UNIVERSIDAD EIA

Administración de Redes

Simulación # 7

OBJETIVOS DE APRENDIZAJE:

- Configurar S1 como servidor VTP.
- Configurar S2 y S3 como clientes VTP.
- Configurar las VLAN en S1.
- Configurar enlaces troncales en S1, S2 y S3.
- Verificar el estado del VTP en S1, S2 y S3.
- Asignar VLAN a puertos en S2 y S3.
- Verificar la implementación de VLAN y probar.

INTRODUCCIÓN:

En esta actividad, se practica la configuración del VTP y la configuración de VLANs y enlaces troncales.

DIAGRAMA DE TOPOLOGÍA:

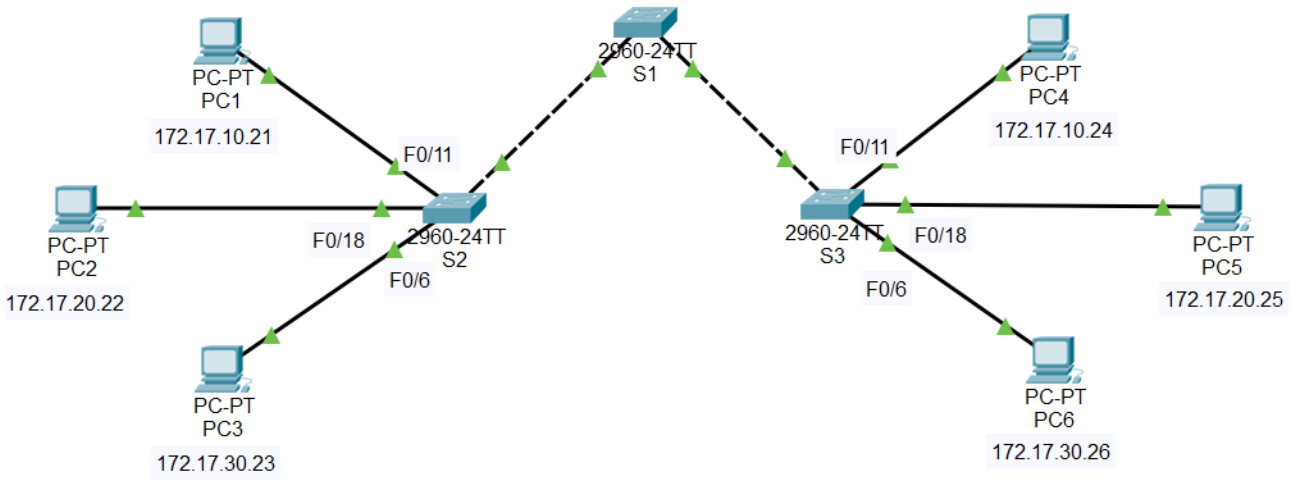

Figura 1 Diagrama de Topología

TABLA DE DIRECCIONAMIENTO:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway Predeterminado
S1	VLAN 99	172.17.99.31	255.255.255.0	NA
S2	VLAN 99	172.17.99.32	255.255.255.0	NA
S3	VLAN 99	172.17.99.33	255.255.255.0	NA
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

TAREA 1: Realizar configuraciones básicas del switch

Realice la configuración básica en los tres switches.

- Configure los nombres de host del switch.
- Deshabilite la búsqueda del DNS.
- Configure una contraseña del modo EXEC privilegiado encriptado en **clase**.
- Configure la contraseña **redes** para las conexiones de consola.
- Configure la contraseña **redes** para las conexiones vty.
- Configure la dirección IP de la interfaz vlan 99 en cada switch

TAREA 2: Configurar el S1 como servidor VTP

Paso 1. Configure el comando del modo VTP.
El S1 es el servidor para el VTP. Establezca el S1 en modo servidor.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Observe que el switch ya está establecido para el modo servidor por defecto. Sin embargo, es importante que usted configure este comando de manera explícita para asegurarse que el switch esté en modo servidor.

Paso 2. Configure el nombre del dominio VTP.
Configure el S1 con **SIMULACION** como nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen mayúsculas de minúsculas.

```
S1(config)#vtp domain SIMULACION
Changing VTP domain name from NULL to SIMULACION
S1(config)#
```

Paso 3. Configure la contraseña de dominio VTP.
Configure el S1 con **redes** como contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

```
S1(config)#vtp password redes
Setting device VLAN database password to redes
S1(config)#
```

Paso 4. Confirme los cambios de configuración.
Utilice el comando **show vtp status** del S1 para confirmar que el modo y el dominio VTP se configuraron correctamente.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : SIMULACION
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Para verificar la contraseña VTP, utilice el comando **show vtp password**.

```
S1#show vtp password
VTP Password: redes
S1#
```

TAREA 3: Configurar S2 y S3 como clientes VTP

Paso 1. Configure el comando del modo VTP.
El S2 y el S3 son clientes VTP. Establezca estos dos switches en modo cliente.

Paso 2. Configure el nombre del dominio VTP.
Antes de que S2 y S3 acepten las publicaciones VTP desde S1, deben pertenecer al mismo dominio VTP. Configure S2 y S3 con **SIMULACION** como el nombre de dominio de VTP. Recuerde que los nombres de dominio VTP distinguen mayúsculas de minúsculas.

Paso 3. Configure la contraseña de dominio VTP.
Además, S2 y S3 deben utilizar la misma contraseña antes de que puedan aceptar las publicaciones VTP del servidor VTP. Configure S2 y S3 con **redes** como la contraseña de dominio de VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

Paso 4. Confirme los cambios de configuración.
Utilice el comando **show vtp status** de cada switch para confirmar que el modo y el dominio VTP se configuraron correctamente. Aquí se muestra el resultado para el S3.

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : SIMULACION
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que el número de revisión de la configuración es 0 en los tres switches. ¿Por qué?
Para verificar la contraseña VTP, utilice el comando **show vtp password**.

```
S3#show vtp password
VTP Password: redes
S3#
```

TAREA 4: Configurar las VLAN en S1

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switches en el dominio VTP. En esta tarea, usted crea 4 VLAN nuevas en el servidor VTP del S1. Estas VLAN se distribuyen al S2 y al S3 por medio del VTP.

Paso 1. Cree las VLAN.

Para efectos de calificación en Packet Tracer, los nombres de las VLAN distinguen mayúsculas de minúsculas.

- VLAN 10 con el nombre **Faculty/Staff**
- VLAN 20 con el nombre **Students**
- VLAN 30 con el nombre **Guest(Default)**
- VLAN 99 con el nombre **Management&Native**

Paso 2. Verifique las VLAN.

Utilice el comando **show vlan brief** para verificar las VLAN y sus nombres.

```
S1#show vlan brief

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
                                            Gig1/1, Gig1/2
10   Faculty/Staff                active
20   Students                     active
30   Guest(Default)               active
99   Management&Native            active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Si usted ingresa el mismo comando en S2 y S3, observa que las VLAN no se encuentran en su base de datos VLAN. ¿Por qué no?

TAREA 5: Configurar los enlaces troncales en S1, S2 y S3

Utilice el comando **switchport mode trunk** para establecer el modo de enlace troncal para cada uno de los enlaces troncales. Utilice el comando **switchport trunk native vlan 99** para establecer la VLAN 99 como la VLAN nativa.

Paso 1. Configure FastEthernet 0/1 y FastEthernet 0/2 en el S1 para el enlace troncal.

Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

Una vez configurado, el Protocolo de enlaces troncales dinámicos (VTP) muestra los enlaces troncales. Puede verificar que el S2 y el S3 se estén enlazando al ingresar el comando **show interface fa0/1 switchport** en S2 y el comando **show interface fa0/2 switchport** en S3.

Si espera unos minutos para que Packet Tracer simule todos los procesos, S1 notifica la configuración VLAN a S2 y S3. Esto se puede verificar en S2 o S3 con los comandos **show vlan brief** y **show vtp status**.

No obstante, se recomienda configurar ambos extremos de los enlaces troncales en el modo **on**.

Paso 2. Configure Fast Ehternet 0/1 en el S2 para el enlace troncal.
Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

Paso 3. Configure Fast Ethernet 0/2 en el S3 para el enlace troncal.
Ingrese los comandos apropiados para configurar el enlace troncal y establecer la VLAN 99 como VLAN nativa.

TAREA 6: Verificar el estado del VTP

Use los comandos **show vtp status** y **show vlan brief** para verificar lo siguiente.

- S1 debe mostrar el estado del servidor.
- S2 y S3 deben mostrar el estado de cliente.
- S2 y S3 deben tener VLAN de S1.

Nota: Las publicaciones de VTP se saturan a través del dominio de administración cada cinco minutos o siempre que se efectúe una modificación en las configuraciones de la VLAN. Para acelerar este proceso, puede alternar entre el modo de tiempo real y el modo de simulación hasta la próxima vuelta de actualizaciones. Sin embargo, es posible que deba hacerlo varias veces, ya que esto sólo adelanta el reloj de Packet Tracer 10 segundos cada vez. Otra opción es cambiar uno de los switches cliente al modo transparente y luego regresar al modo cliente. (Los números de revisión de la configuración pueden variar en los routers reales en comparación con los routers de Packet Tracer. El objetivo de esta actividad no es calificar los números de revisión de la configuración.)

¿Cuál es el número de revisión de la configuración?

¿Es el número de revisión de la configuración mayor que la cantidad de VLAN que creó?

¿Cuál es el número actual de las VLAN existentes?

¿Por qué existen más VLAN que las cuatro que usted creó?

NOTA: Si los switches que se encuentran en modo cliente no poseen la misma información que el switch que se encuentra en modo servidor esto significa que no podrán notificar la información de las VLANs, por lo tanto es necesario que revise que la contraseña en todos los switches sea la misma usando el comando **show vtp password** en el modo EXEC privilegiado.
Si la contraseña no es igual o no existe en alguno de los switches deberá configurarla. Esto solo puede hacerse cuando ya el dominio fue creado o publicado por el switch servidor.
Todos los switches que participen del VTP deben tener el mismo nombre de dominio y la misma contraseña en caso de tenerla.

Tarea 7: Asignar VLAN a los puertos

Use el comando **switchport mode access** para establecer el modo de acceso de los enlaces de acceso. Use el comando **switchport access vlan** *id de la VLAN* para asignar una VLAN a un puerto de acceso.

Paso 1. Asigne VLAN a los puertos de S2.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

Paso 2. Asigne VLAN a los puertos en S3.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

TAREA 8: Verificar la implementación de VLAN y probar la conectividad

Paso 1. Verifique la configuración de la VLAN y las asignaciones de puertos.

Utilice el - para verificar la configuración de la VLAN y la asignación de puertos en cada switch. Compare su resultado con la topología.

Paso 2. Pruebe la conectividad entre las PC.

Los pings entre las PC de la misma VLAN deben tener éxito, mientras que los pings entre PC de diferentes VLAN deben fallar.

Desde PC1, haga ping a PC4.
Desde PC2, haga ping a PC5.
Desde PC3, haga ping a PC6.

PRÁCTICA FINALIZADA. GUARDE LA SIMULACIÓN.

NOTA: Práctica basada en CCNA EXPLORATION, 2010