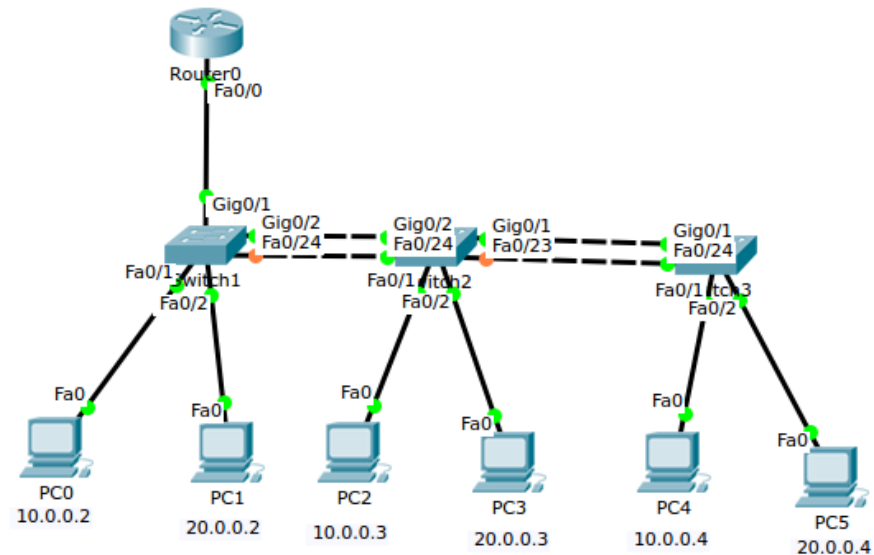


Practica 9 Final

Nombre: Christofer Fabián Chávez Carazas

Se muestra el escenario que debe implementar a partir de las siguientes especificaciones



Arquitectura construida

Pruebe la conectividad haciendo ping entre las PCs de las VLAN

Successful	PC0	PC2	ICMP	0.000	N
Successful	PC0	PC4	ICMP	0.000	N
Successful	PC2	PC4	ICMP	0.000	N

Ping entre las PCs de la VLAN 10

Successful	PC0	PC2	ICMP	0.000	N
Successful	PC0	PC4	ICMP	0.000	N
Successful	PC2	PC4	ICMP	0.000	N

Ping entre las PCs de la VLAN 20

Verificar puertos STP (Spanning-Tree Protocol)

```

S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0002.4A18.C334
            Cost        4
            Port        25 (GigabitEthernet0/1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0005.5EDA.E44E
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20







Interface                Role Sts Cost      Prio.Nbr Type
-----
Gi0/1                    Root FWD 4         128.25 P2p
Gi0/2                    Desg FWD 4         128.26 P2p
Fa0/23                   Desg LSN 19        128.23 P2p
Fa0/24                   Desg FWD 19        128.24 P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
            Address     0002.4A18.C334
            Cost        4
            Port        25 (GigabitEthernet0/1)

```

Puertos STP del Switch 2

Verificar la conectividad total

	Successful	PC4	PC5	ICMP		0.000	N
	Successful	PC3	PC2	ICMP		0.000	N
	Successful	PC0	PC1	ICMP		0.000	N

Ping entre PCs de diferentes VLAN

CUESTIONARIO

1. Describa los protocolos VTP, STP y DTP

VTP

El VLAN Trunk Protocol (VTP) reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo de propiedad de Cisco que está disponible en la mayoría de los productos de la serie Cisco Catalyst. El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se deben resetear los

números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda tener mucho cuidado al usar VTP cuando haya cambios de topología, ya sean lógicos o físicos. Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

STP

El protocolo spanning tree (STP) fue desarrollado para enfrentar estos inconvenientes. STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al realizar un bloque de forma intencional a aquellas rutas redundantes que puedan ocasionar un bucle. Un puerto se considera bloqueado cuando el tráfico de la red no puede ingresar ni salir del puerto. Esto no incluye las tramas de unidad de datos del protocolo comúnmente llamadas (BPDU) utilizadas por STP para evitar bucles. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active.

DTP

El protocolo de enlace dinámico (DTP) se utiliza para negociar la formación de un tronco entre dos dispositivos Cisco. El DTP causa mayor tráfico y está habilitado de forma predeterminada, pero puede estar deshabilitado. Las interfaces troncales Ethernet soportan diferentes modos de trunking. Una interfaz se puede establecer en trunking o no trunking, o para negociar trunking con la interfaz vecina. La negociación de troncales es gestionada por el protocolo de enlace dinámico (DTP), que funciona de forma punto a punto únicamente, entre dispositivos de red.

Switchport mode dynamic auto

Hace que la interfaz sea capaz de convertir el enlace a un enlace troncal. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo troncal o deseable. El modo de switchport predeterminado para las interfaces Ethernet de conmutador Cisco más nuevas es auto dinámico. Tenga en cuenta que si dos switches Cisco se dejan a la configuración predeterminada común de auto, nunca se formará un tronco.

Switchport mode dynamic deseable

Hace que la interfaz intente activamente convertir el enlace a un enlace troncal. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en tronco, deseable o modo automático. Este es el modo de switchport predeterminado en conmutadores antiguos, como los switches Catalyst 2950 y 3550.

Switchport mode trunk

Pone la interfaz en el modo de trunking permanente y negocia para convertir el enlace vecino en un enlace troncal. La interfaz se convierte en una interfaz troncal incluso si la interfaz vecina no es una interfaz troncal.

Switchport nonegotiate

Evita que la interfaz genere marcos de DTP. Puede utilizar este comando sólo cuando el modo switchport de interfaz es acceso o tronco. Debe configurar manualmente la interfaz vecina como interfaz de troncal para establecer un enlace troncal.

2. ¿Qué tipo de seguridad se puede establecer sobre VTP?

VTP puede operar sin autenticación, en cuyo caso resulta fácil para un atacante falsificar paquetes VTP para añadir, cambiar o borrar la información sobre las VLANs. Existen herramientas disponibles gratuitamente para realizar esas operaciones. Debido a eso se recomienda establecer un password para el dominio VTP y usarlo en conjunto con la función hash MD5 para proveer autenticación a los paquetes VTP. Resulta de vital importancia para los enlaces troncales de la VLAN.

CONCLUSIONES

- Las VLAN son muy usadas en la práctica como en organizaciones empresariales grandes, por esta razón es muy importante saber que son las VLAN y cómo se implementan.
- Existen varios protocolos que ayudan a la seguridad, una mejor administración de la red (VTP y DTP) y para evitar errores en la red (STP).

BIBLIOGRAFIA

- “Cómo Comprender VLAN Trunk Protocol (VTP)” CISCO
- “Introducción y Configuración del Spanning Tree Protocol (STP) en los Switches Catalyst” CISCO