UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS

REDES DE COMPUTADORAS 2
ING. MANUEL FERNANDO LOPEZ FERNANDEZ
AUX. ADRIANA MARIÉ GÓMEZ DÁVILA

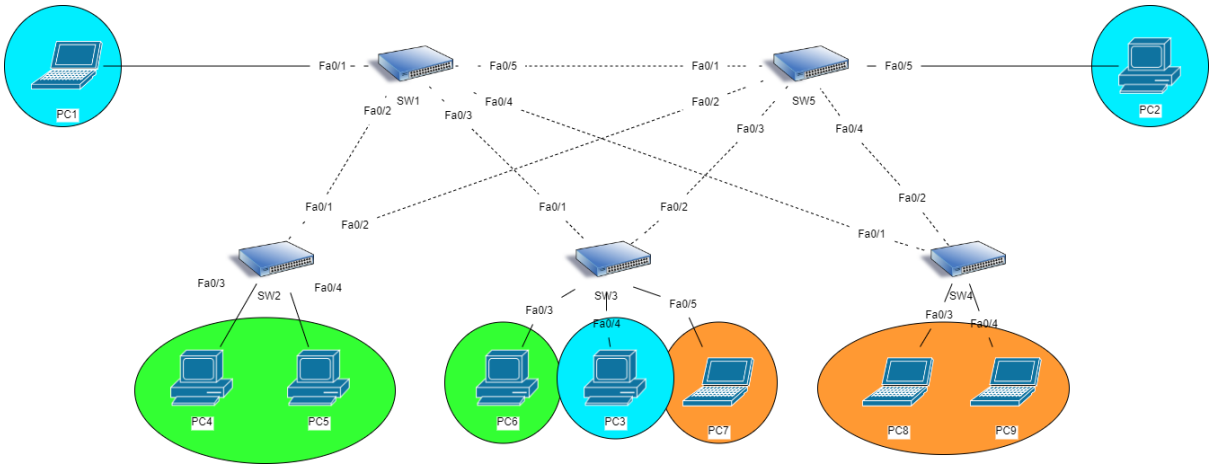
PRÁCTICA 1

JONATHAN MARCOS VALIENTE GONZÁLEZ
201931581
9/03/2023

ÍNDICE

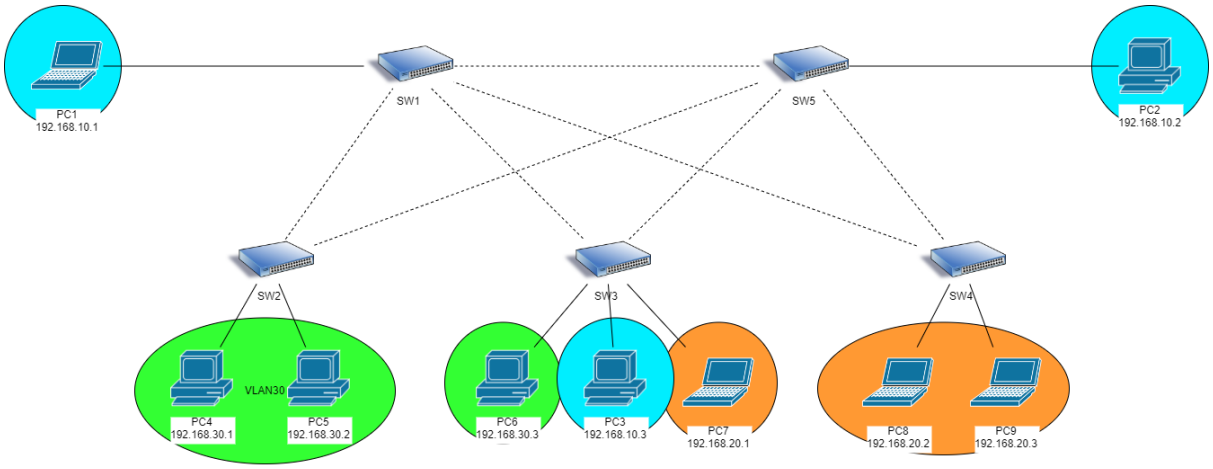
MANUAL TÉCNICO

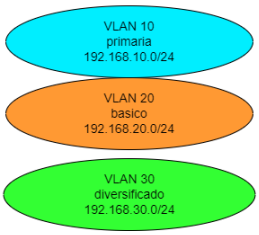
TOPOLOGÍA



Dispositivo	Nombre
Cisco Laptop	PC1
Cisco PC	PC4
Cisco PC	PC5
Cisco PC	PC6
Cisco PC	PC3
Cisco Laptop	PC7
Cisco Laptop	PC8
Cisco Laptop	PC9
Cisco PC	PC2
Cisco Switch	SW1
Cisco Switch	SW2
Cisco Switch	SW3
Cisco Switch	SW4
Cisco Switch	SW5

TOPOLOGÍA VLAN

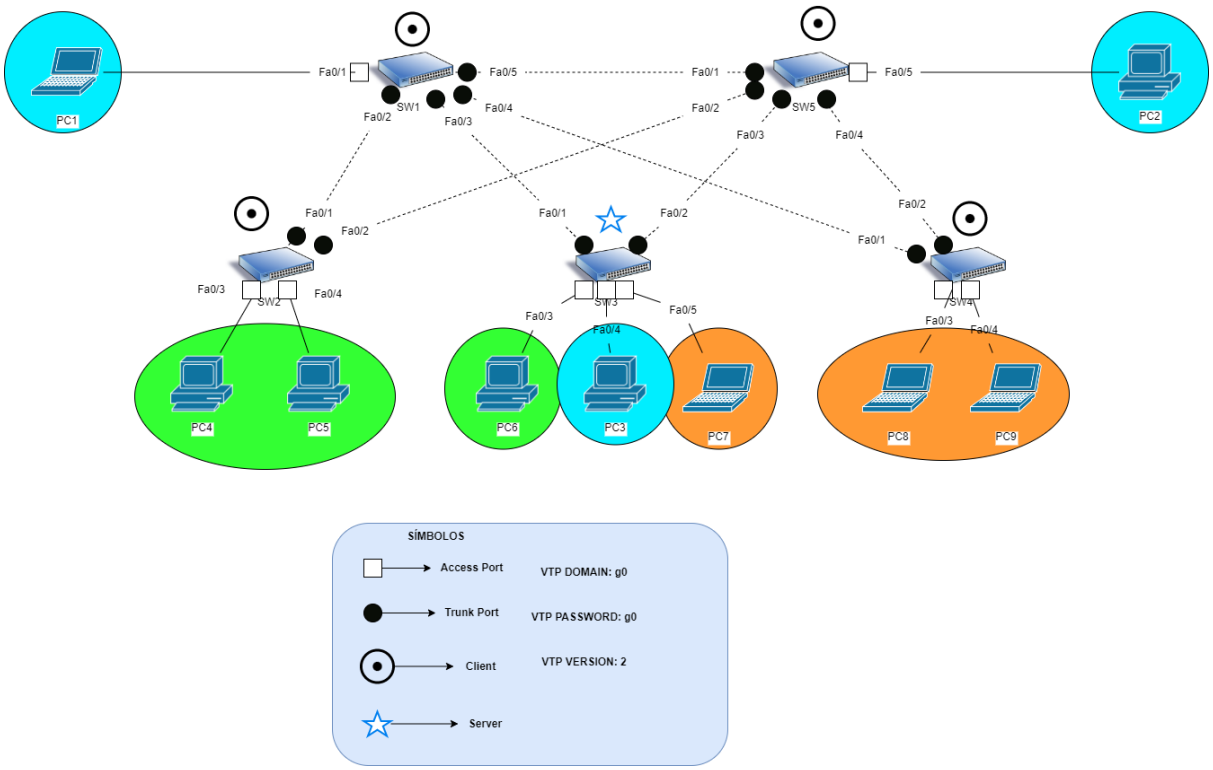




Sólo se asigna IP a los dispositivos finales (end devices), ya que el VTP se trabaja a nivel de capa 2, es decir, por Mac Address. El control de tráfico se realiza por medio de la configuración de los protocolos Spanning-tree (PVST y RPVST).

DISPOSITIVO	VLAN	IP	GATEWAY
PC1	vlan 10	192.168.10.1	192.168.10.0
PC2	vlan 10	192.168.10.2	192.168.10.0
PC3	vlan 10	192.168.10.3	192.168.10.0
PC4	vlan 30	192.168.30.1	192.168.30.0
PC5	vlan 30	192.168.30.2	192.168.30.0
PC6	vlan 30	192.168.30.3	192.168.30.0
PC7	vlan 20	192.168.20.1	192.168.20.0
PC8	vlan 20	192.168.20.2	192.168.20.0
PC9	vlan 20	192.168.20.3	192.168.20.0

TOPOLOGÍA VTP



Establecemos el protocolo VTP de capa 2, el dominio y contraseña serán "g0" y versión de VTP 2.

Para configurar el protocolo VTP de primero tenemos que seleccionar el switch servidor que es el que tendrá los nombres de las VLANs (Vlan 10, 20 y 30; Vlan primaria, básico y diversificado respectivamente), al funcionar como una BD de las VLANs el servidor irá actualizando las BD de los switches configurados como clientes, esta comunicación se logra por medio de los puertos troncales entre switches.

Cabe mencionar limitaciones existentes en el proyecto, por ejemplo:

- La versión del Cisco Packet Tracer no soporta el comando vtp "set vtp pruning enable" por lo que no se pudo configurar el modo pruning para restringir el acceso de las VLANs, ya que si limitamos la cantidad de VLANs de los puertos troncales, los clientes no tendrán acceso a la base de datos del servidor y no se actualizarán.
- El puerto Fa0/1 y Fa0/2 del Switch 2 y el puerto Fa0/1 y Fa0/2 del Switch 4 están configurados como troncales, para cuando el momento que si el Switch 1 caiga, entonces, el Switch 5 puede seguir comunicando el protocolo.
- El manejo de tráfico se maneja exclusivamente con los protocolos spanning-tree.

Configuración Switches

DISPOSITIVO	MODO
SW1	Cliente
SW2	Cliente
SW3	Servidor
SW4	Cliente
SW5	Cliente

Configuración Puertos

SW1

Puerto	Modo	Acceso Vlan
FastEthernet 0/1	acceso	10
FastEthernet 0/2	troncal	10, 20 y 30
FastEthernet 0/3	troncal	10, 20 y 30
FastEthernet 0/4	troncal	10, 20 y 30
FastEthernet 0/5	troncal	10, 20 y 30

SW2

Puerto	Modo	Acceso Vlan
FastEthernet 0/1	troncal	10, 20 y 30
FastEthernet 0/2	troncal	10, 20 y 30
FastEthernet 0/3	acceso	30
FastEthernet 0/4	acceso	30

SW3

Puerto	Modo	Acceso Vlan
FastEthernet 0/1	troncal	10, 20 y 30
FastEthernet 0/2	troncal	10, 20 y 30
FastEthernet 0/3	acceso	30
FastEthernet 0/4	acceso	10
FastEthernet 0/5	acceso	20

SW4

Puerto	Modo	Acceso Vlan
FastEthernet 0/1	troncal	10, 20 y 30
FastEthernet 0/2	troncal	10, 20 y 30
FastEthernet 0/3	acceso	20
FastEthernet 0/4	acceso	20

SW5

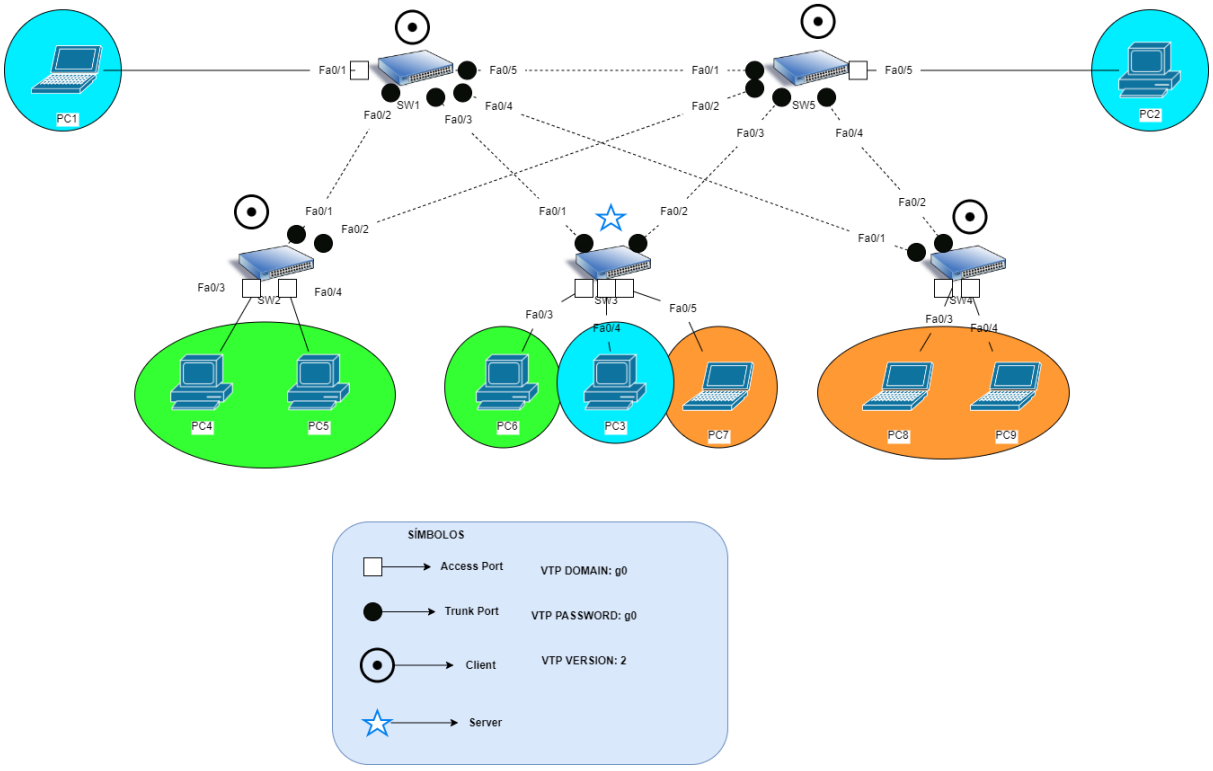
Puerto	Modo	Acceso Vlan
FastEthernet 0/1	troncal	10, 20 y 30
FastEthernet 0/2	troncal	10, 20 y 30
FastEthernet 0/3	troncal	10, 20 y 30
FastEthernet 0/4	troncal	10, 20 y 30
FastEthernet 0/5	acceso	10

Configuración Seguridad

Para asegurar la seguridad de los puertos en capa 2, configuramos las siguientes medidas de seguridad:

1. Desactivación del protocolo DTP de los puertos troncales, se logró agregando el comando "switchport nonegotiate" en cada interfaz troncal de los switches.
2. Uso del modo port-security en los puertos de acceso:
    a. Se configuró el comando "switchport port-security mac-address sticky" en cada puerto de acceso a los dispositivos finales. Se utilizó el comando sticky debido a que la configuración manual de los puertos generaba muchos errores en Cisco Packet Tracer. El comando sticky sirve para guardar la dirección MAC del dispositivo al cual el puerto esté conectado, en este caso al dispositivo final.
    b. Se implementó el comando "switchport port-security maximum 1" como limitante de una sola dirección MAC en el puerto.
    c. Se agregó el comando "switchport port-security violation shutdown" para que en el momento que exista una violación del port-security el puerto se desactive.

TOPOLOGÍA SPANNING-TREE CONFIGURACIÓN DE PUERTOS [vlan 10]



Configuración del Dispositivo Puente

PRIORIDAD	8192	61440	4096	61440	8192
SWITCH	sw1	sw2	sw3	sw4	sw5
MODO	secondario	normal	primario	normal	secondario

Configuración de los Puertos

Tabla de Prioridad

64	El puerto amarillo representa que está configurado a un dispositivo final como una computadora, por lo tanto se agrega también los comandos “spanning-tree portfast” y “spanning-tree bdpuguard enable” para evitar que paquetes BPDU se comuniquen con este puerto, porque debe ser exclusivo de switches

	SW1	**SW2**	**SW3**	**SW4**	**SW5**
FastEthernet0/1	64	240	64	240	128
FastEthernet0/2	240	240	64	240	240
FastEthernet0/3	0	240	240	240	0
FastEthernet0/4	240	240	64	240	240
FastEthernet0/5	128	-	240	-	64

Tabla de Estado

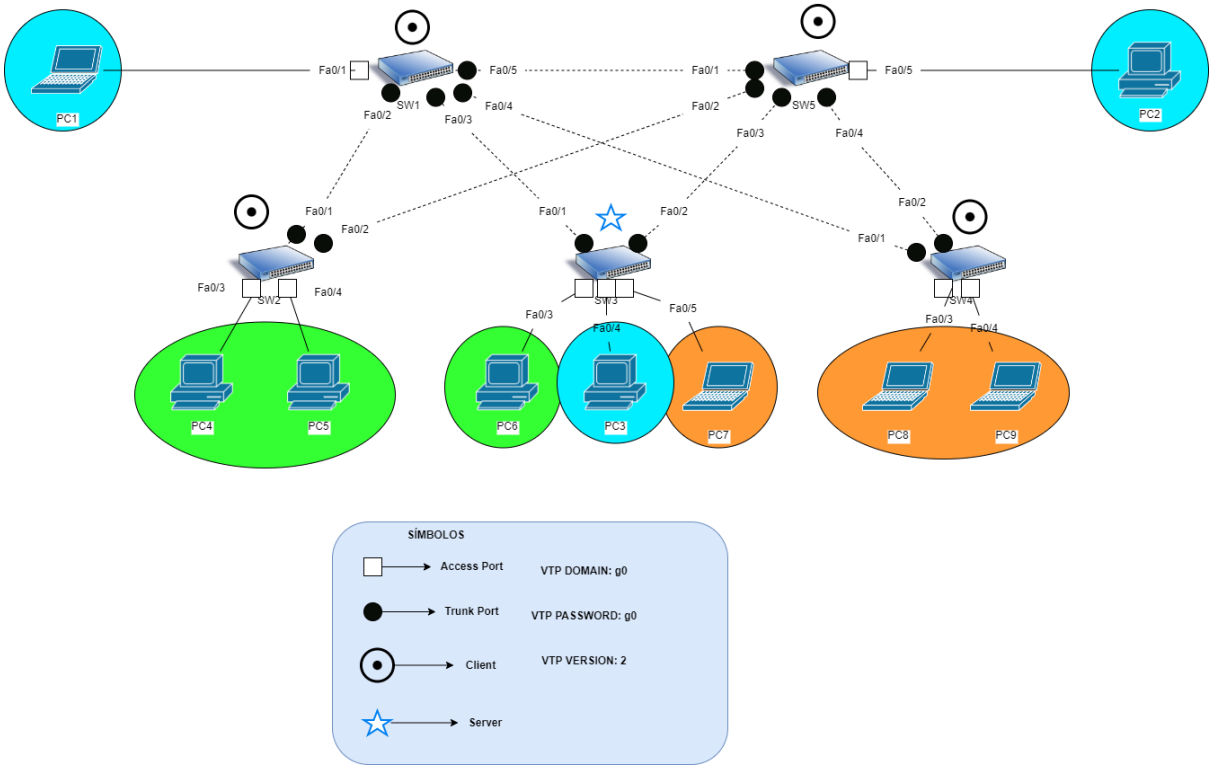
Aunque es cierto que todos los puertos del protocolo PVST y RPVST solo tienen los modos forward y blocked, según su prioridad se pueden comportar como:

- Puerto Root: el puerto que está más cercano al dispositivo puente. Los puertos se configuran según su prioridad, el puerto root tiene prioridad 0, significando que es el camino más cercano al puente.
- Puerto Designated: puerto principal de tráfico, por su nivel de prioridad está configurado en 64.
- Puerto Alternate: puerto que sustituye al designated si se cae para control de tráfico, por su nivel de prioridad está configurado en 128.

- Puerto Blocked: puerto bloqueado por el switch donde nada de tráfico cruzará por ese puerto, por su nivel de prioridad está configurado en 240, el último valor aceptado por el switch (Cisco Packet Tracer no permite configurar puertos exclusivamente bloqueados, por lo que se manejo como de última prioridad..

	SW1	SW2	SW3	SW4	SW5
FastEthernet0/1	designated	blocked	designated	blocked	alternate
FastEthernet0/2	blocked	blocked	designated	blocked	blocked
FastEthernet0/3	root	blocked	blocked	blocked	root
FastEthernet0/4	blocked	blocked	designated	blocked	blocked
FastEthernet0/5	alternate	-	blocked	-	designated

TOPOLOGÍA SPANNING-TREE CONFIGURACIÓN DE PUERTOS [vlan 20]



Configuración del Dispositivo

PRIORIDAD	4096	61440	61440	61440	8192
SWITCH	sw1	sw2	sw3	sw4	sw5
MODO	primario	normal	normal	normal	secundario

Configuración de los Puertos

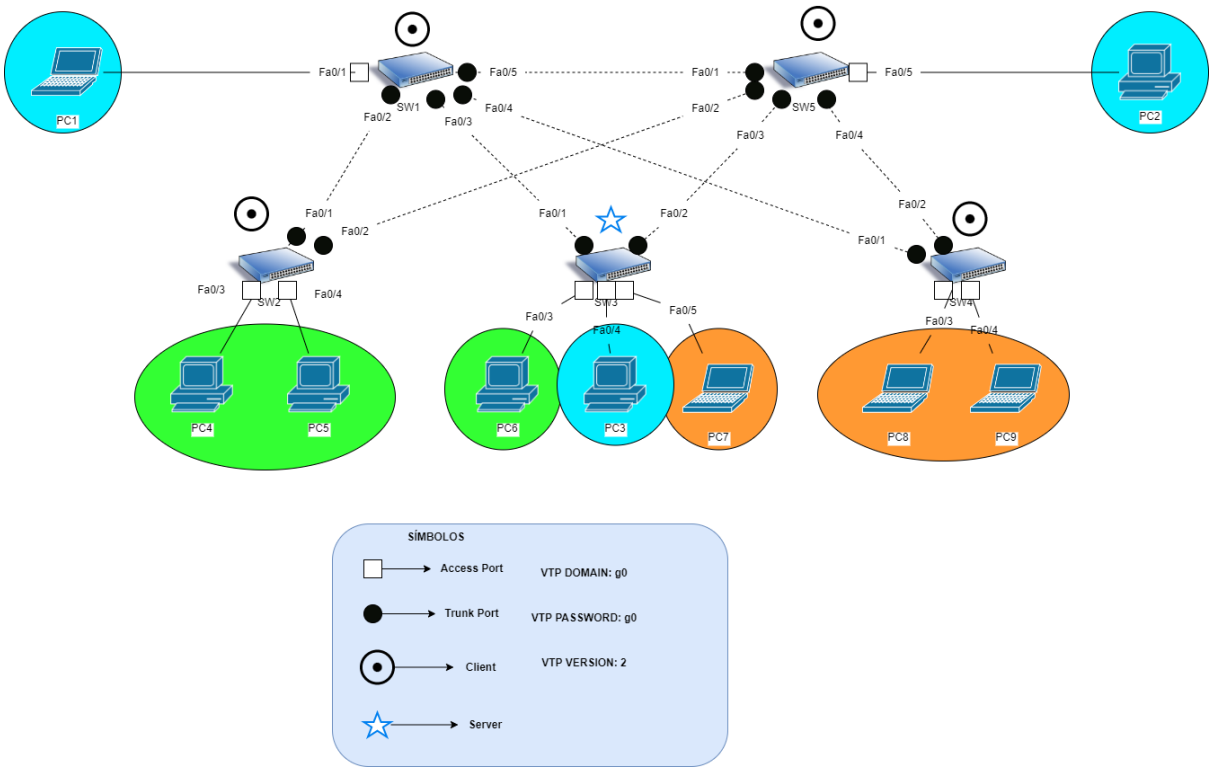
Tabla de Prioridad

	SW1	**SW2**	**SW3**	**SW4**	**SW5**
FastEthernet0/1	240	240	0	0	240
FastEthernet0/2	240	240	64	128	240
FastEthernet0/3	64	240	240	64	128
FastEthernet0/4	64	240	240	64	128
FastEthernet0/5	240	-	64	-	240

Tabla de Estado

	SW1	**SW2**	**SW3**	**SW4**	**SW5**
FastEthernet0/1	blocked	blocked	root	root	blocked
FastEthernet0/2	blocked	blocked	designated	alternate	blocked
FastEthernet0/3	designated	blocked	blocked	designated	alternate
FastEthernet0/4	designated	blocked	blocked	designated	alternate
FastEthernet0/5	blocked	-	designated	-	blocked

TOPOLOGÍA SPANNING-TREE CONFIGURACIÓN DE PUERTOS [vlan 30]



Configuración del Dispositivo

PRIORIDAD	8192	61440	61440	61440	4096
SWITCH	sw1	sw2	sw3	sw4	sw5
MODO	secondario	normal	normal	normal	primario

Configuración de los Puertos

Tabla de Prioridad

	SW1	SW2	SW3	SW4	SW5
FastEthernet0/1	240	128	64	240	240
FastEthernet0/2	128	0	0	240	64
FastEthernet0/3	128	64	64	240	64
FastEthernet0/4	240	64	240	240	240
FastEthernet0/5	240	-	240	-	240

Tabla de Estado

	SW1	SW2	SW3	SW4	SW5
FastEthernet0/1	blocked	alternate	designated	blocked	blocked
FastEthernet0/2	alternate	root	root	blocked	designated
FastEthernet0/3	alternate	designated	designated	blocked	designated
FastEthernet0/4	blocked	designated	blocked	blocked	blocked
FastEthernet0/5	blocked	-	blocked	-	blocked

CONVERGENCIA

Para esta prueba utilizaremos el switch 1 en el spanning-tree configurado para la vlan 10:

```
--------------------------------
Fa0/4            Desg FWD 19        240.4    P2p
Fa0/1            Desg FWD 19        64.1     P2p
Fa0/2            Desg FWD 19        240.2    P2p
Fa0/3            Root FWD 19        0.3      P2p
Fa0/5            Altn BLK 19        128.5    P2p
```

Pasos a seguir para medir la convergencia:

1. Desconectar el puerto Fa0/3 del switch 1 que conecta al switch 3.
2. Medir el tiempo hasta que todos los puertos estén en FWD o BLK.
3. Anotar resultados.
4. Conectar el puerto Fa0/3 del switch 1 al switch 3.
5. Medir el tiempo hasta que todos los puertos estén en FWD o BLK.

6. Anotar resultados.

Tanto en el protocolo PVST y RPVST se realizó este procedimiento, estos son los resultados:

PVST

Puerto Cambiado: el tiempo que le tomó al switch reconocer que no tiene el puerto Fa0/3 y empezar a establecer la nueva configuración.

Puerto FWD/BLK: tiempo que tardó el switch en establecer todos los puertos en FWD y BLK.

Prueba Desconexión

	Puerto Cambiado	**Puerto FWD/BLK**
Tiempo 1	<1s	29.89 s
Tiempo 2	<1s	27.85 s
Tiempo Promedio	INMEDIATO	28.87 s
NOTA	(inmediato, no fue posible documentar correctamente)	(Datos aproximados)

Prueba Conexión

	Puerto Cambiado	**Puerto FWD/BLK**
Tiempo 1	<1s	31.46 s
Tiempo 2	<1s	30.67 s
Tiempo Promedio	INMEDIATO	31.06 s
NOTA	(inmediato, no fue posible documentar correctamente)	(Datos aproximados)

Ya que los tiempos de desconexión y conexión son muy similares sumaremos los tiempos de cada prueba (desconexión y conexión) y nos da como promedio: **29.97 s** que tarda en converger aproximadamente.

RPVST

Prueba Desconexión

	Puerto Cambiado	Puerto FWD/BLK
Tiempo 1	<1s	<1s
Tiempo 2	<1s	<1s
Tiempo Promedio	INMEDIATO	INMEDIATO
NOTA	(inmediato, no fue posible documentar correctamente)	(inmediato, no fue posible documentar correctamente)

Prueba Conexión

Puerto de recuperación de root: Tiempo que tardó el puerto root y demás puertos troncales en recuperarse.

	Puerto Cambiado	Puerto FWD/BLK	Puerto de Recuperación de Root
Tiempo 1	<1s	22.57 s	8.43 s
Tiempo 2	<1s	25.23 s	10.24 s
Tiempo Promedio	INMEDIATO	23.9 s	9.34 s
NOTA	(inmediato, no fue posible documentar correctamente)	(Datos aproximados)	Todos los puertos troncales recuperados excepto el puerto de acceso

El protocolo RPVST demuestra ser el mejor para cuando ocurren problemas de red ya que vuelve a calcular todo el enrutado inmediatamente, es complicado de documentar el tiempo de recuperación.

Sin embargo, en este protocolo ocurren dos fenómenos curiosos:

1. Cuando se vuelve a reintroducir un puerto que había sido eliminado, toma bastante tiempo en volver a configurar todos los puertos para el ruteo, en nuestra prueba tomó casi 23.9 s en promedio y aproximadamente.

2. Sin embargo, los puertos troncales que se comunican a otros switches se recuperan bastante rápido, siendo en promedio su recuperación en 9.34 s.

RESULTADOS

- El protocolo RPVST es más rápido que el PVST en tema de convergencia.
- El protocolo RPVST es inmediato en configurar otra vez sus tablas de ruteos cuando un puerto es desconectado, pero le toma tiempo volver a configurar los ruteos en un puerto que había sido desconectado y es conectado.