

## LABORATORIO 2. REDES VTP

### 2.1. OBJETIVO

En esta práctica veremos cómo dos redes de VLANs a través de conexiones troncales VPT y asignar puertos a ellas en conmutadores con Cisco IOS.

### 2.2. FUNDAMENTO TEORICO

U VTP son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos:

- Servidor
- Cliente
- Transparente

#### **Servidor:**

Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk. Debe haber al menos un servidor. Se recomienda autenticación MD5.

#### **Cliente:**

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

#### **Transparente:**

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar

localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio. Puntos a considerar en los siguientes subtítulos

- Funcionamiento de un puente/conmutador Ethernet
- Otros
- 

### 2.2.1. SUBTITULO 1

Desarrollo del subtítulo 1....

Figura 2.1 Títulos de Grafico

### 2.2.2. SUBTITULO 2

Desarrollo del subtítulo 2....

Figura 1.2 Títulos de Grafico

### 2.2.3. SUBTITULO 3

Desarrollo del subtítulo 2.....

Figura 1.3 Títulos de Grafico

## 2.3. MATERIALES, EQUIPOS, HERRAMIENTAS Y SOFTWARE

### MATERIALES

- 3 cables directos
- 2 cables cruzados

### EQUIPOS

- 3 PCs
- 1 router Cisco con 2 interfaces Ethernet
- 2 conmutadores Cisco Catalyst

### HERRAMIENTAS

- 1 alicate de corte
- 1 alicate de punta

## SOFTWARE

- 1 PC con el software “Simulador Packet Tracer by Cisco Systems”.

## 2.4. DESARROLLO Y PROCEDIMIENTOS DE LA PRÁCTICA

1. Si se requiere implementar muchas vlan en una topología formada por múltiples switch, se deberá sacrificar parejas de puerto de acceso diferentes entre ellos, para que host de cada vlan se comuniquen en toda la red, tal como se muestra en la Figura 2.4.1. siguiente:

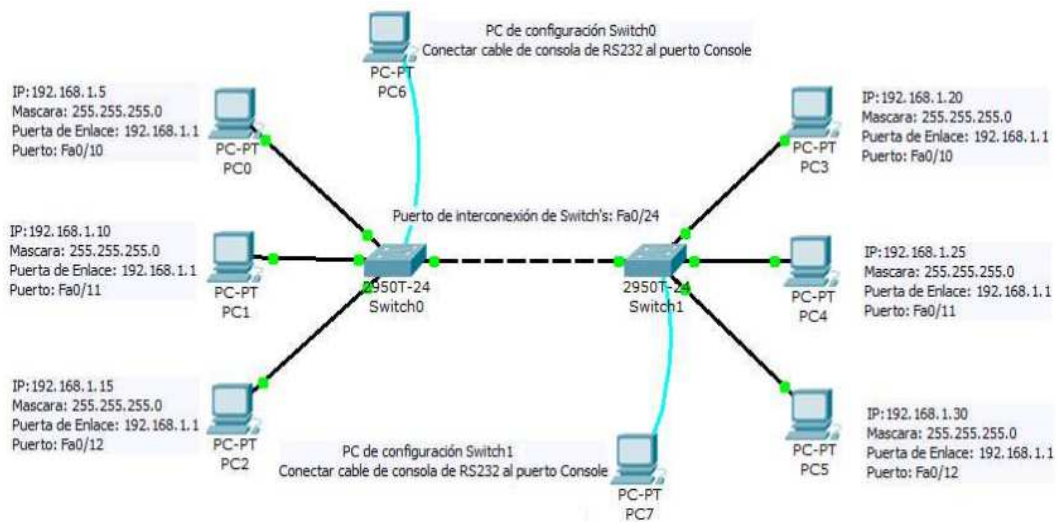


Figura 2.4.1 Circuito de Simular

2. Como respuesta a esta situación, se pueden configurar puertos en modo troncal (mode trunk), que permiten comunicar tráfico de tramas de múltiples vlan entre los diferentes switch.
3. Retorne a la terminal en PC6, para definir al puerto fa0/24 de Switch0 en modo troncal, con los siguientes comandos:

### PARTE 1. CONFIGURACION EN EL CLI DEL IOS DEL SWITCH

4. Retorne a la terminal en PC6, para definir al puerto fa0/24 de Switch0 en modo troncal, con los siguientes comandos:

```

Switch0#configure terminal
Switch0(config)#interface fastethernet 0/24
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#CTRL+Z

```

Figura 2.4.2 Configuración de puertos modo troncal

5. Ejecute los mismos comandos para el Switch1. Al final, con el puerto fa0/24 de ambos switch, se formara un “enlace troncal”.
6. Elimine todos los enlaces que conectan a ambos switch, excepto el del puerto fa0/24.
7. Evalúe si los host de la vlan 20 se logran comunicar ahora. Haga una prueba similar entre las parejas de las vlan restantes.
8. Todas las pruebas deberían ser realizadas con éxito, ya que cada pareja de host pertenecen a la misma vlan y por tanto al mismo dominio de broadcast. Se han creado 3 dominios de broadcast (vlan’s) divididos por agrupación de puertos de acceso en los switch.
9. Proceda a guardar la configuración de cada uno de los switch’s, caso contrario al apagarlos, la configuración hecha en memoria RAM se perderá. Para ello siga los siguientes pasos (Figura 2.4.2) en cada Switch:

Switch1>enable	Pasa a modo privilegiado
Switch1#copy run start	Copia a memoria la configuración del Switch
Destination filename [startup-config]?	Presionar ENTER para proceder a guardar
Building configuration... [OK]	Espere a que muestre OK, indicando que la copia fue guardada.
Switch1#	

Figura 2.4.3 Configuración de puertos modo troncal

10. Guarde los últimos cambios en la simulación y cierre el archivo.
11. Genere la descripción sobre los comandos disponibles en este modo. Presione continuamente a tecla Enter para ver el listado completo de comandos disponibles.
12. Retorne al modo EXEC privilegiado. Después ejecute el comando clock ? y analice la ayuda devuelta.

13. Con el parámetro set, se puede establecer/definir una nueva fecha-hora para el sistema. Escriba clock con el parámetro set y la ayuda contextual: clock set ?
14. Proceda a cambiar la hora del sistema del switch, ejecutando comando clock set 16:30:23 21 february 2016 Confirme si cambio la hora, ejecutando comando show clock
15. Ejecute nuevamente a clock pero con los parámetros incorrectos, así: clock set 16:30:23 40 february 2015 Observe como el CLI responde al ingresar incorrectamente el nombre y/o valor de los parámetros de un comando.

**PARTE 2. VERIFICACION DE VLANs POR DEFECTO**

16. Para continuar, revise el estado de configuración de las VLAN configuradas en Switch0, ejecutando el comando: show VLAN. Observe el resultado en la Figura 1.4.4. Al final de la pantalla se muestra un mensaje que dice: "More", presione Enter para poder ver en su totalidad la información de las VLAN's. Inicialmente ya hay creadas varias vlan. Pero todos los puertos del switch (Fa0/0 hasta el Fa0/24) están asociados a la vlan 1, llamada default.

```
Switch#show vlan
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24

1002 fddi-default         act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup

VLAN Type  SAID      MTU   Parent  RingNo  BridgeNo  Stp    BrdgMode  Trans1  Trans2
-----
1    enet    100001   1500   -       -        -       -         0       0
1002 fddi    101002   1500   -       -        -       -         0       0
1003 tr     101003   1500   -       -        -       -         0       0
1004 fdnet 101004   1500   -       -        -       ieee     0       0
1005 trnet 101005   1500   -       -        -       ibm      0       0

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
Switch#
```

Figura 1.4.4 Pantalla de Configuración VLAN

17. Realice pruebas de conectividad entre PCs haciendo ping entre parejas de los Host's del mismo lado y conectados a switch diferentes. Se deberá de obtener resultados satisfactorios en todos los casos ya que Guía #05: Virtual Local Área Network (VLAN) 12 las 6 Pc's están dentro de una misma subred y todos sus parámetros se encuentran correctamente configurados.
18. Retorne a la ventana del Terminal en la PC6 y observe la tabla de direcciones MAC registradas en el Switch0, ejecutando al comando: show mac-address-table.

### **PARTE 3 CREACION DE VLANs**

19. Proceda a configurar en el Switch0 a las VLANs de Ventas, Bodegas y Finanzas, ejecutando la siguiente secuencia de comandos desde el modo de configuración global: