Capítulo 11

INTERCONEXIÓN DE REDES: PROYECTO Y CASO DE ESTUDIO

Este capítulo propone el desarrollo de un proyecto y de un caso de estudio. Ambas actividades tienen como propósito la implementación de una intranet completamente funcional que involucra las tecnologías hasta ahora abordadas: red Ethernet conmutada, creación e interconexión de VLAN, conexión de conmutadores Ethernet por medio de IEEE 802.1Q, interconexión de redes de área local mediante encaminadores, uso del protocolo de enrutamiento RIP (o de OSPF) y la configuración de circuitos virtuales permanentes del protocolo de retransmisión de tramas –Frame Relay.

El proyecto y el caso de estudio sirven como referencia para implementar una intranet utilizando equipos físicos. No obstante, también se pueden usar programas de emulación/simulación (GNS3, Packet Tracer o NETSIM) para llevar a cabo el mismo cometido; en este último caso, el conmutador capa 3 (modelo 3C16951 con módulo 3C16968), del fabricante 3Com, y el nodo Frame Relay (modelo SPS-3S), del fabricante RAD, pueden remplazarse por los objetos equivalentes del programa escogido y habilitarse para que realicen la función que les corresponde.

Opcionalmente, el proyecto permite incorporar fácilmente el tema de redes inalámbricas del que trata el capítulo 12. Finalmente, cabe resaltar que en el caso de estudio se profundiza una solución más compleja en la interconexión de redes.

Objetivo

Al finalizar el presente capítulo, el estudiante estará en capacidad de:

- Crear y configurar VLAN en conmutadores Ethernet capa 2 y capa 3.
- Interconectar conmutadores Ethernet por medio de 802.1Q.
- Interconectar VLAN por medio de un conmutador Ethernet capa 3.
- Interconectar redes de área local mediante encaminadores Cisco y un nodo Frame Relay.

Aspectos preliminares

Se sugiere familiarizarse con los siguientes conceptos: RIP (Capítulo 4), VLAN (Capítulo 10), IEEE 802.1Q (Capítulo 10) y Frame-Relay (Capítulo 8). Opcionalmente, si se va a trabajar con redes inalámbricas, es necesario revisar dicho tema en el Capítulo 12.

En caso de utilizar equipos físicos para el desarrollo del proyecto, es conveniente revisar los siguientes manuales de apoyo para la configuración de los equipos.

1. Manual del conmutador Ethernet capa 2 marca 3Com, modelo *Switch 1100* (3C16951). Este manual se encuentra en Internet, es un archivo denominado "16950ug4.pdf".
2. Manual del módulo capa 3 marca 3Com, modelo *Layer 3 Module (3C16968)*, módulo opcional e interno del anterior conmutador Ethernet; dicho módulo convierte al *Switch 1100* en un conmutador capa 3. Este manual se descarga de Internet, es un archivo llamado "16968.pdf".
3. Guía de Configuración Software de los conmutadores Catalyst 2950, 3550 ó 3560.
4. Los siguientes manuales del nodo Frame-Relay marca RAD, modelo SPS-3S.
   - Instalación y Operación: "sps3s_instalation_guide.pdf".
   - Guía de Usuario: "psg-5_user_guide.pdf".
   - Guía de Aplicación: "psapg-5_application_guide.pdf".

Procedimiento

Proyecto: Montaje de una intranet básica

Con el propósito de desarrollar la implementación de una intranet básica, se presentan las siguientes directrices y se sugieren ejemplos de configuración de cada uno de los equipos que integran la red.

Preparación de un diseño preliminar

Realizar el diseño para la asignación de direcciones IP y de DLCI en la intranet de la Figura 11.1.

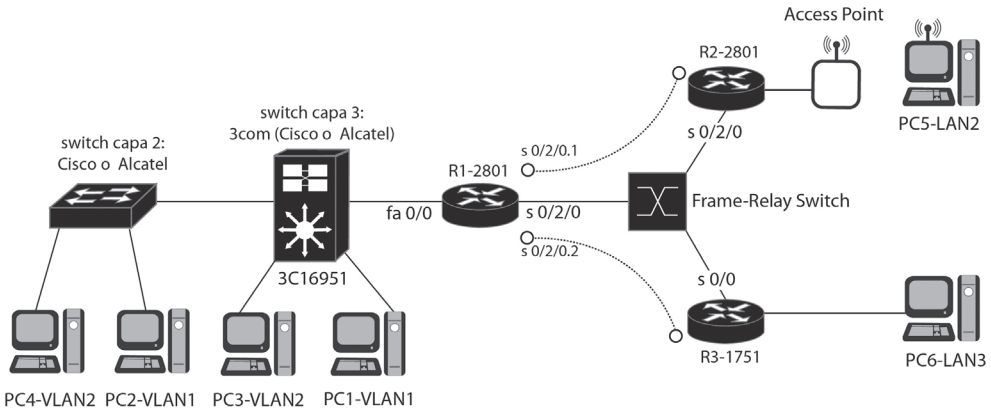

Figura 11.1 Esquema de la intranet del proyecto

Realizar el montaje de la intranet

Realizar el montaje o simulación de la intranet de Figura 11.1, verificar la operación correcta de la misma y probar que:

1. Cada equipo está bien configurado.
2. El PC1 de la VLAN1 le hace ping al PC2 de la VLAN1.
3. El PC1 de la VLAN1 le hace ping al PC3 de la VLAN2.
4. Los dos circuitos Frame-Relay suben después de configurar las interfaces serie de los encaminadores R1, R2, R3 y del nodo Frame-Relay.
5. Los encaminadores R1, R2, R3 y el conmutador capa 3 conocen todas las subredes IP (6 subredes). Si desea, puede trabajar con OSPF o con RIP.
6. El equipo PC5 de la LAN2 puede hacer ping al PC1 de la VLAN1, al PC3 de la VLAN2 y al PC6 de la LAN3.
7. El equipo PC6 de la LAN3 puede hacer ping al PC1 de la VLAN1, al PC3 de la VLAN2 y al PC5 de la LAN2.

Resumen del montaje con el nodo Frame Relay de RAD (SPS-3S) y los tres encaminadores Cisco (R1-2801, R2-2801 y R3-1751)

La siguiente configuración supone que en la Figura 11.1 los puertos 1, 2 y 3 del nodo Frame Relay se conectan a las interfaces S0/2/0 de R1-2801, S0/2/0 de R2-2801 y S0/0 de R3-1751, respectivamente. También se supone que se tienen las siguientes direcciones IP y DLCI asignadas para los puertos de los encaminadores:

En el encaminador R1-2801:
FastEthernet0/0: Dirección IP 10.3.1.1/24
S0/2/0.1: Dirección IP 10.3.2.1/24 y DLCI=48
S0/2/0.2: Dirección IP 10.3.4.1/24 y DLCI=49

En el encaminador R2-2801:
FastEthernet0/0: Dirección IP 10.3.3.1/24
S0/2/0: Dirección IP 10.3.2.2/24 y DLCI=66

En el encaminador R3-1701:
Ethernet0: Dirección IP 10.3.5.1/24
S0/0: Dirección IP 10.3.4.2/24 y DLCI=67

Configuración del nodo Frame Relay RAD (SPS-3S)

En términos generales, en el nodo Frame Relay se realizan los siguientes pasos:

1. Se configuran internamente los tres puertos (interfaces) WAN del nodo Frame Relay SPS-3S para que operen como DCE.
2. Se configuran los tres puertos para que funcionen con Frame Relay como protocolo WAN.
3. En los parámetros de cada puerto, se configura el parámetro 13 para que el puerto proporcione señal de reloj (internal clock) al encaminador, debido a que en el montaje no se usan módems para la conexión entre el nodo y los encaminadores.
4. Se crean los siguientes DLCI.
   Puerto 1: DLCI 48 y DLCI 49
   Puerto 2: DLCI 66
   Puerto 3: DLCI 67
5. Por la opción "Update DLCI parameters", seleccionar cada uno de los DLCI que se hayan creado. Una vez seleccionado un DLCI específico, escoger la opción "Update DLCI configuration", escoger "Destination Id" y definir tanto el puerto como el DLCI destino del DLCI seleccionado –el puerto y el DLCI destino al cual se le asocia. Por ejemplo:

DLCI 48 → Tiene como destino el puerto 2, DLCI 66
DLCI 66 → Tiene como destino el puerto 1, DLCI 48

DLCI 49 → Tiene como destino el puerto 3, DLCI 67
DLCI 67 → Tiene como destino el puerto 1, DLCI 49

Configuración de los encaminadores R1-2801, R2-2801 y R3-1751

En lo que concierne a la operación Frame Relay de los encaminadores, se debe configurar lo siguiente.

En el encaminador R1-2801:

```
(config)# interface s0/2/0
(config-if)# encapsulation frame-relay

(config)# interface s0/2/0.1 point to point
(config-if)# frame-relay interface-dlci 48
(config-if)# ip address 10.3.2.1 255.255.255.0

(config)# interface s0/2/0.2 point to point
(config-if)# frame-relay interface-dlci 49
(config-if)# ip address 10.3.4.1 255.255.255.0
```

Observe que la configuración supone que el encaminador R1-2801 tiene un IOS con versión 11.2 o superior, lo cual permite que éste descubra automáticamente el tipo de LMI (que, por defecto, en el nodo Frame Relay es ANSI).

En el encaminador R2-2801:

```
(config)# interface s0/2/0
(config-if)# encapsulation frame-relay
(config-if)# ip address 10.3.2.2 255.255.255.0
```

Observe que no es necesario especificar el DLCI en la interfaz serie del encaminador, debido a que solamente hay un DLCI configurado en el nodo Frame Relay, el cual es descubierto por el encaminador mediante LMI y asociado a su interfaz serie. Puesto que no se trabaja con subinterfaces, no hay lugar a ambigüedad.

En el encaminador R3-1751:

```
(config)# interface s0/0
(config-if)# encapsulation frame-relay
(config-if)# frame-relay lmi-type ansi
(config-if)# ip address 10.3.4.2 255.255.255.0
```

Observe que la configuración supone que el encaminador R3-1751 tiene un IOS con versión inferior a 11.2, lo cual impide que éste descubra auto-

máticamente el tipo de LMI (que, por defecto, en el nodo Frame Relay es ANSI), razón por la cual hay que especificarlo. No es necesario especificar el DLCI en la interfaz serie del encaminador porque solamente hay un DLCI configurado en el nodo Frame Relay, el cual es descubierto por el encaminador mediante LMI y asociado a su interfaz serie. Puesto que no se trabaja con subinterfaces, no hay lugar a ambigüedad.

Resumen del montaje de los conmutadores 3Com (3C16951 y 3C16968) y Cisco 2950

Para la configuración que sigue a continuación, se supone que los conmutadores de la Figura 11.1 tienen asignadas las siguientes direcciones IP:

El conmutador capa 2 (3C16951) tiene la dirección IP 192.168.55.110. Usar la cuenta por defecto para entrar al equipo, cuyo login es "admin", y, como password, digitar la tecla [Enter]. Para acceder al conmutador 3com capa 2, la configuración del puerto serie del computador personal que se conecte al puerto de consola debe ser: 19200, 8, ninguno, 1, ninguno.

El conmutador capa 3 (3C16968) tiene la dirección IP 192.168.55.106. Usar la cuenta por defecto para entrar al equipo, con el usuario "administer" y password "administer". Para acceder al conmutador capa 3, es necesario hacer telnet con destino a la dirección IP de éste (192.168.55.106) desde un computador personal que se encuentre en red.

El conmutador capa 2 (Cisco 2950) tiene la dirección IP 192.168.55.120. Usar una cuenta previamente configurada con login "lab" y password "univalle" –el usuario y la clave puede variar en su equipo. Para acceder al conmutador capa 2 Cisco, la configuración del puerto serie del computador personal que se conecte a su puerto de consola debe ser: 9600, 8, ninguno, 1, ninguno.

Además de lo anterior, en la Tabla 11.1 se presenta la asignación de los puertos Ethernet de los conmutadores (3Com y Cisco) y sus correspondientes VLAN.

Tabla 11.1 Distribución de puertos en las VLAN de los conmutadores capa 2

VLAN	Puertos del conmutador 3Com	Puertos del conmutador Cisco 2950
1	1, 2, 13	1, 2, 3, 4, Gigabit Ethernet 0/1
2	3, 4	5, 6, 7, 8
3	5, 6	9, 10, 11, 12
4	7, 8	13, 14, 15, 16
5	9, 10	17, 18, 19, 20
6	11, 12	21, 22, 23, 24
802.1Q	14	Gigabit Ethernet 0/2

Configuración del conmutador 3Com 3C16951 (capa 2)

Se realizan los siguientes pasos de configuración del conmutador 3Com capa 2.

1. Se reinicia el conmutador capa 2 para que tenga los valores de fábrica (valores por defecto).
2. Se configura la dirección IP del conmutador capa 2 (3C16951) {por la opción: ip → interface → define} y del módulo capa 3 (3C16968) {por la opción: system → module → define} con las direcciones 192.168.55.110 y 192.168.55.106, respectivamente.
3. Se crean las VLAN 2, 3, 4, 5 y 6 –La VLAN 1 ya está creada, por defecto– {por la opción: bridge → vlan → create} y se verifica la creación de las mismas {por la opción: summary → all}.
4. Se asocian los puertos 3 y 4 a la VLAN 2; los puertos 5 y 6, a la VLAN 3; los puertos 7 y 8, a la VLAN 4; los puertos 9 y 10, a la VLAN 5; los puertos 11 y 12, a la VLAN 6. Se escoge la opción "Tag" en "None", puesto que dichos puertos envían y reciben tramas normales –tanto Ethernet como IEE802.3– sin ninguna modificación, es decir, dichos puertos no son IEEE 802.1Q.
5. Se asocia el puerto 14 a VLAN 2, VLAN 3, VLAN 4, VLAN 5 y VLAN 6. Se escoge la opción "Tag" en "802.1Q" para que dicho puerto pueda enviar las tramas –a otro conmutador– modificándolas con el valor de la VLAN a la que pertenecen, o recibir las tramas –de otro conmutador– e interpretar la VLAN de donde vienen. Dichos puertos son 802.1Q.
6. Verificar que el puerto 14 quede perteneciendo a la VLAN 1 sin "Tag" y al resto de VLAN con "Tag", mediante la opción: Bridge → Port → Detail → 14.
7. Verificar el tráfico unicast en VLAN 2, VLAN 3, VLAN 4, VLAN 5 y VLAN 6 mediante la opción: Bridge → VLAN → Detail → X. Donde X, hace referencia al número de la VLAN que se desea verificar.

Configuración del conmutador Cisco 2950 (capa 2)

Se realizan los siguientes pasos de configuración del conmutador Cisco 2950 capa 2.

1a. Para asociar los puertos 5, 6, 7 y 8 a la VLAN 2:

```
(config)# interface range fastethernet 0/5 - 8
(config-if)# switchport access vlan 2
(config-if)# switchport mode access
```

1b. Para asociar los puertos 9, 10, 11 y 12 a la VLAN 3:

```
(config)# interface range fastethernet 0/9 - 12
(config-if)# switchport access vlan 3
(config-if)# switchport mode access
```

1c. Para asociar los puertos 13, 14, 15 y 16 a la VLAN 4:

```
(config)# interface range fastethernet 0/13 - 16
(config-if)# switchport access vlan 4
(config-if)# switchport mode access
```

1d. Para asociar los puertos 17, 18, 19 y 20 a la VLAN 5:

```
(config)# interface range fastethernet 0/17 - 20
(config-if)# switchport access vlan 5
(config-if)# switchport mode access
```

1e. Para asociar los puertos 21, 22, 23 y 24 a la VLAN 6:

```
(config)# interface range fastethernet 0/21 - 24
(config-if)# switchport access vlan 6
(config-if)# switchport mode access
!para ver el resultado de este punto, se puede ejecutar el comando "show vlan"
```

2. Para que la interfaz GigabitEthernet 0/2 opere con 802.1Q:

```
(config)# interface Gigabitethernet 0/2
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate
! Por defecto, se tiene:
(config-if)# switchport trunk native VLAN 1
(config-if)# switchport trunk allowed VLAN all
```

3. Para monitorear el estado de la interfaz GigabitEthernet 0/2, se pueden usar los siguientes comandos:

```
# show interface gigabitethernet 0/2 trunk
# show interface gigabitethernet 0/2 switchport
```

Configuración del conmutador 3Com 3C16968 (capa 3) y de los computadores personales

A cada VLAN se le asigna una dirección IP de subred con la respectiva máscara. Para realizar la interconexión de las VLAN, en cada una de ellas se reserva una dirección IP (del rango disponible de direcciones IP de la subred de la VLAN) para que sea asignada a una interfaz del conmutador capa 3 (interfaz que denominaremos "Ifx", siendo "x", el número correspondiente de la VLAN); dicha dirección servirá como puerta de enlace para cada uno de los equipos que pertenezcan a la VLAN (PC, servidores, etc.). Las direcciones IP anteriores, además de servir para configurar las interfaces correspondientes del conmutador capa 3 (una interfaz por cada VLAN), deben ser usadas para configurar la puerta de enlace por defecto en cada uno de los equipos que pertenezcan a la misma VLAN. La Tabla 11.2 presenta posibles valores que se pueden usar para implementar la intranet.

Tabla 11.2 Asignación de las direcciones IP en el conmutador 3Com capa 3

Número de VLAN	Dirección IP de subred	Dirección IP de la interfaz del conmutador capa 3 (que sirve como puerta de enlace para los equipos de la VLAN)
VLAN 1	192.168.55.0 /24	If1 = 192.168.55.106 /24
VLAN 2	192.168.56.0 /24	If2 = 192.168.56.1 /24
VLAN 3	192.168.57.0 /24	If3 = 192.168.57.1 /24
VLAN 4	192.168.58.0 /24	If4 = 192.168.58.1 /24
VLAN 5	192.168.59.0 /24	If5 = 192.168.59.1 /24
VLAN 6	192.168.60.0 /24	If6 = 192.168.60.1 /24

La configuración del conmutador capa 3 y de los computadores se describe a continuación.

1. Desde un computador de la VLAN 1, entrar por telnet al conmutador capa 3 –telnet 192.168.55.106– y crear las siguientes interfaces con sus respectivas direcciones IP.
   Usar {ip → interfaces → define}

   If2 = 192.168.56.1, máscara 255.255.255.0
   If3 = 192.168.57.1, máscara 255.255.255.0
   If4 = 192.168.58.1, máscara 255.255.255.0
   If5 = 192.168.59.1, máscara 255.255.255.0
   If6 = 192.168.60.1, máscara 255.255.255.0

Nota: la interfaz If1 ya estará creada en el conmutador capa 3 y debe tener asignada la dirección IP del módulo capa 3 (192.168.55.106). Esto, debido a que la dirección IP para la interfaz If1 es heredada de la dirección IP que se le asigna al módulo capa 3 cuando se configura dicho valor en el conmutador capa 2.

Verificar con {ip → interfaces → summary → all}

2. Para permitir la comunicación con cualquier equipo de la Intranet –incluidos los equipos de las redes locales LAN 2 y LAN 3–, es necesario que el conmutador capa 3 (3C16968) conozca todas las direcciones de red que conocen los encaminadores R1-2801, R2-2801 y R3-1751. También es necesario que dichos encaminadores conozcan las direcciones de red que conoce este conmutador capa 3. Por lo anterior, es necesario habilitar un protocolo de enrutamiento común tanto en el conmutador capa 3 como en los encaminadores R1-2801, R2-2801 y R3-1751; dicho protocolo puede ser RIP u OSPF.

   Si se desea habilitar RIP versión 1.0 en todos los equipos –conmutador 3C16968, R1-2801, R2-2801 y R3-1751, tener en cuenta que para habilitar RIP en la interfaz IF1 del conmutador 3C16968 se entra por la opción: ip → rip → mode → interface 1 → enabled.

   Verificar la tabla de enrutamiento en los equipos, tener en cuenta que para el conmutador 3C16968 se entra por la opción: ip → route → display.

3. La Tabla 11.3 permite configurar los computadores personales de acuerdo a la VLAN a la que pertenecen.

Tabla 11.3. Asignación de las direcciones IP en los PC, de acuerdo a la VLAN a la que pertenece cada uno

Nombre del PC	Numero de VLAN a la que pertenece	Dirección IP	Puerta de enlace
PC1	VLAN 1	192.168.55.31 /24	192.168.55.106
PC2	VLAN 1	192.168.55.32 /24	192.168.55.106
PC3	VLAN 2	192.168.56.31 /24	192.168.56.1
PC4	VLAN 2	192.168.56.32 /24	192.168.56.1
PC5	VLAN 3	192.168.57.31 /24	192.168.57.1
PC6	VLAN 3	192.168.57.32 /24	192.168.57.1
PC7	VLAN 4	192.168.58.31 /24	192.168.58.1
PC8	VLAN 4	192.168.58.32 /24	192.168.58.1
PC9	VLAN 5	192.168.59.31 /24	192.168.59.1
PC10	VLAN 5	192.168.59.32 /24	192.168.59.1
PC11	VLAN 6	192.168.60.31 /24	192.168.60.1
PC12	VLAN 6	192.168.60.32 /24	192.168.60.1

Información complementaria

Uso de un encaminador externo, en lugar del módulo 3Com 3C16968

Configuración para interconectar las VLAN del conmutador 2950 por medio de un encaminador externo. En caso de no poseer el módulo 3C16968 de capa 3, es factible interconectar las VLAN del conmutador 2950 (y del conmutador 3C16951 capa 2) por medio de un encaminador externo, para ello se supone, por ejemplo, que solamente hay dos VLAN en el conmutador 2950, junto con los siguientes equipos conectados.

PC1: Está conectado al puerto 1 del conmutador 2950, el cual pertenece a la VLAN 1 (192.168.55.0 /24); tiene asignada la dirección IP 192.168.55.2 /24 y su puerta de enlace es la dirección 192.168.55.106.

R2: Utilizado como un PC para efectos de prueba, su interfaz FastEthernet 0/0 está conectada al puerto 5 del conmutador 2950, el cual pertenece a la VLAN 2 (192.168.56.0 /24); tiene asignada la dirección IP 192.168.56.2 /24 y su puerta de enlace es la dirección 192.168.56.1. Con lo anterior, R2 tiene la siguiente configuración:

```
(config)# interface Fastethernet 0/0
(config-if)# ip address 192.168.56.2 255.255.255.0
(config)# ip route 0.0.0.0 0.0.0.0 192.168.56.1
```

R1: Hace la función del conmutador capa 3, su interfaz FastEthernet 0/0 (la cual es de tipo 802.1Q) está conectada al puerto GigabitEthernet 0/2 del conmutador 2950 (que también es de tipo 802.1Q). R1 tiene la siguiente configuración:

```
(config)# interface Fastethernet 0/0
(config-if)# no shutdown
(config-if)# exit
(config)# interface Fastethernet 0/0.1
(config-subif)# encapsulation dot1Q 1 native
(config-subif)# ip address 192.168.55.106 255.255.255.0

(config-if)# interface Fastethernet 0/0.2
(config-if)# encapsulation dot1Q 2
(config-if)# ip address 192.168.56.1 255.255.255.0
(config)# router rip
(config-router)# network 192.168.55.0
(config-router)# network 192.168.56.0
```

Reiniciar el conmutador 2950 a la configuración de fábrica (configuración por defecto)

Mantenga presionado el botón "Mode"; después de transcurridos dos segundos, los cuatro LED, ubicados encima de dicho botón, se vuelven intermitentes, continúe presionando el botón "Mode"; después de ocho segundos, los LED dejan de ser intermitentes y el conmutador 2950 se reinicia a la configuración por defecto.

Entrar a la "Configuración rápida" del conmutador 2950

Para permitir su configuración expresa (Express Setup), el conmutador 2950 tiene asignada la dirección IP 10.0.0.1 y funciona como servidor DHCP. Para entrar a la configuración expresa del conmutador 2950, se deben seguir los siguientes pasos:

1. Presione el botón "Mode" –aproximadamente por tres segundos– hasta que los cuatro LED encima de dicho botón se iluminen con el color verde.
   En caso de que los cuatro LED que están encima del botón "Mode" se vuelvan intermitentes, libere el botón "Mode". Lo anterior significa que el conmutador 2950 ya ha sido configurado y no se puede entrar al modo de configuración expresa del equipo.
2. Conecte un computador personal a uno de los puertos Ethernet del conmutador 2950, configure el computador personal para que adquiera una dirección IP por medio de DHCP. Una vez adquirida la dirección IP, ejecute un programa cliente de navegación y digite la dirección URL "http://10.0.0.1". Configure el conmutador 2950.

Caso de estudio

Montaje de una intranet avanzada

Con el propósito de desarrollar la implementación de una intranet avanzada, en el siguiente caso de estudio se presentan las directrices de diseño y de configuración de algunos de los equipos que integran una red de mayor complejidad. Este caso de estudio está basado en los archivos relacionados en la bibliografía bajo el nombre *Smart Business Architecture for Midsize Networks* de Cisco.

La red de la Figura 11.2 consta de los siguientes equipos: un conmutador capa 3 de núcleo, modelo 3750G-12S-S, denominado "SW1", el cual puede consistir de dos o más conmutadores apilados; cuatro conmutadores capa 2 de acceso para equipos clientes, modelo 3750, denominados "SWAx" –la Figura 11.2 muestra solamente uno: SWA1–, cada uno de estos equipos puede constar de dos o más conmutadores apilados, se tienen cuatro arma-

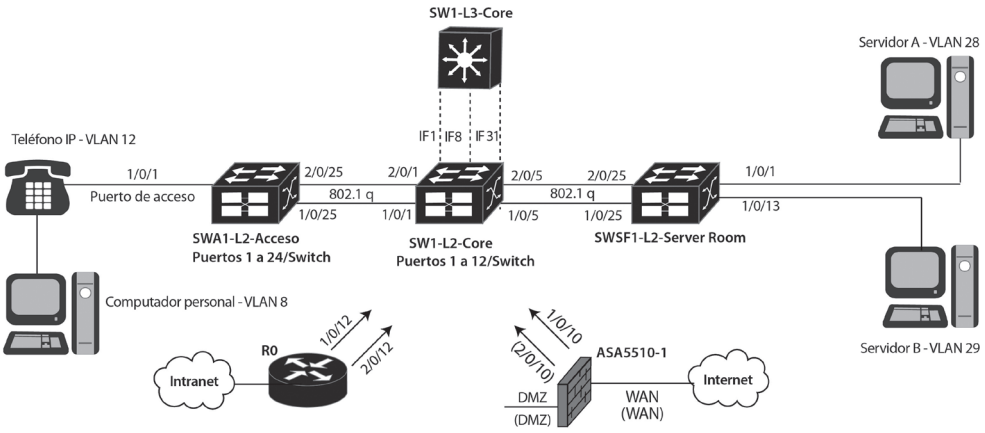

Figura 11.2 Infraestructura básica de la red "LAN1" de Dirección general "Headquarters"

rios de cableado para los conmutadores de acceso; dos conmutadores capa 2 para la granja de servidores, modelo 3750, denominados "SWSFx" –la Figura 11.2 muestra solamente uno: SWSF1–, cada uno de estos equipos puede constar de dos o más conmutadores apilados y se tienen dos armarios de cableado para conmutadores de la granja de servidores. Observe que, en la nomenclatura usada, la letra "x" en los nombres de los conmutadores toma un valor del rango de 1 hasta 4 para los armarios de acceso y de 1 hasta 2 para los armarios de la granja de servidores.

El encaminador, modelo ISR-3845, que se denominará "R0", recibe las oficinas remotas y conforma la Intranet, éste se conecta a la VLAN 31 –no indicada en la Figura 11.2– del conmutador de núcleo SW1, denominada "Core routing", cuya función es ser el núcleo de enrutamiento de la red del campus; dos Firewall, modelo ASA5510, permiten la conexión a Internet, estos también se conectan al núcleo de enrutamiento de la red del campus. Aunque no se muestran en la Figura 11.2, también se conectan al núcleo de enrutamiento de la red del campus un controlador central (WLC) que recibe los puntos de acceso inalámbrico livianos y un acelerador de aplicaciones (WAAA) que mejora el rendimiento de los enlaces de la red de área amplia. En cuanto al número de dominios de difusión capa 2 de la red del campus, denominada "LAN1", el diseño estima que inicialmente se requieren 9 VLAN, cada una con un número máximo de 254 equipos por VLAN con el fin de limitar las tormentas de *broadcast*.

El sistema anterior puede atender entre 200 y 600 empleados en total, permitiendo que usen tanto aplicaciones de datos como de voz (VoIP); se supone, entonces, que estarán distribuidos así: 20 oficinas remotas con 20 empleados cada

una y 200 empleados en Dirección general –para un total de 600 empleados. En caso de requerir que en Dirección general se aumente el número de empleados a 600 –para un total de 1.000 empleados–, se puede usar un conmutador de núcleo con mayor desempeño –por ejemplo, el conmutador modelo 4507R.

Preparación de un diseño preliminar

Las siguientes Tablas (11.4 hasta 11.11) sugieren un diseño que permite planear la asignación de direcciones IP de la intranet de la Figura 11.2.

Tabla 11.4 Asigna direcciones de red a cada una de las VLAN del campus con su respectiva puerta de enlace

VLAN Número	Nombre	Dirección de red	Dirección IP de la puerta de enlace por defecto (configurada en la respectiva interfaz de SW1)
VLAN 1	Management	192.168.1.0/24	192.168.1.1 (IF1)
VLAN 8	HQ Data	192.168.8.0/24	192.168.8.1 (IF8) - Nota: "ip pim sparse-mode" Habilita Multicast en la VLAN 8
VLAN 10	HQ Wireless Data	192.168.10.0/24	192.168.10.1 (IF10)
VLAN 12	HQ Voice	192.168.12.0/24	192.168.12.1 (IF12) - Habilitar Multicast
VLAN 14	HQ Wireless Voice	192.168.14.0/24	192.168.14.1 (IF14)
VLAN 16	Wireless Guest	192.168.16.0/24	Sin acceso a la red interna, solo a Internet
VLAN 28	Server Farm A	192.168.28.0/24	192.168.28.1 (IF28) - Habilitar Multicast
VLAN 29	Server Farm B	192.168.29.0/24	192.168.29.1 (IF29) - Habilitar Multicast
VLAN 31	Core Routing	192.168.31.0/24	192.168.31.1 (IF31) - Habilitar Multicast

Tabla 11.5. Define la VLAN1 como VLAN de gestión, asigna direcciones IP a los equipos activos de red dentro del rango de dicha VLAN y define la respectiva puerta de enlace que estos equipos deben usar

Equipo	Dirección IP	Puerta de enlace por defecto
SW1	192.168.1.1/24	Nota: 192.168.31.254 para SW1 (es la dirección IP física de los firewall para la salida a Internet)
SWSF1	192.168.1.8/24	192.168.1.1
SWSF2	192.168.1.9/24	192.168.1.1
SWA1	192.168.1.10/24	192.168.1.1
SWA2	192.168.1.2/24	192.168.1.1
SWA3	192.168.1.3/24	192.168.1.1
SWA4	192.168.1.4/24	192.168.1.1
Loopback del encaminador R0	192.168.1.12/32	Nota: 192.168.31.254 para R0 (es la dirección IP física de los firewall para la salida a Internet)
Loopback del encaminador de la oficina remota "Rbranch x"	192.168.1.64+x/32	Nota: "x" toma un valor de 1 a 20, de acuerdo al número de la oficina remota que se configure. La puerta de enlace depende de la dirección IP de subred de la oficina remota

Tabla 11.6. Asigna direcciones IP a equipos que tienen conexión a la VLAN31

Equipo	Dirección IP	Nota relacionada o dirección IP real asociada al "Hot Stanby"
SW1	192.168.31.1/24	Nota: "ip pim rp-address 192.168.31.1" lo define como RP (RP=Randezvous Point). "ip multi-cast-routing distributed" habilita el enrutamiento multicast
R0	192.168.31.2/24	Nota: puede ser el servidor NTP
WAAA-CR	192.168.31.3/24	Nota: es un dispositivo que permite optimizar las conexiones WAN
WLC (Controlador central de puntos de acceso inalámbricos livianos, denominados AP)	*192.168.31.64/24 **192.168.31.65/24	Nota: *Dirección IP que permite la administración del WLC. También sirve para acceder al servicio del servidor DHCP habilitado en el WLC **Para recibir la conexión de los AP livianos por medio de un túnel
ASA5510-1	192.168.31.254/24 (Dirección IP Hot Standby o IP física)	192.168.31.253/24 dirección IP real asociada al "Hot Stanby"
ASA5510-2	192.168.31.254/24 (Dirección IP Hot Standby o IP física)	192.168.31.252/24 dirección IP real asociada al "Hot Stanby"

Tabla 11.7. Asigna direcciones IP a equipos con conexión a la VLAN16

Equipo	Dirección IP	Dirección real asociada al "Hot Stanby"
WLC	192.168.16.5/24	Atiende STA (estaciones inalámbricas) del SSID "Guest"
ASA5510-1	192.168.16.254/24 (IP Hot Standby)	192.168.16.253/24
ASA5510-2	192.168.16.254/24 (IP Hot Standby)	192.168.16.252/24

Tabla 11.8. Asigna direcciones IP a equipos con conexión a las VLAN 10 y 14

Equipo	Dirección IP	Dirección real asociada al "Hot Stanby"
WLC	192.168.10.5/24	Atiende STA del SSID "W-HQData"
	192.168.14.5/24	Atiende STA del SSID "W-HQvoice"

Tabla 11.9. Asigna direcciones IP a equipos con conexión a la VLAN30 o "DMZ"

Equipo	Dirección IP	Dirección real asociada al "Hot Stanby"
Servidor Público	192.168.30.1/24	
ASA5510-1	192.168.30.66/24 (IP Hot Standby)	192.168.30.65/24
ASA5510-2	192.168.30.66/24 (IP Hot Standby)	192.168.30.67/24

Tabla 11.10 Asigna direcciones de red local de la oficina remota RBranch1

VLAN número - Nombre	Dirección de red	Dirección IP de puerta de enlace por defecto (R-branch1-ISR2811)
VLAN 64 - Wired Data	192.168.64.0/24	192.168.64.1 (FastEternet0/0.64)
VLAN 65 - Wired Voice	192.168.65.0/24	192.168.65.1 (FastEternet0/0.65)
VLAN 69 - Wireless Data (SSID= "CAB Br1 Access")	192.168.69.0/24	192.168.69.1 (FastEternet0/0.69) Nota 1: Este tráfico es terminado localmente por el AP mediante la interfaz IF=192.168.69.5 (definida en el WLC y funcional en el AP remoto). Dicha WLAN (IF + SSID de datos) es mapeada a la VLAN 69 de la "Branch" u oficina remota.
VLAN 70 - Wireless Voice (SSID= "CAB Br1 Voice")	192.168.70.0/24	192.168.70.1 (FastEternet0/0.70) Nota 2: Este tráfico es terminado localmente por el AP mediante la interfaz IF=192.168.70.5 (definida en el WLC y funcional en el AP remoto). La WLAN (IF + SSID de voz) es mapeada a la VLAN 70 de la "Branch" u oficina remota.

La asignación de las direcciones IP para la red local de las otras 19 oficinas es similar a la que presenta la Tabla 11.10. Por ejemplo, para la asignación de direcciones IP de la oficina RBranch2, se pueden usar cuatro redes consecutivas a partir de la 192.168.71.0/24.

Tabla 11.11 Asigna direcciones IP a las conexiones WAN

WAN número: Equipo-interfaz	Dirección de red	Dirección IP/máscara de la interfaz
WAN 1: R1-Serial 0/0/0:0.1	10.0.1.0/30	10.0.1.1/30
Rbranch 1-Serial 0/0/0:0		10.0.1.2/30
WAN 2: R1-Serial 0/0/0:0.2	10.0.1.4/30	10.0.1.5/30
Rbranch 2-Serial 0/0/0:0		10.0.1.6/30
...		La tabla continúa hasta cubrir los enlaces WAN de 20 oficinas remotas

Configuración de los conmutadores capa 2 y capa 3

A continuación se presentan varios pasos que trazan las directrices para configurar los conmutadores Ethernet de la red del campus de la Figura 11.2. El enfoque está orientado principalmente a la configuración del conmutador de acceso SWA1, puesto que los puertos de acceso del mismo se consideran inseguros (untrusted).

1. Crear, en cada conmutador, solamente las VLAN que requiera tener en operación dicho equipo (SW1, SWAx y SWSFx). Los comandos a ejecutar dependen del modelo del conmutador utilizado; en algunos conmutadores, la VLAN es creada automáticamente cuando se le asigna a un puerto.

   Por ejemplo, para crear la VLAN8 en SWA1 (equipo Cisco 3750), se tiene:

```
SWA1(config)# vlan 8
SWA1(config-vlan)# name HQ Data
```

2. En los conmutadores de acceso SWAx, asignar a cada puerto de acceso la(s) VLAN que le corresponde(n). Adicionalmente, configurar los puertos troncales 802.1Q del conmutador de acceso (por ejemplo, los puertos 1/0/25 y 2/0/25 de SWA1).

   Por ejemplo, para asignar las VLAN 8 y 12 al rango de puertos de acceso 1 a 24 de SWA1, se tiene:

```
SWA1(config)# interface range GigabitEthernet 1/0/1 -24
SWA1(config-if)# switchport mode access
SWA1(config-if)# switchport access vlan 8 !el tráfico de datos no lleva etiqueta
SWA1(config-if)# switchport voice vlan 12 !el tráfico de voz lleva etiqueta (VVID=12)
```

Durante el intercambio inicial CDP (Cisco Discovery Protocol) con el conmutador, el teléfono IP es configurado con el VVID (Voice VLAN ID) 12. La configuración adicional de los puertos de acceso se retoma en el punto 3. Para configurar el encapsulado IEEE 802.1Q en el puerto troncal 1/0/25 de SWA1 y permitir las VLAN 1, 8 y 12 en dicho puerto, se tiene:

```
SWA1(config)# interface GigabitEthernet 1/0/25
SWA1(config-if)# switchport mode trunk
SWA1(config-if)# switchport trunk encapsulation dot1q
SWA1(config-if)# switchport trunk allowed vlan 1,8,12
```

La configuración adicional de los puertos troncales IEEE 802.1Q se retoma en el punto 6.

3. Aplicar los siguientes comandos globales de seguridad DHCP y ARP al conmutador SWA1.

```
SWA1(config)# ip dhcp snooping
SWA1(config)# ip dhcp snooping vlan 1-12
SWA1(config)# no ip dhcp snooping information option
SWA1(config)# ip arp inspection vlan 1-12
```

Los comandos *ip dhcp* permiten diferenciar las interfaces de desconfianza (por ejemplo, los puertos de acceso) de las interfaces de confianza (por ejemplo, los puertos troncales 802.1Q); por defecto, las interfaces son de desconfianza (untrusted). Estos comandos hacen que el conmutador opere como un firewall entre los equipos de desconfianza y los servidores DHCP. Lo anterior tiene dos funciones: filtrar los mensajes DHCP de desconfianza y construir una tabla denominada "dhcp snooping binding table". Dicha tabla tiene una entrada por cada cliente DHCP que se conecte; la entrada se usa para registrar la siguiente información del cliente: dirección MAC, dirección IP, tiempo de arriendo de la dirección IP, tipo de asociación, número de VLAN y la interfaz o puerto que

le corresponde. El comando *ip arp* permite que el conmutador intercepte y valide las solicitudes y respuestas ARP provenientes de los puertos de desconfianza, apoyándose en la información contenida en las entradas de la tabla "dhcp snooping binding table".

4. Afinar los puertos de acceso del conmutador SWA1, en términos de proporcionar un nivel de seguridad razonable en el borde de la red.

```
SWA1(config)# interface range GigabitEthernet 1/0/1 -24
SWA1(config-if)# spanning-tree portfast !El puerto pasa rápidamente a "forwarding"
SWA1(config-if)# spanning-tree bpduguard enable !Protección de ataques spanning tree
SWA1(config-if)# switchport port-security !Permite dos direcciones MAC y
SWA1(config-if)# switchport port-security maximum 2 !evita ataques "MAC flooding"
SWA1(config-if)# switchport port-security aging time 2
SWA1(config-if)# switchport port-security violation {restrict | protect | shutdown}
SWA1(config-if)# switchport port-security aging type inactivity
SWA1(config-if)# ip arp inspection limit rate 100 !Procesa 100 paquetes por segundo y
SWA1(config-if)# ip dhcp snooping limit rate 100 !evita ataques DoS tipo ARP y DHCP
SWA1(config-if)# ip verify source
```

El comando *ip verify source* usa la información de la tabla "dhcp snooping binding table" para configurar dinámicamente una "lista de control de acceso de los puertos" (Port Access Control List) en la capa 2 que le permite controlar el acceso de los equipos clientes.

5. Afinar los puertos de acceso del conmutador SWA1, con el objetivo de proporcionar la calidad de servicio adecuada al tráfico VoIP generado por los dispositivos de confianza (teléfonos IP Cisco).

```
SWA1(config)# interface range GigabitEthernet 1/0/1 - 24
SWA1(config-if)# auto qos voip cisco-phone
```

En general, la configuración automática de la calidad de servicio para el tráfico VoIP se realiza ejecutando el comando *auto qos voip*. En el caso particular de usar teléfonos IP Cisco en la red de área local, se debe usar el comando *auto qos voip cisco-phone*; esto, con el fin de configurar todos los puertos de acceso (alambrados) de los conmutadores SWAx para que proporcionen la respectiva calidad de servicio a los teléfonos IP. Dicho comando, no se debe usar en los puertos de acceso (alambrados)

de los conmutadores SWSFx, puesto que en estos se conectan solamente equipos servidores.

El comando *auto qos voip* admite las siguientes dos opciones (*keywords*):

- *cisco-phone*: significa que en el puerto se confía del valor que tiene el campo CoS del tráfico entrante únicamente cuando dicho tráfico proviene de un dispositivo cliente Cisco (un teléfono IP marca Cisco). CoS (Class of Service) es el campo que indica la calidad del servicio requerida por la trama.
- *trust*: significa que en el puerto se confía del valor que tiene el DSCP (para el caso de "puertos enrutados") o del valor que tiene el CoS (para el caso de "puertos no enrutados") de todo el tráfico entrante. Esta opción se usa en los puertos internos de los conmutadores de acceso SWAx, en todos los puertos de los conmutadores SW1 y SWSFx, o cuando al puerto de acceso de un conmutador SWAx se le conecta un "Access Point".

En un conmutador 3750, los seis comandos siguientes se generan como consecuencia automática del comando *auto qos voip cisco-phone*:

SWA1(config-if)# *mls qos trust device cisco-phon*e (primer comando)

Use el protocolo "Cisco Discovery Protocol" (CDP) para detectar la presencia (o ausencia) de un teléfono IP marca Cisco que se encuentre conectado al puerto. En caso de detectar la presencia de un teléfono IP Cisco, el "estado de confianza" ("trust state") del puerto pasa del estado "not trusted" al estado "trust cos". En caso contrario, el puerto se queda en estado "not trusted". Este comando se debe eliminar para la conexión de teléfonos IP de otras marcas, puesto que crea un "estado de confianza" condicionado a la presencia de un teléfono IP marca Cisco.

SWA1(config-if)# *mls qos trust cos* (segundo comando)

Usado para clasificar las tramas (que entran al puerto) con base en los valores del campo CoS y cambiar el campo DSCP de acuerdo a dichos valores. Este comando hace que el puerto tenga un "modo de confianza" basado en el "cos" (dicho de otro modo, el "trust mode" del puerto es "trust cos"). Sin este comando, el "modo de confianza" del puerto es "no confiar" (dicho de otro modo, el "trust mode" del puerto es "not trusted") y las etiquetas para la calidad de servicio serán puestas en cero.

SWA1(config-if)# *service-policy input* AutoQoS-Police-CiscoPhone (tercer comando)

Este comando tiene tres etapas para el manejo del tráfico: clasificación; control (policing), y etiquetado (mark). El envío a la cola de entrada y de salida (el conmutador 3750 tiene dos colas de entrada y cuatro colas de salida) es la cuarta etapa.

Por ejemplo, las siguientes líneas definen la política "AutoQoS-Police-CiscoPhone".

```
class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3 af31
!
policy-map AutoQoS-Police-CiscoPhone
 class AutoQoS-VoIP-RTP-Trust
 set dscp ef
 police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
 set dscp cs3
 police 32000 8000 exceed-action policed-dscp-transmit
```

SWA1(config-if)# *srr-queue bandwidth share 10 10 60 20* (cuarto comando)

Establece la proporción o tasa a la cual se atienden las colas de salida, usando el servicio de rotación circular compartida (Share Round Robin). Para esta línea, la proporción es: Cola1 (q1) = 10%; Cola2 (q2) = 10%; Cola3 (q3) = 60%; Cola4 (q4) = 20%.

SWA1(config-if)# *priority-queue out* (quinto comando)

Configura la cola q4 para que sea atendida como prioritaria "priority".

SWA1(config-if)# *queue-set 2* (sexto comando)

Hace que el puerto pertenezca al juego de colas número dos (queue-set 2), dicho juego se define previamente y por medio de él se establecen los diferentes umbrales y tamaños de buffer en las cuatro colas de salida.

6. Afinar los puertos troncales IEEE 802.1Q de SWAx. Por ejemplo, los puertos 1/0/25 y 2/0/25 de SWA1 pueden agruparse para formar un solo enlace o “EtherChannel”.

```
SWA1(config)# interface GigabitEthernet 1/0/25
SWA1(config-if)# channel-group 1 mode on !Agrupa el puerto en el “EtherChannel 1”
SWA1(config-if)# spanning-tree link-type point-to-point !Acelera la operación de STP
SWA1(config-if)# ip arp inspection trust !Define un puerto interno de confianza ARP
SWA1(config-if)# ip dhcp snooping trust !Define un puerto interno de confianza DHCP
!
SWA1(config-if)# auto qos voip trust ! Define un puerto interno de confianza QoS
SWA1(config-if)# srr-queue bandwidth share 10 10 60 20
SWA1(config-if)# queue-set 2
SWA1(config-if)# priority-queue out
SWA1(config-if)# mls qos trust dscp
```

7. Configurar el puerto EtherChannel (LACP o IEEE 802.3ad) de SWAx.

```
SWA1(config)# interface Port-channel1
SWA1(config-if)# switchport trunk encapsulation dot1q
SWA1(config-if)# switchport trunk allowed vlan 1,8,12
SWA1(config-if)# switchport mode trunk
SWA1(config-if)# ip arp inspection trust
SWA1(config-if)# ip dhcp snooping trust
```

8. Configurar las interfaces virtuales capa 3 del conmutador de núcleo SW1 (incluidas en la Tabla 11.4 con el nombre IFx. También se les denomina interfaces SVI).

```
SW1(config)# interface vlan 8
SW1(config)# description HQ-Data
SW1(config-if)# ip address 192.168.8.1 255.255.255.0
SW1(config-if)# ip pim sparse-mode
SW1(config-if)# ip helper-address 192.168.1.1 !Por ejemplo.
SW1(config-if)# ip helper-address 192.168.28.255 !Opcional
SW1(config-if)# no ip directed-broadcast !Opcional
```

Repetir el anterior paso para las VLAN 1, 10, 12, 14, 28, 29 y 31; habilitar multicast en las VLAN alambradas.

9. Configurar la dirección IP de gestión (IP Management Address) de los conmutadores SWAx, SWSFx y SW1; usar las direcciones IP de la VLAN de gestión, indicar que la puerta de enlace por defecto es 192.168.1.1.

```
SWA1(config)# interface vlan 1
SWA1(config)# description SWA1-Management-IP
SWA1(config-if)# ip address 192.168.1.10 255.255.255.0
SWA1(config-if)# management !Opcional, por defecto, la vlan 1 es nativa
SWA1(config)# ip default-gateway 192.168.1.1
SWA1(config)# ip name-server 192.168.28.1 !Opcional
SWA1(config)# ip domain-lookup !Opcional
```

Nota: para el caso de SW1, la VLAN de gestión es la VLAN1, pero la puerta por defecto de SW1 es la dirección IP 192.168.31.254 (dirección IP Hot Standby de los dos equipos ASA-5510).

10. Si se desea, se pueden tener dos servidores DHCP. En este caso, por cada VLAN, se configura un pool de direcciones en el servidor "dhcp1" y el otro pool se configura en el servidor "dhcp2".

Glosario

Capa 2: se refiere a las unidades de datos o al procesamiento de las mismas dentro del contexto del segundo nivel del modelo OSI. Por ejemplo, tanto las tramas Ethernet como los conmutadores que las procesan son de capa dos.

Capa 3: se refiere a las unidades de datos o al procesamiento de las mismas dentro del contexto del tercer nivel del modelo OSI. Por ejemplo, tanto los datagramas IP como los conmutadores que los procesan son de capa tres.

DMZ (zona desmilitarizada): corresponde a una subred en la cual se instalan servidores y se permite el acceso a la información de los mismos desde la Internet pública.

Tráfico unicast: se refiere a los paquetes (tramas Ethernet, datagramas IP, segmentos TCP) que envía cualquier emisor hacia un solo destino. En dicho caso, el emisor debe especificar la dirección del destinatario del mensaje.

Reiniciar: regresar la configuración de un equipo a los valores que tenía por defecto (en el momento en que fue fabricado). También significa apagar y volver a encender un equipo.

Bibliografía

CISCO (2009). *Smart Business Architecture for Midsize Networks: Configuration Files Guide*. Disponible en: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/SBA__configG.pdf [consulta: octubre 25 de 2012].

_____ (2009). *Smart Business Architecture for Midsize Networks: Deployment Guide*. [en línea] Disponible en: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/SBA__deployG.pdf [consulta: octubre 25 de 2012].

_____ (2009). *Smart Business Architecture for Midsize Networks: Design Guide*. Disponible en: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/SBA_dg.pdf [consulta: octubre 5 de 2011].

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.