

## CONFIGURACIÓN DEL CONMUTADOR ETHERNET 2950, NAT Y PAT

Las redes de área local modernas se basan en la interconexión de conmutadores Ethernet multicapa: conmutadores de acceso, conmutadores de distribución y conmutadores de núcleo. Dichos dispositivos conforman una infraestructura básica que permite suministrar los diferentes servicios de red –acceso a aplicaciones institucionales, acceso a Internet, acceso al servicio de voz, entre otros– con la seguridad y desempeño requerido por el usuario. En la presente sesión se abordarán los temas y procedimientos básicos de los conmutadores Ethernet multicapa: crear una VLAN, asignar un puerto a la VLAN creada, extender la operación de una VLAN a varios conmutadores por medio de un enlace troncal IEEE 802.1Q, configurar una dirección MAC estática en un puerto del conmutador y habilitar la característica de seguridad que permite limitar el número de estaciones que se pueden conectar a un puerto del conmutador. También se aborda la traducción (o traslado) de direcciones IP y de los números de puerto TCP o UDP mediante el uso de un encaminador que proporciona la función NAT/PAT.

### OBJETIVO

Al finalizar esta unidad, el estudiante estará en capacidad de:

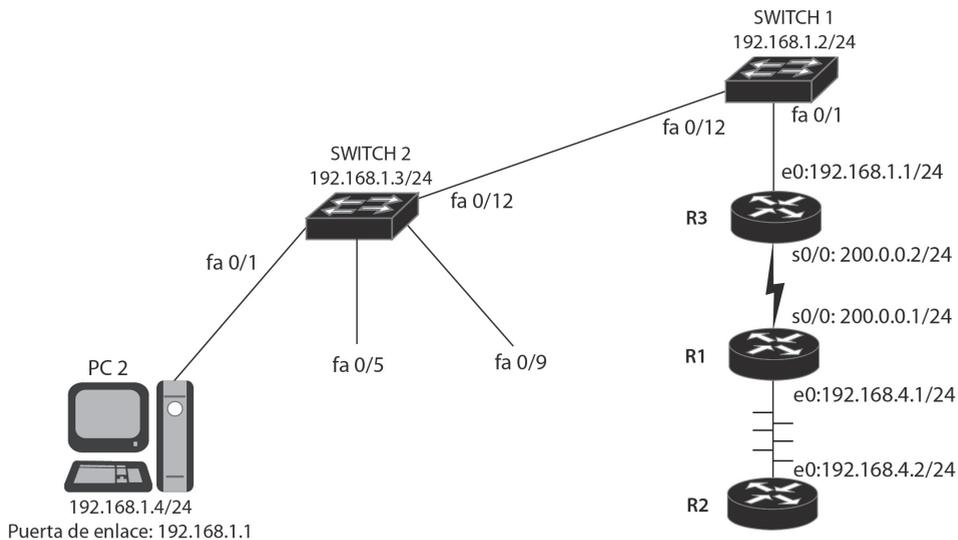
- Usar los comandos básicos para la configuración de un conmutador Ethernet Cisco 2950, 3550 ó 3560.
- Configurar varias VLAN en el conmutador 2950.
- Configurar la función de NAT/PAT en un encaminador Cisco.

## PROCEDIMIENTO

### Configuración del Conmutador Ethernet 2950

#### Actividad 1. Comandos básicos del conmutador 2950

1. Montar la red de la Figura 10.1 usando los equipos del laboratorio, o el GNS3, o el software BOSON NETSIM Router Simulator.



**Figura 10.1. Diagrama de red para practicar conceptos alrededor de VLAN, NAT y PAT**

2. Entrar al Switch1. Conectar el puerto serie de un PC al puerto de consola del Switch1 o establecer dicha conexión de manera virtual. Digitar la tecla [Enter] para obtener el prompt en modo de usuario. Con el comando *enable*, pasarse a modo privilegiado. Usar el comando “?” para ver la lista de comandos del modo privilegiado. Con el comando *disable*, regresar al modo de usuario.

```
Switch> enable
Switch# ?
Switch# disable
Switch>
```

3. En el Switch1, desde el modo privilegiado pasarse al modo de configuración global. Asignarle al conmutador el nombre 2950sw1. Use Exit o [CNTL] Z para salir del modo de configuración.

```
Switch# configure terminal
Switch(config)# hostname 2950sw1
2950sw1(config)# exit
2950sw1#
```

4. En el Switch1, digite el comando *show running-config* para ver la configuración activa.

```
2950sw1# show running-config
```

5. En el Switch1, digite el comando *copy running-config startup-config*. Con el comando *show startup-config*, liste la configuración salvada.

```
2950sw1# copy running-config startup-config
2950sw1# show startup-config
```

6. En el Switch1, borrar la configuración salvada y reiniciar el conmutador.

```
2950sw1# erase startup-config
2950sw1# reload
```

7. En el Switch1, entre a modo de configuración global y asigne nuevamente el nombre del conmutador para que sea 2950sw1, configure el enable password para que sea “univalle”. Asígnele al conmutador la dirección IP 192.168.1.2 con máscara de subred 255.255.255.0. Asígnele al conmutador una puerta de enlace por defecto (default Gateway) de 192.168.1.1 (la dirección IP del encaminador R3).

```
Switch(config)# hostname 2950sw1
2950sw1(config)# enable password univalle
2950sw1(config)# interface vlan1
2950sw1(config-if)# ip address 192.168.1.2 255.255.255.0
2950sw1(config-if)# no shutdown
2950sw1(config-if)# exit
2950sw1(config)# ip default-gateway 192.168.1.1
```

8. En el Switch1, use el comando *show interface vlan1* para verificar que la dirección IP y la máscara tienen los valores correctos.

```
2950sw1# show interface vlan1
```

9. En el Switch1, use el *comando show interface*.

```
2950sw1# show interface
```

- a. ¿Cuál es el estado del spanning tree (IEEE 802.1d) de la interfaz fa0/1? Ver el comando *show spanning-tree*.
  - b. ¿Cuál es la configuración dúplex de la interfaz fa0/2?
10. En el Switch2, entre a modo de configuración global y configure el nombre del conmutador para que sea 2950sw2; configure el enable secret password para que sea “univalle”. Asignele al conmutador la dirección IP 192.168.1.3 con máscara de subred 255.255.255.0. Asignele al conmutador una puerta de enlace por defecto (default Gateway) de 192.168.1.1. ¿Cuál es la versión del IOS del Switch2 que muestra el comando *show version*?

```
Switch(config)# hostname 2950sw2
2950sw2(config)# enable secret univalle
2950sw2(config)# interface vlan1
2950sw2(config-if)# ip address 192.168.1.3 255.255.255.0
2950sw2(config-if)# no shutdown
2950sw2(config-if)# exit
2950sw2(config)# ip default-gateway 192.168.1.1
2950sw2# show version
```

11. En el Switch2, introduzca el comando *show spanning-tree*.

```
2950sw2# show spanning-tree
```

- a. ¿Cuál es la dirección del root bridge (root switch)?
  - b. ¿Cuál es el costo de puerto de la interfaz fa0/1?
  - c. ¿Cuál es el valor para el “MaxAge Timer”?
  - d. ¿Cuál es el valor para el “Hello Timer”?
12. En el Switch2, ingrese el comando *show mac-address-table*. ¿En cuáles puertos hay entradas indicando que hay dispositivos conectados?

```
2950sw2# show mac-address-table
```

13. En el Switch2, asigne permanentemente un dispositivo con dirección MAC 1111-2222-3333 al puerto fa0/5. Use el comando *show mac-address-table* para verificar que el dispositivo está en la tabla como una entrada permanente.

```
2950sw2(config)# mac-address-table static 1111-2222-3333 vlan 1 int fa0/5
2950sw2(config)# exit
2950sw2# show mac-address-table
```

14. En el Switch2, configure la característica de seguridad para el puerto fa0/9 (port security). El conmutador aprenderá de forma permanente la dirección MAC del dispositivo que se conecte por primera vez al puerto fa0/9 (sticky learn) y en el futuro solamente permitirá la operación de dicho dispositivo.

```
2950sw2(config)# interface fa0/9
2950sw2(config-if)# switchport port-security
2950sw2(config-if)# switchport port-security maximum 1
```

### **Actividad 2. VLAN y Troncales (Conmutador Catalyst 2950)**

1. En esta actividad usted configurará una VLAN en el Switch1 y en el Switch2. El funcionamiento de la VLAN lo probará por medio de un ping desde el PC2 hacia el encaminador R3. El encaminador R3 está conectado a la interfaz fa0/1 del Switch1 y el PC2 está conectado a la interfaz fa0/1 del Switch2. Los equipos Switch1 y Switch2 se interconectan por medio de sus interfaces fa0/12.
2. Configurar PC2 con la dirección IP 92.168.1.4 /24 y su puerta de enlace en 192.168.1.1. Configurar la interfaz e0 de R3 con la dirección IP 192.168.1.1 /24.
3. Verificar que se pueda hacer ping entre PC2 y el encaminador R3. En caso de no obtener un ping exitoso, verifique que la dirección IP de la interfaz FastEthernet 0/0 de R3 sea 192.168.1.1 /24 y que ella se encuentra habilitada. También verifique la configuración de PC2.

```
PC2> ping 192.168.1.1
```

4. En los equipos Switch1 y Switch2, ejecute el comando *show vlan*. Se podrá notar que, por defecto, todos los puertos de los conmutadores están en la VLAN 1. Puesto que el PC2, el encaminador R3 y el enlace entre los conmutadores están en la VLAN 1 (que es la VLAN nativa), se debe

tener conectividad entre el PC2 y el encaminador R3 por medio de un ping.

```
2950swx# show vlan
```

5. En los equipos Switch1 y Switch2, configure un dominio llamado **prueba**. Verifique la creación del mismo mediante el comando *show vtp status*. Nota: En la nomenclatura que sigue se utiliza 2950swx para indicar que los comandos se deben ejecutar tanto en el equipo 2950sw1 (Switch1) como en el equipo 2950sw2 (Switch2).

```
2950swx# vlan database
2950swx(vlan)# vtp domain prueba
2950swx(vlan)# ctrl-z
2950swx# show vtp status
```

6. En los equipos Switch1 y Switch2, crear la VLAN 16, llamarla **invitados**. Verifique la creación de la misma mediante el comando *show vlan*.

```
2950swx# vlan database
2950swx(vlan)# vlan 16 name invitados
2950swx(vlan)# exit
2950swx# show vlan
```

¿Hay algún puerto conectado a la VLAN 16? De no ser así ¿cuál es la razón?

7. En los equipos Switch1 y Switch2, asigne los puertos fa0/1 a la VLAN 16. El encaminador R3 y el PC2 están conectados a estos puertos. Ejecute el comando *show vlan* para verificar que los puertos han sido movidos a la VLAN 16.

```
2950swx(config)# interface fa0/1
2950swx(config-if)# switchport mode access
2950swx(config-if)# switchport access vlan 16
2950swx(config-if)# ctrl-z
2950swx# show vlan
```

8. Ahora que tanto el PC2 como el encaminador R3 están en la VLAN 16, trate de hacer ping entre el PC2 y el encaminador R3. ¿Si ambos dispositivos están en la misma VLAN, por qué debe fallar el ping?

9. Haga que el enlace entre el Switch1 y el Switch2 sea una troncal capaz de llevar tráfico de cualquier VLAN de la red. Use el comando *show interface fa0/12 switchport* para verificar que en el puerto fa0/12 de ambos conmutadores está habilitada la capacidad de llevar información de las diferentes VLAN por dicho enlace troncal.  
¿Qué protocolo de troncal usa por defecto el 2950 - ISL o IEEE 802.1Q?

```
2950swx(config)# interface fa0/12
2950swx(config-if)# switchport mode trunk
2950swx(config-if)# ctrl-z
2950swx# show interface fa0/12 switchport
```

10. Haga ping entre PC2 y el encaminador R3. El ping debe dar resultados exitosos, puesto que ambos dispositivos se encuentran en la misma VLAN y el enlace entre los conmutadores es una línea troncal con capacidad de llevar tráfico de cualquier VLAN.

```
PC2> ping 192.168.1.1
```

### INFORME

- Responder las preguntas de los puntos 9, 10, 11 y 12 de la actividad 1.  
Responder las preguntas de los puntos 6, 8 y 9 de la actividad 2.

### EJERCICIOS DE LABORATORIO

#### *NAT y PAT (Network Address Translation y Port Address Translation)*

- Este ejercicio tiene como propósito configurar la función NAT/PAT en el encaminador R1. Se configurarán tres formas de traducción de direcciones: traducción estática de direcciones de red, traducción dinámica de direcciones de red y traducción de la dirección de red junto con el puerto (overloading). Teniendo en cuenta la Figura 10.1, configurar las direcciones IP de las siguientes interfaces: Serie 0/0 de R3, Serie 0/0 de R1, Ethernet 0 de R1 y Ethernet 0 de R2. Configurar la puerta de enlace por defecto en R2 con la dirección IP 192.168.4.1.  
También es necesario habilitar el servicio de telnet en el encaminador R3 mediante el comando *login* de configuración de las líneas vty 0 a 4.
- En el encaminador R1, configure NAT para traducir estáticamente la dirección IP 192.168.4.2 de la interfaz Ethernet 0 de R2 a la dirección IP 200.0.0.5.

```
R1(config)# ip nat inside source static 192.168.4.2 200.0.0.5
R1(config)# interface ethernet 0
R1(config-if)# ip address 192.168.4.1 255.255.255.0
R1(config-if)# ip nat inside
R1(config-if)# no shutdown
R1(config)# interface serial 0
R1(config-if)# ip address 200.0.0.1 255.255.255.0
R1(config-if)# ip nat outside
R1(config-if)# no shutdown
```

3. Pruebe la anterior traducción NAT estática. Haga telnet desde el encaminador R2 hacia el encaminador R3 y, una vez haya entrado a R3, ejecute el comando *show users*. La salida a este comando deberá mostrar que al dispositivo que registra el encaminador R3 le corresponde la dirección IP 200.0.0.5 (que es la dirección traducida).

```
R2# telnet 200.0.0.2
R3# show users
```

4. Liste por pantalla la tabla de traducción NAT en el encaminador R1. La salida deberá mostrar que la “dirección IP local interna” (192.168.4.2) ha sido trasladada a la “dirección IP global interna” (200.0.0.5).

¿La “dirección IP global interna” normalmente representa una dirección IP pública o privada?

```
R1# show ip nat translations
```

5. En el encaminador R1, remueva el comando previo de configuración NAT estática y configure NAT para traducir la dirección IP 192.168.4.2 de la interfaz Ethernet 0 de R2 a una dirección IP que sea asignada dinámicamente. Se debe utilizar un pool de direcciones públicas en el rango de 200.0.0.10 a 200.0.0.20.

```
R1(config)# no ip nat inside source static 192.168.4.2 200.0.0.5
R1(config)# ip nat pool pool1 200.0.0.10 200.0.0.20 netmask 255.255.255.0
R1(config)# access-list 1 permit 192.168.4.0 0.0.0.255
R1(config)# ip nat inside source list 1 pool pool1
```

6. Pruebe la anterior traducción NAT dinámica. Haga telnet desde el encaminador R2 hacia el encaminador R3 y, una vez haya entrado a R3,

ejecute el comando *show users*. La salida a este comando deberá mostrar que al dispositivo que registra el encaminador R3 le corresponde la dirección IP 200.0.0.10 (la dirección traducida). También liste por pantalla la tabla de traducción NAT en el encaminador R1 usando el comando *show ip nat translations*.

```
R2# telnet 200.0.0.2
R3# show users
R1# show ip nat translations
```

7. Remueva el comando NAT previo (*ip nat inside source list 1 pool pool1*). Configure NAT overloading (Port Address Translation) en el encaminador R1 para traducir la dirección IP 192.168.4.2 de la interfaz Ethernet 0 de R2 —o cualquier otra dirección de la red 192.168.4.0 /24— a la dirección IP 200.0.0.01 de la interfaz Serie 0 de R1.

```
R1(config)# no ip nat inside source list 1 pool pool1
R1(config)# access-list 1 permit 192.168.4.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface serial 0 overload
```

8. Pruebe la función PAT overloading. Haga telnet desde el encaminador R2 hacia el encaminador R3 y, una vez haya entrado a R3, ejecute el comando *show users*. La salida a este comando deberá mostrar que al dispositivo que registra el encaminador R3 le corresponde la dirección IP 200.0.0.1 (la dirección traducida). También liste por pantalla la tabla de traducción NAT en el encaminador R1 usando el comando *show ip nat translations*.

```
R2# telnet 200.0.0.2
R3# show users
R1# show ip nat translations
```

### INFORMACIÓN COMPLEMENTARIA

El protocolo de árbol de expansión (Spanning Tree Protocol o STP) detecta y elimina los bucles de capa dos en la topología de los conmutadores con el objetivo de evitar tormentas de broadcast. El STP original (norma IEEE 802.1d) se ha vuelto obsoleto para las necesidades actuales, puesto que solamente puede funcionar en una VLAN o en un conmutador que no soporte las VLAN. Cisco resolvió la necesidad de tener STP funcionando en todas las VLAN, mediante los protocolos propietarios PVSTP+

y RPVSTP+ (este último se basa en el estándar IEEE802.1w), los cuales habilitan una instancia Spanning Tree por cada VLAN. Es decir, para estos dos protocolos, cada VLAN en cada conmutador tiene su propio proceso STP en ejecución que le permite eliminar bucles en el dominio de broadcast de la misma. IEEE 802.1s (Multiple Spanning Tree Protocol o MSTP) es un protocolo estándar abierto, implementado por muchos fabricantes, que permite que varias VLAN compartan el mismo proceso STP.

STP usa mensajes BPDU (Bridge protocol data units) para transmitir información entre conmutadores durante la elección del switch raíz o para indicar el costo que tiene un conmutador para llegar al switch raíz. Las BPDU se envían con destino a la consabida dirección multicast STP 0180:c200:0000, usando la dirección MAC única de cada puerto del conmutador como dirección origen. El conmutador que tenga la prioridad más baja será elegido como switch raíz. Y si la prioridad de todos los conmutadores se deja configurada en el valor por defecto (32768), el conmutador que tenga la dirección MAC más baja será elegido como switch raíz.

STP usa el siguiente proceso para eliminar los bucles capa dos de la red (en la descripción de este proceso, algunas veces se usa el término Bridge en lugar de Switch, esto debido a que STP tiene su origen en el Bridge y luego su uso se extendió al Switch).

1. Elección del Root Bridge (Switch raíz): El conmutador con el menor Bridge ID (BID) se vuelve la raíz (root) del árbol de expansión (spanning tree). El Bridge ID consta de 2 bytes que indican la prioridad del conmutador y 6 bytes que indican la dirección MAC del conmutador. La prioridad está en el rango de 0 a 65535; el valor por defecto es 32768. Cuando se tiene un proceso STP por VLAN, los 2 bytes de la prioridad se redefinen para indicar la prioridad mediante los 4 bits más significativos en incrementos de 4096 y la VLAN para la cual se está ejecutando STP, mediante los 12 bits restantes. Como resultado de lo anterior, un conmutador que tenga configurada una prioridad de 24576 para el STP de la VLAN 20, tendrá un Bridge ID de 24596 (24576+20) para dicha VLAN.
2. Elección del puerto raíz: Con excepción del switch raíz (que es el único conmutador de la red que no tiene puerto raíz), cada conmutador de la red elige como único puerto raíz el que tenga el camino de menor costo al switch raíz (el puerto más cercano al switch raíz en términos de costo). El costo del camino al switch raíz se transporta en las BPDU transmitidas por los conmutadores de la red y cada conmutador que reciba una BPDU a lo largo de un camino, le adiciona el costo de su puerto local. El costo del camino al switch raíz se vuelve acumulativo en la medida

que se generan nuevas BPDU por los diferentes conmutadores. El costo que adiciona un conmutador depende de la velocidad del puerto local, por ejemplo, en operación en modo corto (Short Mode) para 10 Mbps el costo es 100; para 100 Mbps, es 19; para 1 Gbps, es 4, y para 10 Gbps el costo es 2.

3. Elección del puerto designado: Una vez seleccionado el puerto raíz en cada conmutador diferente al switch raíz, para cada segmento de la red se escoge un solo puerto de un conmutador que ejecute la función de reenvío del tráfico de dicho segmento (en cada segmento LAN solamente puede existir un camino hacia el switch raíz). Se volverá el puerto designado del segmento aquel que anuncie el camino con menor costo hacia el switch raíz. Los puertos de acceso se consideran puertos designados para el segmento que ellos mismos atienden.
4. Se eliminan los bucles del Bridge (Switch): Los puertos que no son puertos raíz y que tampoco son puertos designados se ponen en estado de bloqueo. Lo anterior elimina cualquier bucle de la topología.

En STP cada puerto del conmutador progresa en la siguiente secuencia de estados:

***Deshabilitado (Disabled o Discarding)***: cuando el puerto es deshabilitado por el administrador de la red o por una condición de falla.

***Bloqueo (Blocking)***: primer estado al que entra el puerto cuando se prepara para empezar a funcionar (por encendido del conmutador). El puerto no puede recibir ni transmitir tramas con datos, tampoco puede adicionar direcciones MAC a su tabla de direcciones; solamente puede recibir las BPDU. También se entra a este estado cuando el STP detecta y elimina bucles en la topología o cuando un puerto pierde su papel de puerto raíz o de puerto designado.

***Escucha (Listening)***: estado al que pasa el puerto cuando es candidato para ser puerto raíz o puerto designado (cuando el STP va a seleccionar el puerto raíz de un conmutador o los puertos designados de un segmento). En este estado, el puerto no puede recibir ni transmitir tramas con datos, tampoco puede adicionar direcciones MAC a su tabla de direcciones; sólo puede transmitir y recibir las BPDU.

***Aprendizaje (Learning)***: el puerto pasa a este estado después de expirar el temporizador Forward Delay por primera vez (luego de 15 segundos, por defecto). En este estado, el puerto no puede recibir ni transmitir tramas con dato; no obstante, puede aprender las direcciones MAC existentes en la red y adicionarlas a su tabla de direcciones. El puerto también puede transmitir y recibir las BPDU.

**Reenviando (Forwarding):** el puerto pasa a este estado después de expirar por segunda vez el temporizador Forward Delay (luego de otros 15 segundos, por defecto). En este estado, el puerto puede recibir y transmitir tramas con datos, aprender las direcciones MAC existentes en la red y adicionarlas a su tabla de direcciones, y transmitir y recibir las BPDU.

### PROBLEMAS

1. Interfaz VLAN: en los conmutadores capa tres, una interfaz VLAN es una interfaz capa tres que sirve como puerta de enlace a cualquier miembro de la respectiva VLAN. Proponga una configuración de las interfaces VLAN para las VLAN 8 y 12 correspondientes a las redes 192.168.8.0 /24 y 192.168.12.0 /24, respectivamente. Ayuda: se debe usar el comando *interface vlan 8* e *interface vlan 12*.
2. Interfaces Ethernet capa tres de los conmutadores multicapa: una interfaz Ethernet capa tres es una interfaz “enrutada” (routed port) diseñada para realizar procesamiento capa tres a los datagramas IP que entran y salen de esta. Las interfaces físicas de algunos conmutadores multicapas (Cisco 4500, 6500, 3560 ó 3750) pueden configurarse para que operen como puertos capa dos (switchport) o como puertos capa tres (routed). Proponga un ejemplo para que un puerto de un conmutador multicapa opere en la capa tres. Ayuda: se debe usar el comando *no switchport*.
3. En el protocolo de árbol de expansión: ¿cuál es el criterio de desempate para elegir el switch raíz en conmutadores que tengan igual prioridad?, ¿cuál es el criterio de desempate para elegir el puerto raíz en un conmutador que tenga varios puertos con igual costo al switch raíz?, ¿cuál es el criterio de desempate para elegir el puerto designado de un segmento, en conmutadores que anuncien hacia el segmento el mismo costo al switch raíz?
4. EtherChannel: revise las siguientes líneas de configuración que permiten interconectar dos conmutadores Cisco (SW1 y SW2) usando tres puertos troncales de cada uno (Fa0/13, Fa0/14 y Fa0/15), de manera que dichos puertos se agregan para conformar un solo enlace troncal o EtherChannel. ¿Cuál protocolo se usa para formar el EtherChannel: PAgP o LACP?

```
SW1(config)# interface range f0/13 - 15
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# no shutdown
SW1(config-if-range)# channel-group 1 mode active
```

```
SW1(config)# interface Port-channel 1
SW1(config-if# switchport mode trunk
```

Para el caso del conmutador SW2, se realiza la misma configuración anterior, pero con el comando *channel-group 1 mode passive*.

5. Interconecte los conmutadores SW1, SW2 y SW3 formando un bucle en delta (SW1 con SW2, SW2 con SW3 y SW3 con SW1) mediante el uso de dos puertos troncales IEEE 802.1Q de cada conmutador. Cree las VLAN 10, 20 y 30 en cada conmutador. Configure la prioridad de cada conmutador para que: SW1 sea el switch raíz para las VLAN 1 y 10; SW2 sea el switch raíz para la VLAN 20, y SW3 sea el switch raíz para la VLAN 30. Observe e interprete el resultado obtenido ejecutando los comandos *show spanning-tree vlan 10* desde SW2, *show spanning-tree vlan 20* desde SW1 y *show spanning-tree vlan 30* desde SW1.

Sugerencia: Puede usar Packet Tracer o GNS3. En caso de usar GNS3, es necesario usar el módulo NM-16ESW en un encaminador.

Ayuda: Por defecto, el modo de operación de Spanning tree en los equipos Catalyst Cisco es PVSTP+; si se desea cambiar dicho modo a RPVSTP+ (en conmutadores que soporten otros modos de spanning tree), se puede ejecutar el comando global *spanning-tree mode rapid-pvst*. Para hacer que SW2 sea el switch raíz de la VLAN 20, se ejecuta el comando global *spanning-tree vlan 20 root primary* en el conmutador SW2. Para que un puerto troncal opere con la norma IEEE 802.1Q, se debe ejecutar el comando específico de interfaz *switchport trunk encapsulation dot1q* en dicho puerto.

## GLOSARIO

**Hello Timer:** temporizador que establece la periodicidad con la cual un conmutador envía mensajes Hello a los conmutadores vecinos. El rango es de 1 a 10 segundos, el valor por defecto es 2 segundos.

**MaxAge Timer:** temporizador que especifica el tiempo de vida o de almacenamiento de una BPDU recibida sobre un puerto designado; si expira dicho temporizador, los otros puertos del conmutador pueden volverse puertos designados. El rango es de 6 a 40 segundos, el valor por defecto es 20 segundos.

**NAT/PAT (Network Address Translation / Port Address Translation):** solventa el agotamiento de las direcciones IPv4 públicas (siendo una so-

lución parcial) al permitir el acceso a Internet de varios equipos internos de una red privada mediante el uso de una sola dirección IP pública (la solución definitiva es IPv6). Para lograr lo anterior, NAT/PAT transforma el paquete que va desde un origen (equipo de la red privada) hacia un destino (equipo de la red pública) mediante un cambio en los campos “dirección IP origen” y “puerto origen”, dicho cambio es realizado en el equipo de borde (típicamente un cortafuegos). Para el paquete de regreso (en el sentido opuesto), se deben hacer los mismos cambios en los campos “dirección IP destino” y “puerto destino” de manera consistente con el cambio previo.

**Root switch:** conmutador raíz a partir del cual se construye el árbol de expansión.

**Spanning Tree (Árbol de expansión):** las topologías que incorporan bucles físicos pueden proporcionar una mayor disponibilidad de la red. No obstante, en la capa dos es necesario que las topologías lógicas que se encuentren en operación no tengan bucles, puesto que esto causaría tormentas de broadcast. Por lo anterior, los equipos capa dos ejecutan un algoritmo que permite construir una topología lógica en árbol de expansión a partir de una topología física que contenga bucles, colocando algunos puertos en estado de bloqueo para anular dichos bucles.

**VLAN (Virtual Local Area Network):** mediante las VLAN se pueden conformar varios dominios lógicos de difusión capa dos con el propósito de segmentar y controlar el tráfico unicast, multicast y broadcast de capa dos de una red física tipo LAN, con esto se obtienen varias redes lógicas capa dos dentro de la misma LAN. Después de definir las diferentes VLAN en una base de datos interna del conmutador, se signan los puertos que van a pertenecer a cada VLAN.

## BIBLIOGRAFÍA

KOTFILA, D.; MOORHOUSE, J.; PRICE, C.; WOLFSON, R. (2008) *CCNP Building Multilayer Switched Networks (BCMSN 642-812) Lab Portfolio*. Indianapolis, IN: Cisco Press.

MCQUERRY, S.; JANSEN, D.; HUCABY, D. (2009). *Cisco LAN Switching Configuration Handbook*. 2nd Ed. Indianapolis, IN: Cisco Press.

SEIFERT, R.; EDWARDS, J. (2008). *The All-New Switch Book: The Complete Guide to LAN Switching Technology*. 2nd Ed. Indianapolis, IN: Wiley.