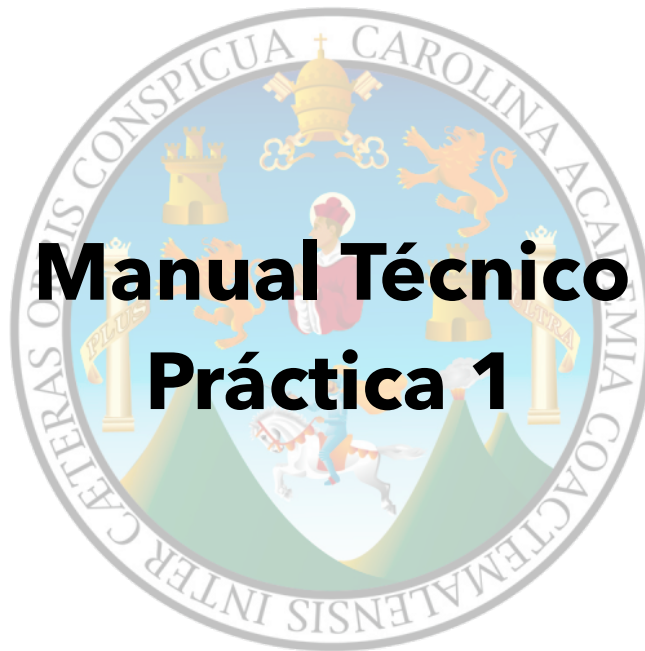


Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Laboratorio Redes de Computadoras 2



Grupo 41

2011-14340 Edgar Mauricio Gómez Flores

Definición del problema	1
Implementación	2
Requerimientos iniciales	2
Topología	2
Configuración	2
Configurar dirección IP de dispositivos finales	3
Configurar Switch	5
Elección de escenario con mejor convergencia	9
Conclusión	10

Definición del problema

Pandora, es un colegio que se dedica a la enseñanza de niños desde la primaria hasta diversificado. Con el inicio de la pandemia muchos empleados decidieron renunciar y, entre ellos, iba el equipo completo del área de informática. El colegio contrató a dos personas para esta área y están en busca de más personal. 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 que deciden contratarlo a usted, experto en redes de computadoras, cobrando un bolsón de horas en el cual 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 su asesoría para poder implementar este sistema de la mejor manera posible.

Implementación

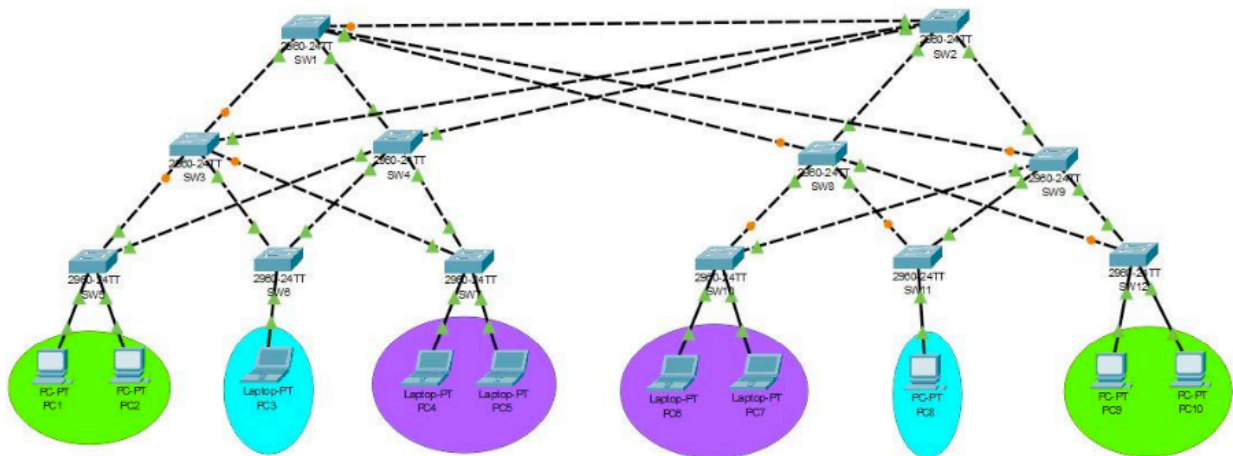
Requerimientos iniciales

- Instalar Cisco Packet Tracer 8.2.1
- Clonar repositorio https://github.com/itolisto/REDES2_2S2023_41

Topología

La topología implementada es la descrita en el enunciado de la práctica, la misma se desglosa de la siguiente manera:

- 12 Switch 2960
- 8 PC's y 2 Laptop



Configuración

Todas las configuraciones se realizaron utilizando la línea de comandos (CLI) - *command-line interface*, por sus siglas en inglés - a excepción de la asignación de direcciones IP para los dispositivos finales (PC y Laptop).

A continuación se describe, en el orden realizado por el estudiante, los pasos necesarios para configurar la topografía, comandos y capturas de pantalla (de ser necesario).

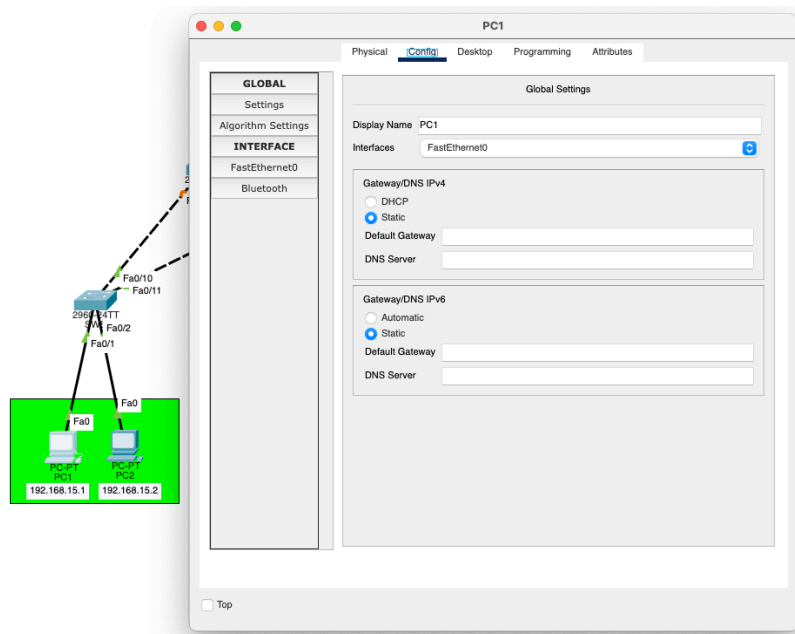
Configurar dirección IP de dispositivos finales

De acuerdo a los criterios descritos en el enunciado, las VLAN se calcularon sumando los dos dígitos del grupo 41, siendo el resultado 5, más el número base de cada VLAN.

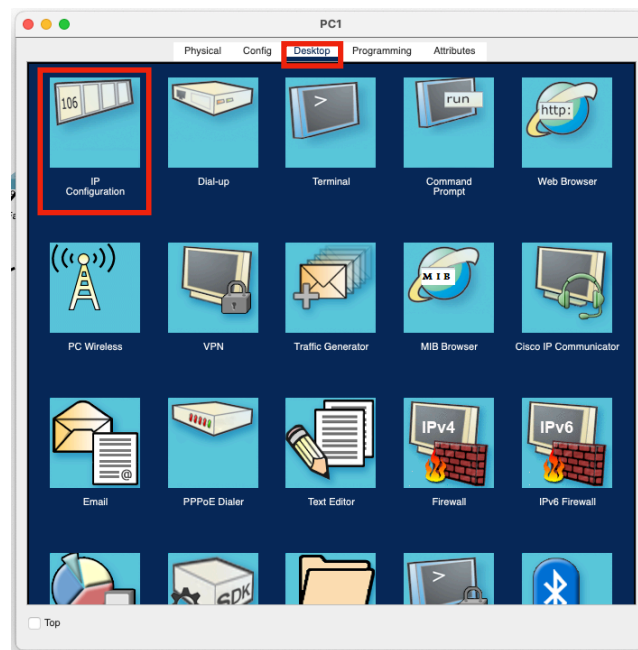
Nombre de VLAN	Base	Número a sumar	VLAN	Direcciones de Red
PRIMARIA	10	$4 + 1 = 5$	15	192.168.15.0/24
BASICOS	20	$4 + 1 = 5$	25	192.168.25.0/24
DIVERSIFICADO	30	$4 + 1 = 5$	35	192.168.35.0/24

Luego de obtener las direcciones de red para cada grupo, se procede a asignar en cada dispositivo final (PC y Laptop) de la siguiente manera:

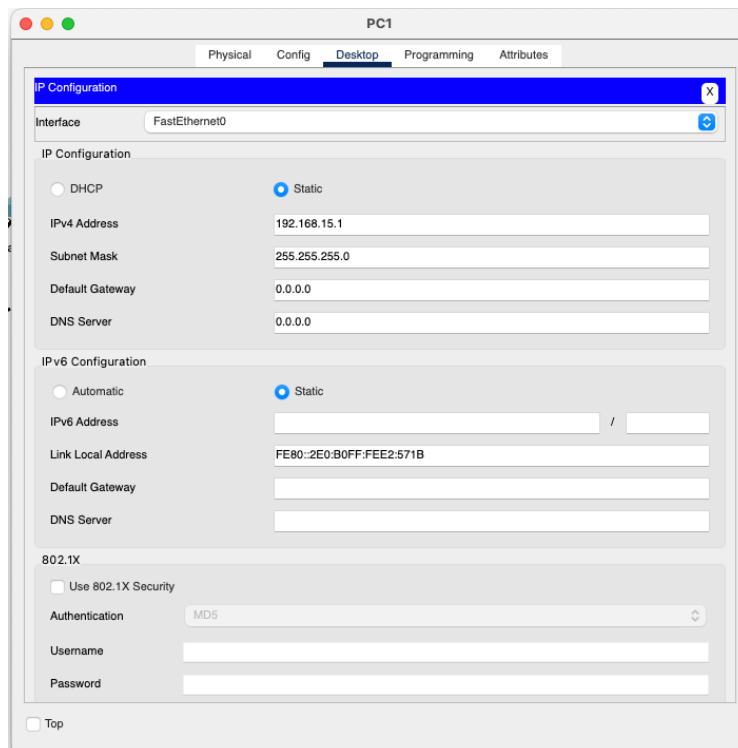
1. Seleccionar dispositivo y dar click



2. Mover a la pestaña "Desktop" y seleccionar opción "IP Configuration"



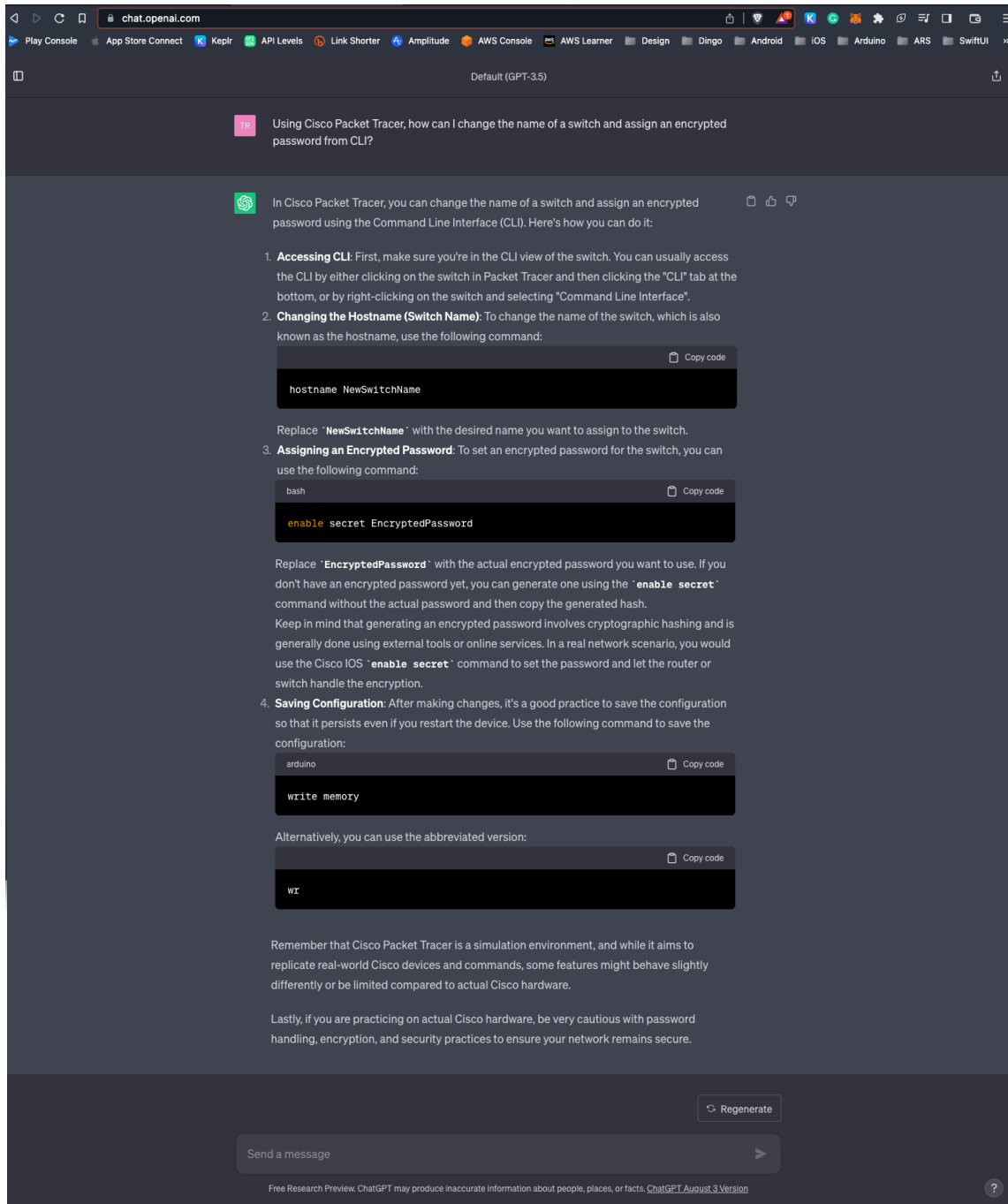
3. Ingresar dirección IP que se desea asignar y dejar máscara de subred por defecto 255.255.255.0



Configurar Switch

Configurar nombre, dominio y contraseña

Cambiar nombre y utilizar contraseña encriptada para un Switch utilizando ChatGPT



chat.openai.com

Default (GPT-3.5)

Using Cisco Packet Tracer, how can I change the name of a switch and assign an encrypted password from CLI?

In Cisco Packet Tracer, you can change the name of a switch and assign an encrypted password using the Command Line Interface (CLI). Here's how you can do it:

- Accessing CLI:** First, make sure you're in the CLI view of the switch. You can usually access the CLI by either clicking on the switch in Packet Tracer and then clicking the "CLI" tab at the bottom, or by right-clicking on the switch and selecting "Command Line Interface".
- Changing the Hostname (Switch Name):** To change the name of the switch, which is also known as the hostname, use the following command:

```
hostname NewSwitchName
```

Replace 'NewSwitchName' with the desired name you want to assign to the switch.
- Assigning an Encrypted Password:** To set an encrypted password for the switch, you can use the following command:

```
enable secret EncryptedPassword
```

Replace 'EncryptedPassword' with the actual encrypted password you want to use. If you don't have an encrypted password yet, you can generate one using the 'enable secret' command without the actual password and then copy the generated hash. Keep in mind that generating an encrypted password involves cryptographic hashing and is generally done using external tools or online services. In a real network scenario, you would use the Cisco IOS 'enable secret' command to set the password and let the router or switch handle the encryption.
- Saving Configuration:** After making changes, it's a good practice to save the configuration so that it persists even if you restart the device. Use the following command to save the configuration:

```
write memory
```

Alternatively, you can use the abbreviated version:

```
WT
```

Remember that Cisco Packet Tracer is a simulation environment, and while it aims to replicate real-world Cisco devices and commands, some features might behave slightly differently or be limited compared to actual Cisco hardware.

Lastly, if you are practicing on actual Cisco hardware, be very cautious with password handling, encryption, and security practices to ensure your network remains secure.

Regenerate

Send a message

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT August 3 Version](#)

1. Nombre

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1_G41
```

2. Dominio

```
SW1_G41(config)#vtp domain practica1.usac.local
```

3. Contraseña

```
SW1_G41(config)#vtp password redes2sgupo41
```

4. Guardar

```
SW1_G41#exit
SW1_G41#
%SYS-5-CONFIG_I: Configured from console by console

SW1_G41#wr
Building configuration...
[OK]
```

Crear y configurar VLAN's

1. Definir switch que tendrá modo servidor, en este caso escogemos el switch SW1_G41 y los demás se actualizaran a modo cliente

```
SW1_G41#configure terminal
SW1_G41(config)#vtp mode server
```

```
SW2-12_G41#configure terminal
SW2-12_G41(config)#vtp mode client
```


2. En el switch en modo servidor, proceder a crear VLAN's

```
SW1_G41#configure terminal
SW1_G41(config)#vlan 15/25/35
SW1_G41(config-vlan)#name PRIMARIA/BASICOS/DIVERSIFICADO
```

Configurar puertos en modo trunk (por cada switch)

```
SW1_G41#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW1_G41(config)#interface f0/12
SW1_G41(config-if)#switchport mode trunk
SW1_G41(config-if)#switchport trunk allowed vlan 15,25,35
SW1_G41(config-if)#exit
SW1_G41(config)#do wr
Building configuration...
[OK]
```

Configurar puertos en modo acceso (por cada switch)

```
SW4_G41#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW4_G41(config)#interface f0/1
SW4_G41(config-if)#switchport mode access
SW4_G41(config-if)#switchport access vlan [insertar numero de vlan]
SW4_G41(config-if)#exit
SW4_G41(config)#do wr
Building configuration...
[OK]
```

Configurar security ports (por cada switch)

```
SW4_G41#config t
SW4_G41(config)#interface f0/1
SW4_G41(config-if)#switchport port-security // activar
SW4_G41(config-if)#switchport port-security mac-address [insertar mac address]
SW4_G41(config-if)#exit
SW4_G41(config)#do wr
Building configuration...
[OK]
```

Lista de MAC addresses en el proyecto:

00E0.B0E2.571B
 0090.2B85.83BA
 00E0.8FC1.37D4
 0040.0B60.6EC7
 0050.0F13.23AE
 00E0.B037.4903
 0001.C920.0E18
 00E0.F9E9.E6CD
 0090.2BBB.2B72
 0006.2AB8.D6C5

Desactivar Dynamic Trunking Protocol (DTP) en puertos trunk

Using Cisco Packet Tracer, how can I deactivate DTP protocol in a trunk port if present?

In Cisco Packet Tracer, you can deactivate the Dynamic Trunking Protocol (DTP) on a trunk port using the Command Line Interface (CLI) of a Cisco switch. DTP is used to negotiate the trunking mode (dynamic desirable, dynamic auto, trunk, access) between switches. To deactivate DTP on a trunk port, follow these steps:

- Accessing CLI:** Make sure you're in the CLI view of the switch. You can usually access the CLI by either clicking on the switch in Packet Tracer and then clicking the "CLI" tab at the bottom, or by right-clicking on the switch and selecting "Command Line Interface".
- Navigate to the Interface Configuration Mode:** To deactivate DTP, you need to go to the interface configuration mode of the trunk port. Assume the port you want to configure is FastEthernet 0/1. Here's the command sequence:


```
kotlin
enable
configure terminal
interface fastEthernet 0/1
```

Replace "FastEthernet 0/1" with the actual interface you want to configure.
- Deactivate DTP:** To disable DTP negotiation on the interface, you need to set the trunk mode to "static" mode using the following command:


```
switchport nonegotiate
```
- Exit Interface Configuration Mode:** After deactivating DTP, you can exit the interface configuration mode:


```
arduino
end
```
- Saving Configuration:** After making changes, it's a good practice to save the configuration so that it persists even if you restart the device. Use the following command to save the configuration:


```
arduino
write memory
```

Alternatively, you can use the abbreviated version:

```
wr
```

Remember that Packet Tracer is a simulation environment, and the commands and behavior might not be exactly the same as on real Cisco hardware. Always refer to Cisco's official documentation and recommended practices when working with actual Cisco devices in a production environment.

```

SW4_G41#config t
SW4_G41(config)#interface f0/1
SW4_G41(config-if)#switchport nonegotiate
SW4_G41(config-if)#exit
SW4_G41(config)#do wr
Building configuration...
[OK]

```

Determinar puerto root, designated o non designated

```
SW1_G41#show spanning-tree vlan 35
```

```

VLAN0035
  Spanning tree enabled protocol ieee
  Root ID    Priority    32803
             Address     0000.0C27.2219
             Cost        38
             Port        2 (FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32803 (priority 32768 sys-id-ext 35)
             Address     0001.643A.8B27
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Altn	BLK	19	128.1	P2p
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/3	Altn	BLK	19	128.3	P2p
Fa0/10	Altn	BLK	19	128.10	P2p
Fa0/11	Altn	BLK	19	128.11	P2p

Elección de escenario con mejor convergencia

Como se aprendió en laboratorio, con las dos configuraciones solicitadas PVST (Per VLAN Spanning-Tree) y RPVST (Rapid Per VLAN Spanning-Tree), para realizar el cambio entre estas dos configuraciones se deben utilizar los siguientes comandos

```

SW1_G41#config t
SW1_G41(config)#spanning-tree mode pvst/rapid-pvst
SW1_G41(config)#spanning-tree vlan 15,25,35
SW1_G41(config)#do wr
Building configuration...
[OK]

```

Luego de configurar el protocolo por VLAN en cada switch, se procedió a realizar un ping extendido desde la máquina A a una máquina B, una vez establecido el ping se apagó el enlace de comunicación (enlace en color verde) y se cronometró el tiempo de convergencia.

```
SW1_G41#config t
SW1_G41(config)#interface f0/11
SW1_G41(config-if)#shutdown

O para prender de nuevo

SW1_G41(config-if)#no shutdown
```

VLAN	Máquina A	Máquina B	Protocolo	Tiempo (segundos)	Switch / Interfaz
15	192.168.15.1	192.168.15.3	PVST	53	SW5 / f0/11
25	192.168.25.1	192.168.25.2	PVST	54	SW6 / f0/11
35	192.168.35.2	192.168.35.4	PVST	40	SW7 / f0/11

VLAN	Máquina A	Máquina B	Protocolo	Tiempo (segundos)	Switch / Interfaz
15	192.168.15.1	192.168.15.3	RPVST	Inmediato	SW5 / f0/11
25	192.168.25.1	192.168.25.2	RPVST	Inmediato	SW6 / f0/11
35	192.168.35.2	192.168.35.4	RPVST	Inmediato	SW7 / f0/11

Conclusión

Se elige el protocolo RPVST ya que el tiempo de convergencia una vez apagado el enlace fue inmediato (o casi inmediato) sin pérdida de paquetes.