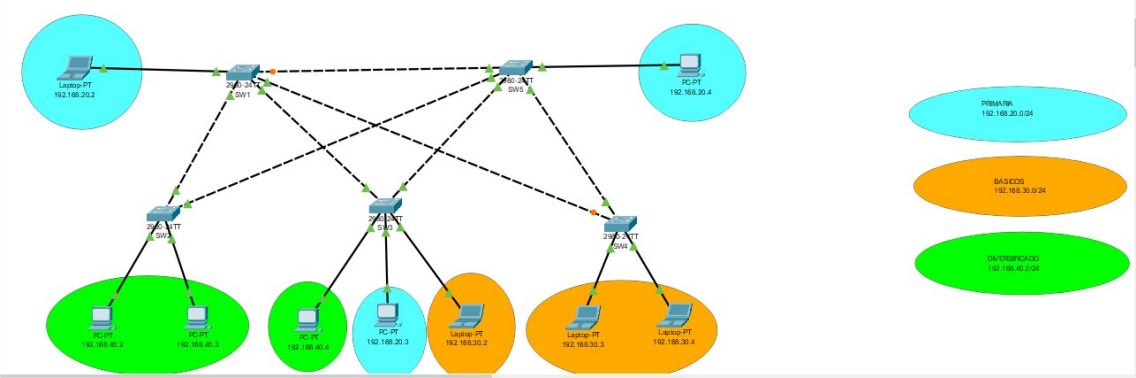
Practica 1 Redes de Computadoras 2 Grupo #10

Grupo	Carnet	Nombre
Coordinador	201602813	Luis Enrique Rivera Najera
Compañero 2	201602880	Bryan Alexander Portillo Alvarado
Compañero 3	201709073	Walter Alexander Guerra Duque
Compañero 4	201602988	Ozmar René Escobar Avila

Glosario de Comandos utilizados

- ***config t*** : este comando permite acceder al modo configuración global desde el modo privilegiado.
- ***int f#/#*** : este comando permite seleccionar algun puerto de un switch para aplicarle alguna configuración.
- ***vtp domain*** : este comando permite asignar un dominio a un switch. Los switches que se encuentren en el mismo dominio de VTP comparten su información de VLAN entre sí, y un switch puede participar en solo un dominio de administración de VTP.
- ***vtp password*** : este comando protege las actualizaciones de VTP estableciendo una contraseña segura.
- ***vtp mode client*** : este comando hace que el switch este en modo cliente, este modo no permite a un switch cambiar su configuración de VLAN. Eso significa que un switch cliente VTP no puede crear ni eliminar VLAN. Sin embargo, las actualizaciones de VTP recibidas se procesan y reenvían.
- ***vtp mode server*** : este comando permite que un switch anuncie sus configuraciones de VLAN a otros switches en el mismo dominio VTP y sincronizar sus configuraciones de VLAN con otros switches en función de los anuncios recibidos a través de enlaces troncales. Estos switches si pueden crear y eliminar VLANs.
- ***vtp mode transparent*** : este comando permite que un switch no sincronice la configuracion de las VLAN con otros switches aunque, puede enviar la informacion de las VLAN. Estos switches si pueden crear y eliminar VLANs pero solo locales no del VTP server.
- ***switchport mode access*** : este comando establece el puerto en modo acceso.
- ***switchport mode trunk*** : este comando pone la interfaz en modo de enlace troncal permanente y negocia para convertir el enlace vecino en un enlace troncal.
- ***sh spanning-tree*** : muestra la configuracion asociada a protocolo STP que funciona en el nivel de la capa 2 del modelo OSI
- ***spanning-tree mode pvst*** : asigna el tipo de spanning-tree asociado al protocolo

Topologia



Configuracion Topologia

SW3 (Server)

```
enable
configure terminal
```

Configurar Interfaces en Modo Trunk

```
interface range fastethernet 0/1-2
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configurar VTP

```
vtp version 2
vtp domain g10
vtp password g10
vtp mode server
exit
```

Configuracion de VLANS

```
vlan 20
name PRIMARIA
exit

vlan 30
name BASICOS
exit

vlan 40
name DIVERSIFICADO
exit
```

Configuracion de Interfaces en Modo Acces

```
interface fastEthernet 0/5
switchport mode access
switchport access vlan 30
exit

interface fastEthernet 0/4
switchport mode access
switchport access vlan 20
exit

interface fastEthernet 0/3
switchport mode access
switchport access vlan 40
exit
```

SW1

Configuracion de Interfaces en Modo Trunk

```
interface range fastethernet 0/1-4
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configuracion del VTP

```
vtp version 2
vtp domain g10
vtp password g10
vtp mode client
exit
```

Configuracion de Interfaces en Modo Acces

```
interface fastEthernet 0/5
switchport mode access
switchport access vlan 20
exit
```

SW2

Configuracion de Interfaces en Modo Trunk

```
interface range fastethernet 0/1-2
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configuracion del VTP

```
vtp version 2
vtp domain g10
vtp password g10
```

```
vtp mode client
exit
```

Configuracion de Interfaces en Modo Acces

```
interface range fastEthernet 0/3-4
switchport mode access
switchport access vlan 40
exit
```

SW4

Configuracion de Interfaces en Modo Trunk

```
interface range fastethernet 0/1-2
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configuracion del VTP

```
vtp version 2
vtp domain g10
vtp password g10
vtp mode client
exit
```

Configuracion de Interfaces en Modo Acces

```
interface range fastEthernet 0/3-4
switchport mode access
switchport access vlan 30
exit
```

SW5

Configuracion de Interfaces en Modo Trunk

```
interface range fastethernet 0/1-4
switchport mode trunk
switchport trunk allowed vlan all
exit
```

Configuracion del VTP

```
vtp version 2
vtp domain g10
vtp password g10
vtp mode client
exit
```

Configuracion de Interfaces en Modo Acces

```
interface fastEthernet 0/5
switchport mode access
switchport access vlan 20
exit
```

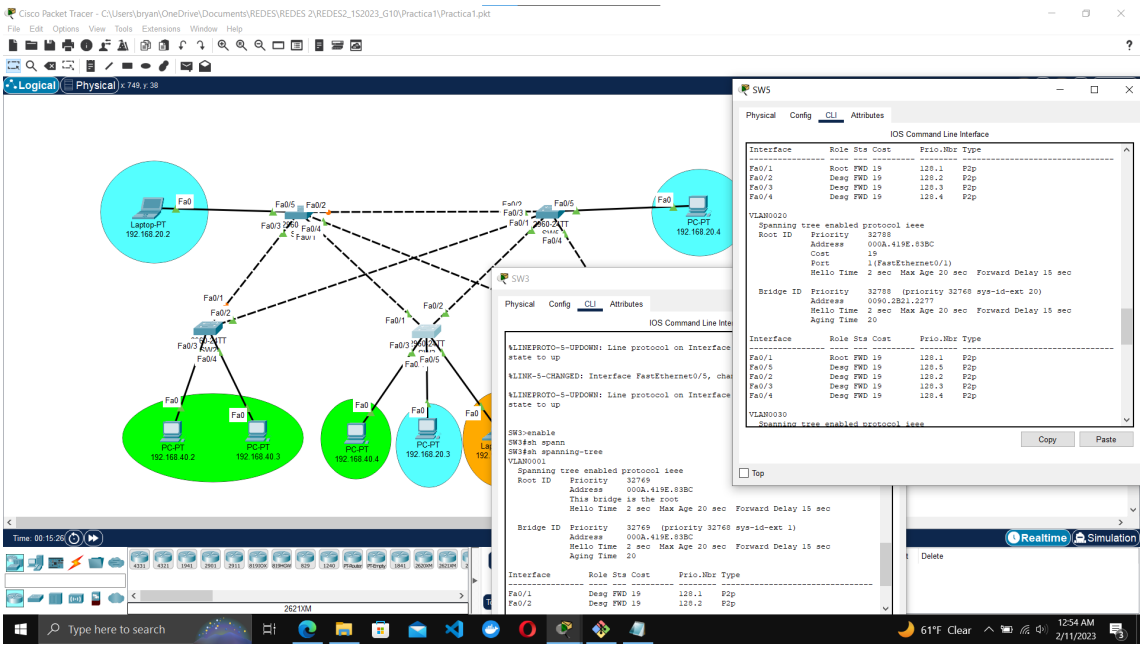
Elección de escenario con mejor resultado de convergencia

1. Escenario PVST

Antes de realizar la prueba debemos localizar cual de nuestros dispositivos es el denomindado "root". Para ello debemos ejecutar el siguiente comando:

```
sh spanning-three
```

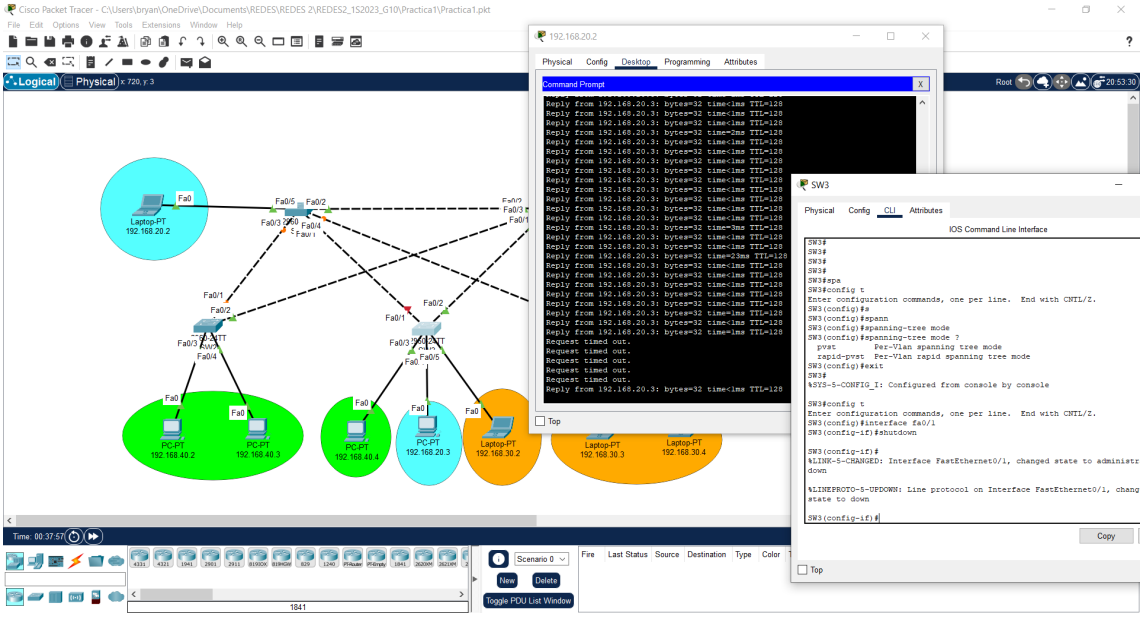
al momento de ejectuar el comando, podremos visualizar elementos descriptivos al protocolo, entre ellos la proximidad, el costo, la direccion, etc. Entre esos datos la consola nos mostrara cual es el dispositivo raiz como podemos observar en la siguiente imagen.



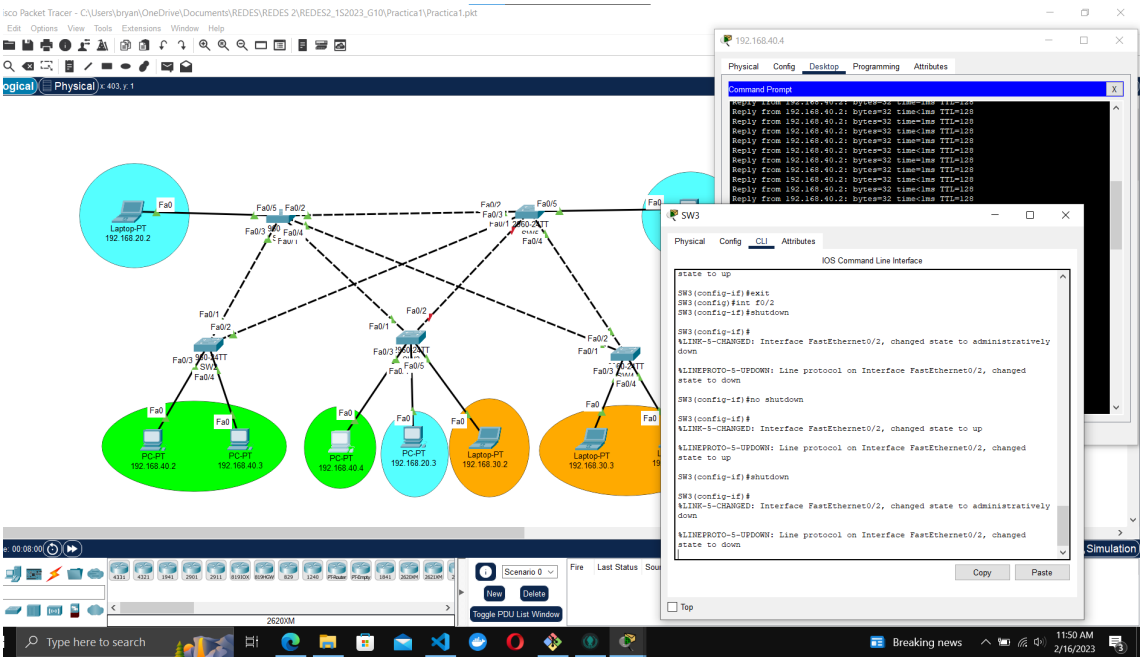
Ya al tener identificado nuestro dispositivo raiz realizamos nuestra pueba de convergencia. Para la prueba se realizo un ping extendido

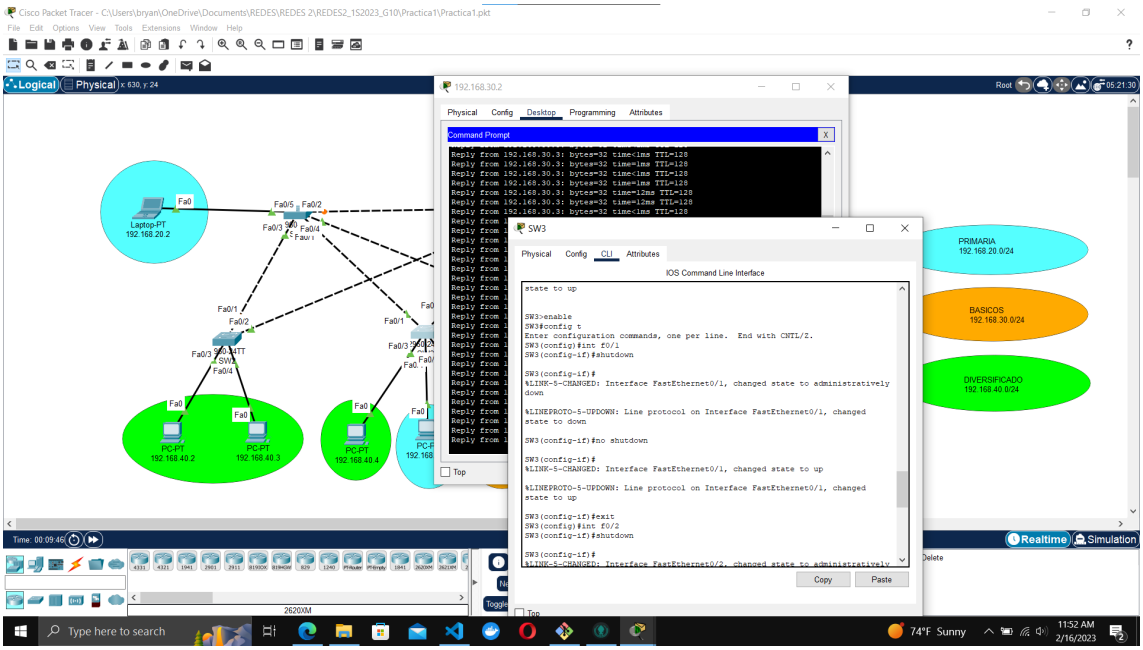
```
ping -t 192.168.20.3
```

desde la maquina con direccion ip 192.168.20.2 perteneciente al grupo de PRIMARIA hacia la maquina con direccion 192.168.20.3 se tomo como referencia el SW3 y se apago la interfaz 0/1; el tiempo que tomo el protocolo en escoger una ruta alternativa fue de de un aproximado de 38 segundos



se realizo el mismo procedimiento anterior con las redes faltantes



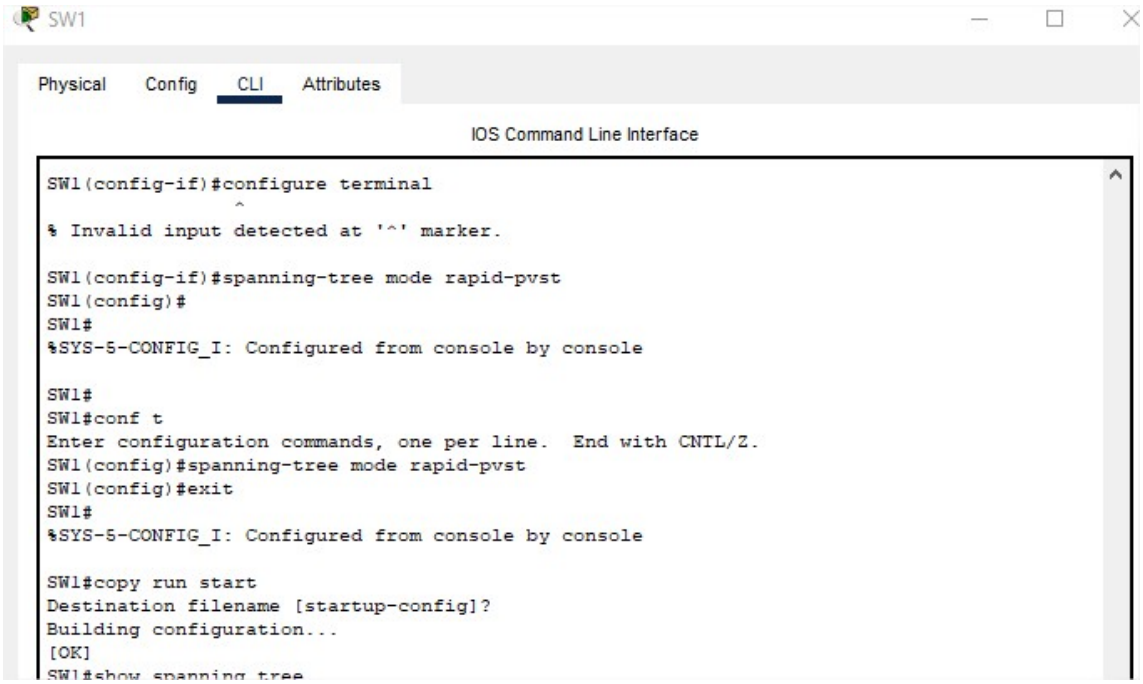


y el tiempo que tomo el protocolo variaba de 1+- segundos con respecto a la red PRIMARIA.

2. Escenario Rapid PVST

Para la prueba de Convergencia primero se cambio el modo spanning-tree de todos los switch con el comando:

```
spanning-tree mode rapid-pvst
```

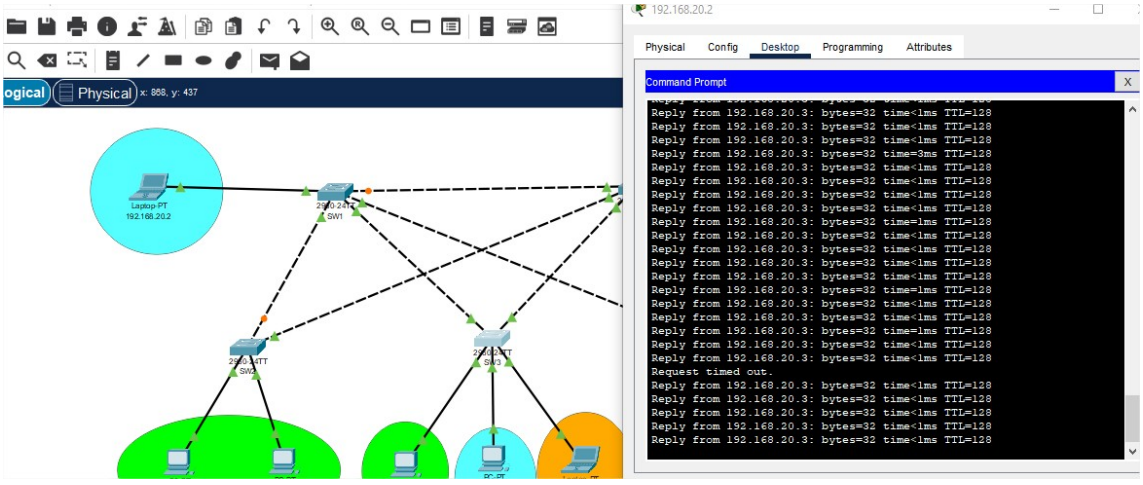


Luego de eso se procedio a hacer ping entre dos computadoras de la misma VLAN para posteriormente apagar un puerto del switch seleccionado para poder ver en cuanto tiempo escoge una ruta alternativa.

```
conf t
int f0/1
shutdown
no shutdown
```

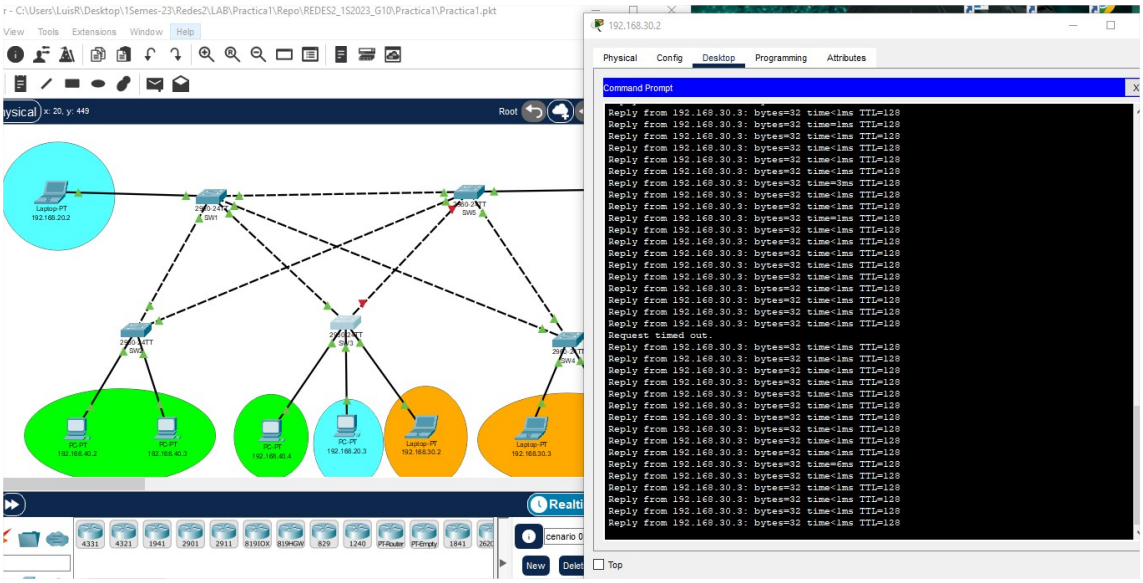
Vlan Primaria

```
---------------- ---- --- --------- -------- --------------------------------

SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#int f0/1
SW3(config-if)#shutdown

SW3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

SW3(config-if)#no shutdown

SW3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```



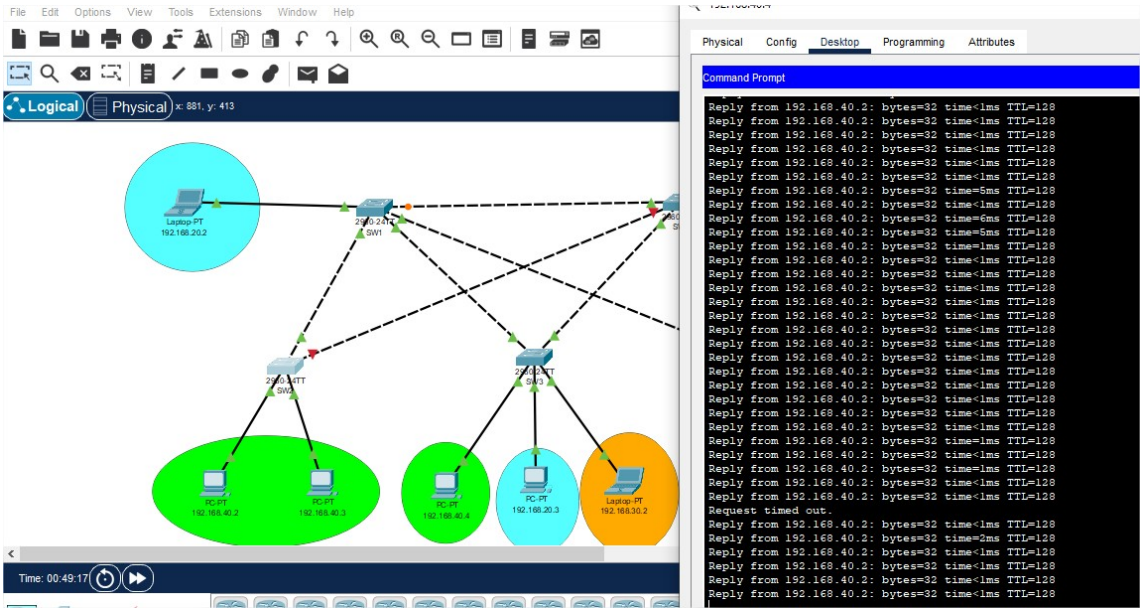
Vlan Basicos

```
SW3(config-if)#
SW3(config-if)#exit
SW3(config)#int f0/2
SW3(config-if)#shutdown

SW3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW3(config-if)#no shutdown

SW3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
```



Vlan Diversificado

```
SW2>
SW2>ENABLE
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#int f0/2
SW2(config-if)#shutdown

SW2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW2(config-if)#
SW2(config-if)#no shutdown

SW2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

SW2(config-if)#
```



El tiempo que les tomo en los tres casos fue de aproximadamente 1 segundo. Por lo que se eligio este protocolo para implementarlo en la practica.

Seguridad de Interfaces de Red

Políticas de puerto compartidas

Para activar el port-security en cualquier switch, se debe desactivar la negociación automática de los puertos truncales (Dynamic Trunking Protocol DTP), para esto se debe configurar explícitamente el modo acceso en las interfaces correspondientes, esto ya se hizo en la configuración de la topologia.

Seguridad para interfaces asignadas a la VLAN

Ahora, se debe activar el port-security en las interfaces de interés, y luego se debe configurar dicha funcionalidad para que permita el tráfico únicamente de las siguientes direcciones MAC:

SW1

Interfaz	VLAN	Tipo de dispositivo	Dirección IP	Dirección MAC
f0/5	20	Laptop	192.168.20.2	0060.705D.C289

SW2

Interfaz	VLAN	Tipo de dispositivo	Dirección IP	Dirección MAC
f0/3	40	Desktop	192.168.40.2	0030.A394.42BC
f0/4	40	Desktop	192.168.40.3	0050.0F73.5214

SW3

Interfaz	VLAN	Tipo de dispositivo	Dirección IP	Dirección MAC
f0/3	40	Desktop	192.168.40.4	0090.2BD7.982E
f0/4	20	Desktop	192.168.20.3	0007.EC1A.7361
f0/5	30	Laptop	192.168.30.2	0000.0C38.A2CD

SW4

Interfaz	VLAN	Tipo de dispositivo	Dirección IP	Dirección MAC
f0/3	30	Laptop	192.168.30.3	0060.70CC.8060
f0/4	30	Laptop	192.168.30.4	00E0.A35E.AAA3

SW5

Interfaz	VLAN	Tipo de dispositivo	Dirección IP	Dirección MAC
f0/5	20	Desktop	192.168.20.4	0060.3E4D.0988

Para hacer esto se deben ejecutar en cada interfaz en modo acceso, los siguientes comandos:

```
conf t
int f0/<numero-de-interfaz>
switchport port-security
switchport port-security mac-address <MAC-address>
exit
```

SW1

```
conf t
int f0/5
```

```
switchport port-security
switchport port-security mac-address 0060.705D.C289
exit
```

SW2

```
conf t
int f0/3
switchport port-security
switchport port-security mac-address 0030.A394.42BC
int f0/4
switchport port-security
switchport port-security mac-address 0050.0F73.5214
exit
```

SW3

```
conf t
int f0/3
switchport port-security
switchport port-security mac-address 0090.2BD7.982E
int f0/4
switchport port-security
switchport port-security mac-address 0007.EC1A.7361
int f0/5
switchport port-security
switchport port-security mac-address 0000.0C38.A2CD
exit
```

SW4

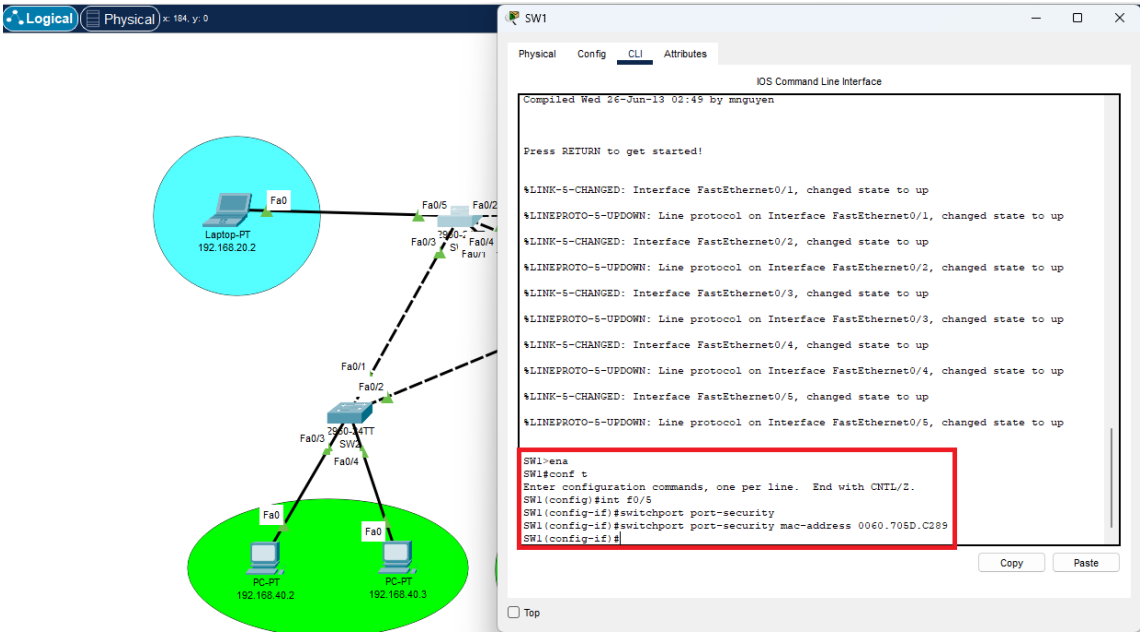
```
conf t
int f0/3
switchport port-security
switchport port-security mac-address 0060.70CC.8060
int f0/4
switchport port-security
switchport port-security mac-address 00E0.A35E.AAA3
exit
```

SW5

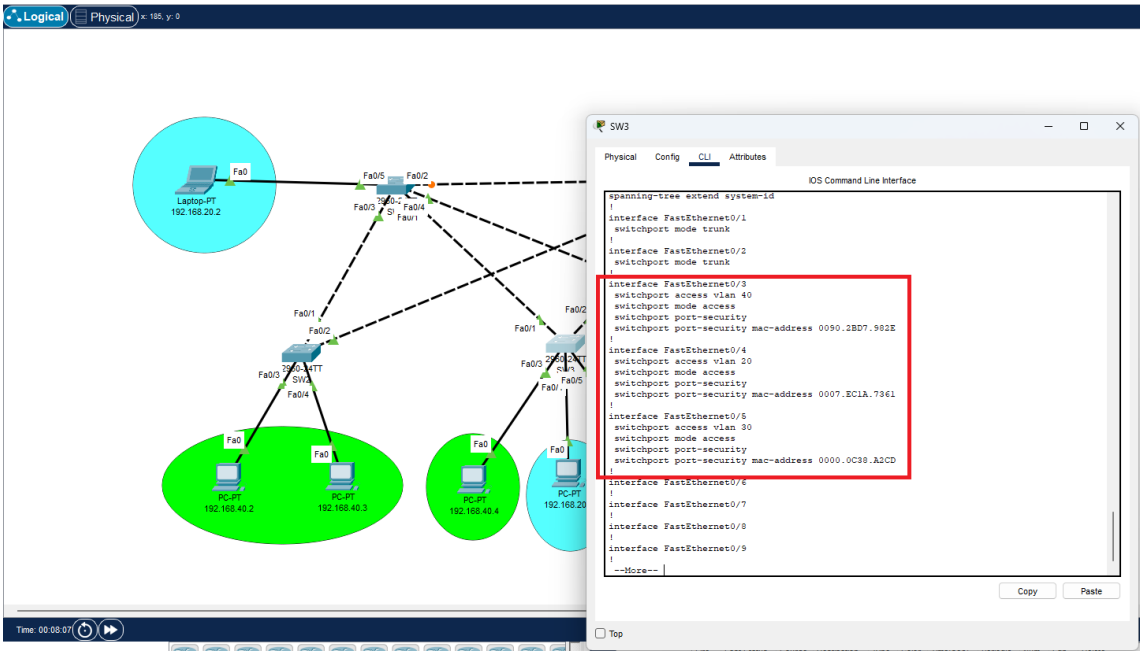
```
conf t
int f0/5
switchport port-security
switchport port-security mac-address 0060.3E4D.0988
exit
```

Y se puede ilustrar de la siguiente forma:

Activando port-security con MAC address en SW1, el proceso se repite para todos los demás switches según los comandos de arriba:



Verificando que esté configurado correctamente el port-security por medio de `sh run`, el proceso se repite para todos los demás switches:



Verificando que el puerto se apagará en caso de una violación de seguridad por medio de `sh port-security interface f0/<numero-de-interfaz>`, el proceso se repite para todos

los demás switches: