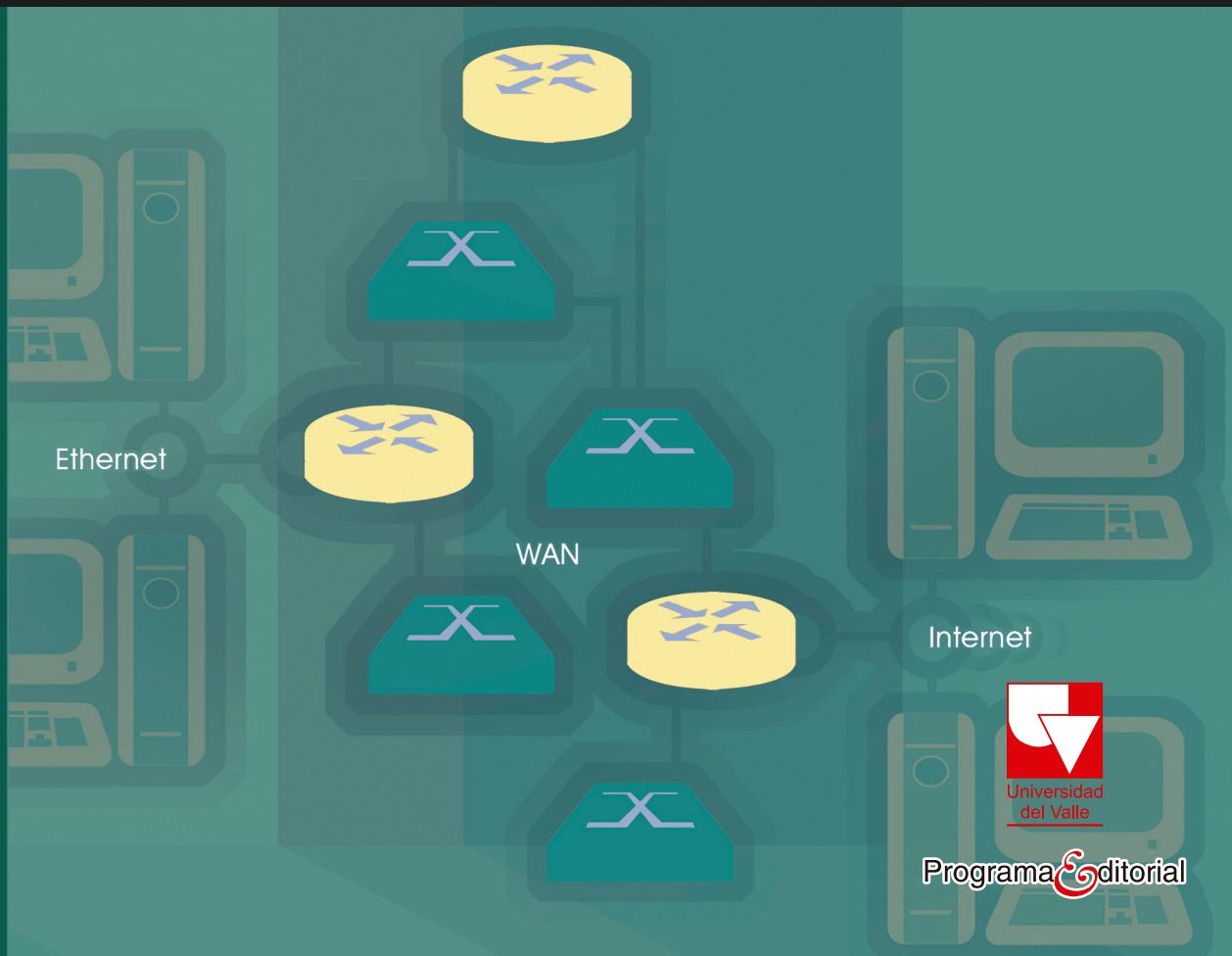


LABORATORIO DE REDES Y COMUNICACIÓN

• OSCAR POLANCO SARMIENTO •





Universidad
del Valle

Programa *E*ditorial

LABORATORIO DE REDES Y COMUNICACIONES



Colección Ingeniería

O S C A R P O L A N C O S A R M I E N T O

Ingeniero Electricista, Universidad del Valle, 1986. Especialista en Computadores y Sistemas Digitales, Universidad del Valle, 1993. Ingeniero de Soporte en Coldatos (1987-1994). Trabajó en la implementación y soporte de la infraestructura de comunicaciones TCP/IP de Financiera FES (1994-2001). Desde el año 2002 se encuentra vinculado como profesor de la Escuela de Ingeniería Eléctrica y Electrónica de la Universidad del Valle. Sus áreas de actuación son: Interconexión de redes TCP/IP, Seguridad en Redes Corporativas, y Modelamiento y Simulación de Redes de Telecomunicaciones.

Oscar Polanco Sarmiento

**LABORATORIO DE
REDES Y COMUNICACIONES**



Colección Ingeniería

Polanco Sarmiento, Oscar
Laboratorio de redes y comunicaciones / Oscar Polanco Sarmiento. -- Cali:
Programa Editorial Universidad del Valle, 2012.
268 p. ; 24 cm. -- (Ciencias Naturales y Exactas)
1. Redes de computadores - Protocolos 2. Redes de telecomunicaciones 3.
Redes de computadores - Manuales de laboratorio 4. TCP/IP (Protocolo de redes
de computadores)
I. Tít. II. Serie.
004.68 cd 21 ed.
A1377054

CEP-Banco de la República-Biblioteca Luis Ángel Arango

**Universidad del Valle
Programa Editorial**

Título: *Laboratorio de Redes y Comunicaciones*

Autor: Oscar Polanco Sarmiento

ISBN: 978-958-765-036-5

ISBN PDF: 978-958-765-498-1

DOI:

Colección: Ingeniería

Primera Edición Impresa Noviembre 2012

Edición Digital Julio 2017

Rector de la Universidad del Valle: Édgar Varela Barrios

Vicerrector de Investigaciones: Javier Medina Vásquez

Director del Programa Editorial: Francisco Ramírez Potes

© Universidad del Valle

© Oscar Polanco Sarmiento

Diseño de carátula: Anna Echavarria. Elefante

Diagramación: Hugo H. Ordóñez Nieves

Corrección de estilo: Luz Stella Grisales H.

Universidad del Valle

Ciudad Universitaria, Meléndez

A.A. 025360

Cali, Colombia

Teléfonos: (57) (2) 321 2227 - 339 2470

E-mail: programa.editorial@correounivalle.edu.co

Este libro, salvo las excepciones previstas por la Ley, no puede ser reproducido por ningún medio sin previa autorización escrita por la Universidad del Valle.

El contenido de esta obra corresponde al derecho de expresión del autor y no compromete el pensamiento institucional de la Universidad del Valle, ni genera responsabilidad frente a terceros.

El autor es responsable del respeto a los derechos de autor del material contenido en la publicación (fotografías, ilustraciones, tablas, etc.), razón por la cual la Universidad no puede asumir ninguna responsabilidad en caso de omisiones o errores.

Cali, Colombia, Julio de 2017

CONTENIDO

INTRODUCCIÓN	11
CAPÍTULO 1 EQUIPOS DE RED E INTERFAZ DE USUARIO.....	13
CAPÍTULO 2 CONFIGURACIÓN BÁSICA DE UN ENCAMINADOR Y FUNCIONES DE SUS COMPONENTES	33
CAPÍTULO 3 ADMINISTRACIÓN BÁSICA DE UN ENCAMINADOR CISCO	61
CAPÍTULO 4 RIP COMO PROTOCOLO DE ENCAMINAMIENTO IP, RUTAS ESTÁTICAS	83
CAPÍTULO 5 EIGRP: PROTOCOLO DE ENCAMINAMIENTO IP.....	105
CAPÍTULO 6 LISTAS DE ACCESO IP ESTÁNDAR	119
CAPÍTULO 7 LISTAS DE ACCESO IP EXTENDIDAS.....	137

CAPÍTULO 8 REDES DE ÁREA AMPLIA Y TECNOLOGÍAS DE ACCESO: RETRANSMISIÓN DE TRAMAS, ATM, ADSL Y CABLE.....	153
CAPÍTULO 9 PROTOCOLO DE ENRUTAMIENTO IP: ABRIR PRIMERO LA RUTA MÁS CORTA (OPEN SHORTEST PATH FIRST - OSPF).....	171
CAPÍTULO 10 CONFIGURACIÓN DEL CONMUTADOR ETHERNET 2950, NAT Y PAT.....	185
CAPÍTULO 11 INTERCONEXIÓN DE REDES: PROYECTO Y CASO DE ESTUDIO..	199
CAPÍTULO 12 REDES INALÁMBRICAS IEEE 802.11 A/B/G	223
CAPÍTULO 13 ENCAPSULADO GENÉRICO DE ENCAMINAMIENTO Y SEGURIDAD IP (GRE/IPSEC).....	239
CAPÍTULO 14 VOZ SOBRE IP	249



Universidad
del Valle

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

INTRODUCCIÓN

Las organizaciones actuales basan gran parte de su operación en el uso de los sistemas de información y de las tecnologías asociadas a estos. Específicamente, ellas se soportan en las redes basadas en TCP/IP como infraestructura de telecomunicaciones, lo cual permite el flujo de información entre sus oficinas, proveedores y usuarios, logrando así satisfacer la demanda de información requerida para su operación y toma de decisiones.

Teniendo en cuenta lo anterior, es importante que los profesionales en las áreas relacionadas con los sistemas de información y las telecomunicaciones tengan una experiencia práctica tanto en la configuración como en la operación y gestión de las redes basadas en TCP/IP.

Con este texto se pretende llevar a la práctica los aspectos relacionados con la arquitectura TCP/IP, posibilitando a través de ella, y de manera progresiva, realizar el montaje básico de una intranet.

En las primeras ocho sesiones se revisan los conceptos relativos al Sistema Operativo de los encaminadores Cisco y sus diferentes modos de operación, asimismo, se practican los comandos más importantes para su configuración y monitoreo. Seguidamente se sugiere una metodología para administrar tanto el archivo del Sistema Operativo como el archivo de configuración de los encaminadores que conforman la red. Posteriormente se interconectan las redes de área local utilizando los protocolos de enrutamiento RIP y EIGRP, y se utilizan las listas de acceso como filtros que ofrecen un nivel básico de seguridad en el sistema. También se revisan los detalles para realizar la configuración de los encaminadores y habilitar su operación en tecnologías de red de área amplia (WAN), utilizando *Frame*

Relay, ATM, ADSL y *Cable módem*. Cada sesión presenta de manera conveniente los diferentes escenarios, las ayudas necesarias y las respectivas soluciones para que, después de su lectura, el estudiante esté en capacidad de configurar un conjunto de encaminadores y probarlos en el laboratorio.

A partir de la sesión número nueve se estudian los tópicos relacionados con el protocolo de enrutamiento *OSPF*, la configuración básica del comutador *Catalyst 2950*, y se propone la interconexión de redes *Ethernet* conmutada mediante un proyecto final y un caso de estudio; aquí se involucran los temas concernientes a: *VLAN*, *IEEE 802.1Q*, comutadores capa tres, seguridad y calidad de servicio. Finalmente, se abordan los temas relativos a las redes inalámbricas, la interconexión de redes mediante *GRE/IPsec* y la configuración del servicio de *Voz sobre IP*.

Este texto es útil como soporte práctico que complementa los cursos de Redes del programa de posgrado de Ingeniería Eléctrica y Electrónica de la Universidad del Valle, como también para el curso Laboratorio de Comunicaciones II de pregrado, ofrecido al programa de Ingeniería Electrónica de la Escuela de Ingeniería Eléctrica y Electrónica.

EQUIPOS DE RED E INTERFAZ DE USUARIO

Los elementos centrales de una red de área local –Local Area Network (LAN)– son los sistemas finales (estaciones de trabajo, servidores, impresoras, etc.) y los conmutadores de capa 2 y de capa 3 (switches). Los encaminadores son los equipos necesarios para interconectar las redes de área local que se encuentran separadas por su ubicación geográfica, conformando lo que se conoce como una intranet. La presente sesión tiene como propósito que el lector identifique algunos equipos de red, sus conexiones físicas y los tipos de conectores que estos tienen. También se pretende que el lector adquiera familiaridad con la interfaz de línea de comando –Command Line Interface (CLI)– de un encaminador Cisco y de un conmutador Cisco. El componente práctico de la presente sesión se puede llevar a cabo mediante el montaje de la red ilustrada en la Figura 1.1, para esto es necesario contar con algunos recursos de hardware o software que dependen de la opción con la cual se desee trabajar. A continuación se presentan dos opciones.

Opción 1: Cuando se desee trabajar con equipos físicos: en este caso se requiere tener un computador personal que cumpla el papel de sistema final, un encaminador Cisco (cualquier modelo) y un conmutador Cisco capa dos o capa tres (cualquier modelo, también). Se puede trabajar con equipos similares de marcas diferentes a Cisco, por ejemplo, se puede usar un switch Alcatel Lucent modelo OS6200. La mayoría de equipos de marcas diferentes a Cisco tienen su propia interfaz de línea de comando, cuya estructura, sintaxis y soporte de comandos, por lo general, son diferentes,

algunas de estas marcas también incorporan la interfaz de línea de comando de Cisco para facilitar el trabajo a aquellas personas acostumbradas al CLI de Cisco.

Opción 2: Cuando se desee trabajar con equipos virtuales como: computadores, encaminadores y commutadores, estos pueden ser simulados o emulados mediante programas basados en software que se ejecutan en el computador personal. Algunos de estos programas son: NETSIM, Packet Tracer, y GNS3 (Graphical Network Simulator), el último es de licencia pública y requiere que el usuario posea el sistema operativo –Internetwork Operating System (IOS)– de una de las plataformas Cisco que dicho software puede emular.

Cualquiera de las dos opciones anteriores que elija le servirá para realizar la mayoría de las prácticas propuestas a lo largo del texto, exceptuando unas pocas en las que se requiere usar exclusivamente los equipos físicos sugeridos. También es posible usar una combinación de las dos opciones anteriores en situaciones que lo requieran.

OBJETIVO

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

- Identificar los equipos de uso más común en las redes.
- Establecer una sesión con el encaminador en modo de ejecución de usuario y en modo de ejecución privilegiado.
- Usar la ayuda contextual.
- Usar la historia de comandos y las propiedades de edición.
- Cerrar la sesión establecida con el encaminador.

PROCEDIMIENTO

Entrando a un encaminador

Al intérprete de comandos de un encaminador se le denomina EXEC. Además de interpretar los comandos, lleva a cabo las operaciones correspondientes que un usuario requiera. Se puede tener acceso a la ejecución de los comandos entrando al encaminador por medio del puerto de consola o de una sesión de terminal virtual (vt). Una vez se entre al encaminador, éste presenta una interfaz de línea de comando que permite ejecutar comandos en el encaminador.

En caso de optar por trabajar con equipos físicos para establecer una sesión con el encaminador por medio del puerto de consola, denominado

con 0, se conecta un cable serie entre el puerto de consola del encaminador (identificado por un conector RJ45 marcado con el nombre *console* en la parte posterior del encaminador) y el puerto serie de una terminal o de un computador personal (PC) (identificado por un puerto con conector DB9 marcado con el nombre Com1 o Com2 en el computador). También es necesario ejecutar un programa de emulación de terminal en el computador personal como, por ejemplo, Hyperterminal para Windows XP, TeraTerm para Windows 7, Screen para Linux o Putty para cualquiera de estos sistemas operativos. Cualquiera sea el caso, el puerto serie de la terminal o del PC debe configurarse con los siguientes parámetros:

- Bits por segundo: 9600
- Bits de datos: 8
- Paridad: Ninguno
- Bits de parada: 1
- Control de Flujo: Ninguno

En caso de optar por trabajar con equipos virtuales mediante el programa GNS3, es necesario realizar los siguientes pasos:

- Descargar de Internet el programa GNS3 e instalarlo en un computador personal.
- Suministrarle a GNS3 el sistema operativo (IOS) de la plataforma que se desea emular, esto se realiza mediante la opción “IOS images and hypervisors” de GNS3. El IOS debe ser obtenido por cuenta del usuario.
- Arrastrar al área de trabajo el equipo de la plataforma que se desea emular y cuyo IOS haya sido previamente cargado en GNS3.
- Adicionar las interfaces que se requieran en el equipo que se va a emular (opcional). Esto se realiza especialmente si es necesario tener conexiones de red de área amplia (WAN) o más conexiones de las que tiene por defecto el equipo. Para este propósito se usa la pestaña “Slots” de la opción “Configure”.
- Entrar por consola al equipo que se va a emular mediante el ícono “Console to all devices” o dando clic derecho en el equipo para seleccionar la opción “Console”.

Después de digitar la tecla [Enter] en la ventana del programa de emulación de terminal (cuando se usan equipos físicos) o en la ventana de la consola del equipo emulado (cuando se usa GNS3), aparecerá el indicador del sistema (prompt) de la interfaz de línea de comando del encaminador. El indicador del sistema permite identificar el nombre del equipo (que por

defecto es “Router”) y el modo de ejecución de usuario mediante el signo mayor “>”, como se presenta a continuación:

Router >

Después de lograr entrar por el puerto de consola en cada equipo (en-caminador R1 y SwitchA), es necesario hacer las conexiones entre estos, basándose en la Figura 1.1. Para trabajar con equipos físicos, se deben realizar las conexiones físicas con cables de par trenzado sin apantallar –Unshielded Twisted Pair (UTP). Para trabajar con equipos virtuales mediante GNS3, se deben realizar las mismas conexiones, utilizando el botón “Add a Link”.

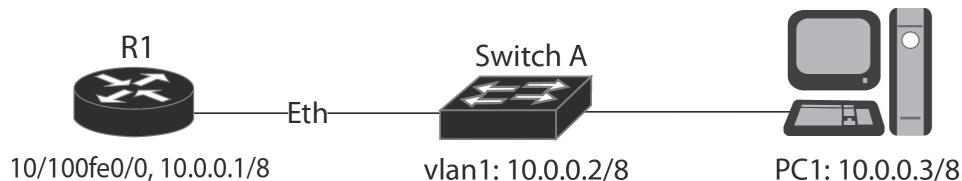


Figura 1.1 Red para el laboratorio de la interfaz de línea de comando (CLI)

Posteriormente, se deben configurar los equipos con las siguientes direcciones IP.

- Configurar la tarjeta de red de R1 con la dirección IP 10.0.0.1 y máscara 255.0.0.0.
- Configurar el conmutador SwitchA con la dirección IP 10.0.0.2 y máscara 255.0.0.0.
- Configurar la tarjeta de red de PC1 con la dirección IP 10.0.0.3 y máscara 255.0.0.0

A continuación se presentan los comandos que permiten entrar al modo de configuración global en los equipos R1 y SwitchA.

Router> *enable*

Password: red –introducir la clave que tenga configurada el equipo o la clave por defecto del mismo.

Router# *configure terminal*

Router(config)#

A continuación se presentan los comandos que permiten configurar los equipos R1 y SwitchA para que acepten la conexión de un cliente telnet.

R1	SwitchA
Router(config)# <i>hostname R1</i> R1(config)# <i>interface fastEthernet0/0</i> R1(config-if)# <i>ip address</i> 10.0.0.1 255.0.0.0 R1(config-if)# <i>no shutdown</i> R1(config-if)# <i>exit</i> R1(config)#	Switch(config)# <i>hostname SwitchA</i> SwitchA(config)# <i>interface vlan 1</i> SwitchA(config-if)# <i>ip address</i> 10.0.0.2 255.0.0.0 SwitchA(config-if)# <i>no shutdown</i> SwitchA(config-if)# <i>exit</i> SwitchA(config)#
R1(config)# <i>line vty 0 15</i> R1(config-line)# <i>password red</i> R1(config-line)# <i>login</i> R1(config-line)# <i>exit</i> R1(config)#	SwitchA(config)# <i>line vty 0 15</i> SwitchA(config-line)# <i>password red</i> SwitchA(config-line)# <i>login</i> SwitchA(config-line)# <i>exit</i> SwitchA(config)#
R1(config)# <i>enable secret univalle</i>	SwitchA(config)# <i>enable secret univalle</i>

Para establecer una sesión con el encaminador R1 –la cual es atendida por una de las terminales virtuales (vty 0 hasta vty15) que dicho equipo tiene–, es necesario ejecutar un programa cliente de telnet desde el computador personal PC1 que se encuentra en red con el encaminador R1, dando como dirección destino la dirección IP de la interfaz Ethernet del enca-minador. Es decir, desde PC1 se ejecuta el comando *telnet 10.0.0.1*. Debe asegurarse, antes de ejecutar el comando anterior, que se hayan realizado las respectivas conexiones de los equipos.

En caso de trabajar con equipos virtuales, el computador personal PC1 puede ser emulado por otro encaminador (por ejemplo, R2) al que se le debe habilitar la interfaz Ethernet, y en esa misma interfaz configurar la dirección IP 10.0.0.3 con máscara 255.0.0.0. Otra posibilidad es integrar el programa de computadores virtuales –Virtual Personal Computers (VPCS)– con GNS3, dicho programa permite emular las funciones básicas de red de un computador personal.

Por razones de seguridad, el EXEC proporciona dos niveles de acceso para la ejecución de comandos, denominados: “modo de ejecución de usuario” y “modo de ejecución privilegiado”. El conjunto de comandos disponibles en el modo de ejecución de usuario son un subconjunto de los comandos disponibles en el modo de ejecución privilegiado.

Para entrar al encaminador R1 (con dirección IP 1.0.0.1 en la tarjeta de red) que se encuentra en la misma red de área local en la que está PC1 (el cual tiene dirección IP 10.0.0.3), se hace lo siguiente:

- Se ejecuta desde PC1 el comando *telnet 10.0.0.1*, inmediatamente aparecerá el siguiente mensaje de verificación:

```
User Access Verification  
Password: red
```

- Despues de digitar una clave válida (“red”, en este caso), el equipo permite trabajar en el modo de ejecución de usuario, esto se evidencia cuando el equipo envíe el indicador del sistema (prompt), compuesto por su nombre y el símbolo “>”.

```
R1>
```

- Posteriormente se puede entrar al modo de ejecución privilegiado, ejecutando el comando *enable*. Para salir del modo de ejecución privilegiado se ejecuta el comando *disable*. Para el primer caso, es necesario conocer la clave asociada al modo de ejecución privilegiado (“univalle”, en este caso). Este modo de ejecución es indicado por el sistema mediante el símbolo “#” (numeral).

```
R1> enable  
Password: univalle  
R1#  
R1# disable  
R1>
```

Desde el modo privilegiado se puede acceder a otros modos, tales como:

1. Modo de configuración Global, el cual es indicado mediante un ligero cambio en el indicador del sistema –prompt– del equipo.

```
R1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config) #
```

2. Modos de configuración específica: de interfaz, de subinterfaz, de la línea de consola, de la línea del puerto auxiliar, de los protocolos de enrutamiento (por ejemplo, del protocolo de enrutamiento RIP), y otros modos, también indicados por cambio en el “prompt” del equipo.

```
R1(config)# interface serial 0/0
R1(config-if)# exit

R1(config)# interface serial 0/0.1
R1(config-subif)# exit

R1(config)# line 0
R1(config-line)# exit

R1(config)# line aux 0
R1(config-line)#

R1(config)# router rip
R1(config-router)# exit
```

AYUDA EN EL MODO DE EJECUCIÓN DE USUARIO

Mediante el signo de interrogación se visualizan los comandos que se pueden ejecutar en el modo de ejecución de usuario

R1> ?

Exec commands:	
<1-99>	Session number to resume
connect	Open a terminal connection
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)
show	Show running system information
slip	Start Serial-line IP (SLIP)
systat	Display information about terminal lines
telnet	Open a telnet connection

—La salida ha sido truncada—

AYUDA EN EL MODO DE EJECUCIÓN PRIVILEGIADO

Mediante el signo de interrogación se pueden visualizar los comandos que se permiten ejecutar en el modo de ejecución privilegiado.

R1# ?

Exec commands:	
<1-99>	Session number to resume
bfe	For manual emergency modes setting
clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode
connect	Open a terminal connection
copy	Copy a config file to or from a tftp server
debug	Debugging functions (see also ‘udebug’)
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
erase	Erase Flash memory
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
mbranch	Trace multicast route down tree branch
mrbranch	Trace reverse multicast route up tree branch
name-connection	Name an existing network connection
no	Disable debugging functions
pad	Open a X.29 PAD connection
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)
reload	Halt and perform a cold restart
resume	Resume an active network connection
rlogin	Open an rlogin connection
rsh	Execute a remote command
send	Send a message to other tty lines
setup	Run the SETUP command facility
show	Show running system information

—La salida ha sido truncada—

En conclusión, digitando el símbolo de interrogación (?) en el indicador del sistema del modo de ejecución de usuario o en el del modo de ejecución privilegiado se obtiene una lista de los comandos que se pueden utilizar. La lista puede variar, dependiendo de la versión del IOS.

AYUDA CONTEXTUAL

Para familiarizarse con la ayuda contextual, a continuación se practica la ejecución de un comando que permite configurar la hora y fecha de R1. La ayuda contextual permite conocer la sintaxis de cualquier comando; además, por medio de la tecla de cursor hacia arriba o con la combinación [CRTL] P puede repetirse un comando que se haya ejecutado previamente.

R1# *clk*

Translating “CLK”...domain server (200.25.53.10)

% Unknown command or computer name, or unable to find computer address

R1# *c?*

call	ccm-manager	cd	clear
clock	cns	configure	connect
copy	credential	crypto	ct-isdn

R1# *clock*

% Incomplete command.

R1# *clock ?*

set Set the time and date

R1# *clock set*

% Incomplete command.

R1# *clock set ?*

Current Time (hh:mm:ss)

R1# *clock set 19:56:00*

% Incomplete command.

R1# *clock set 19:56:00 ?*

<1-31>	Day of the month
MONTH	Month of the year

R1# *clock set 19:56:00 04 11*

^

% Invalid input detected at ‘^’ marker.

```
R1# clock set 19:56:00 04 november  
% Incomplete command.
```

```
R1# clock set 19:56:00 04 november ?  
<1993-2035> Year
```

```
R1# clock set 19:56:00 04 november 2011
```

CARACTERÍSTICAS DE EDICIÓN

La interfaz de usuario proporciona un modo de edición mejorado que permite:

Enrollado automático del cursor en líneas largas (scrolling): cuando un comando se debe extender más allá de la capacidad de una línea de la pantalla (típicamente de 80 caracteres) y el cursor llega al final de dicha capacidad, la línea se desplazará 10 espacios a la izquierda (se enrolla) y el signo “#” es reemplazado por el signo “\$”, indicando que la línea ha sido enrollada.

- [CNTL] A mueve el cursor al inicio de la línea.
- [CNTL] E mueve el cursor al final de la línea.
- [CNTL] B mueve el cursor un carácter a la izquierda –también se puede usar la tecla cursor a la izquierda.
- [CNTL] F mueve el cursor un carácter a la derecha –también se puede usar la tecla cursor a la derecha.
- [CNTL] P presenta al comando anterior –también se puede usar la tecla cursor arriba.
- [CNTL] N presenta al comando posterior –también se puede usar la tecla cursor abajo.
- R1> *show history* muestra los últimos 10 comandos.
- R1> *terminal history size* *número_de_líneas*, configura el número de comandos que se guardan en memoria con el valor del parámetro *número_de_líneas*, por defecto dicho valor es 10.
- [TAB] con la tecla TAB se completa un comando que no sea ambiguo.

- R1> *terminal no editing* deshabilita las características de edición avanzadas.
- R1> *terminal editing* habilita las características de edición avanzadas.

SALIR DEL ENCAMINADOR

Para salir del encaminador se puede usar el comando *quit* o el comando *exit*

R1# *quit* (o *exit*).

INFORME

Describa cuál es la diferencia fundamental de estar bajo el modo de ejecución de usuario y el modo de ejecución privilegiado.

Explore y describa sobre la utilidad y función de los comandos *send*, *systat* y *show*.

Explore y describa el uso de los siguientes programas de emulación: Tera Term, CoolTerm, Putty y Screen.

EJERCICIOS DE LABORATORIO

Estos ejercicios tienen como finalidad practicar algunos de los aspectos estudiados en esta sección, especialmente se pretende ganar familiaridad con la interfaz de comandos de los encaminadores y conmutadores capa 2 Cisco. Los ejercicios están basados en la red de la Figura 1.1.

Ejercicio 1

Permite familiarizarse con la interfaz CLI de un encaminador.

1. Desde PC1, establezca una sesión con R1.
2. Entre al modo de ejecución privilegiado.
3. Regresar al modo de ejecución de usuario.
4. Use la ayuda contextual para ver los comandos que empiezan con la letra “c”.
5. Use la ayuda contextual para ver los comandos *show*.
6. Familiarícese con las características de edición de terminal: [CRTL] A, [CRTL] E, y las teclas [cursor arriba], [cursor abajo], [cursor izquierdo], y [cursor derecho].

7. Cambie a 20 el tamaño de la historia de los comandos, lo cual permitirá mostrar la historia de los últimos 20 comandos previamente digitados.
8. Salga de R1 (ejecute Log out).

Ejercicio 2

Permite familiarizarse con la interfaz CLI de un conmutador capa 2 Cisco.

1. Desde PC1 establezca una sesión por telnet al equipo SwitchA.
2. Acceda a la interfaz de línea de comando del conmutador capa 2.
3. Acceda al modo de ejecución privilegiado.
4. Examine la versión del software del conmutador capa 2.
5. Examine la interfaz e0/1.
6. Cambie el hostname a “SWA”.
7. Inhabilite una interfaz que no esté utilizando en el SwitchA.
8. Cambie la clave de ejecución de usuario a “red1”.
9. Cambie la clave de ejecución privilegiado a “univalle1”.
10. Salga del modo de configuración.
11. Examine los cambios de configuración del equipo en el archivo “running-config”.

INFORMACIÓN COMPLEMENTARIA

Interfaces hardware

La siguiente sección explica la nomenclatura usada en las interfaces hardware de los encaminadores y conmutadores capa 2. Esto es importante para cuando se requiera conectar y configurar una interfaz en particular.

Nomenclatura de las interfaces de los encaminadores

Cisco soporta dos tipos de interfaces en los encaminadores y en los conmutadores capa 2: fija y modular. Las interfaces fijas inicialmente son diferenciadas por su tipo, el cual hace referencia al medio utilizado en el nivel de enlace de datos; por ejemplo, Ethernet, FastEthernet, TokenRing, Serial, etc. El número de la interfaz siempre empieza por 0 y continúa creciendo para cada tipo de interfaz. Si, por ejemplo, un encaminador tiene dos interfaces fijas de tipo Ethernet y dos interfaces fijas de tipo serie, ellas se numeran con 0 y 1 para las interfaces Ethernet, y con 0 y 1 para las interfaces serie. En conclusión, estas interfaces pueden diferenciarse por el *tipo* seguido del *número de la interfaz*, como se indica a continuación.

- Serial 0, Serial 0/0, Serial 0/2/0.
- Serial 1. Serial 0/1, Serial 0/2/1.
- Ethernet 0. FastEthernet 0/0, GigabitEthernet 0/0.
- Ethernet 1. FastEthernet 0/1, GigabitEthernet 0/1.

La Figura 1.2 presenta un encaminador Cisco 2801 con sus interfaces de LAN (Ethernet) y de WAN (Synchronous Serial port).



Figura 1.2 Aspecto físico de un encaminador Cisco 2801

En los equipos modulares, las interfaces se identifican mediante una expresión que contiene: el tipo de interfaz proporcionada por el módulo, el número de ranura (slot) ocupado por el módulo al ser instalado en el equipo y el número que tenga etiquetada la interfaz en el módulo. Por ejemplo, en un equipo con cuatro ranuras, numeradas desde 0 hasta 3, se puede instalar (en una de éstas) un módulo con dos interfaces FastEthernet numeradas como 0 y 1. Cuando se hace referencia a una interfaz específica dentro de una ranura, se utiliza la nomenclatura *type slot_number/interface_number*, es decir, la nomenclatura FastEthernet 0/1 se refiere a la interfaz uno del módulo instalado en la ranura cero, cuyo tipo es FastEthernet. Otros ejemplos pueden ser: Serial 2/0 y Serial 2/1.

NOMENCLATURA DE LAS INTERFACES DE LOS CONMUTADORES

Independientemente de si un conmutador es fijo o modular, siempre se utiliza la nomenclatura *type slot_number/interface_number*, en donde el “slot 0” hace referencia a la primera ranura, la cual puede ser fija o modular. A diferencia de los encaminadores, las interfaces de los conmutadores se numeran a partir de 1 y en orden creciente.

CABLE UNO A UNO (STRAIGHT) Y CABLE CRUZADO (CROSSOVER)

Para conectar equipos en una LAN mediante cable UTP, se utilizan conectores RJ45 de 8 pines. Los conectores RJ45 se conectan a los 8 hilos (4 pares) del cable UTP en los dos extremos del cable, como se muestra en la Figura 1.3.

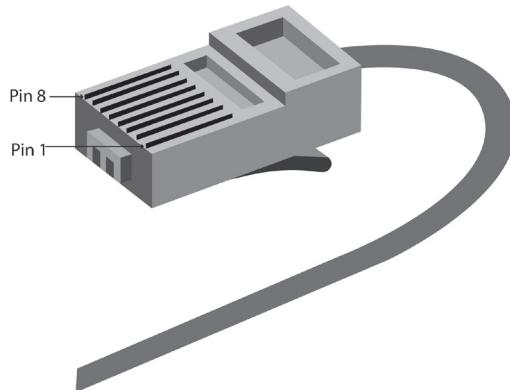


Figura 1.3 Disposición física en un extremo del cable UTP con conector RJ45

Para una red Ethernet se tienen dos tipos de conexiones: el cable uno a uno y el cable cruzado. El *cable uno a uno* tiene el pin 1 de un extremo alambrado al pin 1 del otro extremo, lo mismo para los pines 2 al 8 restantes, como se ilustra en la Figura 1.4 (a).

Un *cable cruzado* tiene los pines 1 y 2 del extremo izquierdo alambrados a los pines 3 y 6 del extremo derecho, respectivamente; y los pines 3 y 6 del extremo izquierdo alambrados a los pines 1 y 2 del extremo derecho, respectivamente, como se ilustra en la Figura 1.4 (b).

Para realizar las conexiones entre equipos de una red de área local, estos se clasifican en dos categorías: equipo terminal de datos –Data Terminal Equipment (DTE)– y equipo de terminación del circuito de datos –Data Circuit-terminating Equipment (DCE). Los equipos que operan como DTE son: computador personal, estación de trabajo, portátil, servidor, impresora, encaminador, punto de acceso inalámbrico, teléfono de voz sobre IP. Los equipos que operan como DCE son: concentrador (Hub), conmutador capa dos o capa tres.

El cable uno a uno se usa para conexiones de DTE a DCE, Figura 1.5 (a). El cable cruzado se usa para conexiones de DTE a DTE o de DCE a DCE Figura 1.5 (b). Algunos equipos DTE o DCE pueden interconectarse con equipos de su misma categoría mediante un cable uno a uno cuando al menos uno de ellos detecta de forma automática la necesidad de realizar el cruce del cable. Algunos concentradores tienen un botón asociado a un determinado puerto que puede realizar el cruce del cable sobre el puerto, Figura 1.5 (c).

Algunos equipos, además de tener puertos con conectores comunes en la red LAN –RJ45 para UTP en 10/100/1000BaseT–, también tienen uno o varios puertos –denominados Gigabit Interface Converter (GBIC)– que permiten hacer la conversión de dicha interfaz a otros tipos de medio físico cuan-

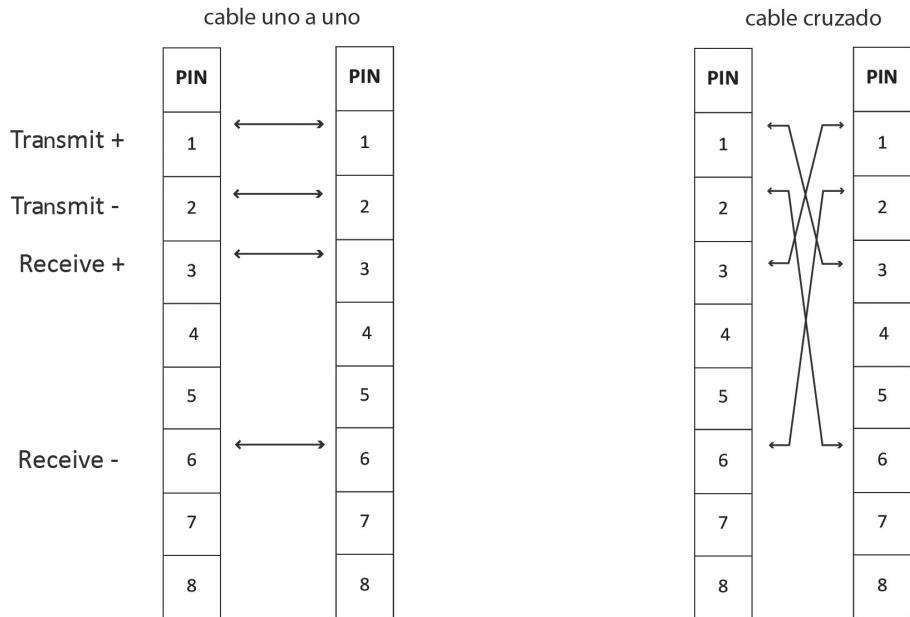


Figura 1.4 Configuración de un cable uno a uno (a) y de un cable cruzado (b)

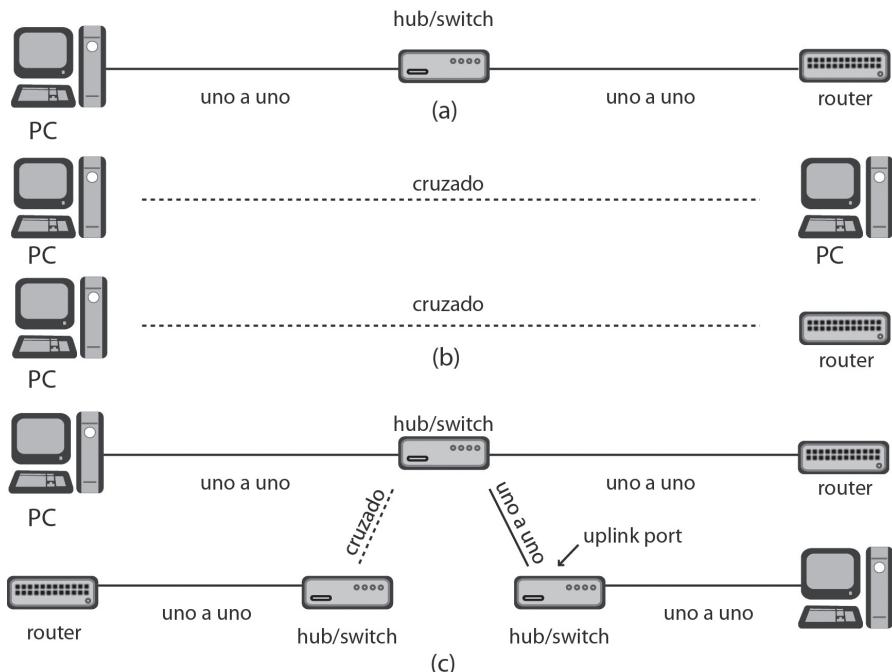


Figura 1.5 Conexión de diferentes tipos de equipos con cables uno a uno y con cables cruzados

do así se requiera, la Figura 1.6 ilustra un conversor 1000BASE-T GBIC de Cisco (WS-G5483=), el cual convierte la interfaz GBIC a 1000Baset.



Figura 1.6 Dispositivo 1000BASE-T GBIC de Cisco para convertir GBIC a 1000BaseT

En principio, una red de área local básica –10/100/1000BaseT– se compone de un arreglo de equipos –estaciones de trabajo y servidores– que se interconectan por medio de un conmutador Ethernet. El conmutador facilita la comunicación local entre los equipos, permitiendo que utilicen un canal con una velocidad de 10, 100 o 1000 megabits por segundo. La Figura 1.7 muestra la disposición física de dos conmutadores Alcatel Lucent de capa dos, acondicionados para su instalación en el armario del centro de cableado.



Figura 1.7 Aspecto físico de dos conmutadores Alcatel Lucent (OS6250-24) de capa dos

CABLE PARA CONEXIÓN A LA RED DE ÁREA AMPLIA

Desde el punto de vista de las interfaces serie (capa física), un encaminador se comporta como DTE, que es un dispositivo de usuario final que se conecta a la red WAN del proveedor. En contraste, un DCE termina la conexión del proveedor y recibe al DTE del usuario, el DCE más común en las redes es el módem, independientemente de la tecnología que éste maneje. Una de las principales funciones de un DCE es proporcionar relojes para la sincronización de la conexión. Con la finalidad de que el puerto serie (WAN) de los encaminadores soporte simultáneamente dos conectores estándar (RS232 y V.35), Cisco utiliza cables con conectores propietarios –DB60 y Smart Serial (SS)– en el extremo que se conecta al puerto del encaminador y con conectores estándar (RS232, V.35) en el extremo que se

conecta al DCE. Por lo anterior, al momento de adquirir un cable, éste se debe especificar de acuerdo a la interfaz estándar del equipo DCE al cual se va a conectar el puerto serie del encaminador. A continuación se listan varios tipos de cable serie, junto con el significado de su representación, y en la Figura 1.8 se ilustra un cable cuya referencia es “CAB-SS-V35MT”.

- CAB-SS-V35MT: conector Smart Serial, interfaz V35, macho (M), DTE(T).
- CAB-SS-V35FC: conector Smart Serial, interfaz V35, hembra (F), DCE(C).
- CAB-V35MT: conector DB60, interfaz V35, macho (M), DTE(T).
- CAB-232MT: conector DB60, interfaz 232, macho (M), DTE(T).
- CAB-232FC: conector DB60, interfaz 232, hembra (F), DCE(C).



*Figura 1.8 Aspecto físico de un cable con número de producto
CAB-SS-V35MT*

PROBLEMAS

1. ¿Cuál es la disposición de pines (pinout) de la interfaz de consola de los siguientes equipos?:
 - Comutador Ethernet capa 3 modelo 3560G Cisco (switch).
 - Encaminador 2801 Cisco (router).
 - Comutador Ethernet capa 3 modelo 6850-24 Alcatel Lucent.
 - Servidor de Terminales modelo CM4116 Opengear.
2. ¿Cuál es la configuración (conexiones RJ45 a RJ45) que debe tener el respectivo cable para conectar un puerto serie del servidor de terminales CM4116 con el puerto de consola de los siguientes equipos?: comutador 3560G Cisco y comutador 6850-24 Alcatel Lucent. Lo anterior con el fin de administrar remotamente dichos equipos por medio del servidor de terminales CM4116.
3. ¿Cuál es la configuración (conexiones RJ45 a RJ45) que debe tener un cable que permita conectar la interfaz E1 de un encaminador 2801 Cis-

- co con la interfaz E1 de otro encaminador 2801 Cisco (conexión “back-to-back”)?
4. ¿Cuál es la disposición de pines (pinout) de la interfaz RJ45 para la especificación 1000BaseT (Gigabit Ethernet)?
 5. Consulte las características principales del equipo CM4116. ¿Cuál es la utilidad de dicho equipo?
 6. Para el encaminador R1 de la Figura 1.1, comente el significado y utilidad que puede tener el comando “reload in 10” en el modo de ejecución privilegiado.

GLOSARIO

Conektor DB9: Es un conector que permite la comunicación serie asincrónica de un equipo. Normalmente los computadores personales tienen este tipo de conector en un puerto que el sistema operativo Windows identifica como COM1 y que Linux identifica como un dispositivo cuyo nombre inicia con “/dev/tty*”.

EXEC: Hace referencia a la posibilidad que tiene el usuario de ejecutar uno o varios comandos mediante la interfaz de línea de comando que presentan los equipos Cisco: commutadores Ethernet, encaminadores, puntos de acceso, etc.

GBIC: Dispositivo que convierte una interfaz Gigabit de un commutador Ethernet o de un encaminador IP para hacerla compatible con el medio requerido por el usuario –el medio típicamente es cable UTP o fibra óptica–, dicho dispositivo hace la función de transceiver (transmisor-receptor). Un equipo con interfaz GBIC proporciona mayor flexibilidad y puede ocupar mayor espacio que su contraparte con puerto fijo.

IOS: nombre que recibe el sistema operativo utilizado por los equipos de red fabricados por Cisco. Otras marcas tienen su propia denominación. Por ejemplo, al sistema operativo del commutador Ethernet modelo 6850-24 de Alcatel Lucent se le denomina AOS.

IP: Es uno de los protocolos más importantes de la arquitectura TCP/IP, se ubica en la capa tres de la arquitectura, funciona con la filosofía del mejor esfuerzo y utiliza como unidad básica de información al datagrama IP compuesto por un encabezado y un campo de datos. En IP versión 4, el encabezado tiene varios campos que entre otras cosas contienen información correspondiente a la dirección IP del emisor, la dirección IP del destino y el tipo de protocolo que transporta el campo de datos.

Prompt: Símbolo usado por el sistema operativo del equipo de red que se ubica en una posición de la pantalla para indicar en donde se debe digitar un

comando para su ejecución. En el caso de los equipos de red marca Cisco, el indicador del sistema depende del modo en que se encuentre el usuario: modo de ejecución de usuario “>”, modo de ejecución privilegiado “#” y modo de configuración global “Router(config)#”.

RIP: Acrónimo de Routing Information Protocol. Hace referencia a un protocolo que utilizan los equipos de capa 3 (conmutadores Ethernet y en-caminadores que interconectan redes IP) para intercambiar información con las direcciones IP de las redes que estos conocen (tablas de enrutamiento). Lo anterior con el propósito de que todos los equipos capa 3 conozcan cómo llegar a dichas redes.

RJ45: Es un toma que especifica los conectores físicos que se pueden utilizar –machos o hembras– y la asignación de ocho pines.

UTP: Acrónimo de Unshielded twisted pair –Par trenzado sin blindar. Es un tipo de cableado en el que dos conductores del mismo circuito están trenzados con el propósito de anular la interferencia electromagnética de fuentes externas.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- LEINWAND, A.; PINSKY, B. (2001). *Cisco Router Configuration*. 2nd Ed. Indianapolis, IN: Cisco Press.
- MCQUERRY, S.; JANSEN, D.; HUCABY, D. (2009). *Cisco LAN Switching Configuration Handbook*. 2nd Ed. Indianapolis, IN: Cisco Press.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

CAPÍTULO 2

CONFIGURACIÓN BÁSICA DE UN ENCAMINADOR Y FUNCIONES DE SUS COMPONENTES

En el proceso de configuración de un encaminador (informalmente denominado *enrutador*), intervienen diferentes componentes internos: memorias e interfaces de red; y externos: puertos serie y programas cliente, con los cuales es necesario familiarizarse para facilitar la administración de dichos equipos. Entender la secuencia de arranque de un encaminador, establecer la configuración básica del mismo y acceder a él remotamente, involucra conceptos básicos que un administrador de red debe dominar, con el propósito de manejar escenarios que involucren la implementación y aprovisionamiento de redes IP con configuraciones más complejas.

OBJETIVO

Respecto a un encaminador, al finalizar este módulo, el estudiante estará en capacidad de:

- Describir los elementos de configuración.
- Describir los modos de operación.
- Describir la secuencia de arranque.
- Usar el comando *setup* para generar la configuración inicial.
- Usar los comandos que permiten examinar el estado de los elementos que lo componen.
- Acceder al equipo (encaminador) de manera remota y probar su operación.

PROCEDIMIENTO

Componentes externos de configuración

El encaminador puede configurarse usando cualquiera de los siguientes componentes:

Puerto de consola

se usa especialmente cuando el encaminador está nuevo; por consiguiente, requiere de una configuración básica para su funcionamiento inicial. Permite la conexión física y directa de una terminal.

Servicio de terminal virtual –Virtual Teletype Terminal (VTY)– del encaminador

Puede recibir simultáneamente varias sesiones iniciadas a través de un programa cliente de telnet (que es inseguro) o a través de un programa cliente de *Secure Shell* (SSH), dichas sesiones se utilizan para acceder remotamente al encaminador.

Servicio de protocolo trivial de transferencia de archivos

–Trivial File Transfer Protocol (TFTP)– del encaminador

Permite que se establezca una sesión remota para respaldar y restaurar la configuración del encaminador en un servidor TFTP.

Servicio de protocolo de transferencia de hipertexto

–Hypertext Transfer Protocol (HTTP)– del encaminador

Permite el acceso remoto al encaminador por medio de un cliente Web.

Servicio de protocolo simple de administración de red –Simple Network Management Protocol (SNMP)– del encaminador

Permite la administración y configuración remota del encaminador.

Puerto auxiliar

Es un puerto físico –similar al puerto de consola– por medio del cual se puede acceder directamente al encaminador.

Componentes internos de configuración

El encaminador tiene los siguientes componentes internos de almacenamiento (memoria):

ROM

Contiene un programa que hace el diagnóstico inicial al encender el equipo; un programa de *Bootstrap*, el cual tiene la función de buscar y car-

gar la imagen del sistema operativo –Internetwork Operating System (IOS), Cisco Systems Inc.– y un miniprograma auxiliar que opera ante la ausencia del IOS.

RAM/DRAM

Memoria principal que contiene el programa de *Bootstrap*, tablas de *enrutamiento*, tablas del protocolo de resolución de direcciones –*Address Resolution Protocol (ARP)*–, tablas de conmutación rápida –*Fast Switching*– y colas (buffers) para almacenar temporalmente paquetes de datos. También proporciona memoria temporal para almacenar el archivo de la configuración activa, siempre y cuando el encaminador permanezca encendido. Normalmente el IOS se carga desde uno de varios posibles recursos de almacenamiento permanente y se ejecuta en la memoria *RAM*, dicha imagen se encuentra en forma binaria –ejecutable– y resulta ininteligible cuando se edita con un procesador de texto. El sistema operativo se organiza en rutinas que manejan procesos asociados con el reenvío de paquetes de datos, las actualizaciones de enrutamiento, los diferentes protocolos en operación, la ejecución de comandos de usuario y la administración de tablas y colas del equipo.

NVRAM (RAM no volátil)

El archivo de configuración contiene las líneas de comando con información en formato de texto –*American Standard Code for Information Interchange* (ASCII)– que puede hacerse visible mediante la consola o mediante una sesión de terminal remota. Este archivo es almacenado permanentemente en *NVRAM* y es retenido aunque se apague el encaminador. Cada vez que se inicializa el encaminador, la versión salvada de la configuración es cargada hacia la memoria principal. El archivo de configuración contiene comandos globales, de procesos y de interfaces que afectan directamente la operación del encaminador.

FLASH EEPROM (Memoria borrable y reprogramable)

Almacena la(s) imagen(es) del sistema operativo IOS y conserva su contenido aunque el encaminador sea apagado, permite la actualización del software sin necesidad de remover hardware. En algunos modelos de equipos también asume el papel de *ROM* y *NVRAM*.

Interfaces

Son conexiones a diferentes tipos de redes por medio de las cuales los paquetes de datos entran y salen del encaminador.

Modos de operación

Un encaminador tiene los siguientes modos de operación:

Modo de configuración inicial (Setup Mode)

El equipo propone un diálogo asistido mediante preguntas para realizar una configuración inicial del encaminador.

Modo de ejecución de usuario (User Exec Mode)

Permite tener acceso limitado a la operación y configuración del encaminador. Se entra a este modo directamente desde la consola o haciendo telnet al encaminador, para el último caso, hay que digitar la clave (*password*) de terminal virtual, entonces aparecerá el indicador del sistema (*prompt*) siguiente.

Router>

Modo de ejecución privilegiado (Privileged Exec Mode)

Permite la manipulación detallada (operación, configuración, depuración y prueba) del encaminador. Se entra a este modo digitando el comando *enable* desde el indicador del sistema anterior.

Router#

Modo de configuración global (Global configuration mode)

Permite ejecutar los comandos de configuraciones simples. Se entra a este modo al digitar el comando *configure terminal* desde el indicador del sistema anterior.

Router(config)#

Otros modos de configuración

Permite la ejecución de comandos relativos a configuraciones complejas y de múltiples líneas.

Por ejemplo, se entraría a uno de estos modos al digitar el comando *interface serial 0/0* desde el indicador del sistema anterior para configurar la interfaz serial 0/0, como se muestra a continuación.

```
Router(config)# interface serial 0/0  
Router(config-if)#
```

Modo de inicio (*RXBOOT Mode*)

Permite recuperarse de situaciones adversas, como la pérdida de la clave o el borrado accidental del sistema operativo que reside en la memoria flash.

Secuencia de arranque del encaminador

Los siguientes eventos se presentan cuando se enciende un encaminador:

Desde la memoria *ROM* se ejecuta un programa que hace un diagnóstico de verificación sobre todos los módulos del equipo –*Power On Self Test (POST)*–, dicho programa verifica la operación básica del procesador, la memoria y los circuitos de interfaz.

Desde la memoria *ROM* se ejecuta el programa cargador genérico (de *Bootstrap*), su propósito es cargar la imagen del sistema operativo hacia la memoria principal (*RAM*).

La manera en que se carga el sistema operativo en la mayoría de equipos la determina el campo *boot* del registro de configuración (denominado *config-register*), los posibles valores hexadecimales del campo *boot* son: cero, para que la carga del IOS se haga manualmente; uno, para que la carga del IOS sea automática, y finalmente el rango dos hasta F para que el IOS se cargue de acuerdo con los parámetros que se definan mediante los comandos de línea *boot system*. Si el campo *boot* del registro de configuración indica una carga mediante los comandos *boot system* guardados en el archivo de configuración en la memoria *NVRAM*, dichos comandos deberán indicar la localización exacta de la imagen en la memoria flash o en el servidor TFTP de la red.

El sistema operativo se carga en la parte baja de la memoria principal; una vez listo y operacional, determina e informa los componentes hardware y software del sistema.

La versión salvada del archivo de configuración es cargada en la memoria principal y ejecutada línea por línea. Dichos comandos inician procesos de enrutamiento, proporcionan direcciones a las interfaces, configuran características de los medios, etc. Si no existe un archivo válido de configuración en la memoria *NVRAM*, el sistema operativo ejecuta una rutina de configuración inicial asistida mediante un diálogo, ésta se denomina diálogo de configuración inicial. Este modo especial también se llama *diálogo de setup*.

El diálogo de configuración inicial preguntará por la información relativa a la configuración deseada por el usuario. En uno de los pasos, el diálogo presentará el resumen de la configuración que el encaminador tenga en ese momento para cada interfaz (si existe alguna configuración para éstas). Una vez el usuario responda a cada una de las preguntas del diálogo de configuración inicial, el resultado es enviado a la pantalla de la terminal de consola

mediante un listado de líneas de comando (*script*). El usuario puede aceptar o rechazar la configuración después de revisar la información presentada. Si la configuración es aceptada por el usuario, el *script* será almacenado en la memoria *NVRAM* mediante un archivo con nombre *startup-config*, el cual será el archivo de configuración a ser cargado por defecto en la próxima inicialización del encaminador. Una vez salvada la configuración, ésta puede ser modificada manualmente en modo privilegiado.

Modo de diálogo de configuración inicial

El diálogo de configuración inicial permite la configuración del nombre del encaminador (*hostname*), las claves (*password*) y al menos de una dirección IP que permita posteriormente el acceso al encaminador. Cuando un encaminador se encuentra nuevo o con la memoria *NVRAM* vacía –en muchos casos la única manera de acceder al encaminador es a través del puerto de consola, dependiendo del modelo–, entra automáticamente al modo de configuración inicial. En dicho modo, el encaminador pregunta los parámetros mínimos para su funcionamiento y propone algunos valores por defecto. En algunas preguntas, las respuestas por defecto aparecerán entre corchetes cuadrados ([]); para aceptarlas, basta con presionar la tecla de retorno (*Enter*).

Otra forma de invocar el modo de configuración inicial es mediante el comando *setup* desde el modo de ejecución privilegiado. Por ejemplo, para tener la configuración mínima de un encaminador se realiza lo siguiente:

1. Se definen los parámetros mínimos a configurar:

Hostname: R1

Enable secret password: univalle

Enable password: eiee

Virtual terminal password: red

Dirección IP de una interfaz Ethernet: 192.168.55.100

Máscara de la red: 255.255.255.0 equivalente a decir que el campo *subnet field* es Cero

2. Se ejecuta el comando *setup* para configurar los parámetros anteriores.

```
Router# setup
```

A continuación se presentan los diálogos propuestos por los encaminadores marca Cisco (Cisco Systems, Inc.), modelos 2503 y 1751 respectivamente,

después de haber ejecutado en estos el comando *setup* (o cuando el equipo está nuevo). Al finalizar el diálogo, los cambios se pueden salvar a *NVRAM* si para el caso de un equipo Cisco 2503 se acepta la propuesta “Use this configuration? [yes/no]:”, o para el caso de un equipo Cisco 1751 se escoge la segunda opción “[2] Save this configuration to nvram and exit”.

Para el encaminador Cisco 2503 se tiene el siguiente diálogo:
--- System Configuration Dialog --- “Encaminador Cisco 2503”

At any point you may enter a question mark ‘?’ for help. Refer to the ‘Getting Started’ Guide for additional help. Use [CNTL] C to abort configuration dialog at any prompt. Default settings are in square brackets ‘[]’.

Continue with configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

Interface	IP-Address	OK?	Method	Status	Protocol
BRI0	192.168.3.1	YES	not set	up	up
Dialer0	192.168.3.1	YES	not set	up	up
Ethernet0	192.168.200.2	YES	NVRAM	up	up
Serial0	192.168.2.1	YES	NVRAM	down	down
Serial1	192.168.3.1	YES	NVRAM	down	down

Configuring global parameters:

Enter host name [Cisco_2500_1]: **R1**

Enter enable secret password [seguro]:**univalle**

Enter enable password [respaldo]:**eiee**

Enter virtual terminal password [telnet]:**red**

Configure SNMP Network Management? [no]:

Configure DECnet? [no]:

Configure IP? [yes]:

Configure IGRP routing? [yes]:

Your IGRP autonomous system number [1]:100

Configure IPX? [no]:

Configure XNS? [no]:

Configure AppleTalk? [no]:

Configure Apollo? [no]:

Configure CLNS? [no]:

Configure Vines? [no]:

Configure bridging? [no]:

Configure LAT? [no]:

Enter ISDN BRI Switch Type [basic-net3]:

Configuring interface parameters:

Configuring interface BRI0:

Is this interface in use? [yes]:

Configure IP on this interface? [yes]:

Configure IP unnumbered on this interface? [yes]:

Assign to which interface [Serial1]:

Configuring interface Ethernet0:

Is this interface in use? [yes]:

Configure IP on this interface? [yes]:

IP address for this interface [192.168.200.2]:**192.168.55.100**

Number of bits in subnet field [0]:**0**

Class C network is 192.168.55.0, 0 subnet bits; mask is 255.255.255.0

Configuring interface Serial0:

Is this interface in use? [yes]:

Configure IP on this interface? [yes]:

Configure IP unnumbered on this interface? [no]:

IP address for this interface [192.168.2.1]:

Number of bits in subnet field [0]:

Class C network is 192.168.2.0, 0 subnet bits; mask is 255.255.255.0

Configuring interface Serial1:

Is this interface in use? [yes]:

Configure IP on this interface? [yes]:

Configure IP unnumbered on this interface? [no]:

IP address for this interface [192.168.3.1]:

Number of bits in subnet field [0]:

Class C network is 192.168.3.0, 0 subnet bits; mask is 255.255.255.0

The following configuration command script was created:

```
hostname R1
enable secret 5 $1$p2Lc$PPOfRxI4.siG3bIwZendU0
enable password eiee
line vty 0 4
password red
no snmp-server
!
no decnet routing
ip routing
no ipx routing
no xns routing
no appletalk routing
no apollo routing
no clns routing
no vines routing
no bridge 1
isdn switch-type basic-net3
!
interface BRI0
no ip address
ip unnumbered Serial1
no mop enabled
!
interface Ethernet0
ip address 192.168.55.100 255.255.255.0
no mop enabled
!
interface Serial0
ip address 192.168.2.1 255.255.255.0
no mop enabled
!
interface Serial1
ip address 192.168.3.1 255.255.255.0
no mop enabled
!
router igrp 100
network 192.168.55.0
network 192.168.2.0
network 192.168.3.0
!
end
Use this configuration? [yes/no]: yes
```

Para el encaminador Cisco 1751 se tiene el siguiente diálogo:
--- System Configuration Dialog --- “Encaminador Cisco 1751”

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark ‘?’ for help. Use [CNTL] C to abort configuration dialog at any prompt. Default settings are in square brackets ‘[]’.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes

Configuring global parameters:

Enter host name [Cisco_2500_1]:**R1**

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret [<Use current secret>]:**univalle**

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **eiee**

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password [telnet]:**red**

Configure SNMP Network Management? [no]:

Current interface summary

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.55.100	YES	NVRAM	up	up
Serial0/0	10.3.2.1	YES	NVRAM	down	down
Serial0/0.1	10.3.2.1	YES	NVRAM	down	down
Serial0/1	unassigned	YES	NVRAM	administratively down	down

Enter interface name used to connect to the management network from the above interface summary: **FastEthernet0/0**

Configuring interface FastEthernet0/0:

Use the 100 Base-TX (RJ-45) connector? [yes]:

Operate in full-duplex mode? [no]:

Configure IP on this interface? [yes]:

IP address for this interface [192.168.200.2]: **192.168.55.100**

Subnet mask for this interface [255.255.255.0] :

Class C network is 192.168.55.0, 24 subnet bits; mask is /24

The following configuration command script was created:

```
hostname R1
enable secret 5 $1$p2Lc$PPOfRxI4.siG3bIwZendU0
enable password eiee
line vty 0 15
password red
no snmp-server
!
no ip routing

!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
half-duplex
ip address 192.168.55.100 255.255.255.0
!
interface Serial0/0
shutdown
no ip address
!
interface Serial0/1
shutdown
no ip address
!
end
```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

Enter your selection [2]: 2

Comandos para examinar el estado y los elementos de un encaminador

Verificar la versión

El comando *show version* muestra la versión del IOS, el nombre del archivo imagen, la fuente desde donde la imagen ha sido cargada, los recursos hardware que se tienen en el equipo y el valor que tiene el registro de configuración.

R1# *show version*

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(2)XK, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 26-Oct-01 13:15 by ealyon
Image text-base: 0x80008124, data-base: 0x80D34BD8

ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
ROM: C1700 Software(C1700-SV3Y-M), Version 12.2(2)XK, EARLY DEPLOYMENT
RELEASE
SOFTWARE (fc1)

R1 uptime is 2 hours, 9 minutes
System returned to ROM by power-on
System image file is “flash:c1700-sv3y-mz.122-2.xk.bin”

cisco 1751 (MPC860P) processor (revision 0x200) with 55706K/9830K bytes of
memory.
Processor board ID JAD05510EL9 (2036500650), with hardware revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Verificar los procesos activos

El comando *show processes* permite verificar los procesos activos del encaminador.

R1# *show processes*

CPU utilization for five seconds: 2%/0%; one minute: 0%; five minutes: 0%									
PID	Q	T	PC	Runtime (ms)	Invoked	uSecs	Stacks	TTY	Process
1	L	E	30343B8	104612	1187	88131	918/1000	0	Check heaps
2	M	E	30554F2	0	2	0	966/1000	0	Timers
3	L	E	3078DF6	6472	14430	448	728/1000	0	ARP Input
4	L	E	309E764	0	1	0	926/1000	0	Probe Input
5	M	E	309E302	0	1	0	964/1000	0	RARP Input
6	H	E	30913E0	25160	33486	751	1548/2000	0	IP Input
7	M	E	30B473C	0	14414	0	744/1000	0	TCP Timer
8	L	E	30B607C	20	6	333	690/1000	0	TCP Prot
9	M	E	309B734	2020	8245	244	818/1000	0	BOOTP Ser
10	M	*	0	396	41	9658	1456/2000	2	Virtual Exec
11	L	T	317CE16	0	1189	0	958/1000	0	IP Cache
12	M	E	302BC32	72	2459	29	688/1000	0	Net Backgro
13	L	E	3050B64	4	6	666	880/1000	0	Logger
15	M	T	3034F30	28384	71331	397	736/1000	0	TTY Backgr
16	H	E	302BE9E	5628	28607	196	374/500	0	Net Input
17	M	T	302BB68	28520	1189	23986	746/1000	0	Per-min Job
18	M	E	33C91F8	20	3	6666	942/1000	0	ISDN
19	M	E	30CA2AE	0	1	0	960/1000	0	PPP Manage
20	M	E	31445D2	7628	2567	2971	1294/1500	0	IGRP Route

PID = Process ID
 Q = Process queue priority; posibles valores son: H (High), M (Medium) y L (Low)
 T = Scheduler Test; posibles valores son: E (Event), T (Time) y S (Suspended)
 PC = Current program counter
 Runtime(ms) = Tiempo que el proceso ha utilizado la CPU
 Invoked = Número de veces que el proceso ha sido invocado
 uSecs = Tiempo de CPU en microsegundos para cada llamada
 Stacks = Low water mark/Espacio total disponible
 TTY = Terminal que controla el proceso
 Process = Nombre del proceso.

Activar y verificar los protocolos

El comando *ip routing* activa el enrutamiento del protocolo IP (el encañamiento de los datagramas IP) y el comando *show protocols* muestra los estados globales y específicos de cualquier protocolo de capa 3 que haya sido configurado; por ejemplo, IP.

```
R1(Config)# ip routing  
R1# show protocols
```

Global values:

Internet Protocol routing is enabled
Ethernet0 is up, line protocol is up
Internet address is 192.168.55.100, subnet mask is 255.255.255.0
Serial0 is down, line protocol is down
Internet address is 192.168.2.1, subnet mask is 255.255.255.0
Serial1 is down, line protocol is down
Internet address is 192.168.3.1, subnet mask is 255.255.255.0

Verificar información de la memoria Flash

El comando *show flash* muestra el tamaño de la memoria flash y el nombre y tamaño del(los) archivo(s) residente(s) en la memoria flash.

```
R1# show flash: all
```

Partition	Size	Used	Free	Bank-Size	State	Copy Mode
1	32768K	7712K	25055K	16384K	Read/Write	Direct

System flash directory:

File	Length	Name/status
	addr	fcksum ccksum
1	7897312	c1700-sv3y-mz.122-2.xk.bin
	0x40	0xE4FF 0xE4FF

[7897376 bytes used, 25657056 available, 33554432 total]

32768K bytes of processor board System flash (Read/Write)

Chip	Bank	Code	Size	Name
1	1	8918	16384KB	INTEL 28F128J3
1	2	8918	16384KB	INTEL 28F128J3

Verificar las interfaces

El comando *show interface nombre_de_la_interfaz* muestra los parámetros configurables y estadísticas relativas a la interfaz.

```
R1# show interface serial 0/0
```

```
Serial0 is down, line protocol is down
Hardware is HD64570
Internet address is 192.168.2.1, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 2473 interface resets, 0 restarts
 0 carrier transitions
DCD=up DSR=up DTR=down RTS=down CTS=up
```

Otros comandos Show

Show memory

Muestra estadísticas de la memoria del encaminador.

Show stacks

Muestra los niveles de uso de la *pila (stack)* por parte los procesos y rutinas de interrupción.

Show buffers

Proporciona las estadísticas de los *buffers*.

Show configuration

Muestra el archivo de configuración residente en *NVRAM*, es equivalente al comando *show startup-config*.

Write terminal

Muestra el archivo de configuración activa residente en *RAM*, es equivalente al comando *show running-config*.

Comandos comunes para la configuración del encaminador

Pasarse al modo configuración.

```
R1# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#
```

Configurar el nombre del equipo para que en adelante se llame Router.

```
R1(config)# hostname Router
```

```
Router(config)#
```

Configurando el *enable secret password* para que sea “univalle1”, y la clave del rango de las VTY 0 hasta 15 para que sea “red1”.

```
Router(config)# enable secret 0 univalle1
```

```
Router(config)# line vty 0 15
```

```
Router(config-line)# password red1
```

Configurando el mensaje de bienvenida (*Banner*) con la frase “Bienvenido al Router del Laboratorio”.

```
Router(config)# banner motd +
```

```
Bienvenido al Router del Laboratorio
```

```
Universidad del Valle
```

```
+
```

Salir del encaminador y verificar que aparezca el mensaje de bienvenida.

Configurar el parámetro que maneja la señal de reloj (*clock rate*) del puerto serial 0/0 (útil para el funcionamiento sincrónico del puerto) en 64.000 ciclos por segundo, lo cual permitirá conectar dicho puerto directamente por medio de un cable cruzado (*null cable*) al puerto serie de otro encaminador (sin necesidad de usar dos módems).

```
Router(config)# interface serial 0/0
```

```
Router(config-if)# clock rate 64000
```

Desactivar y activar la interfaz serial 0/0.

```
Router(config)# interface serial 0/0
Router(config-if)# shutdown
Router(config)# interface serial 0/0
Router(config-if)# no shutdown
```

Configurar una dirección IP a la interfaz serial 0/0.

```
Router(config)# interface serial 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

Comandos para verificar y guardar la configuración del encaminador

Con cualquiera de los siguientes dos comandos (equivalentes) se verifican los cambios hechos a la configuración del encaminador (residente en RAM) sin haber sido aún salvados en la memoria NVRAM.

```
Router# write terminal (o Router# show running-config)
Current configuration : 979 bytes
!
version 12.2
```

Con cualquiera de los siguientes dos comandos (equivalentes) se guardan los cambios hechos en la configuración que reside en la memoria *RAM* del encaminador hacia la memoria *NVRAM* para hacer que dichos cambios queden permanentes.

```
Router# write memory (o Router# copy running-config startup-config)
Building configuration...
[OK]
Router#
```

Borrado completo del archivo de configuración permanente del encaminador (archivo residente en la memoria *NVRAM*).

```
Router# write erase
Erasing the nvram filesystem will remove all files! Continue? [confirm]: n
```

Para reiniciar el encaminador se usa el comando *reload*.

```
Router# reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]: y
```

Comandos para probar conectividad

Comando *ping*: conformado por mensajes de solicitud y respuesta de eco, es útil en varios protocolos (IP, Novel IPX, DECnet y XNS) que requieren la realización de pruebas básicas de conectividad, dicho comando puede ser usado de manera interactiva. En el resultado final, los cinco signos de admiración (!!!!!) indican que el equipo remoto respondió a cada uno de los cinco mensajes enviados; no obstante, los cinco signos del punto (.....) indican que el equipo remoto no respondió a ninguno de los cinco mensajes enviados.

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.55.100
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.55.100, timeout is 2 seconds:
!!!!!
```

Comando *telnet*: en el encaminador se puede conseguir la traducción automática de nombres a direcciones IP mediante la configuración de una tabla estática con el comando *ip host* o configurando la dirección IP del servidor de dominio de nombres –si se tiene dicho servicio. Para establecer una sesión telnet, se puede usar cualquiera de los cuatro comandos presentados a continuación que preceden al comando *exit*; para finalizar dicha sesión, se usa el comando *exit* o el comando *logout*.

```
Router(config)# ip host cali 192.168.55.100

Router# telnet cali
Router# connect cali
Router# cali
Router# 192.168.55.200
Router# exit
```

Comando *trace*: permite descubrir la ruta que seguirán los paquetes que viajan hacia un destino, para ello se ejecuta un programa que utiliza el campo “Tiempo de vida” –*Time to Live (TTL)*– del datagrama IP y que hace uso del mensaje de error que reportan los encaminadores cuando les llega un datagrama que ha excedido el tiempo de vida (el TTL ha llegado a cero). Inicialmente el programa envía tres datagramas IP de prueba con el TTL puesto en un valor de uno. Esto da origen a que el primer encaminador descarte el datagrama de prueba y envíe de regreso un mensaje de error, posteriormente el programa incrementa el TTL en una unidad para que el segundo encaminador reporte el error. Finalmente el programa continúa incrementando el TTL y enviando datagramas de prueba hasta alcanzar el destino.

```
Router# trace 192.168.57.10
```

```
Type escape sequence to abort.  
Tracing the route to 192.168.56.1
```

```
1 Router2 (192.168..55.1) 1000 msec 8 msec 4 msec  
2 Router3 (192.168..56.2) 1000 msec 8 msec 4 msec  
3 Host1 (192.168..57.10) 1000 msec 8 msec 4 msec
```

Comando *show ip route*: muestra las tablas de *enrutamiento* que tiene el encaminador, es decir, las redes que conoce dicho equipo.

```
Router # show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
C 192.168.55.0 is directly connected, Ethernet0  
C 192.168.200.0 is directly connected, Ethernet0
```

Comando *show interface*: permite ver cada una de las interfaces del enrutador (ver el comando relacionado *clear counters*).

```
Router# show interfaces
Serial0 is down, line protocol is down
Hardware is HD64570
Internet address is 192.168.2.1, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 402 interface resets, 0 restarts
0 carrier transitions
DCD=up DSR=up DTR=down RTS=down CTS=up
```

Comando *debug*: el sistema operativo incluye este comando para ayudar a hacer seguimiento de los problemas con el enrutador o con otros equipos de la red; no se recomienda el uso de este comando, al menos que sea indispensable. La salida del comando *debug* es presentada en la consola, para redirigirla a una sesión de telnet se usa el comando *terminal monitor*.

```
Router# debug arp
ARP packet debugging is on
```

Mensajes de registro de eventos (logging) –salida de depuración y mensajes de error del sistema. Por defecto, el enrutador dispone la salida de los mensajes de error del sistema y la salida del comando *debug* hacia el puerto de consola. Los siguientes comandos dirigen dicha salida a otros destinos.

```
Router(config)# logging on (habilita logging a los destinos soportados)
Router# show logging
```

Router(config)# *logging buffered* (salida a buffer)

Router(config)# *no logging buffered*

Router(config)# *logging console* (salida a consola)

Router(config)# *logging 192.168.55.16*

(salida al host 192.168.55.16 que ejecuta un programa servidor de syslog)

Router# *terminal monitor* (habilita salida a la sesión actual de telnet)

Router# *terminal no monitor* (deshabilita la salida a la sesión actual de telnet)

El protocolo *Cisco Discovery Protocol* (CDP) permite que un equipo Cisco descubra otros equipos Cisco conectados a la red, dicho protocolo se habilita cuando se ejecuta el comando *cdp enable* sobre una interfaz.

Router(config-if)# *cdp enable*

Router# *show cdp* parámetro (monitorea el tráfico del protocolo CDP)

Cuando se ejecuta el comando *setup* se inicia el diálogo de configuración inicial. ¿Cuáles son los parámetros más importantes que se deben contestar en dicho diálogo?

¿Cuáles comandos se pueden utilizar para mostrar la configuración residente en la memoria *NVRAM* y en la memoria *DRAM*?

¿Qué función realiza el comando *clear counters* en un encaminador?

¿Cuál es el tamaño típico de la memoria *flash* y de la memoria *NVRAM* en un encaminador?

EJERCICIOS DE LABORATORIO

Este ejercicio de laboratorio tiene como finalidad proporcionar mayor familiaridad con los comandos CLI de los encaminadores Cisco.

1. Establecer una conexión de consola al encaminador y borrar su configuración (o en GNS3 ejecutar el comando *setup* y pasar al paso 3).
2. Reiniciar el encaminador R1.
3. Usar el diálogo de configuración inicial y asignar los siguientes parámetros:

Hostname: Router1
Enable secret password: “univalle2”
Enable password: “eiee2”
VTY password: “red2”
Conteste “n” a todos los protocolos
Conteste “n” a todas las interfaces excepto a “FastEthernet 0/0”
Salve la configuración

4. Entrar al modo de ejecución privilegiado.
5. Entrar al modo de configuración global y cambiar el nombre del enca- minador a “router2”.
6. Listar y revisar el archivo de configuración que está corriendo en *RAM*.
7. Listar y revisar el archivo de configuración salvado en *NVRAM*.
8. Salvar el archivo de configuración que reside en RAM hacia la memoria NVRAM.
9. Configurar un mensaje de bienvenida que contenga varias líneas de in- formación.
10. Asignar la clave de consola para que sea “red2”.
11. Asignar la clave de telnet para que sea “red2”.
12. Asignar la clave con el comando *enable secret password* para que sea “univalle2”.
13. Para evitar que los mensajes de error y registro del sistema (enviados al puerto de consola por el encaminador) se mezclen e interfieran con los comandos que introduce por teclado el usuario, se debe habilitar en el puerto de consola la función de sincronización de dichos mensajes mediante el comando *logging synchronous*.
14. Para la interfaz serial 0/0 realice lo siguiente.
Habilitarla, configurar la señal de reloj en 64.000 ciclos por segundo –comando *clock rate*–, configurar el ancho de banda a 64 Kbps –coman- do *bandwidth*.
15. Verifique la configuración de la *interfaz FastEthernet 0/0*.
16. Verifique la configuración de la *interfaz Serial 0/0*.
17. Examine la versión del software que está corriendo en el encaminador.
18. Salvar la configuración y salir del encaminador.

INFORMACIÓN COMPLEMENTARIA

A continuación, y a modo de resumen, la Tabla 2.1 presenta los diferentes modos de operación del encaminador Cisco y las respectivas funciones que se pueden realizar. La primera columna indica el modo de operación del equipo.

Para cada uno de los modos, la segunda columna especifica las funciones y permisos asociados; la tercera muestra el indicador del sistema, y las dos últimas presentan la manera de entrar y salir de cada uno de los modos.

Tabla 2.1 Modos de operación del encaminador Cisco y sus respectivas funciones

Modo de comando del IOS	Función del modo de comando	Indicador del modo	Cómo entrar a este modo	Cómo salir de este modo
Modo de usuario	<ul style="list-style-type: none"> Conjunto de comandos limitados, por ejemplo: traceroute, ping, telnet, etc. No permite cambio de parámetros del sistema. 	R1>	<ul style="list-style-type: none"> Conexión serial por el puerto de consola (puede requerir password). Telnet a una dirección IP del router (requiere un password de login) 	exit
Modo de ejecución privilegiado	<ul style="list-style-type: none"> Administra los archivos de configuración, examina el estado del enrutador. Control de acceso con password 	R1#	enable	disable
Modo de configuración global	<ul style="list-style-type: none"> Cambia parámetros generales del sistema 	R1(config)#	configure terminal	CRTL Z
Modo de configuración de interface	<ul style="list-style-type: none"> Modifica la configuración específica de una interfaz 	R1(config-if)#	interface tipo_de_interface, Ej: Interface serial 0/0	exit
Modo de configuración del enrutamiento	<ul style="list-style-type: none"> Modifica la configuración de un protocolo de enrutamiento específico 	R1(config-router)#	router router_protocol, ej: "router rip"	exit

Finalmente, cuando se ejecuta el comando *show interface FastEthernet 0/0*, la salida contiene los valores de algunos parámetros cuyo significado se amplía a continuación:

Ethernet x is up/down: Presenta el estado físico de la interfaz.

Line protocol is up/down: Presenta el estado a nivel de enlace de la interfaz. Pasa a estado *down* cuando se pierden tres mensajes *keepalive*.

Address: Muestra la dirección MAC de la interfaz. BIA significa “Burn in MAC address” del controlador Ethernet; el BIA puede ser sobrescrito con el comando *mac-address*.

Internet address: Muestra la dirección IP de la interfaz.

MTU (Maximum Transmission Unit): Muestra el máximo tamaño de octetos soportado por la trama en dicha interfaz. Ethernet por defecto tiene un valor de 1500 en su MTU.

BW: Métrica de velocidad usada por algunos protocolos de enrutamiento. Para las interfaces LAN su valor por defecto es la velocidad física de la interfaz; para las interfaces serie su valor por defecto es de 1544.

DLY: Retardo en microsegundos del enlace, es una métrica usada por algunos protocolos de enrutamiento. Para Ethernet, por defecto, es de 1000 microsegundos; para una interfaz serie, por defecto, es de 20 000 microsegundos.

Rely: Confiabilidad del enlace, es una métrica usada por algunos protocolos de enrutamiento. Es calculada en intervalos de 5 minutos y medida con valores en el rango de 1 hasta 255, un valor de 255 significa que es 100% confiable.

Load: Carga de la interfaz, es una métrica usada por algunos protocolos de enrutamiento; es calculada en intervalos de 5 minutos y medida con valores en el rango de 1 hasta 255, un valor de 255 indica que se está utilizado al 100%.

Encapsulation: Éste es el formato de la trama del nivel de enlace de datos para la interfaz; ARPA es muy utilizada para datagramas IP.

Five minute rates: Estos campos contienen la rapidez –en paquetes y en bits por segundo– para el tráfico saliente y entrante en la interfaz durante los últimos cinco minutos.

Runts (input): Número de tramas menores de 64 bytes.

Giants (input): Número de tramas mayores que 1518 bytes.

Ignored (input): Número de tramas que fueron recibidas e ignoradas porque la interfaz no tenía espacio interno en el buffer.

Output errors: Estos campos contienen el número total de diferentes tipos de errores de salida.

Collisions (output): Número de colisiones que ocurrieron mientras se intentaba transmitir una trama por la interfaz de salida; este valor debe corresponder a menos del 0,1% del tráfico total de la interfaz.

PROBLEMAS

1. Escriba un fragmento con líneas de comando que configure el máximo tiempo que una sesión por consola puede permanecer inactiva, de manera tal que, una vez transcurran 30 minutos de inactividad, la conexión sea cerrada por el encaminador.

2. Escriba un fragmento con líneas de comando que permita acceder al encaminador de manera segura a través de una sesión de VTY usando el protocolo SSH del programa Putty.
3. Configure un encaminador con el fragmento anexo y pruebe el funcionamiento de los comandos *show*, *show ip*, *show ip route* y *configure terminal* para los usuarios user1, user10 y user15. Compruebe el nivel de privilegio que tiene cada usuario con el comando *show privilege*. Note que al comando *show ip route* se le ha incrementado el nivel de privilegio.

```
Router(config)# username user1 privilege 1 password clave1
Router(config)# username user10 privilege 10 password clave10
Router(config)# username user15 privilege 15 password clave15
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local
Router(config)# privilege exec level 10 show ip route
Router(config)# privilege exec level 1 show ip
Router(config)# privilege exec level 1 show
```

Después de introducir las dos siguientes líneas de comando y entrar al encaminador con el usuario user1 (y clave1 como password), pruebe los comandos *enable 10* y *enable 15* para cambiar su nivel de privilegio usando las claves univalle10 y univalle15 respectivamente.

```
Router(config)# enable secret level 10 univalle10
Router(config)# enable secret level 15 univalle15
```

GLOSARIO

Archivo imagen: hace referencia al sistema operativo del encaminador, es un archivo binario que reside en la memoria flash y es cargado a la memoria RAM cuando se enciende el encaminador.

Cliente Web: hace referencia a un programa cliente cuyo uso permite navegar en la red y obtener información (texto, imágenes, audio, video) residente en uno o más servidores. Por ejemplo, el uso del programa Firefox de Mozilla.

Encaminador: equipo de red que es utilizado con el propósito de conseguir la interconexión de redes distantes y heterogéneas. Su función central consiste en recibir datagramas IP y reenviarlos hacia la red destino

con base en la dirección IP destino del datagrama recibido y en la información local que el encaminador posea acerca de cómo alcanzar las diferentes redes que conforman el sistema.

Enrutamiento: es el proceso mediante el cual un encaminador, después de recibir un datagrama IP, decide el camino o ruta que debe seguir dicho datagrama. Una vez tomada la decisión, el encaminador envía el datagrama al destino final (si es el último paso en el recorrido del datagrama) o lo reenvía hacia el próximo encaminador (si el destino final está en una red diferente a las redes a las que está directamente conectado el encaminador).

Puerto auxiliar: puerto serie de los encaminadores (similar al puerto de consola) al cual se le puede conectar un módem y una línea telefónica para acceder remotamente a la línea de comandos del encaminador; este puerto también permite el acceso remoto de un usuario a la red IP mediante una llamada conmutada, así como la configuración y uso del protocolo punto a punto –Point-To-Point Protocol (PPP).

Puerto de consola: interfaz serie de un equipo de red (encaminador, conmutador Ethernet) mediante la cual se accede de manera directa a la línea de comandos de dicho equipo, para esto se requiere la ejecución de un programa de emulación de terminal en un computador (programas como Putty, HyperTerminal, TeraTerm, CoolTerm, Screen) cuyo puerto serie (COM) esté conectado al puerto de consola del equipo de red.

Servidor TFTP: es un servicio o programa de aplicación que se puede ejecutar en un computador o en un equipo de red para permitir la transferencia de archivos sin requerir autenticación; el intercambio de información se hace mediante el protocolo TFTP (que reside en la capa de aplicación), el cual a su vez hace uso del Protocolo de Datagrama de Usuario –User Datagram Protocol (UDP)– que reside en la capa de transporte.

Terminal virtual: la mayoría de equipos de red pueden ejecutar un servicio denominado servidor de Telnet, este servicio permite tener acceso a la línea de comandos de dichos equipos mediante la ejecución de un programa cliente de Telnet desde un computador que se encuentre conectado en red con el equipo de red, la sesión así establecida se denomina “Terminal virtual”. Actualmente, Telnet ha sido reemplazado por el protocolo SSH, que es más seguro.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- LEINWAND, A.; PINSKY, B. (2001). *Cisco Router Configuration*. 2nd Ed. Indianapolis, IN: Cisco Press.
- MCQUERRY, S.; JANSEN, D.; HUCABY, D. (2009). *Cisco LAN Switching Configuration Handbook*. 2nd Ed. Indianapolis, IN: Cisco Press.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

CAPÍTULO 3

ADMINISTRACIÓN BÁSICA DE UN ENCAMINADOR CISCO

La mayoría de equipos de red, por lo general, almacenan el (los) archivo(s) del sistema operativo en memoria permanente y el (los) archivo(s) de configuración en memoria no volátil. Puesto que estos archivos están expuestos a dañarse en algún momento, dejando inútil al equipo sobre el cual residen y cuya operación depende de estos, se hace necesario contar con un respaldo de los mismos y tener la capacidad de restaurarlos; el presente capítulo apunta en dicho sentido, abordando el tema con equipos del fabricante Cisco. También se revisa el procedimiento que el administrador de la red debe realizar para recuperar las claves de acceso a un encaminador Cisco cuando éstas sean olvidadas o se tenga algún inconveniente con las mismas. Finalmente, se indica cómo controlar el acceso al encaminador y se insiste en identificar los diferentes modos a los que el administrador de la red puede acceder.

OBJETIVO

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

- Administrar los archivos de configuración desde el modo de ejecución privilegiado del encaminador.
- Moverse entre los diferentes modos de configuración y usarlos para modificar la configuración activa (en memoria RAM) de un encaminador.
- Controlar el acceso al encaminador.
- Configurar un encaminador para que cargue en la memoria RAM una copia del IOS –Internetwork Operating System– desde la memoria Flash, desde un servidor TFTP o desde la ROM.

- Actualizar la versión del IOS de un encaminador equipado con memoria Flash.
- Realizar la recuperación de las claves (password) del encaminador.

PROCEDIMIENTO

Manejo de los archivos de configuración

La información de configuración de un encaminador puede generarse mediante varios mecanismos. En el modo de ejecución privilegiado, el comando *configure* puede utilizarse para configurar el encaminador desde una terminal virtual remota (usando telnet o ssh) o desde la consola, permitiendo que en cualquier instante se introduzcan cambios a la configuración existente. El comando *configure* también permite cargar la configuración desde un servidor TFTP hacia el encaminador, facilitando de esta manera activar la configuración (previamente almacenada) desde un sitio central hacia el encaminador.

Resumen de comandos de configuración

A continuación se describen los comandos que se utilizan para manejar los archivos de configuración, es importante indicar que muchos comandos antiguos tienen un comando equivalente más reciente; los comandos más recientes tienen mayor flexibilidad, razón por la cual se recomienda trabajar especialmente con estos.

Write terminal: muestra en pantalla la configuración activa residente en la memoria RAM del encaminador; el comando equivalente es *show running-config*.

R1# write terminal

```
Building configuration...
Current configuration : 956 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R1
-Salida truncada-
```

Write memory: guarda de manera permanente la configuración actual residente en la memoria RAM hacia la memoria NVRAM; el comando equivalente es *copy running-config startup-config*.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Write network: guarda la configuración residente en la memoria RAM hacia un servidor de TFTP, es muy útil para respaldar la configuración del encaminador en un PC que se habilite como servidor de TFTP; el comando equivalente es *copy running-config tftp*.

```
R1# write network
Remote host []? 192.168.55.18
Name of configuration file to write [R1-config]?
Write file R1-config on host 192.168.55.18? [confirm]
#####
Writing R1-config !!!!!!!! [ok]
R1#
```

Show configuration: despliega la configuración salvada que está contenida en la NVRAM; el comando equivalente es *show startup-config*.

```
R1# show startup-config
```

```
interface FastEthernet0/0
ip address 192.168.55.100
speed auto
!
interface Serial0/0
ip address 10.3.2.1 255.25
encapsulation frame-relay
no ip mroute-cache
frame-relay lmi-type ansi
!
interface Serial0/0.1 point
ip address 10.3.2.1 255.25
frame-relay interface-dlci
!
-Salida truncada-
```

Write erase: permite borrar el contenido de la memoria NVRAM; así, esta memoria queda sin configuración del encaminador (después de reiniciar el encaminador, se activa la configuración por defecto de fábrica). El comando equivalente es *delete nvram:startup-config*.

```
R1# write erase
```

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]: n
```

Configure terminal: permite configurar manualmente el encaminador desde la consola o desde la terminal virtual. Permite cambiar directamente las líneas de configuración contenidas en el archivo de configuración residente en la memoria RAM del encaminador, archivo con el cual éste se encuentra operando. Los cambios se pierden al reiniciar el encaminador, si previamente dichos cambios no han sido salvados en la memoria NVRAM.

Configure memory: permite cargar nuevamente el archivo de configuración residente en la memoria NVRAM hacia la memoria RAM, dicho archivo –en caso de existir– ha sido previamente cargado durante el proceso de encendido del encaminador. El comando equivalente es *copy startup-config running-config*.

```
R1# configure memory
```

```
[OK]
```

```
R1#
```

Configure network: permite cargar el archivo de configuración residente en un servidor TFTP –conectado en red– hacia la memoria RAM. Previamente se debe activar el servicio TFTP en el computador que se designe como servidor TFTP y disponer del archivo de configuración en un directorio de dicho servidor. Los comandos equivalentes son *copy tftp running-config* y también *copy tftp://192.168.55.18/R1-cfg system:/running-config* –bajo el supuesto que la dirección IP del servidor TFTP es 192.168.55.18.

```
R1# configure network
```

```
Host or network configuration file [host]? host
```

```
Address of remote host [255.255.255.255]? 192.168.55.18
```

```
Name of configuration file [R1-cfg]?
```

```
Configure using R1-cfg from 192.168.55.18? [confirm]: y
```

```
Booting R1-cfg from 192.168.55.18:!!!! [OK - 879 / 32762 bytes]
```

Modos de operación

El intérprete de comandos tiene dos niveles de acceso: nivel de usuario y nivel privilegiado. Desde el modo privilegiado se puede acceder al modo de configuración global y desde el modo de configuración global, a los otros modos específicos de configuración. La Tabla 3.1 relaciona los modos de ejecución de usuario y privilegiado.

Tabla 3.1. Modo de usuario y privilegiado

Modo	Indicador del sistema	Comentario
Ejecución de usuario	R1> <i>enable</i>	Para pasarse al modo privilegiado.
Ejecución privilegiado	R1# <i>disable</i> R1# <i>configure terminal</i>	Para pasarse al modo usuario. Para pasarse al modo de configuración global.

Modo de configuración global

Los comandos de configuración global se aplican a características generales que afectan todo el sistema, por ejemplo, para habilitar la función de enrutamiento en particular, se usa el comando de configuración global *ip routing*. Para pasarse desde el modo de configuración global al modo de configuración específico de la interfaz serie 0/0, se ejecuta el comando *interface serial 0/0*.

R1(config)# *interface serial 0/0*

R1(config-if)# desde aquí se ejecutan los comandos específicos para el modo de configuración de la interfaz serial 0/0.

Otros modos de configuración son:

- interface
- subinterface
- controller
- map-list
- map-class
- line
- router
- route-map

Modo de enrutamiento del protocolo IP

Después del comando *router* se puede usar el signo de interrogación (?) para listar los comandos relativos al protocolo de enrutamiento a configurar. Una vez seleccionado el protocolo de enrutamiento mediante un comando global (por ejemplo, *router rip*), aparece como indicador del sistema la secuencia R1(config-router)#.

R1 (config)# *router ?*

bgp	Border Gateway Protocol (BGP)
egp	Exterior Gateway Protocol (EGP)
eigrp	Enhanced Interior Gateway Routing Protocol (EIGRP)
igrp	Interior Gateway Routing Protocol (IGRP)
isis	ISO IS-IS
iso-igrp	IGRP for OSI networks
mobile	Mobile routes
ospf	Open Shortest Path First (OSPF)
rip	Routing Information Protocol (RIP)
static	Static routes

R1 (config)# *router rip*

R1 (config-router)# ?

Router configuration commands:

default-metric	Set metric of redistributed routes
distance	Define an administrative distance
distribute-list	Filter networks in routing updates
exit	Exit from routing protocol configuration mode
help	Description of the interactive help system
neighbor	Specify a neighbor router
network	Enable routing on an IP network
no	Negate or set default values of a command
offset-list	Add or subtract offset from IGRP or RIP metrics
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol
timers	Adjust routing timers
validate-update-source	Perform sanity checks against source address of routing updates

Modo de configuración de una interfaz

Con los comandos de configuración de interfaz se modifica la operación de los puertos Ethernet y Serie. Con el comando *interface* se define el tipo de interfaz que se desea configurar; posteriormente se pueden ejecutar sub-comandos que afectan la operación de la interfaz.

```
R1 (config)# interface type port  
R1 (config)# interface type slot/port
```

El parámetro “type” puede tomar los siguientes valores: Serial, Ethernet, FastEthernet, Loopback, Dialer, Null, Async, Atm, Bri, Tunnel. Por ejemplo, para configurar características de la interfaz serie 0/0 se tiene:

```
R1(config)# interface serial 0/0  
R1 (config-if)# no shutdown  
R1 (config-if)# bandwidth 64  
R1 (config-if)# clock rate 64000
```

El último comando (*clock rate 64000*) es útil para que, al operar en modo sincrónico sin la existencia de módems, la interfaz serie 0/0 del encaminador R1 le proporcione señal de reloj, a 64000 ciclos por segundo, a otro encaminador al cual se conecta mediante un cable cruzado –en dicha conexión física, el comando se debe ejecutar sobre el encaminador que tenga conectado el cable que se comporta como DCE.

En algunos equipos se selecciona si la interfaz FastEthernet usa el tipo de conector RJ45 (10BaseT) o AUI (Attachment Unit Interface) con transceiver externo.

```
R1 (config)# interface Fastethernet 0/0  
R1 (config-if)# media-type 10baset
```

Metodología de configuración

A continuación se describe la metodología o secuencia de pasos que se debe seguir cuando se está configurando un encaminador; esto con la finalidad de minimizar el impacto por errores que se puedan llegar a cometer al realizar los cambios.

1. Inicio.

2. Haga los cambios necesarios en el modo de configuración: R1(config)#

3. Examine los cambios con el comando *write terminal*: R1# *write terminal*

4. Si los cambios producen los resultados deseados:

{

 Salve los cambios con el comando *write memory*: R1# *write memory*

 Examine el archivo de configuración salvado, esto se hace con el comando
show startup-config: R1# *show startup-config*

 Opcionalmente, respalde los cambios en un servidor TFTP con el comando
copy startup-config tftp: R1# *copy startup-config tftp*

}

5. De otra manera.

{

 Remueva los cambios por cualquiera de los siguientes métodos:

 a. Niegue la configuración anteponiendo “no” al comando que requiera borrar:

 R1(config)# *no comando-a-borrar*

 b. Cargue la configuración desde el archivo en la memoria NVRAM hacia la memoria RAM: R1# *configure memory*

 c. Cargue la configuración desde el archivo previamente salvado en la red hacia la memoria RAM: R1# *copy tftp running-config*

 d. De ser necesario, reinicie el encaminador o borre completamente el archivo de configuración de la memoria NVRAM del mismo: R1# *delete nvram:startup-config*

 Regresar al punto 1.

}

6. Finalizar.

Control de acceso a la configuración del encaminador

Configuración de claves secretas

El acceso al encaminador puede restringirse por medio de claves secretas. Se pueden definir claves para la consola (line console 0), las sesiones de telnet (line vty 0 15) y para el modo de ejecución privilegiado (comandos *enable password* o *enable secret 0*).

Configuración de la clave secreta de consola:

```
R1 (config)# line console 0  
R1 (config-line)# login  
R1 (config-line)# password red2
```

Configuración de la clave secreta de terminal virtual:

```
R1 (config)# line vty 0 15  
R1 (config-line)# login  
R1 (config-line)# password red2
```

Configuración del password del modo privilegiado:

```
R1 (config)# enable password univalle2
```

Identificación del encaminador

Para configurar la identificación de un encaminador como, por ejemplo, Dirección_General, se puede utilizar el siguiente comando:

```
R1 (config)# hostname Cali-DG
```

Para la descripción de una interfaz del encaminador con el mensaje “Esta Interfaz se comunica con la sede Bogotá”, se puede utilizar el siguiente comando:

```
R1 (config)# interface serial 0/0  
R1 (config-if)# description Esta Interfaz se comunica con la sede Bogotá
```

Internetwork Operating System

Localización del IOS

El orden en que el encaminador busca la información de arranque del sistema depende de la configuración que tenga el campo “boot” del registro de configuración “config-register” (ver comando *show version*). El registro de configuración es un registro de 16 bits y sus cuatro bits menos significativos (bits 0, 1, 2 y 3) conforman el campo “boot”.

Para cambiar el campo “boot” y dejar los otros bits con los valores por defecto, hay que seguir los siguientes delineamientos:

1. Cuando se desee cargar el sistema operativo de manejo manual, usando el comando “b” (boot) bajo el prompt del programa monitor de la memoria ROM, es necesario configurar el registro de configuración en 0x2100. Este valor configurará los 4 bits del campo “boot” con el valor 0-0-0-0.
2. Cuando se desee que el sistema operativo se cargue automáticamente desde la memoria ROM, es necesario configurar el registro de configuración en 0x2101. Este valor configura los bits del campo “boot” con el valor 0-0-0-1.
3. Cuando se desee que el sistema operativo se cargue automáticamente, utilizando los comandos “boot system” configurados en la memoria NVRAM, es necesario configurar el registro de configuración en cualquier valor del rango 0x2102 hasta 0x210F. Este valor configura los bits del campo “boot” a un valor dentro del rango 0-0-1-0 hasta 1-1-1-1.

En resumen, los diferentes modos de carga del IOS son:

- 0x2100. Modo RXBOOT o rommon, permite hacer carga manual del IOS usando el comando “b” desde el indicador del sistema “rommon>”.
- 0x2101. La carga del IOS se ejecuta de forma automática desde la memoria ROM.
- 0x2102-0x210F. Para cargar el IOS, el sistema primero examina los comandos “boot system” guardados en la memoria NVRAM.

Por ejemplo, para este último caso, mediante los siguientes dos comandos *boot system*, se puede especificar que se ejecute la carga del IOS usando el archivo cuyo nombre es “c1700-sv3y-mz.122-2.xk.bin”, residente en la memoria flash o en un servidor TFTP con dirección IP 192.168.55.18.

```
R1# configure terminal  
R1(config)# boot system flash c1700-sv3y-mz.122-2.xk.bin  
R1(config)# boot system tftp c1700-sv3y-mz.122-2.xk.bin 192.168.55.18  
R1(config)# exit  
R1# write memory
```

En caso que los comandos “boot system” anteriores no hayan sido digitados y guardados en la memoria NVRAM, si el registro de configuración se encuentra entre 0x2102 y 0x210F, el encaminador –al ser reiniciado– buscará el IOS de la siguiente forma: al no encontrar los comandos *boot system* en NVRAM, obtiene el IOS por defecto desde la memoria flash.

Verificando y cambiando el registro de configuración

El registro de configuración se cambia mediante el comando *config-register*. La modificación del registro de configuración tomará efecto la próxima vez que se reinicie el encaminador, a pesar que no se haya ejecutado el comando *write memory*; esto se debe a que no es necesario salvar dicha modificación. Por ejemplo, para cambiar el registro de configuración al valor 0x2103, se ejecutan los siguientes comandos.

```
R1(config)# config-register 0x2103
R1(config)# exit
R1#
```

Para verificar el anterior cambio, se ejecuta el comando *show versión*, el cual mostrará en la última línea el nuevo valor para el registro de configuración.

```
R1# show version
```

```
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9_IVS-M), Version
12.4(15)T8, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 01-Dec-08 19:46 by prod_rel_team
ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-ADVENTERPRISEK9_IVS-M), Version 12.4(15)T8,
RELEASE SOFTWARE (fc3)
R1 uptime is 2 hours, 18 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_
COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"
Cisco 3725 (R7000) processor (revision 0.1) with 249856K/12288K bytes of memory.
R7000 CPU at 240MHz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
2 FastEthernet interfaces
2 Serial network interfaces.
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of NVRAM.
16384K bytes of ATA System CompactFlash (Read/Write)
Configuration register is 0x2102 (will be 0x2103 at next reload)
```

Opciones de carga del IOS (bootstrap) por software

En la memoria NVRAM se pueden configurar múltiples comandos *boot system* que constituyen métodos de respaldo para cargar el IOS del encaminador. Los métodos son:

Desde la memoria Flash

No vulnerable a fallas en la red; en la flash se pueden copiar nuevas imágenes del IOS sin necesidad de cambiar los circuitos integrados internos.

```
R1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)# boot system flash c1700-sv3y-mz.122-2.xk.bin
```

Desde la red

Método de respaldo en caso de falla de la memoria flash.

```
R1(config)# boot system tftp c1700-sv3y-mz.122-2.xk.bin 192.168.55.18
```

Desde la memoria Rom

Método final de respaldo; las imágenes del sistema almacenadas en ROM no son tan completas como las almacenadas en la memoria flash o en servidores TFTP.

```
R1(config)# boot system rom
```

Trabajando con la memoria flash (Respaldo y actualización del IOS)

Para salvaguardar (respaldar) el IOS desde la memoria flash del enca-minador hacia un servidor TFTP en red, y para recuperar el IOS desde un servidor TFTP en red hacia la memoria flash del encaminador, se utilizan los comandos *copy flash tftp* y *copy tftp flash*, respectivamente. Es de anotar que, previamente a la ejecución de estos comandos, se debe tener disponi-bilidad de un servidor TFTP en la red.

A continuación se muestran los procedimientos, suponiendo que la di-rección IP del servidor TFTP es 192.168.55.18.

Verificando la memoria flash y copiando archivos desde la flash hacia un servidor tftp:

```
R1# show flash: all
```

Partition	Size	Used	Free	Bank-Size	State	Copy Mode					
1	32768K	7712K	25055K	16384K	Read/Write	Direct					
File	Length	Name/status									
	addr	fcksum ccksum									
1	7897312	c1700-sv3y-mz.122-2.xk.bin									
	0x40	0xE4FF 0xE4FF									
[7897376 bytes used, 25657056 available, 33554432 total]											
32768K bytes of processor board System flash (Read/Write)											
Chip	Bank	Code	Size	Name							
1	1	8918	16384KB	INTEL 28F128J3							
1	2	8918	16384KB	INTEL 28F128J3							

R1# *copy flash tftp*

System flash directory:

File	Length	Name/status
1	7712	c1700-sv3y-mz.122-2.xk.bin

[7897376 bytes used, 25657056 available, 33554432 total]

Address or name of remote host [255.255.255.255]?192.168.55.18

Source file name? c1700-sv3y-mz.122-2.xk.bin

Destination file name [c1700-sv3y-mz.122-2.xk.bin]?

Verifying checksum for 'c1700-sv3y-mz.122-2.xk.bin' (file # 1)... OK

Copy 'c1700-sv3y-mz.122-2.xk.bin' from Flash to server

as 'c1700-sv3y-mz.122-2.xk.bin'? [yes/no]y

!!!!

Successful tftp write

Copiando archivos hacia la memoria flash desde un servidor tftp:

R1# *copy tftp flash*

Proceed? [confirm]y

Address or name of remote host [255.255.255.255]? 192.168.55.18

Source file name? c1700-sv3y-mz.122-2.xk.bin

Destination file name [c1700-sv3y-mz.122-2.xk.bin]?

Accessing file 'c1700-sv3y-mz.122-2.xk.bin' on 192.168.55.18...

Erase flash before writing?[confirm y/n]

Clearing and initializing flash memory (please wait) #####....#

Loading from 192.168.55.18!!!!!!!!!!!!!!

Verifying checksum ...

vvvvvvvvvvvvvvvvvvvvvvvv

Recuperación de las claves secretas

Es posible que por alguna circunstancia se pierdan o se olviden las claves que permiten el acceso al encaminador. Para la recuperación de dichas claves, se debe seguir un procedimiento específico que dependerá de la versión del IOS que esté ejecutando el encaminador y, en algunas ocasiones, del modelo del mismo. A continuación se muestran las alternativas según diferentes circunstancias que se pueden presentar.

IOS versión 11.2 o posterior; por ejemplo, para el equipo Cisco 1751

1. Apagar y volver a encender el encaminador.
2. Dentro de los primeros segundos de encendido el encaminador, digitar la secuencia [CNTL][Break], la finalidad de dicha secuencia es la de abortar la carga normal del IOS y obtener el prompt “rommon>”; una vez se obtenga dicho prompt, se pueden utilizar los comandos del programa monitor de la memoria ROM. Digitando el signo de interrogación “?” se obtiene ayuda sobre los comandos que se pueden utilizar en el modo rommon.

rommon 1 > ?

alias	set and display aliases command
boot	boot up an external process
break	set/show/clear the breakpoint
confreg	configuration register utility
cont	continue executing a downloaded image
contex	display the context of a loaded image
cookie	display contents of cookie PROM in hex
dev	list the device table
dir	list files i
dis	display instruction stream
dnld	serial download a program module
frame	print out a selected stack frame
help	monitor builtin command help
history	monitor command history
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
set	display the monitor variables
stack	produce a stack trace
sync	write monitor environment to NVRAM

Continua

Viene

sysret	print out info from last system return
tftpdnld	tftp image download
unalias	unset an alias
unset	unset a monitor variable
xmodem	x/ymodem image download

3. Cambiar el registro de configuración con la utilidad *confreg* del programa rommon para que, al inicializar la próxima vez, el encaminador no tenga en cuenta la configuración residente en la memoria NVRAM, es decir, no tenga en cuenta las claves que se desconocen.

El diálogo de la utilidad *confreg* es un ciclo de preguntas al cual se puede entrar varias veces. Después de haber ejecutado el comando *confreg* se entra al primer ciclo de preguntas y se responden positivamente solo las siguientes:

```
do you wish to change the configuration? y/n [n]: y
enable "ignore system config info"? y/n [n]: y
```

Al final del primer ciclo de preguntas, la utilidad muestra un resumen de la configuración actual y propone entrar nuevamente al mismo ciclo de preguntas mediante la pregunta:

```
do you wish to change the configuration? y/n [n]: n
```

Por lo tanto, para salir del diálogo se responde negativamente a dicha pregunta. A continuación se muestra el diálogo que presenta la utilidad *confreg* y las respuestas que se deben digitar en cada opción presentada (la tecla Enter acepta la opción propuesta por defecto en el diálogo).

```
rommon 2 > confreg
Configuration Summary
(Virtual Configuration Register: 0x2103)
enabled are:
load rom after netboot fails
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco3-C1700
```

do you wish to change the configuration? y/n [n]: y
enable “diagnostic mode”? y/n [n]:
enable “use net in IP bcast address”? y/n [n]:
disable “load rom after netboot fails”? y/n [n]:
enable “use all zero broadcast”? y/n [n]:
enable “break/abort has effect”? y/n [n]:
enable “ignore system config info”? y/n [n]: y
change console baud rate? y/n [n]:
change the boot characteristics? y/n [n]:

Configuration Summary

(Virtual Configuration Register: 0x2143)

enabled are:

load rom after netboot fails
ignore system config info
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco3-C1700

do you wish to change the configuration? y/n [n]: n

You must reset or power cycle for new config to take effect
rommon 3 >

4. Al reiniciar el encaminador, éste no tendrá en cuenta el archivo de configuración residente en la memoria NVRAM debido a que el registro de configuración fue modificado en el paso anterior con dicho propósito. El encaminador ejecutará automáticamente el diálogo inicial de configuración (*setup*), proponiendo preguntas para obtener una configuración inicial básica. Dichas preguntas se responden negativamente con el fin de evadir la función de dicho diálogo y obtener el prompt “Router>”. En adelante, se digitán los siguientes comandos con el fin de cambiar dos claves antiguas y desconocidas (univalle2 y red2) por dos claves nuevas y conocidas (univalle y red).
5. Router> *enable !*para obtener el prompt “Router#”!
6. Router# *copy startup-config running-config !*para cargar NVRAM hacia RAM!
7. R1# *configure terminal !*para cambiar la RAM!
8. R1(config)# *enable secret 0 univalle*

9. R1(config)# *line vty 0 15*
R1 (config-line)# *password red*
10. R1# *copy running-config startup-config* !para salvar la RAM hacia la NVRAM!
11. Regresar el registro de configuración a su valor original (0x2103) ya sea por medio de la utilidad *confreg* del programa rommon o por configuración directa con el comando *config-register* del encaminador:

R1(config)# config-register 0x2103

IGS versión 9.1 a 10.2, útil para el equipo Cisco 2503, por ejemplo

1. Apagar y volver a encender el encaminador.
2. Presionar la secuencia [CNTL][Break] o [CNTL][Pausa] dentro de los primeros 60 segundos de encendido el encaminador. Aparecerá el prompt “>”; desde dicho prompt digitar los siguientes tres comandos.
3. > *e/s 20000002* [CR], para ver el valor original del registro de configuración (por ejemplo, 0x2102). Anotar el valor mostrado porque posteriormente va a necesitarse.
4. > *o/r* [CR] para que, al reiniciar el encaminador, éste no tenga en cuenta la configuración contenida en la memoria NVRAM, permitiendo obviar las claves.
5. > *i* [CR] para reiniciar el encaminador.
6. Al reiniciar el encaminador, contestar “no” a todas las preguntas que presente el dialogo inicial de configuración, aparecerá el prompt “Router>”; se deben digitar los siguientes comandos.
7. Router> *enable* [CR]. El encaminador no solicitará la clave de ejecución privilegiada y dejará entrar directamente. Presentará el prompt “Router(boot)#”.
8. Digitar el comando “*show configuration*” y anotar la clave que se tenía olvidada (se recupera la clave).
9. Entrar al modo de configuración global y restaurar el valor original del registro de configuración anotado en el paso 3; por ejemplo, si el valor anotado en dicho paso fue 0x2102, el comando a ejecutar debe ser: Router(boot-config)# *config-register 0x2102*
10. Reiniciar el encaminador apagándolo y encendiéndolo, o con el comando *reload* Router(boot)# *reload*

INFORME

Comente las razones por las cuales advierte que es importante la administración de los archivos de configuración y del sistema operativo de un encaminador.

Discuta sobre las ventajas y desventajas que se tienen cuando un encaminador facilita la recuperación de la clave. ¿Qué precauciones de seguridad se deben tener en dicho caso?

EJERCICIOS DE LABORATORIO

La finalidad de este ejercicio es proporcionar mayor familiaridad con la administración de los archivos de configuración y del IOS del encaminador R1 de la Figura 1.1. Nota: si va a utilizar GNS3, omitir los pasos del 1 al 3 y del 11 al 13.

1. Reiniciar el encaminador R1 y examinar el proceso de carga del IOS.
¿Qué versión de software está corriendo en el encaminador?
2. Cambiar el registro de configuración del encaminador al valor “0x2142”,
¿Qué sucederá al reiniciar el encaminador?
3. Reiniciar el encaminador y abortar la carga del IOS, cambiar el registro
de configuración a “0x2102” y reiniciar nuevamente el encaminador.
4. Salvar el archivo de configuración activo en RAM hacia la memoria
NVRAM.
5. Salvar el archivo de configuración activo en RAM hacia un servidor
TFTP.
6. Salvar el archivo de configuración de la memoria NVRAM hacia el ser-
vidor TFTP.
7. Restaurar el archivo de configuración (del punto 5) desde el servidor
TFTP a la RAM
8. Restaurar el archivo de configuración (del punto 6) desde el servidor
TFTP a la NVRAM.
9. Borrar el archivo de configuración de la memoria NVRAM.
10. Salvar el archivo de configuración desde la memoria RAM a la memoria
NVRAM.
11. Examinar el contenido de la memoria flash.
12. Respaldar el IOS desde la memoria flash al servidor TFTP.
13. Restaurar el IOS desde el servidor TFTP a la memoria flash.
14. Reiniciar el encaminador y verificar su operación.

INFORMACIÓN COMPLEMENTARIA

El ping extendido permite especificar diferentes opciones del encabezado del datagrama IP; para ejecutar el ping extendido se debe estar en modo de ejecución privilegiado. A continuación se enlistan los parámetros que puede solicitar este comando.

Protocol: protocolo a ser usado por el programa ping (IP, por defecto).

Target IP address: dirección IP o el nombre del equipo destino que se va a probar.

Repeat count: número de solicitudes de eco (echo request) que se deben enviar en la prueba (5, por defecto).

Datagram size: tamaño, en bytes, del paquete de ping (100, por defecto).

Timeout in seconds: cantidad de tiempo que se espera por una respuesta (echo reply) antes de indicar un tiempo excedido (2 segundos, por defecto).

Extended commands: pregunta si se debe o no hacer preguntas subsiguientes (“n” que significa no, por defecto).

Source address: dirección IP que debe aparecer como dirección origen en el encabezado del datagrama IP (Por defecto, es la dirección IP de la interfaz usada con la que el ping sale del encaminador).

Type of service: permite especificar un valor para el campo “tipo de servicio” del datagrama IP (0, por defecto).

Set DF bit in the IP header?: determina si el datagrama puede o no ser fragmentado cuando alcance un segmento que soporte una MTU menor que su tamaño (no, por defecto).

Data pattern: patrón de datos que lleva el ping, éste es un número hexadecimal de cuatro dígitos (0xABCD, por defecto).

Loose, Strict, Record, Timestamp, Verbose: son opciones del encabezado IP (“none” que significa: ninguna de éstas, por defecto). El parámetro record registra la ruta que el datagrama IP tomará. Si se escoge record, aparecerá una pregunta relativa al máximo número de saltos que se le permiten registrar al datagrama IP (9, por defecto, y puede estar en el rango de 1 hasta 9).

Sweep range of sizes: permite enviar pings que varíen en tamaño (“n” que significa no, por defecto).

PROBLEMAS

1. Cuando el archivo running-config tiene un tamaño superior al que la memoria NVRAM puede almacenar, se puede hacer uso del comando

global “*service compress-config*”. Habilite este servicio y verifique su funcionamiento mediante los comandos “*copy running-config startup-config*” y “*show startup-config*”.

2. Suponga que en la memoria flash de un encaminador se almacenan los archivos “c1700-sv3y-mz.121-1.xk.bin” y “c1700-sv3y-mz.122-2.xk.bin”, correspondientes a dos versiones diferentes de IOS del equipo. Explique el resultado que se obtiene después de ejecutar cada uno de los siguientes comandos en secuencia.

```
R1# delete flash: c1700-sv3y-mz.121-1.xk.bin  
R1# undelete flash: c1700-sv3y-mz.121-1.xk.bin  
R1# delete flash: c1700-sv3y-mz.122-2.xk.bin  
R1# squeeze flash:
```

¿Qué sucede si el encaminador no soporta el comando “*squeeze*” y se ejecuta “*erase flash:*” en su lugar?

3. Suponiendo que la memoria flash de un encaminador tiene un tamaño de 32 Megabytes y que contiene dos IOS que ocupan menos de 16 Megabytes cada uno, explique el propósito de los siguientes comandos.

```
R1(config)# partition flash: 2 16 16  
R1(config)# end  
R1# show flash:  
R1# erase flash:2:  
R1# show flash:  
R1(config)# no partition flash: 2 16 16
```

4. Intente descargar el archivo de configuración “*running-config*” y el archivo del sistema operativo “c1700-sv3y-mz.122-2.xk.bin” desde un servidor FTP hacia el encaminador. Las siguientes líneas pueden ser de ayuda si se reemplazan los parámetros de acuerdo a su situación: usuario, clave, dirección IP y nombre del archivo del IOS.

```
R1(config)# ip ftp username usuario  
R1(config)# ip ftp password clave  
R1(config)# end  
R1# copy ftp: running-config  
R1# copy ftp://usuario:clave@192.168.55.18/ c1700-sv3y-mz.122-2.xk.bin flash:
```

5. Ejecute el comando de configuración global “*warm-reboot*” y reinicie el encaminador. Después de lo anterior, intente lo siguiente:
 - Reiniciar el encaminador en caliente, use el comando “*reload warm*”.
 - Cargar un IOS en caliente, use el comando “*reload warm file flash:nombre-del-IOS*”

¿Cuál es la diferencia de reiniciar el equipo en frío o reiniciarlo en caliente?
6. Con el propósito de tener un historial de archivos con la configuración que se tenía antes de ejecutar el comando “*copy running-config startup-config*” o el comando “*write memory*”, se usa la función “*archive*”; explore el resultado de las siguientes líneas que utilizan dicha función. Esto requiere una versión del IOS igual o mayor a 12.3(4).

```
R1# cd flash:  
R1# mkdir configs  
R1(config)# archive  
R1(config-archive)# path flash:/configs/$h  
R1(config-archive)# write-memory  
R1(config-archive)# end  
R1# write memory  
R1(config)# no ip routing  
R1# write memory  
R1# show archive  
R1# show archive config differences flash:/configs/R1-1  
R1# archive config  
R1# configure replace flash:/configs/R1-1
```

7. Explique el uso del comando de configuración global “*configuration mode exclusive manual*”, y de los comandos de ejecución privilegiado “*configure terminal lock*” y “*show configuration lock*”.

GLOSARIO

Boot: es el paso que realiza un programa de carga (bootstrap), residente en la memoria ROM del encaminador, para buscar el sistema operativo (IOS que se encuentra residente en la memoria flash o en un servidor de la red) y cargarlo en la memoria RAM.

Reiniciar: hace referencia a apagar (físicamente o mediante el comando *reload*) el encaminador y volverlo a encender de nuevo.

Salvar: guardar de forma permanente el archivo running-config (que se ejecuta en memoria RAM) en memoria NVRAM o en un servidor TFTP. También se refiere a respaldar el IOS en un servidor TFTP.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- LEINWAND, A.; PINSKY, B. (2001). *Cisco Router Configuration*. 2nd Ed. Indianapolis, IN: Cisco Press.

CAPÍTULO 4

RIP COMO PROTOCOLO DE ENCAMINAMIENTO IP, RUTAS ESTÁTICAS

RIP es un protocolo de enrutamiento que permite interconectar varias redes y conformar una red unificada de cara al usuario. Aunque RIP es fácil de configurar y puede resultar útil en muchas situaciones, hay que tener en cuenta sus principales limitaciones. En primer lugar, la versión 1 (estandarizada en el RFC 1058) no soporta máscara de subred de longitud variable. En segundo lugar, tanto la versión 1 como la versión 2 (documentada en el RFC 1723) están limitadas a tener un número máximo de 15 saltos.

Una de las características de RIP es que distribuye toda la tabla de enruteamiento cada vez que se completa un ciclo de actualización de 30 segundos. Un encaminador considera una ruta como inválida cuando no es recibida tras 6 ciclos (180 segundos) y la elimina cuando no es recibida luego de 8 ciclos (240 segundos). En el presente capítulo se pretende realizar la interconexión básica de redes por medio del protocolo RIP, experimentar con algunas opciones adicionales de dicho protocolo e interpretar los resultados obtenidos.

OBJETIVO

Al finalizar la presente unidad, el estudiante estará en capacidad de:

- Configurar direcciones IP en las interfaces del encaminador (enrutador).
- Mapear un nombre de host estático a una dirección IP del encaminador.
- Especificar uno o más servidores de dominio de nombres en el enrutador.

- Describir cómo los encaminadores aprenden información de la red.
- Listar algunos protocolos de enrutamiento soportados por IP.
- Explicar el término Métrica de enrutamiento.
- Configurar el protocolo de enrutamiento RIP.
- Verificar el funcionamiento del protocolo RIP.

Prerrequisitos: Manejo del esquema de direccionamiento IP tipo classful y de la extensión para establecer subredes.

PROCEDIMIENTO

Configuración de direcciones IP en un encaminador

El comando *ip address* se usa para configurar una dirección lógica de red –dirección IP– en la interfaz en referencia.

A continuación se muestra de qué manera se asigna una dirección IP y una máscara de subred, y cómo se inicia el procesamiento de IP sobre esta interfaz.

```
R1(config)# in s0  
R1(config-if)# ip address ip-address subnet-mask
```

Descripción de los campos del comando IP:

- ip-address: número de 32 bits en notación punto decimal.
- subnet-mask: número de 32 bits en notación punto decimal que indica la parte de la dirección IP que corresponde a la red física –mediante los bits cuyo valor lógico sea “uno”– y la parte de la dirección IP que corresponde a los hosts –mediante los bits cuyo valor sea “cero”.

Mapeo de direcciones IP a hostname

El comando *ip host* crea una entrada estática de nombre-dirección en el archivo de configuración del encaminador.

```
R1(config)# ip host name [tcp-port-number] address [address]
```

Por ejemplo, para mapear un nombre de host estático a una (o varias) dirección(es) IP:

```
R1(config)# ip host mafalda 10.0.0.5 10.0.0.6
```

Las interfaces y los hosts son seleccionados por su nombre.

El comando *show hosts* puede usarse para ver la lista de los hostnames y las direcciones asociadas.

Asignación del servidor de nombres

El comando *ip name-server* define cuáles hosts proporcionan el servicio de nombres DNS (Domain Name Services). Se pueden especificar un máximo de seis direcciones de servidores de nombres en un solo comando. El comando *no ip domain-lookup* desactiva el servicio de nombres, lo cual significa que el encaminador no difundirá paquetes solicitando dicho servicio.

Especifica uno o más servidores que suministran información de nombres:

```
R1(config)# ip name-server server-address1 [server-address2]
...[server-address6]
```

Deshabilita el servicio de nombres:

```
R1(config)# no ip domain lookup
```

Ejemplo:

```
R1(config)# ip domain-lookup
R1(config)# ip name-server 10.0.0.20
```

Protocolos de enrutamiento IP

Contenido de la tabla de enrutamiento IP

Inicialmente un encaminador solamente sabe cómo llegar a las redes que están directamente conectadas a él. Por ejemplo, el encaminador R1, conectado directamente por medio de las interfaces Ethernet 0 (Eth0) a Net1, Ethernet 1 (Eth1) a Net2 y Serial 0 (S0) –como se representa en la Figura 4.1–, tendrá inicialmente información en su tabla de enrutamiento como la incluida en la Tabla 4.1.

**Tabla 4.1 Tabla de enrutamiento del encaminador R1:
al inicio R1 conoce solamente las redes directamente conectadas**

Network	Next Hop	Interfaz
10.3.1.0/24	Directa	EO
10.3.2.0/24	Directa	E1
8.3.1.4/30	Directa	SO



Figura 4.1 Conexión directa de R1 a las redes Net1, Net2 y HDLC

Rutas estáticas

Las rutas estáticas son configuradas manualmente por el administrador de la red; se utilizan para conectar redes de tipo “stub” en las que solamente hay un camino hacia el destino. Conservan ancho de banda y, aunque se usan más frecuentemente con enlaces seriales, también se pueden definir para cualquier tipo de medio.

La sintaxis del comando que configura una ruta estática es:

```
R1(config)# ip route network [mask] {address | interface}[distance]
```

Por ejemplo, el siguiente comando crea una entrada en la tabla de enrutamiento de R1, esta entrada le permite saber que para llegar hasta la red 30.0.0.0 se deben enviar los datagramas a la dirección IP “8.3.1.6” del próximo salto (next hop).

```
R1(config)# ip route 30.0.0.0 255.0.0.0 8.3.1.6
```

Ruta por defecto

La ruta por defecto la define manualmente el administrador de la red, ésta indicará el camino a seguir al encaminador cuando no conozca la ruta hacia un destino específico; se utiliza, por ejemplo, para interconectar una compañía con Internet.

Si la compañía X –conformada por varias redes físicas– cuya dirección de red es la 192.168.0.0 se conecta a la Internet por medio de la red 193.50.1.0, y al encaminador que une la compañía X con Internet se le asigna como red por defecto la dirección 193.50.1.0, dicho encaminador informará a los otros encaminadores de la compañía X sobre esta dirección (la 193.50.1.0) para que la usen como red por defecto.

Cuando los encaminadores de la red 192.168.0.0 tengan que enviar un datagrama cuya ruta de destino no se encuentre en la tabla de enrutamiento, estos enviarán dicho paquete al próximo salto (next hop) que conduzca hacia la red por defecto.

La sintaxis del comando es.

```
R1(config)# ip default-network network-number
```

Por ejemplo, para configurar la red 193.50.1.0 para que sea la red por defecto, se ejecuta el comando

```
R1(config)# ip default-network 193.50.1.0
```

Rutas dinámicas

Los encaminadores aprenden los caminos que llevan hacia los diferentes destinos por medio de las actualizaciones que reciben periódicamente de sus vecinos, para ello usan un protocolo en común (protocolo de enrutamiento) que les permite intercambiar información de enrutamiento, dicho intercambio se realiza mediante el envío de información de actualización de enrutamiento –Routing updates– a intervalos fijos de tiempo o cuando se presenta un cambio topológico de la red. Las actualizaciones de enrutamiento llevan información acerca de las redes que se pueden acceder y del valor de la métrica asociado con cada camino utilizable. De lo anterior se puede concluir que: el camino hacia un destino cambia en la medida en que las condiciones de la red cambien.

Métricas de los protocolos de enrutamiento

El mejor camino entre las redes, o entre las subredes, es determinado por la métrica de enrutamiento. Las variables usadas como métricas incluyen las siguientes:

Hop count: número de paradas intermedias que hace un paquete en su viaje hacia el destino. El paso a través de un encaminador suma un salto (Hop count). Usado por: IP RIP, IPX RIP.

Bandwidth: capacidad que tiene un enlace para transportar datos, usualmente medida en bits por segundos (bps). Usado por: IP EIGRP, IP IGRP.

Delay: cantidad de tiempo asociado con el uso de un enlace en particular, usualmente medido en milisegundos (msec). Usado por: IP EIGRP, IP IGRP.

Reliability: valor asignado a cada enlace para indicar la probabilidad de que el paquete sea despachado exitosamente, usualmente expresado como un valor fraccional; algún número dividido por 255. Usado por: IP EIGRP, IP IGRP.

Load: valor dinámico que indica la utilización de un enlace, usualmente expresado como un valor fraccional; algún número dividido por 255. Usado por: IP EIGRP, IP IGRP.

MTU (Maximun Transfer Unit): expresado en bytes, es el tamaño más grande de la unidad de datos del nivel de red que puede encapsularse en el campo de datos de una trama. Usado por: IP EIGRP, IP IGRP.

Cost: valor arbitrario que indica el costo de usar una interfaz, usualmente expresado como un valor entero y asignado a una interfaz de salida. Usado por: IP OSPF, IPX NLSP.

Ticks: valor arbitrario asociado con el retardo al usar una interfaz o un enlace. El valor preciso es 1/18 de segundo. Usado por: IPX RIP.

Sistema Autónomo

Un sistema autónomo –Autonomous System (AS)– está constituido por un conjunto de encaminadores que comparten información a través del mismo protocolo de enrutamiento. Estos encaminadores están normalmente bajo el control de una administración común.

A cada sistema autónomo se le asigna un número único que es requerido por algunos protocolos de enrutamiento –como el Interior Gateway Routing Protocol (IGRP).

Protocolos de enrutamiento interiores vs. protocolos de enrutamiento exteriores

Los protocolos de enrutamiento interiores (RIP, OSPF, IGRP y EIGRP) son usados dentro del mismo sistema autónomo. Los protocolos de enrutamiento exteriores son usados para comunicar diferentes sistemas autónomos.

Dos protocolos de enrutamiento interiores son:

Routing Information Protocol (RIP) version 1.0

Especificado en el RFC 1058. RIP fue liberado con BSD UNIX como un programa denominado “routed”; debido a sus limitaciones, se recomienda usar la versión actual (RIPv2.0), las características claves de RIPv1 son:

- Es un protocolo abierto de enrutamiento tipo “vector distancia” –distance vector.
- Usa como métrica la variable número de saltos “Hop count”.
- El máximo número de saltos es 15.
- Las actualizaciones de enrutamiento son difundidas cada 30 segundos.
- Soporta seis caminos iguales –de igual costo– para una sola ruta, estos pueden colocarse en la tabla de enrutamiento y permiten hacer balanceo de carga hacia un destino único.
- Es un protocolo classful, limitado al uso de una máscara de subred uniforme en toda la red.

Interior gateway Routing Protocol (IGRP)

Es un protocolo de enrutamiento propietario de Cisco tipo “vector distancia” con un número de saltos máximo de 100 (por defecto).

Su métrica es la combinación de las variables Bandwidth, Delay, Load, Reliability y MTU, soporta múltiples caminos de costo desigual para balanceo de cargas.

Envía actualizaciones a intervalos fijos de 90 segundos y soporta el envío de actualizaciones activadas por cambios topológicos (triggered updates) de la red.

Tiene soporte de sistema autónomo –Autonomous System (AS).

Configuración de RIP

En términos generales, la selección de un protocolo de enrutamiento para IP incluye la configuración de parámetros Globales y de Interfaz.

Tareas Globales

Seleccionar un protocolo de enrutamiento (RIP, IGRP, EIGRP, OSPF).

Asignar los números de red IP sin especificar los valores de subred.

Tareas de Interfaz

Asignar las direcciones IP a las interfaces y la máscara apropiada.

Ejemplo de tareas globales:

```
R1(config)# router protocol [keyword]
```

Con lo anterior se define un protocolo de enrutamiento IP.

El comando *router* arranca un proceso de enrutamiento, “protocol” define el protocolo de enrutamiento que se arrancará (RIP, IGRP, EI-GRP, OSPF), mientras que keyword es requerida por algunos protocolos de enrutamiento para asignarle una identificación al sistema autónomo. Una vez se digite el comando anterior, el indicador del sistema (prompt) cambia a:

```
R1(config-router)#
```

Entonces, se ejecuta el subcomando de configuración, que es obligatorio para cada proceso de enrutamiento IP.

```
R1(config-router)# network network-number
```

El comando *network* es requerido porque permite que el proceso de enrutamiento determine cuáles interfaces participarán en el intercambio –envío y recepción– de las actualizaciones de enrutamiento (routing updates). En el campo *network-number* se especifica una o varias redes que se encuentran directamente conectadas. Este campo está basado en los números de red classful, no en números de subred o en direcciones IP individuales.

Ejemplo de configuración de RIP para la red de la Figura 4.1:

```
R1(config)# router rip  
R1(config-router)# network 10.0.0.0  
R1(config-router)# network 8.0.0.0
```

```
R2(config)# router rip  
R2(config-router)# network 30.0.0.0  
R2(config-router)# network 8.0.0.0
```

En R1 el comando *router rip* selecciona a RIP como protocolo de enrutamiento IP, mientras que los comandos *network 10.0.0.0* y *network 8.0.0.0* especifican las redes directamente conectadas al encaminador R1; las interfaces de R1 conectadas a estas redes intercambiarán información de en-

rutamiento (por medio de RIP) con otros encaminadores vecinos que se conecten directamente a dichas redes.

Monitoreo de IP

El comando *show ip protocols* muestra los valores de los temporizadores de enrutamiento, filtros e información de la(s) red(es) asociada(s) con el encaminador.

```
R1# show ip protocols
```

```
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 21 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 1, receive any version
      Interface      Send      Recv Triggered RIP Key-chain
      FastEthernet0/0    1          12
      Serial0/0         1          12
      FastEthernet0/1    1          12
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  8.0.0.0
  10.0.0.0
Routing Information Sources:
      Gateway      Distance      Last Update
      8.3.1.6        120          00:00:05
Distance: (default is 120)
```

El comando *show ip route* muestra el contenido de la tabla de enruteamiento, ésta contiene las redes y subredes que el encaminador conoce y un código que indica cómo se obtuvo la información (cuál fue el protocolo de enruteamiento utilizado).

R1# *show ip route*

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

8.0.0.0/30 is subnetted, 1 subnets

C 8.3.1.4 is directly connected, Serial0/0

10.0.0.0/24 is subnetted, 2 subnets

C 10.3.1.0 is directly connected, FastEthernet0/0

C 10.3.2.0 is directly connected, FastEthernet0/1

R 30.0.0.0/8 [120/1] via 8.3.1.6, 00:00:15, Serial0/0

INFORME

Consulte las ventajas y desventajas que tienen los protocolos de enrutamiento de tipo “vector distancia” –Distance vector– y de tipo “estado de enlace” –Link state.

Por medio del software Configmaker de Cisco, interconectar dos redes de área local (LAN) sobre las cuales corren aplicaciones TCP/IP. Utilizar dos encaminadores cisco de la serie 1751, un enlace HDLC a 64.000 bps y el protocolo de enrutamiento RIP versión 2. Entregar los archivos de configuración generados y hacer los comentarios respectivos del significado de las líneas de configuración.

Distinguir en qué situación se justifica utilizar la redistribución de rutas.

EJERCICIOS DE LABORATORIO

Este ejercicio tiene como finalidad configurar los encaminadores R1, R2 y R3 de la red de la Figura 4.2, utilizando el protocolo de enrutamiento

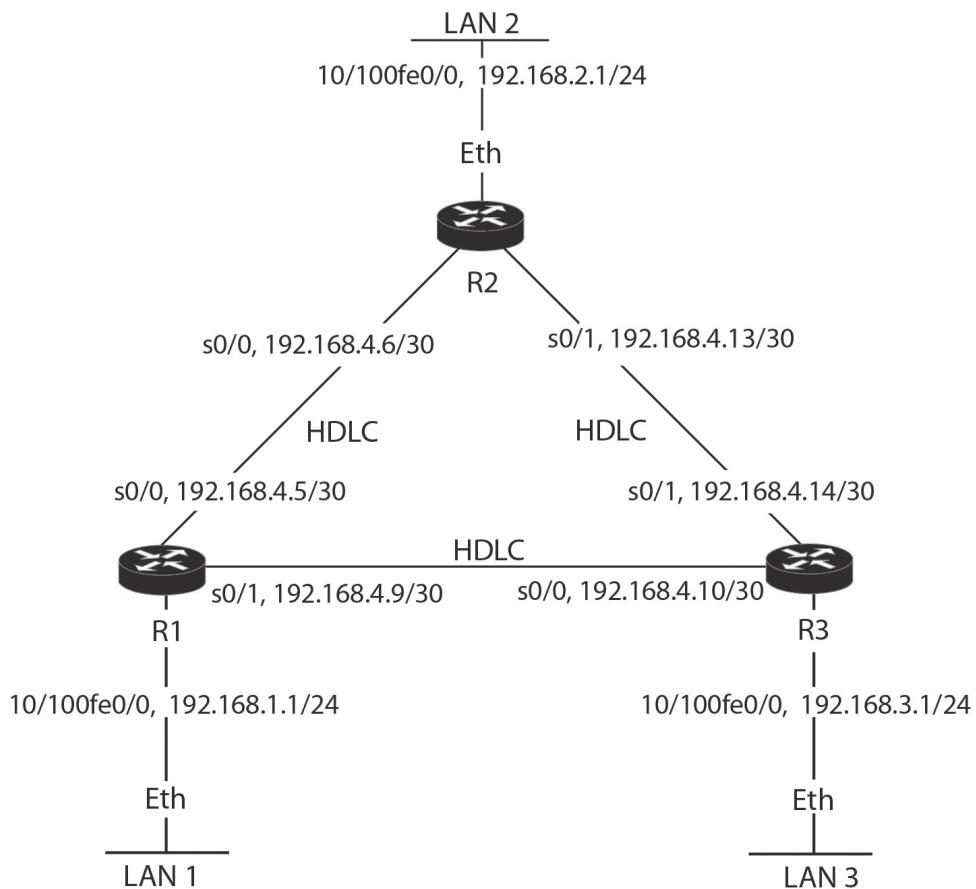


Figura 4.2 Red en delta, funcionando con protocolo RIP

RIP.

Configurar los encaminadores R1, R2 y R3 para que intercambien tablas utilizando el protocolo RIP versión 2.

INFORMACIÓN COMPLEMENTARIA

Repaso de enrutamiento

Los encaminadores funcionan en el nivel 3 o nivel de red del modelo de referencia OSI. Un encaminador tiene dos funciones: encontrar caminos a un destino y commutar los datagramas a dicho destino. Para realizar la primera función, el encaminador requiere información sobre:

- La localización de los diferentes números de red destino.
- Los encaminadores desde los cuales se puede aprender redes de destino.
- El mejor camino para alcanzar la red destino.
- Actualizaciones regulares sobre las redes destino que son alcanzables.

Para realizar la segunda función, el encaminador tiene que examinar la dirección IP destino del datagrama y diferenciar entre el componente de red y el componente de host de dicha dirección. Para tomar una decisión de enrutamiento, el encaminador utiliza el componente de red, puesto que éste es el único componente en su tabla de enrutamiento.

El enrutamiento dinámico se consigue ejecutando en el encaminador un protocolo de enrutamiento que permite aprender la ubicación de las redes destino de forma automática. El enrutamiento dinámico –del encaminador– depende de que el protocolo de enrutamiento en ejecución –por ejemplo, RIP– comparta información de enrutamiento relativa a los números de red del protocolo enrutado –por ejemplo, IP– y de que dichas redes se puedan alcanzar. En la Tabla 4.2 se presentan, a modo de ejemplo, algunos protocolos enrutados (enrutables) y los protocolos de enrutamiento que ellos pueden usar.

Tabla 4.2 Protocolos enrutados y protocolos de enrutamiento

Protocolos Enrutados	Protocolos de enrutamiento
IP	RIP, OSPF, IGRP, EIGRP, BGP, IS-IS
IPX	RIP, NLSP, EIGRP
AppleTalk	RMTP, AURP, EIGRP

Un protocolo enrutado es el protocolo que define los mecanismos para adicionar y procesar la información de capa 3. Asimismo, determina cómo conseguir esta información entre dos máquinas.

Ruta por defecto

Es un caso especial de ruta estática; puede ser usada cuando el encaminador no conozca la red destino.

Por defecto, si un encaminador no tiene un camino hacia el destino, descartará el datagrama; este comportamiento es diferente al de un bridge o un switch capa 2, los cuales inundan la red cuando desconocen el destino. Una ruta por defecto cambia este comportamiento en el encaminador: si

éste no conoce el destino, entonces usa la ruta por defecto para reenviar el datagrama.

Cuando se configura una ruta por defecto, se usa el comando de configuración global *ip route*. Para la red destino y la máscara de subred se usa el valor 0.0.0.0 0.0.0.0.

Por ejemplo, el siguiente comando permite tener una ruta por defecto:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 "Dir IP del next hop vecino" | "interfaz de salida"  
["distancia administrativa"] [permanent]
```

En esta nomenclatura 0.0.0.0 0.0.0.0 representa todas las redes.

Rutas por defecto y protocolos vector distancia

Por defecto, para IP un protocolo vector distancia no usará la ruta por defecto configurada, aunque esta ruta por defecto se encuentre en la tabla de enrutamiento. Esto se debe a que para IP los protocolos vector distancia, tales como RIP v1 e IGRP, son classful –estos no entienden una máscara de subred de 32 ceros: 0.0.0.0. Para cambiar este comportamiento se usa el siguiente comando de configuración global:

```
R1(config)# ip classless
```

Esto permite que un encaminador que ejecuta un protocolo classful use la ruta por defecto que se haya configurado.

Distancia administrativa

Es una convención de Cisco para medir la importancia de los protocolos de enrutamiento IP. Por ejemplo, si un encaminador tiene que escoger entre dos protocolos de enrutamiento –tal como una ruta estática o una ruta aprendida por RIP que apuntan al mismo destino–, escogerá la ruta del protocolo que considere mejor. Realmente, la distancia administrativa es una medida que determina cuál selección será la mejor.

Para el parámetro de distancia administrativa, Cisco asigna un peso entre 0 y 255 a cada protocolo de enrutamiento IP. Cuando se toma una decisión de enrutamiento, el protocolo que tenga el menor peso es el preferido sobre los otros. La Tabla 4.3 presenta una lista de los protocolos de enrutamiento y sus respectivas distancias administrativas por defecto.

Tabla 4.3 Distancia administrativa por defecto de los diferentes protocolos de enrutamiento

Tipo de ruta	Distancia administrativa
Interfaz conectada	0
Ruta estática	1
Ruta interna EIGRP	90
Ruta IGRP	100
Ruta OSPF	110
Ruta RIP	120
Ruta externa EIGRP	170
Ruta desconocida (considerada ruta inválida y no será usada)	255

Dadas las anteriores distancias administrativas, si un encaminador Cisco aprende acerca de la red destino 172.16.0.0/16 por medio de RIP y de IGRP simultáneamente, le creerá más a la ruta de IGRP, puesto que tiene una mejor distancia administrativa.

Tipos de Protocolos de enrutamiento dinámicos

Los protocolos de enrutamiento caen en una de las siguientes categorías:

- Vector distancia –*Distance Vector*.
- Estado de enlace –*Link State*.
- Híbrido –*Hybrid*.

Cada uno de estos toma un enfoque diferente para compartir información de enrutamiento y escoger caminos hacia los destinos. Debido a sus diferencias, cada uno presenta ventajas y desventajas cuando se compara con los otros. La selección de cuál protocolo de enrutamiento debe utilizar el encaminador es algo que se debe hacer teniendo en cuenta las ventajas y desventajas de dicha decisión. A continuación se indican algunos de los factores a considerar cuando se decide el protocolo de enrutamiento que se implementará:

- Métricas usadas por el protocolo.
- Cómo es compartida la información de enrutamiento por el protocolo.
- La velocidad de convergencia del protocolo.
- Cómo procesan la información los encaminadores.

Protocolos Distance Vector

Los protocolos de enrutamiento “vector distancia” usan la distancia (costo) y la dirección (vector) para encontrar caminos hacia las redes de destino. Algunas veces los protocolos “vector distancia” son llamados protocolos por rumor, porque los encaminadores que los utilizan aprenden información de enrutamiento por medio de los encaminadores vecinos directamente conectados, los cuales, a su vez, no están necesariamente conectados físicamente a las direcciones de red que anuncian. Ejemplos de protocolos de enrutamiento “vector distancia” para IP son RIP v1.0 e IGRP.

Con estos protocolos, los encaminadores periódicamente anuncian su tabla de enrutamiento por medio de la dirección local de broadcast –con una dirección IP destino de 255.255.255.255. Estos anuncios se hacen periódicamente, independientemente de que haya o no haya información nueva para compartir. Una vez el periodo del temporizador expira, estos difunden su tabla de enrutamiento a sus vecinos.

Un encaminador con protocolo “vector distancia” conoce de la existencia de otras redes por medio de la tabla de enrutamiento difundida por sus vecinos (no hay un proceso de “handshake” o “hello” formal para descubrir a los encaminadores vecinos). Igualmente, no hay una supervisión para asegurarse de que los vecinos recibieron la tabla de enrutamiento difundida por un encaminador. Puesto que las actualizaciones de la tabla de enrutamiento (routing updates) se envían periódicamente, se asume que los vecinos eventualmente aprenderán la información difundida por el encaminador, aunque se pierdan algunas actualizaciones.

Procesando las actualizaciones de enrutamiento

Cada vez que un encaminador recibe una actualización de la tabla de enrutamiento enviada por un encaminador vecino, realizará lo siguiente:

1. Incrementa la métrica a cada una de las rutas anunciadas por su vecino –para RIP, le suma 1 al número de saltos (hop count).
2. Compara cada entrada de la actualización recibida del vecino con las entradas que él tiene en su propia tabla de enrutamiento (routing table).
3. Si la información del vecino es mejor, pone dicha entrada en su tabla de enrutamiento y remueve la entrada vieja.
4. Si la información del vecino es peor, ignora dicha entrada.
5. Si la información del vecino es exactamente igual que la entrada de su tabla, reinicia el temporizador para dicha entrada en su tabla de enruteamiento –en otras palabras, el encaminador ya aprendió de esta ruta por medio del mismo vecino.

6. Si la información del vecino contiene una ruta diferente, pero tiene la misma métrica que una ruta ya existente en la tabla del encaminador, éste añadirá dicha entrada a su tabla de enrutamiento, asumiendo que no se ha excedido el número máximo de caminos de igual costo para esa red destino. En esta situación, el encaminador está aprendiendo acerca de la misma red destino, pero de dos vecinos diferentes, y ambos vecinos han anunciado un número de red destino con la misma métrica.

Una de las ventajas de los protocolos “vector distancia” es que son muy fáciles de configurar y depurar, adicionalmente, demandan poca memoria y procesamiento del encaminador. Esto puede deducirse, porque en el proceso de actualización lo que se hace es básicamente incrementar la métrica de las rutas anunciadas y comparar el resultado con la información que el encaminador tiene en su tabla de enrutamiento.

Protocolos “Estado de enlace” (Link State)

Los protocolos de enrutamiento de “Estado de enlace” usan un algoritmo llamado Shorted Path First (SPF), inventado por Dijkstra para encontrar los caminos hacia las redes destino. A diferencia de los protocolos “vector distancia”, los protocolos de “Estado de enlace” tienen un gráfico exacto de la topología de la red: conocen cuál encaminador está conectado a qué número de red. Note que algunos protocolos “link state”, como OSPF, permiten limitar el conocimiento del encaminador, esto tiene como objetivo aumentar la velocidad de convergencia y disminuir la disruptión de enrutamiento en la red. Ejemplos de protocolos de “Estado de enlace” incluyen a OSPF e IS-IS de IP, y a NLSP de IPX. OSPF está definido en el RFC 2328.

Para compartir la información de enrutamiento, los encaminadores que ejecuten el algoritmo SPF anunciarán el estado de sus enlaces, lo cual se conoce como LSA (Link State Advertisements) –algunas veces también referido como LSP (Link State Packets). Un LSA es un mensaje que proviene de un encaminador y contiene información acerca de quién generó el anuncio, así como el número de red que está siendo anunciada.

Los LSA típicamente son generados solo cuando se presentan cambios. En otras palabras, las actualizaciones periódicas suceden muy poco. Los LSA son compartidos como mensajes multicast y se intercambian de manera confiable; el destino le enviará una confirmación (acknowledge) de regreso al origen de la actualización. Se puede distinguir que este funcionamiento es muy diferente al de los protocolos “vector distancia”.

Cuando todos los datos de los LSA son recibidos, los encaminadores de “Estado de enlace” pueden construir la topología completa de la red,

conociendo exactamente cuáles encaminadores están conectados a qué redes; a menudo esto es denominado como enrutamiento por propaganda. Los LSA son almacenados en una base de datos local del encaminador. Una vez haya un cambio en la base de datos, el encaminador ejecuta el algoritmo SPF; con base en este algoritmo, el encaminador construirá un árbol SPF (SPF tree), ubicándose él mismo en la raíz del árbol. Usando el árbol, el encaminador poblará la tabla de enrutamiento con el camino más corto (shortest path) a cada red destino.

Ventajas de los protocolos Link State

Para limitar el alcance del viaje de los LSA y reducir el impacto que causan los cambios topológicos en la ejecución del algoritmo SPF, los protocolos de “Estado de enlace” soportan una estructura jerárquica. Esto es bien diferente a los protocolos “vector distancia”; por ejemplo, RIP es una red plana, donde un cambio en un encaminador afecta a todos los encaminadores. Con los protocolos de “Estado de enlace”, esto no es necesariamente cierto.

Otra ventaja de los protocolos de “Estado de enlace” es que estos soportan enrutamiento *classless* o Variable Length Subnet Masking (VLSM). Esto permite que un encaminador use diferentes máscaras de subred para el mismo número de red de una determinada clase (A, B o C), maximizando la eficiencia del direccionamiento. Por medio de este proceso se puede tomar un conjunto de subredes y resumirlas en una sola entrada de la tabla de enrutamiento. Este proceso, llamado “resumen de rutas” (route summarization), ayuda a contener problemas de enrutamiento (como una condición de ruta oscilante, en la que el enlace baja y sube permanentemente, esto es disruptivo para los encaminadores, especialmente para los que ejecutan protocolos de “Estado de enlace”) y reduce el tamaño de las tablas de enrutamiento en el encaminador.

A diferencia de los protocolos “vector distancia” que realizan actualizaciones usando una dirección IP de broadcast, los protocolos de “Estado de enlace” usan dirección IP multicast y solamente envían actualizaciones incrementales. Una actualización incremental, comparada con una actualización periódica, es una actualización que se genera solamente cuando sucede un cambio. Cuando se analiza un protocolo “vector distancia”, se concluye que no tiene sentido anunciar una tabla de enrutamiento cada 30 ó 90 segundos cuando no han ocurrido cambios porque ello gasta recursos valiosos de computación y ancho de banda de la red.

Desventajas de los protocolos Link State

Aunque los protocolos de “Estado de enlace” permiten escalar redes de mayor tamaño, en comparación a lo que permiten los protocolos “vector distancia”, los protocolos de “Estado de enlace” también tienen sus inconvenientes.

Un problema con los protocolos de “Estado de enlace” es que usan intensivamente la memoria RAM y la CPU debido a que estos requieren tener una tabla de vecinos, una base de datos del estado de los enlaces y una tabla de enrutamiento. Estos protocolos requieren más memoria del encaminador, comparada con la requerida por un protocolo “vector distancia”. Igualmente, cada vez que ocurre un cambio topológico en la red, los encaminadores de “Estado de enlace” deben actualizar sus bases de datos, ejecutar el algoritmo SPF, construir el árbol SPF y reconstruir la tabla de enrutamiento. En particular, este proceso emplea de forma intensiva la CPU.

Protocolos Híbridos

Combinan las ventajas de los protocolos “vector distancia” y “Estado de enlace”. Dos ejemplos de protocolos híbridos son los protocolos RIP V2.0 de IP y el protocolo propietario de Cisco llamado EIGRP. Estos protocolos reducen el uso de la memoria y de la CPU, comportándose de manera similar a un protocolo “vector distancia” cuando procesan nueva información de enrutamiento. No obstante, los protocolos híbridos reducen la utilización del ancho de banda, compartiendo solamente actualizaciones incrementales (no actualizaciones periódicas). Esto lo realizan usando direcciones multicast por medio de mecanismos confiables orientados a la conexión. Los protocolos híbridos también soportan otras características de los protocolos de “Estado de enlace”, como redes jerárquicas, VLSM y resumen de rutas.

Características de RIPv2

- Es un protocolo abierto.
- Soporta actualizaciones generadas por eventos “triggered updates”.
- Usa dirección IP de multicast (224.0.0.9) en lugar de dirección IP de broadcast (255.255.255.255).
- Es un protocolo de tipo classless VLSM; soporta muchas máscaras de subred para una clase de dirección dada, permitiendo maximizar la eficiencia de las direcciones y realizar un resumen de rutas para crear redes escalables muy grandes.

PROBLEMAS

1. Configurar el encaminador R1 de la Figura 4.2 para que redistribuya una ruta estática –192.168.5.0/24– hacia RIP. Probar el siguiente trozo de código y verificar el resultado en R2 y R3 usando el comando “*show ip route*”.

```
R1(config)# ip route 192.168.5.0 255.255.255.0 192.168.1.2  
R1(config)# router rip  
R1(config-router)# redistribute static
```

2. Configurar el encaminador R1 de la Figura 4.2 para que, de las tres rutas estáticas que tiene configuradas, solamente redistribuya dos rutas estáticas hacia RIP –las rutas 192.168.5.0/24 y 192.168.6.0/24–; usar “Route Maps”. Probar el siguiente trozo de código y verificar el resultado en R1 mediante los comandos “*show route-map NOMBRE*” y “*show ip rip database*”.

```
R1(config)# ip route 192.168.5.0 255.255.255.0 192.168.1.2  
R1(config)# ip route 192.168.6.0 255.255.255.0 192.168.1.2  
R1(config)# ip route 192.168.7.0 255.255.255.0 192.168.1.2  
R1(config)# access-list 50 permit 192.168.5.0  
R1(config)# access-list 51 permit 192.168.6.0  
R1(config)# route-map NOMBRE permit 10  
R1(config-route-map)# match ip address 50  
R1(config-route-map)# set metric 3  
R1(config-route-map)# set tag 3  
R1(config-route-map)# exit  
R1(config)# route-map NOMBRE permit 20  
R1(config-route-map)# match ip address 51  
R1(config-route-map)# set metric 5  
R1(config-route-map)# exit  
R1(config)# route-map NOMBRE deny 30  
R1(config-route-map)# exit  
R1(config)# router rip  
R1(config-router)# redistribute static route-map NOMBRE
```

3. Configurar el encaminador R1 de la Figura 4.2 para que propague una ruta por defecto hacia RIP. Probar el siguiente trozo de código y verificar el resultado en R2 y R3 usando el comando “*show ip route*”.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.3  
R1(config)# router rip  
R1(config-router)# default-information originate
```

4. Configurar el encaminador R1 de la Figura 4.2 para que la única interfaz que pueda participar de RIP sea la interfaz Serial 0/0 –y las interfaces Serial 0/1 y FastEthernet 0/0 se vuelvan pasivas. Probar el siguiente trozo de código y verificar el resultado en R1 usando el comando “*show ip protocols*”.

```
R1(config)# router rip  
R1(config-router)# passive-interface default  
R1(config-router)# no passive-interface default serial 0/0  
R1(config-router)# network 192.168.1.0  
R1(config-router)# network 192.168.4.0
```

5. Configurar los encaminadores R1, R2 y R3 de la Figura 4.2 para que usen RIP versión 2. Habilitar la autenticación MD5 entre R1 y R2. Probar el siguiente trozo de código y verificar el resultado en R1 usando el comando “*show ip protocols*”.

Para R1, R2 y R3:

```
Router(config)# router rip  
Router(config-router)# version 2
```

Para R1 y R2:

```
Router(config)# key chain LAB  
Router(config-keychain)# key 1  
Router(config-keychain-key)# key-string laboratorio  
Router(config-keychain-key)# exit  
Router(config)# interface serial 0/0  
Router(config-if)# ip rip authentication key-chain LAB  
Router(config-if)# ip rip authentication mode md5
```

GLOSARIO

AppleTalk: conjunto de protocolos propietarios desarrollados por Apple Inc. para la interconexión de redes –obsoleto a favor de TCP/IP.

Encapsular: transporte de un paquete –o unidad de datos– de un protocolo de capa superior dentro del campo de datos de un protocolo de capa inferior.

Enrutamiento: proceso que permite decidir la interfaz por la que se debe enviar un datagrama IP y la dirección IP del próximo equipo al que se le debe enviar.

IPX (Internetwork Packet Exchange): protocolo de capa tres de la arquitectura de protocolos IPX/SPX que usa el sistema operativo NetWare de Novell –obsoleto a favor de IP.

Proceso de handshake: es aquel en el que hay un intercambio de mensajes entre varios equipos que permite descubrir y mantener sus relaciones de vecindad, como es el caso del protocolo OSPF.

Red tipo classful: hace referencia a una red clase A (máscara 255.0.0.0), clase B (máscara 255.255.0.0) o clase C (máscara 255.255.255.0).

Red tipo colilla (stub): hace referencia a la red (conformada por varias redes interconectadas por encaminadores) caracterizada por tener solamente una conexión que le permite llegar al resto de redes, razón por la cual sus encaminadores requieren tener una entrada en la tabla de enrutamiento que apunte a una puerta de enlace por defecto.

BIBLIOGRAFÍA

- COMER, D. (2005). *Internetworking with TCP/IP, Vol. 1: Principles, Protocols, and Architecture*. 5th Ed. Upper Saddle River, NJ: Pearson Prentice Hall.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™* 2nd Ed. Sebastopol, CA: O'Reilly.
- DOYLE, J.; CARROLL, J. (2007). *Routing TCP/IP*. 2nd Ed. Indianapolis, IN: Cisco Press. Vol. 1.
- KUROSE J. F.; ROSS, K. W. (2012). *Computer Networking: A Top-down Approach*. 7th Ed. Boston: Addison-Wesley.
- STEVENS, W. R. (1994). *TCP/IP Illustrated, Vol. 1: The Protocols*. Reading, MA: Addison-Wesley.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

CAPÍTULO 5

EIGRP: PROTOCOLO DE ENCAMINAMIENTO IP

EIGRP (Enhanced Interior Gateway Routing Protocol) es un protocolo de enrutamiento propietario de Cisco, concebido para que funcione en aquellas redes implementadas solamente con equipos marca Cisco. No obstante, la fortaleza de este protocolo consiste en que es fácil de configurar, eficiente, confiable y soporta características que se requieren en las grandes redes: máscara de longitud variable y CIDR (Classless Interdomain Routing). La eficiencia de EIGRP se basa en que distribuye únicamente información de las rutas que cambian y que lo hace solamente en el momento en que se presenta el cambio. En una red estable, los encaminadores que utilizan EIGRP solamente requieren intercambiar unos paquetes denominados “Hello”, esto con el propósito de verificar la disponibilidad de los encaminadores vecinos. OSPF es una alternativa a EIGRP con características similares, pero con la ventaja adicional de ser un protocolo abierto, por ser estándar. En el presente capítulo se aborda la configuración de redes que utilizan el protocolo de enrutamiento EIGRP y la verificación del funcionamiento de las mismas.

OBJETIVO

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

- Configurar el protocolo de enrutamiento EIGRP.
- Verificar y monitorear el funcionamiento del protocolo EIGRP.

PROCEDIMIENTO

Configuración de EIGRP

El comando *router eigrp* selecciona a EIGRP como protocolo de enrutamiento IP.

Tareas Globales

```
R1(config)# router eigrp process-ID-number
```

El comando anterior define a EIGRP como protocolo de enrutamiento IP. Después de ejecutar dicho comando, el indicador del sistema cambia para señalar que el usuario está en modo de configuración específica del protocolo de enrutamiento EIGRP.

```
R1(config-router)# network network-number
```

La configuración del protocolo de enrutamiento EIGRP es obligatoria para el proceso de enrutamiento IP. El comando *network* es requerido porque permite que el proceso de enrutamiento determine cuáles interfaces participarán en el intercambio (envío y recepción) de las actualizaciones de enrutamiento (routing updates).

El campo *network-number* especifica una o varias redes que se encuentran directamente conectadas al encaminador, este campo está basado en los números de red classful, no en números de subred o en direcciones IP individuales.

Ejemplo de configuración de EIGRP para la red de la Figura 4.1:

```
R1(config)# router eigrp 100  
R1(config-router)# network 10.0.0.0  
R1(config-router)# network 8.0.0.0
```

```
R2(config)# router eigrp 100  
R2(config-router)# network 30.0.0.0  
R2(config-router)# network 8.0.0.0
```

Después de configurar las respectivas direcciones IP en las interfaces de R1, el comando *router eigrp 100* selecciona a EIGRP (con el número de identificación del proceso igual a 100) como protocolo de enrutamiento IP, mientras que los comandos *network 10.0.0.0* y *network 8.0.0.0* especifican

las redes directamente conectadas al encaminador R1; las interfaces de R1 conectadas a estas redes intercambiarán información de enrutamiento (por medio de EIGRP) con otros encaminadores vecinos que se conecten directamente a dichas redes.

Monitoreo de IP

El comando *show ip protocols* muestra los valores de los filtros, temporizadores de enrutamiento e información de la red asociada con el encaminador. El comando *show ip route* muestra el contenido de la tabla de enrutamiento; ésta contiene las redes y subredes que el encaminador conoce y un código que indica cómo se obtuvo la información.

```
R1# show ip protocols
```

```
Routing Protocol is "eigrp 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
EIGRP NSF-aware route hold timer is 240s
Automatic network summarization is in effect
Automatic address summarization:
10.0.0.0/8 for Serial0/0
Summarizing with metric 281600
8.0.0.0/8 for FastEthernet0/0, FastEthernet0/1
Summarizing with metric 2169856
Maximum path: 4
Routing for Networks:
8.0.0.0
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
(this router) 90 00:01:11
Gateway Distance Last Update
8.3.1.6 90 00:00:52
Distance: internal 90 external 170
```

```
R1# show ip route
```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D 8.0.0.0/8 is a summary, 00:05:59, Null0
C 8.3.1.4/30 is directly connected, Serial0/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.3.1.0/24 is directly connected, FastEthernet0/0
D 10.0.0.0/8 is a summary, 00:05:59, Null0
C 10.3.2.0/24 is directly connected, FastEthernet0/1
D 30.0.0.0/8 [90/2195456] via 8.3.1.6, 00:05:33, Serial0/0

El comando *terminal monitor* redirige la salida de los mensajes que normalmente van a consola, haciendo que estos vayan hacia la sesión vty que se haya establecido con el encaminador. El comando *debug* permite que el encaminador presente lo que realmente está sucediendo con un protocolo específico.

```
R1# terminal monitor  
R1# debug ip eigrp transmit
```

```
R1# EIGRP protocol debugging is on  
Sep 11 08:37:39.599: First peer: startup anchor at serno 1, target serno 6  
Sep 11 08:37:39.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 8.3.1.6  
(Serial0/0) is up: new adjacency  
Sep 11 08:37:39.603: New peer 8.3.1.6 on Serial0/0  
Sep 11 08:37:39.603: Enqueuing NULL update to 8.3.1.6, flags 0x1  
Sep 11 08:37:39.611: Building unicast STARTUP packet for 8.3.1.6, serno 0-0  
Sep 11 08:37:39.611: No items in range  
Sep 11 08:37:39.615: Packetizing timer expired on Serial0/0  
Sep 11 08:37:39.615: Packets pending on Serial0/0  
Sep 11 08:37:39.615: Intf Serial0/0 startup packetized UPDATE 1-5  
Sep 11 08:37:39.615: Interface is now quiescent  
Sep 11 08:37:39.691: Packet acked from 8.3.1.6 (Serial0/0), serno 0-0  
Sep 11 08:37:39.695: Startup update acked from 8.3.1.6, serno 0-0
```

El comando *show ip interface* muestra las características de funcionamiento de las interfaces del encaminador.

R1# *show ip interface*

```

FastEthernet0/0 is up, line protocol is up
Internet address is 10.3.1.1/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

Serial0/0 is up, line protocol is up
Internet address is 8.3.1.5/30
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
-Salida truncada por brevedad-

```

INFORME

Por medio del software Configmaker de Cisco, interconecte dos redes de área local sobre las cuales corren aplicaciones TCP/IP. Utilizar dos enrutadores Cisco de la serie 1600, un enlace HDLC a 64.000 bps (bits por segundo) y el protocolo EIGRP. Interpretar los archivos de configuración generados y hacer los respectivos comentarios sobre las líneas más importantes que usted desconozca.

Explique las ventajas y desventajas de utilizar EIGRP en lugar de RIP v2.0. Compare el protocolo EIGRP con el protocolo OSPF.

EJERCICIOS DE LABORATORIO

Este ejercicio de laboratorio tiene como finalidad configurar los enrutadores R1, R2 y R3 de la red en la Figura 4.2, utilizando el protocolo de enrutamiento EIGRP. Configurar los enrutadores R1, R2 y R3 para que intercambien tablas de enrutamiento utilizando el protocolo EIGRP.

INFORMACIÓN COMPLEMENTARIA

EIGRP usa el algoritmo de actualización difusa –Diffusing Update Algorithm (DUAL)– el cual permite: que cada enrutador de la red se asegure de que su tabla de enrutamiento esté libre de bucles; que un enrutador use simultáneamente varios caminos posibles hacia un mismo destino, siempre y cuando estos caminos tengan igual métrica o costo; que cuando un camino hacia el mismo destino tenga una métrica mayor, éste quede como candidato para remplazar al mejor camino, en caso que este último falle.

En contraste con EIGRP, el problema principal con los protocolos vector distancia –RIP V1.0 e IGRP (predecesor de EIGRP)– es que estos convergen muy lentamente y tienen dificultades con los bucles de enrutamiento, dichas limitaciones se tratan a continuación.

Convergencia

Es definida como el tiempo que se requiere para que todos los enrutadores conozcan la topología de la red.

Debido a que los protocolos tipo vector distancia usan períodos temporizados para anunciar sus tablas, la convergencia es lenta, esto se agudiza cuando la red está conformada por muchos enrutadores.

A modo de ejemplo, suponiendo que se tienen las redes Net1, Net2, Net3 y Net4 interconectadas por medio de los enrutadores R1, R2 y R3, y

que se presenta un evento en el cual falla la interfaz Ethernet de R1 que se conecta a Net1 (R1 elimina a Net1 en su tabla de enrutamiento), y suponiendo también que el periodo del temporizador de R1 es de 30 segundos, entonces: R1 deberá esperar un tiempo que puede llegar a ser hasta de 30 segundos para anunciar dicho evento a R2; a su vez, cuando R2 reciba la actualización (y elimine de su tabla de enrutamiento a Net1), deberá esperar un tiempo que puede llegar a ser hasta de 30 segundos para anunciar el evento a R3 (y para que este último elimine la entrada de Net1). Como se puede apreciar, el tiempo de convergencia de esta internet puede llegar a ser de 60 segundos; tiempo que puede ser superior, si la internet es más grande, es decir, si la conforman un mayor número de encaminadores y de redes.

Actualizaciones provocadas (Triggered updates)

Un problema al usar periodos temporizados es que la convergencia es muy lenta. Para aumentar la rapidez de convergencia, algunos protocolos vector distancia usan actualizaciones provocadas. Tan pronto como se presenta un cambio en la topología, el encaminador inmediatamente difunde su tabla de enrutamiento. IGRP es un ejemplo de un protocolo de enrutamiento que usa actualizaciones provocadas. La desventaja de usar este tipo de actualizaciones se observa cuando se tiene una ruta que oscila; cada cambio en el estado de una red conectada a un encaminador causará que éste difunda su tabla de enrutamiento, creando posiblemente una tormenta de “broadcast”.

Bucles de Enrutamiento

Otro problema con los protocolos vector distancia radica en que estos son propensos a bucles de enrutamiento, lo cual básicamente consiste en un desacuerdo acerca de cómo alcanzar una red destino. La Figura 4.1 se puede utilizar para describir un caso muy simple de bucle de enrutamiento, si se supone que la Tabla 5.1 representa las entradas en la respectiva tabla de enrutamiento de R1 y R2.

Tabla 5.1 Entradas en la tabla de enrutamiento de R1 y R2

Tabla de enrutamiento de R1			Tabla de enrutamiento de R2		
Network	Next Hop	Interface	Network	Next Hop	Interface
10.3.1.0/24	Directa	E0	8.3.1.4/30	Directa	S0
10.3.2.0/24	Directa	E1	30.0.0.0/8	Directa	E0
8.3.1.4/30	Directa	S0	10.3.1.0/24	8.3.1.5	S0
30.0.0.0/8	8.3.1.6	S0	10.3.2.0/24	8.3.1.5	S0
20.0.0.0/8	8.3.1.6	S0	20.0.0.0/8	8.3.1.5	S0

En este caso el encaminador R1 cree que para alcanzar la red 20.0.0.0/8 deberá reenviar el tráfico (paquetes IP) al encaminador R2; no obstante, el encaminador R2 cree que para alcanzar la misma red (20.0.0.0/8) le debe reenviar el tráfico a R1, por lo cual se ha formado un bucle de enrutamiento.

Los protocolos vector distancia tienen ciertos mecanismos que pueden usar para resolver los bucles de enrutamiento. No obstante, dichas soluciones crean un problema adicional: los protocolos vector distancia convergen muy lentamente, en comparación con los protocolos de estado de enlace (link state), como OSPF, y con los protocolos híbridos, como EIGRP.

Conteo a infinito

Un síntoma de un bucle de enrutamiento es llamado “conteo a infinito”. En esta condición, existe un bucle de enrutamiento y cada datagrama IP con destino a la red 20.0.0.0/8 (continuando con el ejemplo anterior) quedará circulando continuamente alrededor del anillo, gastando ancho de banda y ciclos de CPU en los encaminadores que forman parte del bucle.

Para prevenir este problema, los protocolos vector distancia definen el máximo número de encaminadores (hops) que se le permite visitar a un datagrama IP. Esto asegura que, si se presentase un bucle, los datagramas IP no circularán indefinidamente. En IP, esta función la hace el campo TTL (Time-To-Live) del encabezado del datagrama IP. No obstante, este mecanismo no resuelve el problema de los bucles de enrutamiento; lo que hace es evitar que los datagramas IP circulen indefinidamente, descartándolos después de que exceden su TTL. El RIP de IP y el RIP de IPX, por defecto, permiten un máximo número de saltos (hop count) de 15, mientras que IGRP permite, por defecto, un máximo número de saltos de 100.

Para resolver los problemas de los bucles de enrutamiento, los protocolos vector distancia implementan diversas soluciones, algunas se describen a continuación.

División horizontal (Split horizon)

La primera solución, Split horizon, ayuda a resolver problemas de bucles de enrutamiento pequeñas; establece que, si un encaminador vecino (R2) envía información sobre una ruta que conoce hacia otro encaminador (R1), el encaminador que recibe la información de la ruta (R1) no debe propagarla de regreso por la misma interfaz que fue previamente recibida.

Si en la Figura 4.1 se asume que el encaminador R2 le anuncia la red 30.0.0.0/8 (la cual está conectada a su interfaz de Lan Ethernet 0) al encaminador R1 y que posteriormente la interfaz Ethernet 0 de R2 falla, se tiene que, sin split horizon en efecto, el encaminador R1 anunciaría la red

30.0.0.0/8 de regreso al encaminador R2, indicándole que para alcanzar dicha red el encaminador R2 debería enviar los datagramas IP al encaminador R1. Obviamente, de acuerdo a la topología de la Figura 4.1, esto sería imposible, puesto que solamente el encaminador R2 está conectado a la red 30.0.0.0/8. Con split horizon en efecto, el Encaminador R1 solamente anunciará al encaminador R2 las dos redes que tiene directamente conectadas (10.3.1.0/24 y 10.3.2.0/24) y que no han podido ser previamente anunciadas por el encaminador R2.

Envenenamiento de ruta (Route poisoning)

Para resolver los problemas de bucles de enrutamiento grandes, los protocolos vector distancia utilizan dos soluciones complementarias: envenenamiento de ruta y temporizadores de cuenta regresiva. El envenenamiento de ruta se deriva de split horizon, se basa en que, cuando el encaminador detecta un cambio en una entrada de la tabla de enrutamiento (por falla de una de sus interfaces), envenenará dicha entrada asignándole una métrica infinita, haciéndola muy indeseable para ser escogida. Por ejemplo, en RIP, un número de saltos de 16 es considerado como una red inalcanzable (métrica infinita); RIP permite que el tráfico tenga un máximo de 15 saltos. Cuando el encaminador comparte la ruta envenenada con los encaminadores vecinos, estos enviarán de regreso hacia el encaminador origen de la ruta envenenada un envenenamiento inverso (poison reverse). En tal circunstancia, los encaminadores que envían el envenenamiento inverso violan las reglas de split horizon. Esta violación excepcional se permite para asegurarse que todos los encaminadores reciban el cambio anunciado por el encaminador que envía la ruta envenenada.

Una ruta envenenada es una ruta que tiene asignada una métrica infinita. Las rutas envenenadas se usan para resolver problemas de bucles de enrutamiento grandes. Cuando un encaminador recibe una ruta envenenada, viola las reglas de split horizon y envía una actualización de envenenamiento inverso de regreso al origen de la ruta envenenada.

Temporizadores de cuenta regresiva (Hold down timers)

Con el propósito de que los encaminadores tengan suficiente tiempo para propagar las rutas envenenadas, y asegurarse de que no ocurran bucles inadvertidamente mientras esto está sucediendo, los encaminadores emplean un mecanismo denominado “temporizadores de cuenta regresiva” (hold-down timers), que congelan las rutas envenenadas en la tabla de enrutamiento por un periodo de tiempo específico. Este intervalo es usualmente igual a tres veces el intervalo del periodo de actualización.

Cada temporizador hará una cuenta regresiva durante la cual mantendrá congelada la ruta envenenada en la tabla de enrutamiento (con su métrica en infinito) hasta que la cuenta llegue a cero. No obstante, si el encaminador recibe una actualización de un encaminador vecino que anuncia una métrica mejor de la que tenía la ruta original antes de ser envenenada, el encaminador eliminará el temporizador y actualizará su tabla de enrutamiento con el nuevo camino hacia la red destino. Si el encaminador recibe una actualización de un encaminador vecino con una métrica peor que la de la ruta original, asumirá que este camino alterno es parte del bucle de enrutamiento, ignorará la información y continuará con el conteo regresivo. Mientras este proceso está ocurriendo, la tabla de enrutamiento en el encaminador mostrará la ruta como posiblemente caída (possibly down).

Los temporizadores de cuenta regresiva trabajan en conjunto con el envenenamiento de ruta. Con el fin de dar suficiente tiempo a una ruta envenenada para que se propague a través de la red, los encaminadores la congelan en la tabla de enrutamiento hasta que el temporizador de cuenta regresiva expire o hasta que estos aprendan un camino alterno para alcanzar el destino, siempre y cuando este camino tenga una mejor métrica que el camino original.

Ejemplo de ruta envenenada y temporizadores de cuenta regresiva

Con la finalidad de proporcionar un ejemplo sobre el funcionamiento de la ruta envenenada y los temporizadores de cuenta regresiva, se asumirá que en los encaminadores de la Figura 4.2 se está ejecutando RIP V1.0. En este caso, se asume que la red conectada al encaminador R1, la red 192.168.1.0/24, falla. Sin actualizaciones provocadas, el encaminador R1 tendrá que esperar la expiración del temporizador de actualización de enrutamiento antes de poder difundir su tabla de enrutamiento hacia los encaminadores R2 y R3. Para RIP V1.0 de IP, por defecto, este temporizador está configurado en 30 segundos. En esta circunstancia, el encaminador R1 envenenará la ruta, asignándole una métrica infinita (de 16). Cuando los encaminadores R2 y R3 reciban la ruta envenenada, enviarán de regreso al encaminador R1 un envenenamiento inverso y congelarán la ruta envenenada (en su tabla de enrutamiento) por un periodo de tiempo igual al indicado en el temporizador de cuenta regresiva (en el caso de RIP V1.0, tiene un valor de 180 segundos). Los encaminadores R2 y R3 también anunciarán a las interfaces restantes la existencia de la ruta envenenada. No obstante, para realizar dicho anuncio, tendrán que esperar a que su temporizador de actualización de enrutamiento expire (30 segundos). Al tiempo que esto ocurre, los encaminadores R2 y R3 estarán haciendo un conteo regresivo de su temporizador de cuenta regresiva.

Si otro encaminador anuncia un camino alterno para llegar a la red 192.168.1.0/24 con una métrica mayor a la que estuvo anunciando el encaminador R1 (en el caso de RIP V1.0, la métrica se basa en el número de saltos), los encaminadores R2 y R3 no utilizarán dicho anuncio hasta que expire el temporizador de cuenta regresiva, la razón: el camino anunciado puede corresponder a un bucle y no ser un camino válido. El problema con este enfoque se presenta cuando existe otro camino alterno real para alcanzar la red 192.168.1.0/24, aunque con una métrica peor, puesto que, debido a las reglas de los temporizadores de cuenta regresiva, los encaminadores R2 y R3 no pueden usar dicho camino hasta que sus temporizadores expiren.

Si en cualquier momento se restaura la conexión de la red 192.168.1.0/24 con la interfaz del encaminador R1, éste empezará a anunciar la disponibilidad de dicha red a los encaminadores R2 y R3. Por lo que la métrica que el encaminador R1 anuncia ahora para la red 192.168.1.0/24 no es peor que la de la ruta original, los encaminadores R2 y R3 inmediatamente reemplazarán la ruta envenenada con la ruta anunciada.

PROBLEMAS

- Si un commutador tiene 10 interfaces VLAN capa 3 (Vlan1 a Vlan10) con sus respectivas direcciones IP configuradas (192.168.1.1/24 para Vlan1, 192.168.2.1/24 para Vlan2, etc.), explique cuál es el resultado de los siguientes comandos:

```
SW1(config)# router eigrp 100
SW1(config-router)# network 192.168.0.0 0.0.255.255
SW1(config-router)# no auto-summary
SW1(config-router)# passive-interface default
SW1(config-router)# no passive-interface Vlan10
```

- Al configurar los temporizadores “hello intervalo” en 4 segundos y “hold time” en 12 segundos en la interfaz serial 0 ¿cuál es el resultado respecto al funcionamiento del protocolo EIGRP (con número de identificación del proceso igual a 100)?

```
R1(config)# interface Serial 0
R1(config-if)# ip hello-interval eigrp 100 4
R1(config-if)# ip hold-time eigrp 100 12
```

3. Intente configurar a R1 y R2 de la Figura 4.1 para habilitar la autenticación del protocolo EIGRP. Ayuda: el siguiente trozo de código configura la autenticación MD5 de eigrp 100 en el encaminador R1.

```
R1(config)# key chain LAB
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string laboratorio
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0
R1(config-if)# ip authentication mode eigrp 100 md5
R1(config-if)# ip authentication key-chain eigrp 100 LAB
```

4. Después de configurar las direcciones IP de las respectivas interfaces de los dos encaminadores de la Figura 4.1, y de habilitar el protocolo eigrp 100 en R1 y R2, intente configurar a R1 para que distribuya solo la ruta por defecto y suprima el resto de rutas. Ayuda: utilice el siguiente trozo de código.

```
R1(config)# interface serial 0
R1(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
R1(config-if)# end
```

GLOSARIO

Bucle de enrutamiento: es cuando se presentan inconsistencias en la información que contienen las tablas de enrutamiento, causando que un datagrama IP quede viajando en un círculo vicioso.

Convergencia: se presenta cuando todos los encaminadores de la red logran tener la misma información topológica de ella.

Enrutamiento: proceso que permite decidir la interfaz por la que se debe enviar un datagrama IP y la dirección IP del próximo equipo al que se le debe enviar.

Envenenamiento de ruta: mecanismo por el cual se asocia un costo excesivamente alto a una entrada de la tabla de enrutamiento con el propósito de evitar que dicha entrada sea considerada por el proceso de enrutamiento.

Red tipo classful: hace referencia a una red clase A (máscara 255.0.0.0), clase B (máscara 255.255.0.0) o clase C (máscara 255.255.255.0).

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOYLE, J.; CARROLL, J. (2007). *Routing TCP/IP*. 2nd Ed. Indianapolis, IN: Cisco Press. Vol. 1.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

CAPÍTULO 6

LISTAS DE ACCESO IP ESTÁNDAR

Una lista de control de acceso (Access Control List o ACL) es el método utilizado para comparar patrones de información de los diferentes protocolos de la arquitectura TCP/IP. Hay varias situaciones en la que se puede necesitar realizar esta comparación, por ejemplo, para limitar el acceso a una subred por razones de seguridad o para limitar el tamaño de las tablas de enrutamiento de un encaminador por razones de desempeño. Las listas de control de acceso se pueden aplicar de diferentes maneras. Cuando una ACL se aplica a una interfaz, dicha ACL puede diseñarse para que se acepten o rechacen datagramas IP entrantes o salientes de la misma, la aceptación o rechazo de los paquetes se puede basar en los diferentes campos de los protocolos TCP/IP. Cuando una ACL se aplica a un protocolo de enrutamiento (como RIP u OSPF), ejecutándose en un encaminador, ésta puede evitar que el encaminador envíe información de una ruta en particular. El propósito de este capítulo es presentar la lista de control de acceso IP estándar, que es una de las formas más básica de las ACL.

OBJETIVO

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

- Conocer los diferentes tipos de listas de acceso y el rango de números asignados a estas.
- Entender el procesamiento “top-down” de las listas de acceso.
- Conocer qué es una negación implícita.
- Usar los comandos de las listas de acceso.
- Usar la máscara comodín (wildcard mask) en las listas de acceso.
- Crear una lista de acceso IP estándar numerada.

- Configurar filtros de tráfico utilizando listas de acceso IP estándar numeradas.
- Activar una lista de acceso sobre una interfaz.
- Verificar la operación de las listas de acceso.

PROCEDIMIENTO

Controlando el acceso IP

Las listas de control de acceso son una de las características más versátiles de los encaminadores en general, las listas de acceso pueden realizar, entre otras, las siguientes funciones:

Filtrar tráfico

- Filtrar paquetes que intentan pasar a través del encaminador.
- Restringir acceso VTY (telnet) al encaminador.
- Filtrar información de enrutamiento intercambiada por los encaminadores.
- Activar llamadas telefónicas con DDR (Dial-on-demand routing).
- Priorizar tráfico de la red de área amplia con *priority queuing* y *custom queuing*.

Aunque la anterior lista de funciones puede seguir creciendo, el alcance de este capítulo se concentra en el primer ítem (el filtrado del tráfico TCP/IP que atraviesa un encaminador).

En términos generales, una lista de acceso consiste en un conjunto de comandos de filtro que se agrupan bajo un mismo número (el número escogido para la lista de acceso). Estos comandos definen a cuáles paquetes se les permite o se les niega el paso. Las listas de acceso se crean bajo el modo de configuración global. Para activar la lista de acceso, la cual contiene los comandos de filtrado, ésta se debe aplicar sobre un objeto físico o lógico. Por ejemplo, si se desea filtrar el tráfico que atraviesa a un encaminador, se debe aplicar la lista a una interfaz física del mismo.

Cuando se aplica una lista de acceso a una interfaz, hay dos opciones posibles:

Inbound (in): prueba solamente el tráfico que trata de entrar por la interfaz en cuestión. Con esta opción, los paquetes que entran por una interfaz son comparados inmediatamente con las sentencias de la lista antes de ser conmutados a una interfaz de salida (antes de utilizar la tabla de enruteamiento).

Outbound (out): prueba solamente el tráfico que trata de salir por la interfaz en cuestión. Con esta opción, a los paquetes que hayan sido admitidos por el encaminador (mediante otra interfaz) y commutados hacia la interfaz de salida se les aplicará la lista de acceso antes de permitirles dejar la interfaz de salida (después de haber utilizado la tabla de enrutamiento).

Especificamente, las listas de acceso IP pueden ser usadas para controlar el flujo de datagramas IP a través de las interfaces del encaminador. Después de aplicar una ACL –en el sentido de entrada o de salida de la interfaz–, ésta puede permitir o negar el paso de los datagramas IP que entran o que salen de la interfaz, es decir, antes o después de ejecutarse el procesamiento de decisión de enrutamiento. Una lista de acceso es una colección secuencial de condiciones que se aplican a las direcciones IP de un datagrama IP o a los protocolos de capa superior a IP, esto se hace con el propósito de permitir o negar el flujo de tráfico de acuerdo a los patrones que se definan en la lista.

La Tabla 6.1 indica los diferentes tipos de listas de acceso numeradas y los correspondientes números que pueden ser utilizados como identificadores de la lista.

Tabla 6.1. Tipos de listas de control de acceso numeradas, identificadas por un número

Tipo de lista de acceso	Rango numérico
ACL IP estándar	1-99
ACL IP extendida	100-199
ACL Ethernet Type Code	200-299
ACL Decnet estándar y extendida	300-399
ACL XNS estándar	400-499
ACL XNS extendida	500-599
ACL Appletalk estándar y extendida	600-699
ACL 48 bit MAC address	700-799
ACL IPX estándar	800-899
ACL IPX extendida	900-999
ACL IPX SAP	1000-1099
ACL 48 bit MAC address extendida	1100-1199
ACL IP estándar, rango expandido	1300-1999
ACL IP extendida, rango expandido	2000-2699
ACL SS7 (voz)	2700-2999

Existen dos clases de listas de control de acceso IP numeradas: la estándar y la extendida. Las listas de acceso IP estándar permiten o niegan el paso de los datagramas IP, basándose solamente en la dirección origen de

los mismos (y probablemente en la dirección destino). Las ACL estándar no tienen en cuenta el tipo de protocolo (TCP, UDP e ICMP, por ejemplo) ni el tipo de aplicación que se transporta (como telnet, e-mail, ftp o web). Asimismo, le dan igual trato a todo el tráfico dentro de una misma pila (suite) de protocolos.

En contraste, las listas de control de acceso IP extendidas proporcionan una mayor granularidad cuando se toman decisiones de filtrado. Con estas listas se pueden filtrar datagramas IP con base en: la dirección IP origen, la dirección IP destino, el protocolo específico (TCP, UDP, ICMP), los números de puerto (el puerto 23 para telnet o el puerto 25 para e-mail en aplicaciones TCP/IP), la información que contenga el protocolo (como los mensajes ICMP echo request e ICMP echo reply) y otros patrones.

Los encaminadores Cisco soportan listas de acceso IP estándar (más simples) y listas de acceso IP extendidas (más complejas y versátiles). Es importante resaltar que en la interfaz, en un mismo sentido (de entrada o de salida), solamente se puede asociar una lista de acceso en un instante dado. Una vez creada una lista de acceso, ésta se puede aplicar a varias interfaces. El rango de valores que se pueden usar para definir una lista de acceso IP estándar está entre 1 y 99.

Es de notar que el uso de las listas de acceso IP demandan un sobrecoste computacional (overhead) del procesador; esto se debe a que para cada datagrama IP procesado es necesario comparar uno o más de sus campos con cada sentencia en la lista hasta encontrar una coincidencia. Por esta razón, las listas de acceso deben usarse solamente en caso de ser estrictamente necesarias.

Las listas de acceso son procesadas desde arriba hacia abajo (top-down); esto significa que el(s) campo(s) de interés del datagrama IP se comparará(n) con la primera sentencia de la lista, y, si se presenta una coincidencia (un match) entre el contenido del datagrama IP y la(s) condición(es) de la sentencia, se aplicará la acción que se haya definido en la sentencia. Cuando se presenta una coincidencia hay dos posibles acciones que se pueden ejecutar en el datagrama IP (la acción específica se define previamente en la sentencia con la cual se buscó la coincidencia), éstas son:

- Permit: permite el paso o reenvío del datagrama IP.
- Deny: descarta el datagrama IP.

Si se presenta una coincidencia en una sentencia, las siguientes sentencias no serán procesadas. Si no se presenta una coincidencia, el encamino-dor procederá a hacer una comparación con la siguiente sentencia de la lista.

Entonces, el orden de las sentencias de la lista de acceso es muy importante: las sentencias más específicas deberán colocarse al inicio de la lista y las más generales deberán ir al final.

Cuando se crea una lista de control de acceso, ésta conservará estrictamente el orden en que sean digitadas las sentencias (mediante comandos). El orden que se le da a las sentencias es muy importante debido a que, cuando el encaminador procesa un datagrama IP, busca coincidencias en las sentencias de la lista y se detiene en la búsqueda cuando encuentra la primera coincidencia. Por lo tanto, la definición y creación de la lista debe hacerse de lo específico a lo general.

Para ilustrar lo anterior, a modo de comparación se aborda el funcionamiento de las listas 80 y 90 definidas a continuación y con las cuales se persigue el objetivo de dejar pasar todo el tráfico proveniente de los equipos de la red 172.16.0.0/16, excepto que este tráfico se origine en el equipo con dirección 172.16.0.1/16, en cuyo caso se descartará.

Lista 80:

1. Permitir todo el tráfico proveniente de los equipos de la red 172.16.0.0/16
2. Negar todo el tráfico proveniente del dispositivo de red con la dirección 172.16.0.1/16

Lista 90:

1. Negar todo el tráfico proveniente del dispositivo de red con la dirección 172.16.0.1/16
2. Permitir todo el tráfico proveniente de los equipos de la red 172.16.0.0/16

Cuando un datagrama IP enviado por el equipo 172.16.0.1/16 enfrente la lista 80, se presentará una coincidencia en la primera entrada de dicha lista (el equipo pertenece a la red 172.16.0.0/16) y, por lo tanto, se aplicará la acción de reenvío del datagrama; como resultado, la lista 80 no cumplirá la función deseada.

Cuando un datagrama IP enviado por el equipo 172.16.0.1/16 enfrente la lista 90, se presentará una coincidencia en la primera entrada de dicha lista (el equipo es el 172.16.0.1/16) y, por lo tanto, se aplicará la acción de descartar el datagrama; como resultado, la lista 90 cumplirá la función deseada. Para los otros equipos de la red 172.16.0.0/16, la coincidencia se presentará en la segunda entrada de la lista 90, la cual permitirá su reenvío.

Negación implícita

Hay una condición especial en la lista de acceso que no ha sido discutida: ¿qué pasa si ante la llegada de un paquete (datagrama IP) se procesan todas las entradas (sentencias) de una lista, pero no se presenta una coincidencia? La respuesta es que el encaminador descartará todo paquete al cual no se le presente una coincidencia. Este proceso se conoce como negación implícita (*deny implicit*). Las listas de acceso tienen una sentencia imaginaria (escondida ante nuestros ojos y ubicada al final de la lista) que descartará todo el tráfico al que no se le presente una coincidencia en alguna de las sentencias anteriores de la lista. Entonces, desde una perspectiva de sentido común, cada lista de acceso deberá tener al menos una sentencia con una acción *permit*, de otra manera, todo el tráfico será descartado.

A continuación se presentan las sugerencias y los aspectos a tener en cuenta en la definición y creación de las listas de acceso:

- El orden de las sentencias en las listas de acceso es importante.
- Las sentencias más restrictivas deben colocarse al inicio de la lista y las más generales, al final.
- El procesamiento de una lista de acceso es top-down –desde la primera hacia la última sentencia– hasta que se encuentre una coincidencia.
- Hay una negación implícita al final de cada lista que descarta todo el tráfico que no fue explícitamente permitido en las sentencias anteriores de la lista.
- Se puede tener una lista de acceso por protocolo, por interfaz, por dirección (in/out), en otras palabras, no se pueden tener dos listas de acceso IP aplicadas en la salida de la misma interfaz.
- Cada lista de acceso es diferenciada por un número y varios protocolos tienen un rango de números reservados para su uso.
- Nunca aplique una lista de acceso vacía a una interfaz; por defecto, las listas de acceso vacías dejan pasar todo el tráfico por una interfaz, pero, tan pronto como se cree la primera sentencia de la lista, la negación implícita de la lista descartará todo el tráfico que no haya sido definido en dicha sentencia.
- El encaminador no puede filtrar el tráfico con una lista de acceso cuando éste se origina dentro del mismo encaminador.

Por las condiciones anteriores se puede concluir que las listas de acceso son difíciles de entender y de implementar, no son un tema simple y pueden, fácilmente, causar problemas.

Comandos para la configuración de listas de acceso IP estándar

En esta sección se cubrirán los aspectos básicos para la configuración de una lista de acceso IP estándar y los ejemplos específicos para la creación de filtros de tráfico TCP/IP.

Tareas a realizar

Configurar parámetros de entrada en la lista

Para crear una lista de acceso IP estándar se usa el comando de configuración global *access-list*.

```
R1(config)# access-list "ACL#" permit | deny "condiciones"
```

Antes de la versión 11.2 del IOS, el usuario tenía que asignar un número a la lista de acceso (ACL#), este número identifica de manera única a la lista de acceso y agrupa las sentencias hacia una sola entidad. No obstante, a partir de la versión 11.2, se pueden dar nombres en lugar de números para usar listas de acceso con nombres o “named access-list”.

Para agrupar las sentencias en la lista de acceso se debe usar el mismo número (ACL#) en todas las sentencias que constituyan la lista de acceso. Las “condiciones” en la lista de acceso definen lo que deberá coincidir al comparar el contenido del datagrama IP para ejecutar la acción de permitir o negar.

Para IP se tiene la siguiente sintaxis:

```
R1(config)# access-list access-list-number {permit | deny} source [wildcard-mask] log
```

Descripción de los campos que acompañan al comando *access-list*:

- **Access-list-number:** un número en el rango de 1 hasta 99 para identificar la lista a la cual pertenecen las entradas.
- **Permit/deny:** indica la acción que ejecutará la entrada, en el sentido de permitir o bloquear el tráfico proveniente de la dirección especificada.
- **Source:** identifica la dirección IP origen.
- **Wildcard-mask:** “máscara de comodín”, identifica cuáles bits del campo de dirección deben tenerse en cuenta. Los bits que tengan 0 en cualquier posición deben examinarse estrictamente y los bits que tengan 1 en cualquier posición no deben examinarse (don’t care); si dicho valor se omite, éste toma por defecto el valor 0.0.0.0

Activar la lista sobre una interfaz

La lista de acceso, por sí misma, no hace nada; una vez se crea la lista, ésta se debe activar sobre una interfaz con la finalidad de que el encamino-dor empiece a filtrar el tráfico sobre dicha interfaz.

La sintaxis, en general, para asociar una lista de acceso a una interfaz, es la siguiente:

```
R1(config)# interface fastethernet 0/0  
R1(config-if)# "protocol" access-group "ACL#" in | out
```

El parámetro "*protocol*" es el protocolo que la lista de acceso filtrará, tal como IP, IPX, Appletalk, etc. Los parámetros "*in*" y "*out*" se refieren a la dirección de filtrado.

La sintaxis para asociar una lista de acceso IP estándar a una interfaz es:

```
R1(config)# interface fastethernet 0/0  
R1(config-if)# ip access-group access-list-number {in | out}
```

En la línea anterior, el comando *ip access-group* asocia una lista existente a la interfaz FastEthernet 0/0. Solo se permite una lista de acceso por protocolo para cada interfaz.

Descripción de los campos del comando *ip access-group*:

Access-list-number: indica el número que identifica la lista a ser asocia-da a la interfaz.

In/out: selecciona si la lista de acceso será aplicada a los paquetes que estén entrando o saliendo de la interfaz; al no especificar nada, el valor por defecto es "*out*" (en versiones posteriores a la 12.x del IOS hay que especificarlo).

Ejemplo 1. Permitiendo el tráfico de una dirección de red

La siguiente lista de acceso permite que solamente el tráfico proveniente de la red 172.16.0.0/16 sea despachado (reenviado) por las interfaces Ether-net 0 y Ethernet 1 del encaminador Router de la Figura 6.1, el tráfico de otras fuentes será bloqueado.



Figura 6.1 Encaminador que permite el paso solamente de datagramas IP con la dirección origen de la red 172.16.0.0/16

```
Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255 [primera entrada]
```

Siempre hay una última entrada creada por el sistema, ésta no es visible en la lista y su función es implícitamente negar el resto de condiciones que no se hayan cumplido. Similar a la siguiente línea.

access-list 1 deny 0.0.0.0 255.255.255.255 [última entrada] (equivalente a access-list 1 deny any)

```
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 1 out
```

```
Router(config)# interface ethernet 1
Router(config-if)# ip access-group 1 out
```

Nota: Una entrada en la lista con “permit o deny” puede parar el tráfico de información de los algoritmos de enrutamiento cuyo destino sea de difusión (broadcast); para solucionar dicho problema es necesario adicionar explícitamente la siguiente entrada, la cual permitirá el tráfico de broadcast:

```
ip access-list 1 permit 255.255.255.255 0.0.0.0
```

Ejemplo 2. Negando tráfico de un host específico

La siguiente lista de acceso está diseñada para bloquear el tráfico de la dirección específica 172.16.4.20 del host de la Figura 6.2 y, al mismo tiempo, permitir el resto de tráfico sobre la interfaz Ethernet 0.

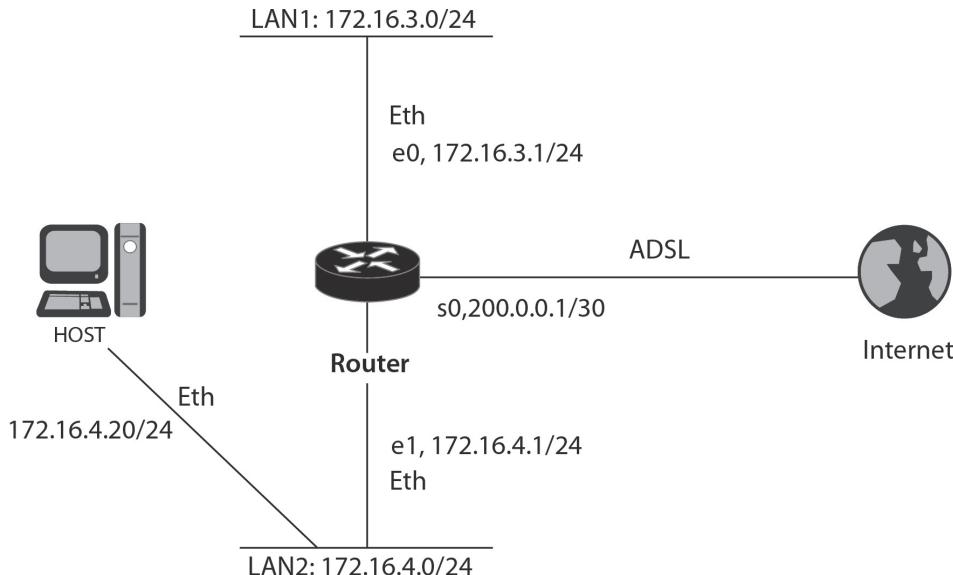


Figura 6.2 Encaminador que permite sobre la interfaz e0 todos los datagramas IP, excepto los que tengan dirección origen 172.16.4.20

```
Router(config)# access-list 2 deny 172.16.4.20 0.0.0.0 [primera entrada]
Router(config)# access-list 2 permit 0.0.0.0 255.255.255.255 [segunda entrada]
(Permite todo el tráfico incluyendo el de broadcast)
```

```
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 2
```

Ejemplo 3. Negando tráfico de una subred

Esta lista de acceso está diseñada para bloquear el tráfico proveniente de la subred 172.16.4.0 y permitir que el resto del tráfico sea despachado.

```
Router(config)# access-list 3 deny 172.16.4.0 0.0.0.255 [primera entrada]
Router(config)# access-list 3 permit 0.0.0.0 255.255.255.255 [segunda entrada]
```

```
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 3 out
```

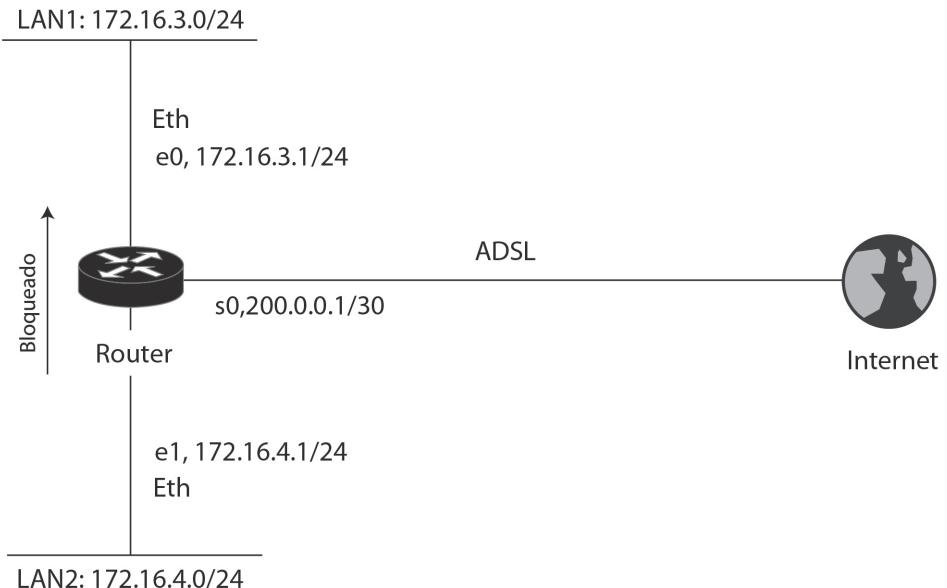


Figura 6.3 Encaminador que permite sobre la interfaz e0 todos los datagramas IP, excepto los que vengan de la red 172.16.4.0/24

Verificando las listas de acceso

El comando *show acces-list* muestra el contenido de las listas de acceso número 2 y 3.

```
Router# show access-lists
```

```
Standard IP access list 2
deny 172.16.4.20
permit 0.0.0.0, wildcard bits 255.255.255.255
Standard IP access list 3
deny 172.16.4.0, wildcard bits 0.0.0.255
permit 0.0.0.0, wildcard bits 255.255.255.255
```

El comando *show ip interface* muestra la información IP de las interfaces e indica si éstas se asocian una lista de acceso.

```
Router# show ip interface
```

```
Serial0 is up, line protocol is up
Internet address is 192.168.2.1, subnet mask is 255.255.255.0
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is 3
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP SSE switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
```

INFORME

Proponga una red en la que se controle el acceso de un equipo por medio de una lista de acceso estándar, mencione las ventajas y desventajas que se tienen al utilizar una lista de acceso estándar.

Encuentre los errores de la siguiente lista de acceso IP estándar y proponga la lista de acceso IP corregida.

```
Router(config)# access-list 1 permit 192.168.2.1
Router(config)# access-list 1 deny 192.168.2.2
Router(config)# access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)# access-list 1 deny any
Router(config)# interface serial 0/0
Router(config-if)# ip access-group 1 in
```

Encuentre los errores de la siguiente lista de acceso IP estándar y proponga la lista de acceso IP corregida.

```
Router(config)# access-list 2 deny 192.168.2.0
Router(config)# access-list 2 deny 172.20.0.0
Router(config)# access-list 2 permit 192.168.2.1
Router(config)# access-list 2 permit 0.0.0.0 255.255.255.255
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip access-group 1 out
```

EJERCICIOS DE LABORATORIO

En este ejercicio se requiere configurar una lista de acceso en el Encaminador Router_A para permitir que el telnet a dicho encaminador lo pueda realizar únicamente cualquier equipo que forme parte de la red 192.168.1.0/24. La misma restricción se desea aplicar en los encaminadores Router_B y Router_C.

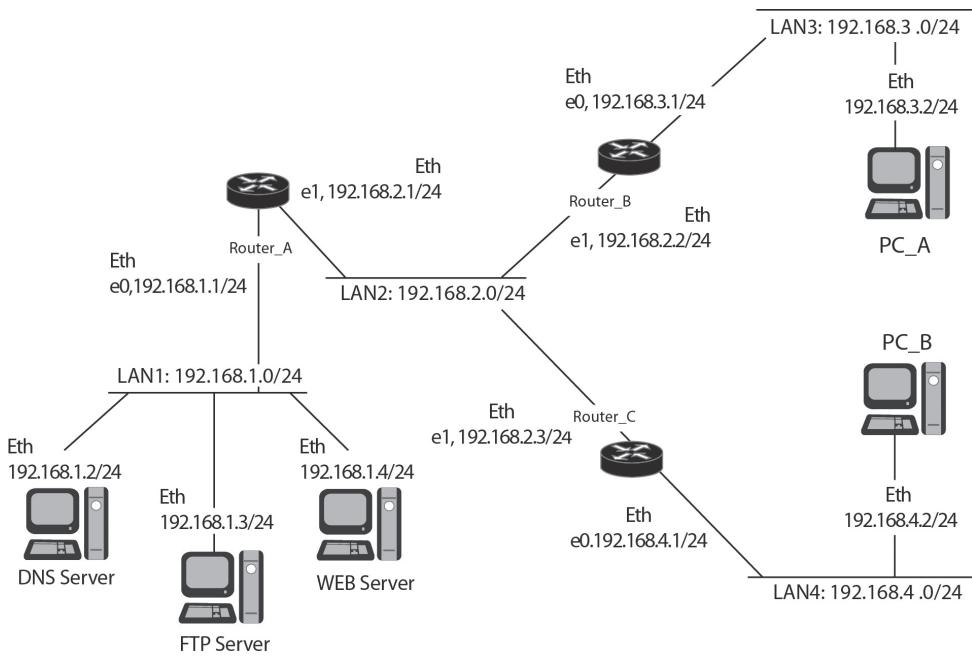


Figura 6.4 Red con listas de acceso

Procedimiento: para cumplir la primera función se debe entrar al encaminador Router_A, crear una lista de acceso IP estándar y aplicarla de la siguiente manera:

Configuración del Encaminador Router_A:

```
Router_A(config)# access-list 1 permit 192.168.1.0 0.0.0.255  
Router_A(config)# line vty 0 4  
Router_A(config-line)# access-class 1 in
```

(La misma configuración se debe aplicar a los encaminadores Router_B y Router_C).

Tareas adicionales: Verificar la configuración de los encaminadores haciendo lo siguiente:

1. Desde los PC intente hacer telnet a los encaminadores.
2. Desde cualquier encaminador, intente hacer telnet hacia otro.
3. Desde un equipo en la red 192.168.1.0/24, intente hacer telnet a los encaminadores.

Sugerencia: se puede usar GNS3 para emular los encaminadores y VPCS (Virtual PC Simulator) para simular los PC; otra posibilidad es usar Packet Tracer.

INFORMACIÓN COMPLEMENTARIA

Corrección de las entradas de una lista de acceso

Una vez construida una lista de acceso IP estándar, sus entradas no pueden ser borradas ni insertadas (las listas de acceso con nombres facilitan su edición; ver sección “Información complementaria” del capítulo 7). Si se ejecuta el comando *no access-list* para tratar de remover una sola entrada, el encaminador borrará la lista de acceso completa. Asimismo, cada comando que se digite en una lista de acceso será colocado al final de la lista. Para editar una línea de una lista de acceso es mejor visualizarla con el comando *show running-config*, pegarla a un editor de texto, corregirla en el editor de texto, desasociarla de la interfaz, copiarla desde el editor de texto hacia el encaminador y finalmente asociarla a la interfaz.

Máscara comodín (Wildcard mask)

Una máscara comodín no es una máscara de subred, tal como una dirección IP; una máscara comodín tiene una longitud de 32 bits y se usa para verificar sobre cuáles de los 32 bits de una dirección IP debe buscarse una coincidencia o simplemente ignorar dicho bit.

Un 0 en una posición de bit de la máscara comodín significa que se debe buscar coincidencia en el bit de la dirección IP que tenga la misma posición.

Un 1 en una posición de bit de la máscara comodín significa que no se debe buscar coincidencia en el bit de la dirección IP que tenga la misma posición.

Algunas veces a la máscara comodín se le denomina *máscara invertida*; cuando se desea buscar una coincidencia con una dirección de red o de subred, todo lo que se debe hacer para obtener la máscara comodín a partir de la máscara de red es: al valor 255 se le resta el valor decimal de cada octeto (byte) de la máscara de red.

Ejemplos:

- Para buscar una coincidencia con la subred 255.255.255.0 se requiere una máscara comodín de 0.0.0.255
- Para buscar una coincidencia con la subred 255.255.240.0 se requiere una máscara comodín de 0.0.15.255

Nótese que la máscara comodín se obtiene siempre de tomar el número 255 y restarle el valor que tenga la máscara de red.

Máscaras comodín especiales

La máscara comodín 0.0.0.0 establece que todos los 32 bits de la dirección del paquete deben coincidir con la dirección especificada en la sentencia, por ejemplo, el valor **172.16.1.1 0.0.0.0** representa una condición en la cual, por medio de la máscara comodín, se requiere que la dirección del paquete sea exactamente igual a **172.16.1.1** para que haya una coincidencia. La expresión **172.16.1.1 0.0.0.0** puede ser remplazada en el comando por la expresión **host 172.16.1.1**.

La máscara comodín 255.255.255.255 realiza la función opuesta a la máscara comodín 0.0.0.0. Es decir, con 255.255.255.255 no se requiere coincidencia en ningún bit de la dirección del paquete y, como consecuencia, cualquier dirección en el paquete dará una coincidencia. Normalmente el valor 0.0.0.0 255.255.255.255 sirve en una sentencia para tener una coincidencia, independientemente de la dirección del paquete, pues, aunque obviamente no existen paquetes con una dirección IP de 0.0.0.0, el valor de cualquier dirección que tenga el paquete coincidirá si la máscara comodín fuera 255.255.255.255. La expresión **0.0.0.0 255.255.255.255** puede ser reemplazada en el comando por la expresión **any**.

PROBLEMAS

1. Al aplicar una lista de control de acceso como salida en la interfaz de un encaminador (mediante el comando *ip access group número-de-lista out*) se presenta una peculiaridad de la cual se debe estar consciente: el comando no filtra los datagramas IP que se originan en el encaminador mismo. Verifique dicha peculiaridad.
2. Las listas de acceso permiten que sus expresiones o sentencias queden comentadas en el archivo de configuración para aclarar lo que hacen. Verifique esta característica con el siguiente código.

```
R1(config)# ip access-list standard ACL-COMENTADA
R1(config-std-nacl)# remark Impide el paso de uno de los equipos de la red 192.168.1.0
R1(config-std-nacl)# deny host 192.168.1.2
R1(config-std-nacl)# permit 192.168.1.2 0.0.0.255
R1(config-std-nacl)# permit any
R1(config-std-nacl)# end
```

GLOSARIO

Coincidencia (match): se presenta cuando los campos de un datagrama IP (incluido el campo de datos) cumplen las condiciones definidas en una línea de la lista de control de acceso IP.

Host: estación de trabajo, computador, servidor, portátil, impresora que se encuentra conectado(a) como sistema final de una red IP.

Máscara comodín (wildcard mask): cadena de 32 bits, los cuales determinan la posición de los bits de la dirección IP que se deben tener en cuenta (bits del comodín puestos en cero) y de los que no se deben tener en cuenta (bits del comodín puestos en uno). Generalmente, su valor se representa con notación punto decimal, similar a la representación de una dirección IP o a la representación de la máscara de subred.

Pila: es el conjunto de protocolos definidos en la arquitectura TCP/IP. Por ejemplo, los protocolos IP, TCP, UDP, DHCP, etc. son algunos de los que conforman la pila TCP/IP.

Sobrecosto computacional: cualquier procesamiento computacional adicional que se haga por encima del requerido en condiciones normales.

Top-down: procesamiento ordenado y secuencial que se realiza con las sentencias que conforman la lista de control de acceso; siempre se inicia con la primera sentencia y, en caso de no encontrar una coincidencia, se conti-

núa con la siguiente. Este proceso se repite hasta encontrar una coincidencia o hasta llegar al final de la lista.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- SEDAYAO, J. (2001). *Cisco IOS Access Lists*. Sebastopol, CA: O'Reilly.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

LISTAS DE ACCESO IP EXTENDIDAS

Comparadas con las listas de control de acceso (ACL) estándar, las listas de control de acceso extendidas son más flexibles y tienen un mayor potencial de aplicación en la configuración de los equipos de una red. En general, las listas de control de acceso revisten mucha importancia debido a que la implementación de una red medianamente compleja hace necesario su uso. Cisco tiene diferentes clases de ACL, las más comunes son las listas de control de acceso numeradas, un subconjunto perteneciente a ellas son las listas de control de acceso extendidas, las cuales dan soporte al protocolo TCP/IP; en este capítulo se aborda el estudio y manejo de estas últimas.

Es importante indicar que existen otros tipos de listas de acceso, también de mucha importancia: listas de acceso con nombres, listas de acceso reflexivas, listas de acceso de tiempo, listas de acceso basadas en el contexto (Context-Based Access Control) y listas de acceso para limitar velocidad. Algunas de ellas se abordan en la sección de “Problemas”.

OBJETIVO

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

- Diferenciar las listas de control de acceso estándar de las listas de control de acceso extendidas.
- Configurar filtros de tráfico utilizando la lista de acceso IP extendidas.

PROCEDIMIENTO

Controlando el acceso IP

Las listas de control de acceso IP estándar permiten realizar una configuración rápida, presentando un bajo sobrecosto (overhead) en la función de limitar el tráfico con base en la dirección IP origen. Las listas de acceso extendidas proporcionan un mayor grado de control, permitiendo crear filtros basados en: la dirección IP origen y destino, los tipos de protocolos (tal como IP, TCP, UDP, ICMP, etc.) y los números de puerto usados por las aplicaciones. Estas características hacen posible limitar el tráfico con base en el uso que se le de a la red.

Para que un datagrama IP (paquete) cumpla las diferentes condiciones configuradas en una línea (o expresión) de una lista de acceso, y mediante dicha línea se pueda permitir o negar el tránsito del paquete, es necesario que cada condición que se coteje en dicha línea coincida (haga match) con el respectivo campo del paquete. Tan pronto como el paquete no cumpla una condición de la línea, se pasa a comparar las condiciones de la próxima línea de la lista de acceso frente a los respectivos campos del paquete.

La lista de acceso extendida tiene la capacidad de revisar: la dirección IP origen, la dirección IP destino y diferentes opciones que dependan del protocolo seleccionado.

Comandos para la configuración de listas de acceso IP extendidas

Tareas a realizar:

Configurar parámetros de entrada en la lista

Una de las mayores diferencias entre la lista de acceso IP estándar y la lista de acceso IP extendida es que en la última se puede especificar tanto la dirección IP origen como la dirección IP destino. A diferencia de la lista de acceso IP estándar, en la de acceso IP extendida, el “comodín” (wildcard) no es opcional. A continuación se presenta la sintaxis y se describen los parámetros de este comando en mayor detalle.

```
R1(config)#  
access-list access-list-number {permit | deny} {protocol | protocol keyword}  
{source address with wildcard mask | any} [{"operator"} {"source port number"}]  
{destination address with wildcard mask | any} [{"operator"} {"destination port number"}]  
[established] [log]
```

Descripción de los parámetros del comando *access-list*:

Access-list-number: se escoge un número en el rango de 100 hasta 199 para identificar la lista de acceso IP extendida (que contiene una o más entradas).

Permit/deny: especifica la acción que se ejecutará sobre el paquete (permitir o bloquear su paso), en caso que éste cumpla las condiciones definidas en la línea.

Protocol | protocol keyword: define el protocolo que se desea comparar en el paquete. Estos protocolos incluyen a: ip, icmp, tcp, udp, igrp, eigrp, igmp, ipinip, nos, ospf, gre.

Source address y destination address: identifican las direcciones IP origen e IP destino del paquete, respectivamente.

Source wildcard mask y destination wildcard mask: identifican cuáles bits del campo de dirección deben tenerse en cuenta. Los bits que tengan 0 en cualquier posición deben examinarse estrictamente y los bits que tengan 1 en cualquier posición no deben examinarse (no importan).

Any(opcional): Se utiliza como abreviación de “0.0.0.0 255.255.255.255” para los parámetros: “source address”, “source wildcard mask”, “destination address” y “destination wildcard mask”.

Operator: Para los protocolos TCP y UDP. En la expresión se puede especificar el número del puerto o, algunas veces, el nombre del mismo. Cuando se requiere buscar una coincidencia sobre un puerto, es necesario utilizar un operador. El propósito del operador es proporcionar alguna flexibilidad sobre el(los) número(s) de puerto(s) que se desea(n) hacer coincidir. Los operadores válidos son:

- lt less than (menor que)
- gt greater than (mayor que)
- neq not equal to (no igual a)
- eq equal to (igual a)
- range range of port numbers (rango)

Port number y message type: La información referente al protocolo puede dividirse en dos áreas: números de puerto (“port Lumber” para los protocolos TCP y UDP) y tipos de mensajes (“message type” para otros protocolos, incluyendo a ICMP). Para los números de puerto de TCP y UDP, se puede usar el número de puerto reservado para la aplicación como, por ejemplo, el 21 para telnet, o se puede usar el nombre de la aplicación, como *ftp* para el puerto 21. ICMP no usa números de puerto, en su lugar, usa tipos de mensajes (esto reemplaza los parámetros *operator* y *port number* usados en TCP y UDP). Si en una expresión de la lista de acceso IP extendida se

omite el *port number* (para TCP o UDP), o el *message type* (para ICMP), significa que se acepta cualquier puerto o tipo de mensaje del paquete.

Established: verifica si el datagrama IP forma parte de una conexión TCP previamente establecida, es decir, si el segmento TCP tiene el bit ACK o el bit RST en uno. Esta opción tiene aplicación en situaciones en las que desde una red privada se establecen conexiones hacia Internet y se quiere permitir solamente el tráfico de respuesta a dichas conexiones.

Es importante recordar que cada lista de control de acceso (ACL) tiene una línea implícita tipo “*deny all*” al final de la lista. Como consecuencia, si no se presenta una coincidencia (match) con las líneas explícitamente definidas, el paquete será bloqueado.

A modo de ejemplo, a continuación se explican las listas de acceso IP extendida número 100 y 101.

Lista de acceso número 100

```
access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established log  
access-list 100 permit udp any host 172.16.1.1 eq dns log  
access-list 100 permit tcp 172.17.0.0 0.0.255.255 host 172.16.1.2 eq telnet log  
access-list 100 permit icmp any 172.16.0.0 0.0.255.255 echo-reply log  
access-list 100 deny ip any any log
```

```
Router(config)# interface ethernet 0  
Router(config-if)# ip access-group 100 in
```

En la primera línea de la lista de acceso IP extendida se establece que cualquier sesión TCP que venga desde cualquier dirección IP con destino a la red 172.16.0.0/16 será permitida, siempre y cuando el encabezado TCP tenga el bit ACK o el bit RST puesto en uno; adicionalmente, cualquier coincidencia con esta sentencia será impresa en la consola del encaminador. Otra observación de este comando es que no tiene especificado los números de puerto, esto significa que todos los puertos serán incluidos y que cualquier valor en el número del puerto será aceptado como coincidencia.

La segunda línea de la lista de acceso IP extendida establece que permitirá una operación de búsqueda DNS (DNS lookup) proveniente de cualquier dirección IP con destino al servidor DNS con dirección IP 172.16.1.1.

La tercera línea permite tener conexiones telnet provenientes de la red 172.17.0.0/16, siempre y cuando la dirección destino sea 172.16.1.2; este comando restringe a que se haga telnet solamente a la máquina 172.16.1.2.

La cuarta línea permite respuestas de un mensaje ping, siempre y cuando la dirección IP destino pertenezca a la red 172.16.0.0/16. Esta sentencia no permite solicitudes de ping (echo-request).

La quinta línea no es necesaria debido a la negación implícita (implicit deny) que hay al final de cada lista de acceso. No obstante, los paquetes que no coincidan con las primeras cuatro líneas serán registrados en la consola mediante esta quinta línea (debido al parámetro “log”).

Lista de acceso número 101

```
access-list 101 permit tcp host 199.199.199.1 200.200.200.1 eq dns
access-list 101 permit udp any host 200.200.200.1 eq dns
access-list 101 permit tcp any host 200.200.200.2 eq www
access-list 101 permit icmp any 200.200.200.0 0.0.0.255
access-list 101 permit tcp any host 200.200.200.3 eq smtp
access-list 101 permit udp any any eq rip
```

```
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 in
```

1. La primera línea de la lista de acceso número 101 establece que se permite la transferencia de zona DNS desde el servidor DNS 199.199.199.1 hacia el equipo 200.200.200.1.
2. La segunda línea permite una solicitud de búsqueda DNS desde cualquier dirección IP hacia el servidor DNS con dirección IP 200.200.200.1.
3. La tercera sentencia de la lista 101 permite cualquier conexión web, siempre y cuando dicho tráfico tenga como destino la dirección IP 200.200.200.2; restringe que el tráfico web tenga como destino a la máquina 200.200.200.2.
4. La cuarta sentencia permite cualquier tipo de mensaje ICMP, siempre y cuando tenga como destino un equipo cuya dirección IP se encuentre en la red 200.200.200.0/24.
5. La quinta sentencia permite el tráfico correspondiente al correo electrónico, siempre y cuando éste tenga como destino al servidor de correo cuya dirección es 200.200.200.3.
6. La sexta sentencia permite el tráfico del protocolo de enrutamiento RIP IP (desde cualquier encaminador vecino RIP).

Activar la lista sobre una interfaz:

```
R1(config-if)# ip access-group access-list-number {in | out}
```

El comando *ip access-group* asocia una lista existente a una interfaz. Sólo se permite una lista de acceso por protocolo para cada interfaz.

Descripción de los parámetros del comando *ip access-group*:

Access-list-number: indica el número de la lista a ser asociado a la interfaz.

In/out: selecciona si la lista de acceso será aplicada a los paquetes que entran o salen de la interfaz; cuando no se especifica este parámetro, por defecto es out.

Protocolos que se pueden configurar con la lista de acceso IP extendida

Para la pila de protocolos TCP/IP, los diferentes protocolos que pueden servir como parámetros del filtro son:

```
R1(config)# access-list 101 permit ?
```

<0-255>	An IP protocol number
dvmrp	DVMRP IP over IP encapsulation
gre	Cisco's GRE tunneling
icmp	Internet Control Message Protocol
igmp	Internet Gateway Message Protocol
igrp	Cisco's IGRP routing protocol
ip Internet	Protocol
nos	KA9Q NOS compatible IP over IP tunneling
tcp	Transmission Control Protocol
udp	User Datagram Protocol

Por ejemplo, si se escoge ICMP, las opciones son las siguientes:

```
R1(config)# access-list 101 permit icmp any any ?
```

<0-255>	ICMP message type
administratively-prohibited	Administratively prohibited
alternate-address	Alternate address
conversion-error	Datagram conversion
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo (ping)
echo-reply	Echo reply
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachab	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
log	Log matches against this entry
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Net redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Net unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present

En otro caso, si se escoge TCP, entonces las opciones son las siguientes:

```
R1(config)# access-list 101 permit tcp any any eq ?
```

<0-65535>	Port number
bgp	Border Gateway Protocol (179)
chargen	Character generator (19)
cmd	Remote commands (rcmd, 514)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name Service (53)
echo	Echo (7)
exec	Exec (rsh, 512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (used infrequently, 20)
gopher	Gopher (70)
hostname	NIC hostname server (101)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
login	Login (rlogin, 513)
lpd	Printer service (515)
nntp	Network News Transport Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
smtp	Simple Mail Transport Protocol (25)
sunrpc	Sun Remote Procedure Call (111)
syslog	Syslog (514)
tacacs	TAC Access Control System (49)
talk	Talk (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nickname (43)
www	World Wide Web (HTTP, 80)

Finalmente, cuando se escoge UDP, las opciones son las siguientes:

```
R1(config)# access-list 102 permit udp any any eq ?
```

<0-65535>	Port number
biff	Biff (mail notification, comsat, 512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (69)
discard	Discard (9)
dnsix	DNSIX security protocol auditing (195)
domain	Domain Name Service (DNS, 53)
echo	Echo (7)
mobile-ip	Mobile IP registration (434)
nameserver	IEN116 name service (obsolete, 42)
netbios-dgm	NetBios datagram service (138)
netbios-ns	NetBios name service (137)
ntp	Network Time Protocol (123)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs	TAC Access Control System (49)
tftp	Trivial File Transfer Protocol (69)
time	Time (37)
who	Who service (rwho, 513)
xdmcp	X Display Manager Control Protocol (177)

***Ejemplo 1. Firewall que permite acceso a Internet
y tráfico de correo electrónico***

En este ejemplo, la red 128.88.3.0/24 (clase B) de la Figura 7.1 es una red desprotegida que no tiene restricción en comunicarse con Internet. Para proteger la red a la izquierda de Router1 (red 172.16.0.0) se crea un filtro en la interfaz Ethernet 1 del Router1, de tal manera que los equipos de la red protegida puedan iniciar cualquier tipo de sesión hacia la red desprotegida y hacia Internet, pero impidiendo que desde la parte derecha de Router1 se pueda iniciar cualquier tipo de sesión hacia la red protegida (intranet), con excepción del equipo 128.88.3.2, el cual puede iniciar una sesión de correo electrónico hacia la red protegida.

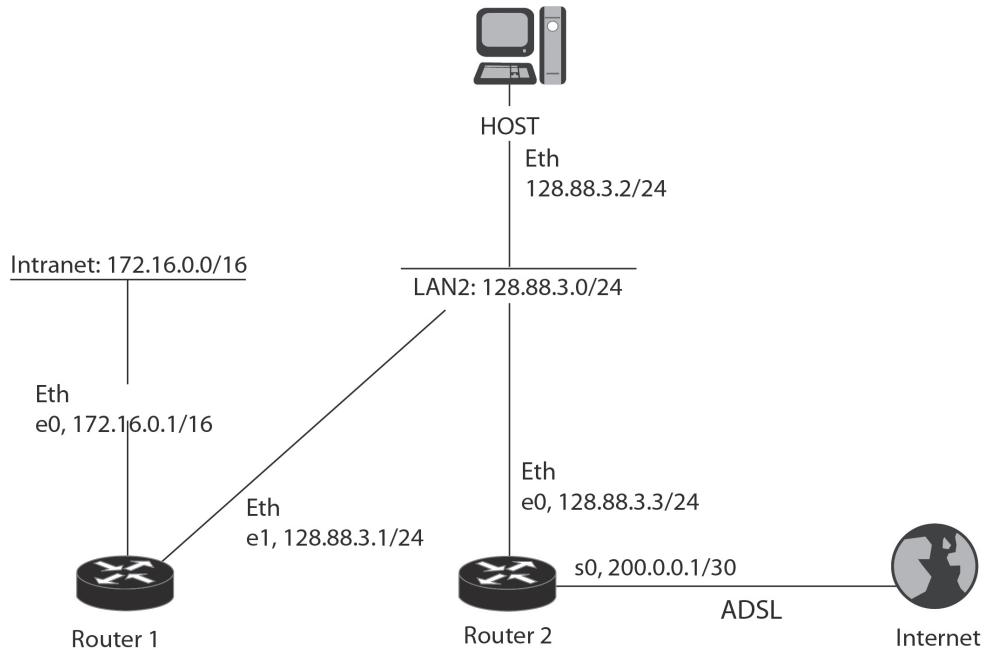


Figura 7.1 El Router1 permite iniciar cualquier tipo de sesión desde la intranet, pero solamente permite tráfico de correo electrónico desde el equipo 128.88.3.2/24 (HOST) hacia la intranet

```
Router1(config)# access-list 103 permit tcp any 172.16.0.0 0.0.255.255 established  
Router1(config)# access-list 103 permit tcp host 128.88.3.2 172.16.0.0 0.0.255.255 eq smtp
```

```
(config)# (access-list 103 deny 0.0.0.0 255.255.255.255) o access-list 103 deny any  
(niega todo implícitamente, creada por el sistema, no está visible en la lista)
```

```
Router1 (config)# interface ethernet 1  
Router1 (config-if)# ip access-group 103 in
```

Ejemplo 2. Permitir acceso a Internet, correo, DNS y PING

En este ejemplo, el Router1 de la Figura 7.2 permite que desde cualquier equipo de la red 172.16.0.0/16 (clase B) se pueda iniciar una o más sesiones hacia Internet y que dichos equipos, en consecuencia, puedan recibir los datagramas IP correspondientes a sus respectivas sesiones. También se permite: el servicio de correo electrónico SMTP bajo TCP; el servicio DNS bajo los protocolos TCP y UDP, y el mensaje PING bajo el protocolo ICMP.

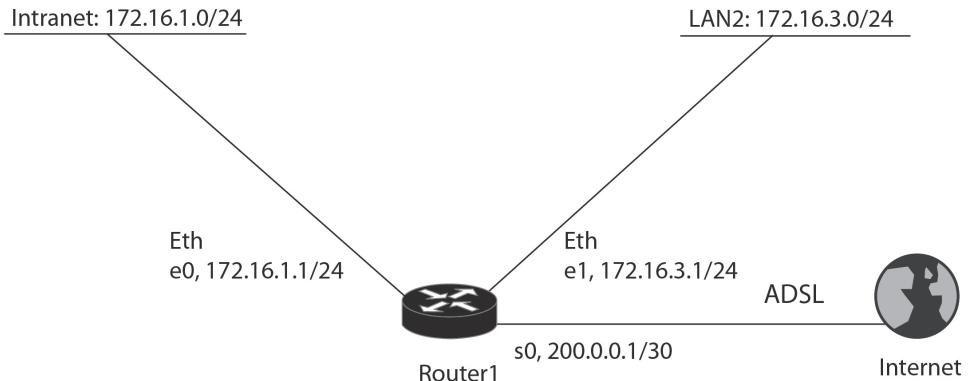


Figura 7.2 El Router1 permite iniciar cualquier tipo de sesión desde la red 172.16.0.0/16 hacia Internet, pero solamente permite tráfico SMTP, DNS y PING desde Internet

```
Router1(config)# access-list 104 permit tcp any 172.16.0.0 0.0.255.255 established
Router1(config)# access-list 104 permit tcp any 172.16.0.0 0.0.255.255 eq smtp
Router1(config)# access-list 104 permit tcp any 172.16.0.0 0.0.255.255 eq domain
Router1(config)# access-list 104 permit udp any 172.16.0.0 0.0.255.255 eq domain
Router1(config)# access-list 104 permit icmp any 172.16.0.0 0.0.255.255 echo
Router1(config)# access-list 104 permit icmp any 172.16.0.0 0.0.255.255 echo-reply
```

Router1(config)# (access-list 104 deny 0.0.0.0 255.255.255.255) o *access-list 104 deny any* (Niega todo implícitamente, no está visible en la lista)

```
Router1(config)# interface serial 0
Router1(config-if)# ip access-group 104 in
```

INFORME

El programa Configmaker de Cisco tiene un tutorial de EasyIP y NAT que se recomienda leer con atención. Una vez hecho lo anterior, use el software Configmaker de Cisco para interconectar una intranet con la Internet global; utilizando un Firewall con EasyIP y NAT. Revise el archivo de configuración generado y haga los respectivos comentarios acerca de las líneas de configuración que determinan el funcionamiento de EasyIP y NAT.

EJERCICIOS DE LABORATORIO

En este ejercicio se requiere configurar una lista de acceso numerada en el encaminador Router_A de la Figura 6.4 para obtener lo siguiente:

- Cualquier equipo estará en capacidad de realizar una solicitud DNS al servidor DNS de la red 192.168.1.0/24.
- Cualquier equipo de la red 192.168.3.0/24 estará en capacidad de acceder al servidor Web de la red 192.168.1.0/24.
- Solamente el PC_B podrá hacer FTP al servidor de FTP de la red 192.168.1.0/24.
- Cualquier equipo de la red 192.168.1.0/24, incluyendo al encaminador Router_A, será capaz de hacer ping a cualquier equipo del lado derecho de la red y recibir respuestas (echo-reply) de los equipos destinos.

INFORMACIÓN COMPLEMENTARIA

Ubicación de las listas de acceso

La ubicación del equipo de red seleccionado para aplicarle una lista de acceso específica, es crítica. Las listas de acceso IP estándar deberán colocarse tan cerca del destino como sea posible. En contraste, las listas de acceso IP extendidas deberán colocarse tan cerca del origen como sea posible.

Listas de acceso con nombres

La versión 11.2 o superior del IOS de Cisco soporta las nuevas “listas de acceso con nombres” (named access lists). La limitación de las “listas de acceso numeradas” tradicionales consiste en que el máximo número de listas que se pueden configurar es 100. La ventaja de usar “listas de acceso con nombres” es que éstas no tienen la anterior limitación. Además, proporcionan un poco más de control en el proceso de edición de la lista: se puede borrar una entrada de la lista; no obstante, no puede insertarse ni modificarse individualmente una entrada en la lista. Las “listas de acceso con nombres” son soportadas para los protocolos IP e IPX en la versión 11.2 del IOS.

Crear Listas de acceso con nombres

Para crear una lista de acceso con nombres, se usa el siguiente comando en modo de configuración global:

```
Router(config)# ip | ipx access-list standard | extended "name of the list"
```

El nombre de la lista (“name of list”) debe ser único para cada lista de acceso configurada dentro del encaminador. Al ejecutarse el comando de la “lista de acceso con nombres”, el sistema cambia el indicador (prompt) al modo de configuración de lista de acceso:

```
Router(config-std-acl)#
-o-
Router(config-ext-acl)#
```

En este modo se pueden digitar los comandos para construir las sentencias de la lista de acceso, tal como se hace con las “listas de acceso numeradas”, pero omitiendo la palabra *access-list* y el número de la lista de acceso (ACL#).

Activando una Lista de acceso con nombres

Para aplicar una lista de acceso con nombres, se usa el siguiente comando en la interfaz sobre la que se desea aplicar:

```
Router(config)# interface "type" "port #"
Router(config-if)# ip access-group "name of list" in |out
```

La única diferencia entre activar una “lista de acceso nombrada” y “una lista de acceso numerada” sobre la interfaz es que con la primera se debe especificar el nombre que la identifica, mientras que con la segunda se especifica el número que la identifica.

A continuación se ilustra cómo construir una “lista de acceso nombrada”:

```
Router(config)# ip access-list extended no_entrar
Router(config-ext-acl)# permit tcp any 172.16.0.0 0.0.255.255 established log
Router(config-ext-acl)# permit udp any host 172.16.1.1 eq dns log
Router(config-ext-acl)# permit tcp 172.17.0.0 0.0.255.255 host 176.16.1.2 eq telnet log
Router(config-ext-acl)# permit icmp any 172.16.0.0 0.0.255.255 echo-reply log
Router(config-ext-acl)# deny ip any any

Router(config)# interface ethernet 0
Router(config-if)# ip access-group no_entrar in
```

PROBLEMAS

1. Analice y pruebe la operación de la ACL 105, la cual tiene el propósito de registrar el número de sesiones telnet que transitan por la interfaz serie 0/0 de un encaminador R1. Para confirmar el número de sesiones establecidas, usar el comando *show access list 105*.

```
R1(config)# access-list 105 permit tcp any any eq telnet syn log  
R1(config)# access-list 105 permit tcp any any eq telnet  
R1(config)# access-list 105 permit ip any any  
R1(config)# interface serial0/0  
R1(config-if)# ip access-group 105 in
```

2. Analice y pruebe la operación de las listas de acceso extendidas “ICMP-SALIENTE” e “ICMP-ENTRANTE” aplicadas a la interfaz serial 0/0 de R1. La lista de acceso “ICMP-SALIENTE” crea la regla reflejada “REGLA-ICMP-REFLEJADA” cuando salen paquetes ICMP por la interfaz serie 0/0 de R1, dicha regla dura 10 segundos. La lista de acceso “ICMP-ENTRANTE” hace uso de la expresión “evaluate REGLA-ICMP-REFLEJADA” para permitir solamente los mensajes ICMP entrantes que respondan a los mensajes ICMP salientes.

```
R1(config)# ip access-list extended ICMP-SALIENTE  
R1(config-ext-nacl)# permit icmp any any reflect REGLA-ICMP-REFLEJADA timeout 10  
R1(config-ext-nacl)# permit ip any any  
R1(config-ext-nacl)# exit  
R1(config)# ip access-list extended ICMP-ENTRANTE  
R1(config-ext-nacl)# evaluate REGLA-ICMP-REFLEJADA  
R1(config-ext-nacl)# deny icmp any any log  
R1(config-ext-nacl)# permit ip any any  
R1(config-ext-nacl)# exit  
R1(config)# interface Serial0/0  
R1(config-if)# ip access-group ICMP-SALIENTE out  
R1(config-if)# ip access-group ICMP-ENTRANTE in
```

3. Analice y pruebe la operación de la lista de acceso extendida NO-NAVIGAR, la cual tiene en cuenta la hora del día y el día de la semana. Dicha lista se aplica a la interfaz FastEthernet 0/0 de R1. ¿Cuáles aplicaciones se prohíben en el horario LABORAL?

```
R1(config)# time-range LABORAL
R1(config-time-range)# periodic weekdays 8:00 to 18:00
R1(config-time-range)# exit
R1(config)# ip access-list extended NO-NAVEGAR
R1(config-ext-nacl)# deny tcp any any eq 80 23 25 time-range LABORAL
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface FastEthernet0/0
R1(config-if)# ip access-group NO-NAVEGAR in
```

4. ¿Cuál es la diferencia de usar la expresión A o la expresión B en una lista de acceso extendida?

- A. R1(config-ext-nacl)# permit tcp any any match-all +syn
- B. R1(config-ext-nacl)# permit tcp any any match-any +syn

5. ¿Cuál es el propósito de la lista de acceso “LISTA-IPV6” definida a continuación? ¿Cuál es la diferencia en la sintaxis que usa la lista de acceso “LISTA-IPV6” respecto a la sintaxis de una lista IPv4 tradicional?

```
R1(config)# ipv6 access-list LISTA-IPV6
R1(config-ipv6-acl)# permit ipv6 AAAA:1::/64 any
R1(config-ipv6-acl)# exit
R1(config)# interface FastEthernet0/0
R1(config-if)# ipv6 traffic-filter LISTA-IPV6 in
R1(config-if)# exit
```

GLOSARIO

Bit ACK: indica acuse de recibo del segmento TCP. Este bit es usado en conjunto con el campo “Acknowledge number” del segmento TCP para que un extremo de la conexión TCP confirme positivamente la recepción continua del flujo de datos e indique al otro extremo la secuencia del próximo octeto que está esperando.

Bit RST: indica el cierre abrupto de la conexión TCP.

Coincidencia (match): se presenta cuando los campos de un datagrama IP (incluido el campo de datos) cumplen las condiciones definidas en una línea de la lista de control de acceso IP.

Comodín (del término wildcard): cadena de 32 bits que determinan la posición de los bits de la dirección IP que se deben tener en cuenta (bits

del comodín puestos en cero) y la posición de los bits de la dirección IP que no se deben tener en cuenta (bits del comodín puestos en uno). Generalmente, su valor se expresa con un número de notación punto decimal, similar a la representación de una dirección IP o a la representación de la máscara de subred.

Línea: hace referencia a las condiciones definidas en una expresión o sentencia de una lista de control de acceso.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- SEDAYAO, J. (2001). *Cisco IOS Access Lists*. Sebastopol, CA: O'Reilly.

CAPÍTULO 8

REDES DE ÁREA AMPLIA Y TECNOLOGÍAS DE ACCESO: RETRANSMISIÓN DE TRAMAS, ATM, ADSL Y CABLE

Los encaminadores pueden utilizar diversas tecnologías de red de área amplia y de acceso con el propósito de interconectar las redes de área local y extender su alcance, conformando un sistema completamente unificado que se basa en el protocolo IP. En este capítulo se aborda el protocolo de retransmisión de tramas (Frame Relay), que es un protocolo maduro que está siendo ampliamente reemplazado por el protocolo de conmutación de etiquetas (MPLS: Multiprotocol Label Switching). Al abordar el protocolo de retransmisión de tramas, se revisa el concepto de circuito virtual permanente o PVC.

En la sección “Información complementaria”, se discute la configuración básica de un encaminador para el uso de las tecnologías ATM, ADSL (Asymmetric Digital Subscriber Line) y de Cable. El estudio de la tecnología MPLS queda por fuera del alcance de este libro por lo amplio del tema; para tener una descripción detallada de MPLS y de sus características, se recomienda el texto *MPLS Fundamentals* de Luc De Ghein (Cisco Press).

OBJETIVO

Al finalizar la presente unidad, el estudiante estará en capacidad de:

- Configurar la interfaz serie del encaminador para que opere usando el protocolo Frame Relay.
- Monitorear la operación del protocolo Frame Relay en el encaminador.
- Configurar un encaminador en escenarios básicos que demanden su conexión a las tecnologías ATM, ADSL y Cable módem.

PROCEDIMIENTO

Configuración del protocolo de retransmisión de tramas –Frame Relay– *Términos y características claves de Frame Relay*

Frame Relay funciona en las dos capas inferiores del modelo OSI –capa física y capa de enlace– y tiene algunas características en común con las tecnologías de WAN antiguas como X.25, en el sentido de permitir que varios circuitos transitén por un solo enlace físico, en este caso, multiplexa dichos circuitos a nivel de la capa 2 del modelo OSI. A diferencia de X.25, Frame Relay ofrece un servicio más fluido, permitiendo obtener altas velocidades de transferencia gracias a que proporciona un servicio no confiable –sin control de error, sin reconocimientos y sin control de flujo entre los nodos intermedios– basado en la filosofía del mejor esfuerzo. Frame relay asume que el medio de transmisión es altamente confiable y que los errores marginales y el control de flujo serán problemas resueltos por los protocolos superiores de los sistemas finales.

Frame Relay es un servicio de enlace de datos principalmente orientado a la conexión, y por su alto desempeño es muy adecuado para interconectar redes LAN a través de una red WAN. Los encaminadores se comportan como DTE y se conectan directamente a los nodos de conmutación Frame Relay de la WAN, los cuales se comportan como DCE.

Particularmente, en el caso de que un encaminador proporcione comunicación local de los DLCI (Data link connection identifiers) sobre sus interfaces seriales Frame Relay, estas interfaces se deben especificar como DCE.

Frame Relay opera principalmente sobre circuitos virtuales permanentes (PVC), esto significa que las conexiones son estáticas y que la operación de dichos circuitos se logra mediante un comando de configuración. Múltiples PVC pueden interconectar diferentes DTE a sus destinos a través de la infraestructura física de la red Frame Relay. El “identificador de conexión de enlace de datos”, o DLCI, identifica a cada PVC, proporcionando con esto un mecanismo de direcciones que permite conectar los encaminadores que operan en modo Frame Relay a un servicio de WAN Frame Relay.

La interfaz de administración local o LMI (Local Management Interface) hace referencia general al procesamiento adicional requerido para establecer y mantener las diferentes conexiones entre el encaminador y el nodo Frame Relay (también denominado switch Frame Relay). Ésta mantiene información relativa al establecimiento de los PVC, a las solicitudes de estado, al intercambio de “keepalives” y a la utilización de los DLCI.

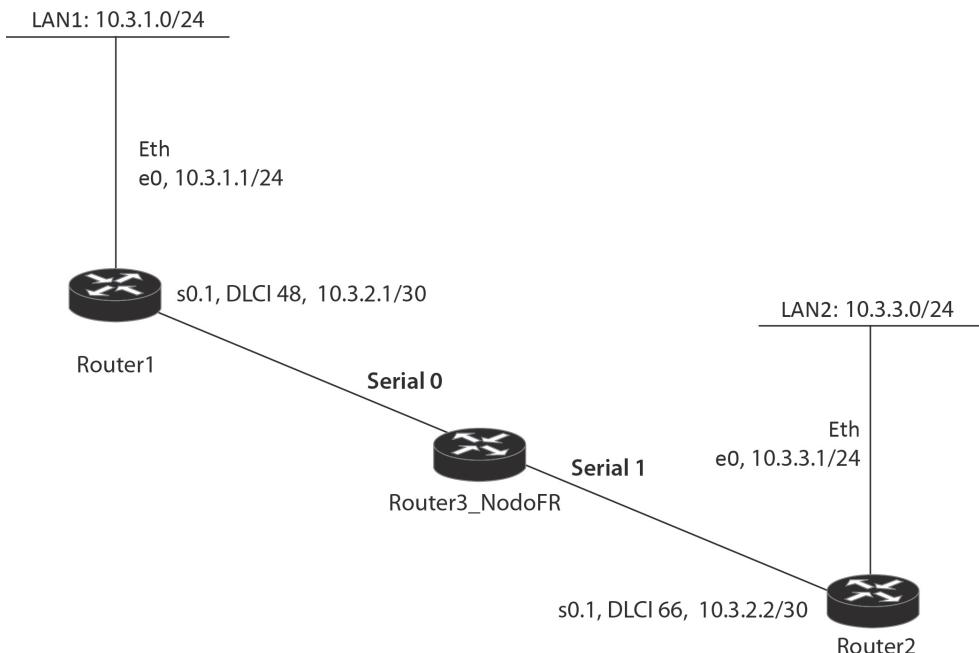
Los encaminadores Cisco soportan 3 tipos de LMI:

- LMI ANSI: T1.167 - Annex D.
- LMI ITU-T: Q.933 - AnnexA (Signaling).
- LMI CISCO: Grupo de los cuatro (Cisco, DEC, Northern Telecom, StrataCom).

Al configurar una conexión de un encaminador para conectarlo a una red Frame Relay, se debe escoger el tipo apropiado de LMI para conseguir su correcta operación.

Configuración Frame Relay básica

Basados en la red de la Figura 8.1 y en las direcciones DLCI e IP de las interfaces seriales de los encaminadores R1 y R2, se procederá a realizar la configuración de los encaminadores R1 y R2.



El encaminador R3 hace las veces de una red Frame Relay

Figura 8.1 LAN1 se interconecta con LAN2 por medio de R1 y R2.

Para el encaminador R1 la configuración debe ser la siguiente:

```
R1(config)# interface serial 0
R1(config-if)# ip address 10.3.2.1 255.255.255.0
!
!Asigna una dirección DLCI a la interfaz (no siempre es necesario hacerlo)
R1(config-if)# frame-relay interface-dlci 48 (valor en el rango 16 a 1007)
!
!Habilita encapsulado sobre Frame Relay usando o no el estándar IETF (RFC1294/1490)
R1(config-if)# encapsulation frame-relay [IETF|CISCO]
!
!Establece que el tipo de LMI usado se base en CCITT (ITU-T Q933a), Cisco o ANSI
!(no siempre es necesario hacerlo)
R1(config-if)# frame relay lmi-type [ccitt|cisco|ansi]
!
!Establece una asociación estática de la IP del próximo salto con el DLCI local
!(no siempre es necesario hacerlo)
R1(config-if)# frame-relay map ip 10.3.2.2 48 broadcast
```

Para el encaminador R2 la configuración debe ser la siguiente:

```
R2(config)# interface serial 0
R2(config-if)# ip address 10.3.2.2 255.255.255.0
R2(config-if)# frame-relay interface-dlci 66
R2(config-if)# encapsulation frame-relay [IETF|CISCO]
R2(config-if)# frame relay lmi-type [ccitt|cisco|ansi]
R2(config-if)# frame-relay map ip 10.3.2.1 66 broadcast
```

Para obtener dentro de la misma interfaz serie física, varias interfaces serie lógicas o subinterfaces, la interfaz serie principal se configura en forma general de la siguiente manera.

```
R1(config)# interface serial 0/0
R1(config-if)# encapsulation frame-relay [IETF|CISCO]
```

Posteriormente, para configurar particularmente cada una de las subinterfaces punto a punto (point-to-point) que se requieran, se utilizan los siguientes comandos (denominados comandos de subinterface).

```

!para la primera subinterface
R1(config)# interface serial 0/0.1 point-to-point
R1(config-if)# ip address 10.3.2.1 255.255.255.0
R1(config-if)# frame-relay interface-dlci 48
!
!para la segunda subinterface
R1(config)# interface serial 0/0.2 point-to-point
R1(config-if)# ip address 10.3.4.1 255.255.255.0
R1(config-if)# frame-relay interface-dlci 49

```

Observe que, para el caso en que se requiera conectar un encaminador Cisco modelo 2503 con un nodo Frame Relay, es requisito configurar en el encaminador 2503, el *frame relay lmi-type*, de acuerdo con el tipo de LMI del nodo Frame Relay. Lo anterior se debe a que los equipos Cisco 2503 no aprenden de manera automática el tipo de LMI usado por el nodo Frame Relay.

La configuración del encaminador R3 para que haga la función de nodo Frame Relay y commute el PVC por los puertos seriales S0 (hacia S0/0 de R1) y S1 (hacia S0/0 de R2), puede ser:

```

R3(config)# frame-relay switching

R3(config)# interface serial 0
R3(config-if)# encapsulation frame-relay
R3(config-if)# frame-relay lmi-type ansi
R3(config-if)# frame-relay intf-type dce
R3(config-if)# frame-relay route 48 in s1 66

R3(config)# interface serial 1
R3(config-if)# encapsulation frame-relay
R3(config-if)# frame-relay lmi-type ansi
R3(config-if)# frame-relay intf-type dce
R3(config-if)# frame-relay route 66 in s0 48

```

Monitoreo de Frame Relay

Para monitorear el estado de los DLCI en el lado del encaminador R1, se usa el comando *show frame-relay pvc*. Para verificar la asociación entre el DLCI local y la dirección IP del otro extremo del circuito virtual, se usa el comando *show frame-relay map*.

R1# *show frame-relay pvc*

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 48, DLCI USAGE = LOCAL, PVC STATUS =ACTIVE, INTERFACE = Serial0
input pkts 50 output pkts 40 in bytes 50000
out bytes 40000 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
pvc create time 0:00:22 last time pvc status changed 0:00:22

R1# *show frame-relay map*

Serial0 (up): ip 10.3.2.2 dlci 48(0x30,0xC00), static,
IETF, status known,active
Verifying Frame Relay

INFORME

Usar los programas Configmaker de Cisco y GNS3 para interconectar tres redes de área local –sobre las cuales corren aplicaciones TCP/IP– por medio de tres encaminadores Cisco y una red de área amplia Frame Relay. Realizar la configuración y montaje de la red e interpretar los archivos de configuración.

EJERCICIOS DE LABORATORIO

En este ejercicio se desea establecer una conexión virtual permanente Frame Relay entre un encaminador Cisco y un encaminador de una marca diferente. Se requiere configurar solamente el encaminador del lado izquierdo de la Figura 8.2, asumiendo que en dicho lado la detección automática del tipo de LMI y el ARP inverso no funcionan bien. También se desea que las actualizaciones de RIP pasen por la conexión virtual permanente de la nube Frame Relay.

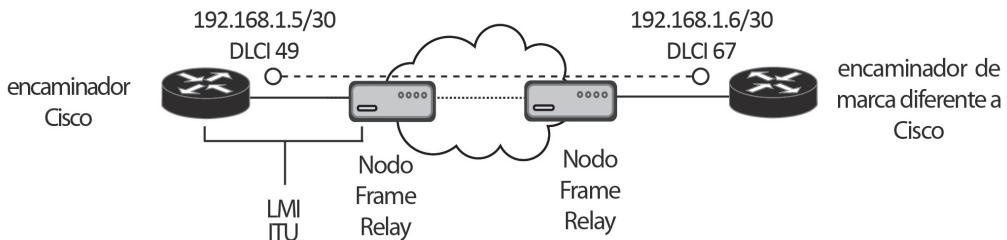


Figura 8.2 Conexión Frame Relay entre dos encaminadores de diferentes fabricantes

Tareas de configuración a realizar

1. Configure la dirección IP de la interfaz serie.
2. Configure el tipo de encapsulado de la interfaz para que sea Frame Relay.
3. Configure el tipo de LMI en la interfaz.
4. Configure la resolución manual DLCI a IP para Frame Relay.

Tareas de monitoreo a realizar

1. Verifique el tipo de encapsulado en la interfaz.
2. Verifique el estado de LMI.
3. Verifique el estado de la conexión virtual permanente.
4. Verifique la resolución manual DLCI a IP.

INFORMACIÓN COMPLEMENTARIA

El propósito de LMI

El propósito de LMI es permitir que un DTE Frame Relay (Encaminador IP) y un DCE Frame Relay (nodo Frame Relay) intercambien información acerca del estado de sus conexiones Frame Relay y acerca de ellos mismos. Para realizar esto, un DTE Frame Relay envía una solicitud LMI (*LMI status enquiry*) al nodo Frame Relay. Asumiendo que el nodo está operando y que entiende el mensaje LMI, éste responderá con el mensaje *Status Reply*. En cierto sentido, esto funciona como un mecanismo *keepalive* en el que el encaminador hace la pregunta: ¿estás ahí?, y el nodo Frame Relay responde: sí, aquí estoy. Por defecto, solamente el DTE origina dichas solicitudes, mientras que el nodo Frame Relay las escucha pasivamente.

Después del envío periódico de varias solicitudes, el DTE envía un mensaje especial de solicitud de estado, denominado “solicitud de estado completa” (*full status update*), en el que se detalla toda la información relacionada con el DTE solicitante. El nodo responderá con una lista de todos los circuitos virtuales (VC) conectados al DTE, sus respectivas direcciones

(DLCI), sus configuraciones (CIR, Bc y Be) y sus estados sobre la interfaz física que lo conecta con el DTE.

Para que funcione la comunicación entre el DTE y el DCE, la información LMI debe viajar sobre un circuito virtual (VC). Tanto el DTE como el DCE deben buscar dicha información en las tramas Frame Relay, por lo cual, ambos deben conocer el DLCI por el cual se intercambian la información LMI. Dependiendo de la implementación LMI que se esté usando (hay tres posibles implementaciones), se reserva un número DLCI para el intercambio LMI, que puede ser uno de los siguientes:

LMI ANSI: T1.167-Annex D → DLCI 0.

LMI ITU-T: Q.933-AnnexA (Signaling) → DLCI 0.

LMI CISCO: Grupo de los cuatro (Cisco, DEC, Northern, StrataCom) → DLCI 24.

Ejemplo: Si un DTE del usuario y un DCE del proveedor funcionan con un LMI de tipo Annex A, entonces todos los mensajes LMI tendrán el DLCI 0 en el encabezado de las tramas Frame Relay.

Un encaminador Cisco, por defecto, genera los mensajes LMI de solicitud de estado cada 10 segundos y en el sexto mensaje LMI genera una solicitud de actualización de estado completa (una vez por minuto).

A partir de la versión 11.2 del IOS, los encaminadores Cisco pueden detectar automáticamente el tipo de LMI. En otras palabras, el usuario no tiene que configurar el tipo de LMI. Con la detección automática, el encaminador enviará una solicitud de estado por cada tipo de LMI posible en el nodo y esperará para ver qué solicitud es contestada por el nodo. Una vez el DTE reciba la respuesta de la solicitud LMI, éste conocerá el tipo de LMI que debe usar para comunicarse con el nodo Frame Relay.

Estados de los circuitos virtuales

Los circuitos virtuales Frame Relay pueden estar en uno de los tres estados siguientes.

- **Active:** la conexión extremo a extremo entre el DTE local y el DTE remoto está arriba y operacional.
- **Inactive:** la conexión entre el DTE local y el DCE local está arriba y operacional, pero hay algo malo entre el DCE local (al cual se conecta el DTE local) y el DTE remoto del otro extremo.
- **Deleted:** el DTE local no está recibiendo mensajes LMI del DCE local.

Resolución Dinámica

En lugar de indicarle manualmente al encaminador la dirección IP de la interfaz del otro extremo del circuito virtual, se puede utilizar un proceso llamado ARP inverso (Inverse ARP), el cual permite que el encaminador descubra automáticamente los circuitos virtuales que terminan en su interfaz y las direcciones IP que tiene el otro extremo de cada circuito virtual.

El encaminador obtiene información acerca del estado de sus circuitos virtuales cuando envía una solicitud de actualización completa de estado al nodo local y obtiene una respuesta de parte de éste; esta actualización de estado es recibida cada minuto. Una vez que el circuito virtual se encuentre en estado activo, el encaminador Cisco ejecutará ARP inverso cada 60 segundos sobre él, teniendo como propósito descubrir la dirección IP del otro extremo del circuito virtual.

Cuando el circuito virtual esté activo, el DTE local enviará una trama especial a través del circuito virtual con destino al DTE remoto. Esta trama contiene información acerca de la dirección de capa 3 del DTE local, como también del hecho de que se está enviando un mensaje ARP inverso. El DTE remoto examina el DLCI de la trama Frame Relay que le llega y extrae la dirección de la capa 3 del mensaje ARP inverso que lleva la trama. El DTE remoto adiciona esta información a su tabla de resolución, y hará lo mismo que el DTE local, una vez descubra que el circuito virtual se encuentra en estado activo. Una vez ambos lados hayan recibido del otro extremo un mensaje ARP inverso, podrán empezar a transferirse datos por medio del circuito virtual. Observe que el circuito virtual debe estar activo para que el ARP inverso tenga lugar.

Configuración de una interfaz ATM

Suponiendo que el encaminador R1 de la Figura 8.1 tiene una interfaz ATM, se pueden configurar varias subinterfaces ATM para que funcionen con circuitos virtuales permanentes de dicha tecnología. A continuación, a modo de ejemplo, se presentan unas líneas del archivo de configuración de R1, que permiten su operación con el circuito virtual permanente número 30, identificado con el VPI/VCI 0/48 –Virtual Path Identifier/Virtual Channel Identifier– por parte del proveedor de la red ATM. El método de encapsulado que se usa en este caso es “aal5snap”; con dicho método, todo tipo de tráfico puede cursar por el mismo circuito virtual. Finalmente, se hace una asociación o mapeo estático entre el circuito virtual permanente y la dirección IP del otro extremo de dicho circuito.

```
interface atm 0/0
no shutdown
!
interface atm 0/0.1
! Se asigna una dirección IP a uno de los extremos del circuito virtual permanente.
ip address 10.3.2.1 255.255.255.0
! Se crea el PVC 30 identificado con un VPI de 0 y un VCI de 48 (equivale al DLCI).
atm pvc 30 0 48 aal5snap
map-group atm-map1
!
map-list atm-map1
ip 10.3.2.2 atm-vc 30 broadcast
```

Como alternativa, se puede habilitar el ARP inverso; con esto se evita tener que hacer el mapeo estático y se simplifica la configuración anterior. Las siguientes líneas de configuración presentan esta opción.

```
interface atm 0/0
no shutdown
!
interface atm 0/0.1
ip address 10.3.2.1 255.255.255.0 inarp
atm pvc 30 0 48 aal5snap
```

Configuración de una interfaz ADSL

A continuación se sugiere y comenta la configuración de un encaminador Cisco para que funcione con la tecnología ADSL, que es de uso popular para las conexiones de banda ancha (otro método de uso popular es el Cable módem). A modo de ejemplo, se presentan unas líneas del archivo de configuración de un encaminador domiciliario, el cual sirve para acceder a Internet a través de un proveedor de servicios de Internet (ISP). En este caso, se usa el “Traslado de direcciones de red” (Network Address Translation o NAT) y el “Protocolo punto a punto sobre Ethernet” (Point-To-Point Protocol over Ethernet o PPPoE). Este último es usado por los ISP para proporcionar las funciones de autenticación, cifrado y compresión.

En el ejemplo, se supone que el ISP proporciona una conexión ATM mediante un PVC identificado por el VPI/VCI 8/35. También se supone que el ISP proporciona el método de marcación a través de un cliente PPPoE desde el encaminador.

Se habilita y configura VPDN (Virtual Private Dialup Network) para que PPPoE requiera marcación para conectar. La interfaz virtual de marcación

“dialer1” se encarga de la dirección IP pública de la conexión, de la autenticación PPP y de la información NAT externa. La configuración de la interfaz ATM consiste en aplicar el valor del PVC suministrado por el ISP.

```

hostname router-domiciliario
!
! Habilita VPDN.
vpdn enable
!
! Configura un grupo VPDN denominado “pppoe”, este grupo es usado para establecer
! sesiones PPPoE y requiere “marcación” (hace del encaminador un cliente PPPoE).
vpdn-group pppoe
request-dialin
protocol pppoe
!
! Crea la interfaz virtual de marcación “dialer1”, dicha interfaz hace la marcación hacia
! el ISP y es utilizada por la subinterfaz ATM0.1. A la MTU se le restan 8 bytes del
! encabezado de PPPoE. El ISP nos informa nuestro usuario (acceso) y nuestra clave
! (secreto).
interface dialer1
ip address negotiated
encapsulation ppp
ip mtu 1492
ip nat outside
dialer pool 1
ppp authentication pap callin
ppp pap sent-username acceso password secreto
!
interface FastEthernet 0
description ésta es nuestra interfaz interna de red
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
interface ATM0
description ésta es nuestra interfaz ADSL
no ip address
no atm ilmi-keepalive
dsl operating-mode auto
!
! El ISP nos informa que nuestro PVC es 8/35.
! Se le asocia la interfaz virtual de marcación “dialer1” a la subinterfaz ATM0.1
interface ATM0.1 point-to-point
pvc 8/35
protocol pppoe
pppoe-client dial-pool-number 1
!
! Se aplica la lista de acceso 1 para hacer NAT sobre la interfaz “dialer1”.
ip nat inside source list 1 interface dialer1 overload
!
! La ruta por defecto es la interfaz virtual de marcación “dialer1”
ip route 0.0.0.0 0.0.0.0 dialer1
!
! La lista de acceso 1 es utilizada por el comando ip nat inside.
access-list 1 permit 192.168.1.0 0.0.0.255

```

Configuración de una interfaz Cable-modem

A continuación se sugiere y comenta la configuración de un encaminador Cisco para que funcione con una interfaz cable-modem. En este caso, el encaminador no utiliza PPPoE y se configura para que opere en la capa 3 en modo de “routing” en lugar del modo de “bridging”.

```
interface FastEthernet0
description esta es nuestra interfaz interna de red
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
! Se configura la interfaz “cable-modem 0” para operar en modo de “Routing”
interface cable-modem 0
ip address negotiated
ip nat outside
! Los valores siguientes los proporciona el ISP o son reportados automáticamente por el
! cable-modem.
cable-modem downstream saved channel 500000000 32 1
cable-modem mac-timer t2 60000
! Se escoge el modo “routing” en lugar del modo “bridging”
no cable-modem compliant bridge
!
! Se aplica la lista de acceso 1 para hacer NAT sobre la interfaz “cable-modem0”.
ip nat inside source list 1 interface cable-modem0 overload
!
ip routing
ip classless
!
! La ruta por defecto apunta al encaminador del ISP
ip route 0.0.0.0 0.0.0.0 10.0.6.21
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

Configuración de la interfaz T1/E1

El encaminador Cisco 2801 de la Figura 1.2 tiene una interfaz T1/E1 instalada en la posición 0/1/0 (ranura 1). La conexión en modo “back to back” de dos encaminadores 2801 (que denominaremos R1 y R2) a través de dichas interfaces se hace por medio de un cable cruzado UTP categoría 5, el cual tiene la disposición de conectores presentada en la Tabla 8.1.

Tabla 8.1 Cable de conexión E1 a E1

RJ48 (de R1)	RJ48 (de R2)
1	4
2	5
4	1
5	2

Para activar la tarjeta T1/E1 (VWIC2-1MFT-T1/E1) de R1 y R2, se puede ejecutar el siguiente comando –escoger solamente una opción: t1 o e1.

```
(config)# card type t1|e1 0 1
```

Para conformar el “channel-group 0”, el cual agrupa 15 canales DS0 de 64 Kbps, y tiene el propósito de proporcionar el servicio de canal de datos, se pueden ejecutar los siguientes comandos.

```
(config)# controller t1|e1 0/1/0
(config-controller)# channel-group 0 timeslots 1-15
(config-controller)# cablelength short 133ft
```

Para realizar la configuración y sincronización de la señal de reloj en los equipos R1 y R2, se pueden ejecutar los siguientes comandos.

```
R1(config-controller)# clock source internal
R1(config)# network-clock-participate wic 1
```

```
R2 (config-controller)# clock source line
R2 (config)# network-clock-participate wic 1
R2 (config)# network-clock-select 1 t1|e1 0/1/0
```

El comando “*network-clock-participate wic 1*” tiene como finalidad que los equipos R1 y R2 usen el reloj de la línea T1|E1 para sincronizar el reloj de la tarjeta principal (board).

El comando “*network-clock-select 1 t1|e1 0/1/0*” tiene como finalidad que el equipo R2 seleccione el reloj de la línea T1|E1 como “fuente de reloj” del IOS (por defecto, el reloj de la línea T1|E1 está desconectado del backplane). Con esto, el IOS utiliza el reloj de la línea T1|E1 para transmitir datos en las otras interfaces (en lugar de usar el reloj interno del backplane,

lo cual haría por defecto). Lo anterior es equivalente a conectar la señal de reloj recibida en la interfaz T1|E1 al backplane.

La sincronización de los encaminadores se verifica con los comandos “*show controllers t1|e1*” y “*show network-clocks*”. El primer comando no debe presentar errores después de ejecutarse varias veces por un lapso de tiempo de dos minutos.

Finalmente, para configurar la dirección IP y el protocolo de encapsulado del canal de datos, se pueden ejecutar los siguientes comandos en R1 (y los correspondientes comandos en R2).

```
R1(config)# interface serial 0/1/0:0
R1(config-if)# ip address 10.3.2.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# encapsulation hdlc | frame-relay | atm-dxi
```

Por ejemplo, para usar Frame Relay en una disposición “back to back” entre R1 y R2, se habilita en R1 la operación *frame-relay switching*, en su interfaz serial 0/1/0:0 se encapsula *frame-relay*, dicha interfaz se pone a funcionar en modo *frame-relay intf-type dce*, se le asigna un DLCI y una dirección IP. Respecto a R2, solamente es necesario encapsular *frame-relay* en la interfaz y asignarle una dirección IP a la misma.

PROBLEMAS

1. Suponga que el encaminador R1 tiene dos conexiones de tipo Frame Relay por medio de los DLCI 48 (con destino a R2) y 49 (con destino a R3). Describa el resultado que se obtiene con las líneas subrayadas en el archivo de configuración de R1 (que definen las clases “clase-A” y “clase-B”). ¿Cuál función realiza la línea resaltada?

```
interface serial0/0
no ip address
encapsulation frame-relay
frame-relay traffic-shaping
!
interface serial0/0.48 point-to-point
ip address 10.3.2.1 255.255.255.0
frame-relay interface-dlci 48
class clase-A
!
```

Continua

Viene

```

interface serial0/0.49 point-to-point
ip address 10.3.4.1 255.255.255.0
frame-relay interface-dlci 49
class clase-B
frame-relay payload-compression frf9 stac
!
map-class frame-relay clase-A
frame-relay traffic-rate 128000 256000
frame-relay adaptive-shaping becn
!
map-class frame-relay clase-B
frame-relay traffic-rate 32000 64000
```

- En el punto anterior la configuración de Frame Relay utiliza dos subinterfaces punto a punto y dos subredes IP; esta opción es la más recomendada, puesto que se tiene mayor control sobre cada conexión individual. Otra alternativa utiliza solamente una interfaz multipunto en R1 y una subred IP; tal como lo indica el presente archivo de configuración. En este caso ¿cuál es la razón de inhabilitar split-horizon en la interfaz principal cuando se tiene una topología de tipo “parcialmente en malla” (partially-meshed)? ¿Es necesario inhabilitar split-horizon en una topología de tipo “completamente en malla” (fully meshed)?

```

interface serial0/0
no ip address
encapsulation frame-relay ietf
! Inhabilitar split-horizon
no ip split-horizon
no shutdown
!
interface serial0/0.1 multipoint
ip address 10.3.2.1 255.255.255.0
! Escribir todos los DLCI que llegan a R1 y dejar que ARP inverso haga su trabajo
frame-relay interface-dlci 48
frame-relay interface-dlci 49
frame-relay interface-dlci 50
```

GLOSARIO

Bc (Committed Burst Rate): tráfico promedio (por ejemplo, 8.000 bits) sobre un periodo de tiempo T fijo (por ejemplo, 125 milisegundos) que un proveedor garantizará para un circuito virtual. [CIR = Bc/T].

Be (Excessive Burst Rate): tráfico adicional al Bc que un proveedor le proporcionará a un circuito virtual durante el periodo T, pero sin dar garantía de él.

BECN (Backward Explicit Congestion Notification): el nodo Frame Relay del proveedor puede usar este campo del encabezado de una trama Frame Relay que esté fluyendo en dirección contraria al sentido en que se experimenta congestión cuando quiera indicar que hay congestión dentro de la red al dispositivo origen de la trama afectada por la congestión.

DE (Discard Eligibility): campo de una trama Frame Relay utilizado para marcar la trama como de baja prioridad. El proveedor marcará como tramas de baja prioridad aquellas que durante el periodo de tiempo T excedan los valores del Bc (o del CIR).

DLCI (Data Link Connection Identifier): son los valores usados para identificar un extremo de cada circuito virtual en la interfaz física Frame Relay, dichos valores representan las direcciones de los circuitos virtuales en un extremo de la conexión. Esto proporciona la capacidad de multiplexar tráfico para varios destinos sobre la misma interfaz física; para hacer esto, cada conexión requiere tener una dirección única o DLCI en cada extremo. El DLCI tiene significado local y puede cambiarse en cada enlace, el nodo Frame Relay hará los respectivos cambios del valor del DLCI cuando haga el reenvío de las tramas Frame Relay. El rango de DLCI que va desde 0 hasta 15 y desde 1008 hasta 1023 es reservado.

FECN (Forward Explicit Congestion Notification): el nodo Frame Relay del proveedor usará este campo del encabezado de una trama Frame Relay cuando quiera indicarle al dispositivo destinatario de la trama que se presenta congestión dentro de la red.

LMI (Local Management Interface): define cómo el DTE (dispositivo Frame Relay, como, por ejemplo, un encaminador) interactúa con un DCE (nodo Frame Relay).

Sobre suscripción: hace referencia a un enlace cuya velocidad de acceso es inferior a la suma de las velocidades de las conexiones lógicas que lo utilizan. Cuando se suman todos los CIR de los circuitos virtuales de una interfaz y el resultado excede el valor de la velocidad de acceso de la interfaz, se le está apostando a que los circuitos virtuales no operarán simultáneamente a sus velocidades contratadas.

Velocidad contratada o CIR (Committed Information Rate): es la rapidez contratada para un circuito virtual (por ejemplo, 64.000 bits por segundo) que garantiza el proveedor independientemente de los niveles de congestión en la red.

Velocidad de acceso o Access Rate: es la velocidad de la conexión física entre el encaminador del usuario y el nodo Frame Relay del proveedor –puede ser, por ejemplo, un enlace T1 o E1.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DE GHEIN, L. (2007). *MPLS Fundamentals*. Indianapolis, IN: Cisco Press.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

PROTOCOLO DE ENRUTAMIENTO IP: ABRIR PRIMERO LA RUTA MÁS CORTA (OPEN SHOREST PATH FIRST - OSPF)

OSPF es un protocolo de enrutamiento interior altamente flexible y escalable que permite interconectar diferentes tipos de redes de una organización (o las redes de un proveedor de Internet) para obtener una sola red unificada basada en el protocolo IP (lo que comúnmente se denomina intranet). El protocolo OSPF posibilita que el intercambio de información de enrutamiento quede confinado a los equipos que pertenecen a una misma área y que se pueda obtener información de otras áreas por medio de los encaminadores de borde de área (que interconectan dichas áreas).

La motivación del presente capítulo se orienta a que el lector gane experiencia en la interconexión de redes basadas en IP mediante el uso del protocolo de enrutamiento OSPF, razón por la que se aborda la configuración de OSPF para operar en el ambiente de área cero y en el ambiente multi-área.

OBJETIVO

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

- Configurar los encaminadores de red para que operen con OSPF en el área cero.
- Configurar OSPF para lograr una operación adecuada en un ambiente multi-área.

- Configurar el resumen de rutas con el propósito de reducir el tamaño de las tablas de enrutamiento y de la base de datos del “estado de los enlaces OSPF” en los encaminadores.

PROCEDIMIENTO

La Figura 9.1 representa una red con el conjunto de equipos E1 (equipos administrados por usted, el estudiante E1) y E2 (equipos administrados por un compañero, el estudiante E2) sobre los que se va a configurar el protocolo de enrutamiento OSPF en el área cero.

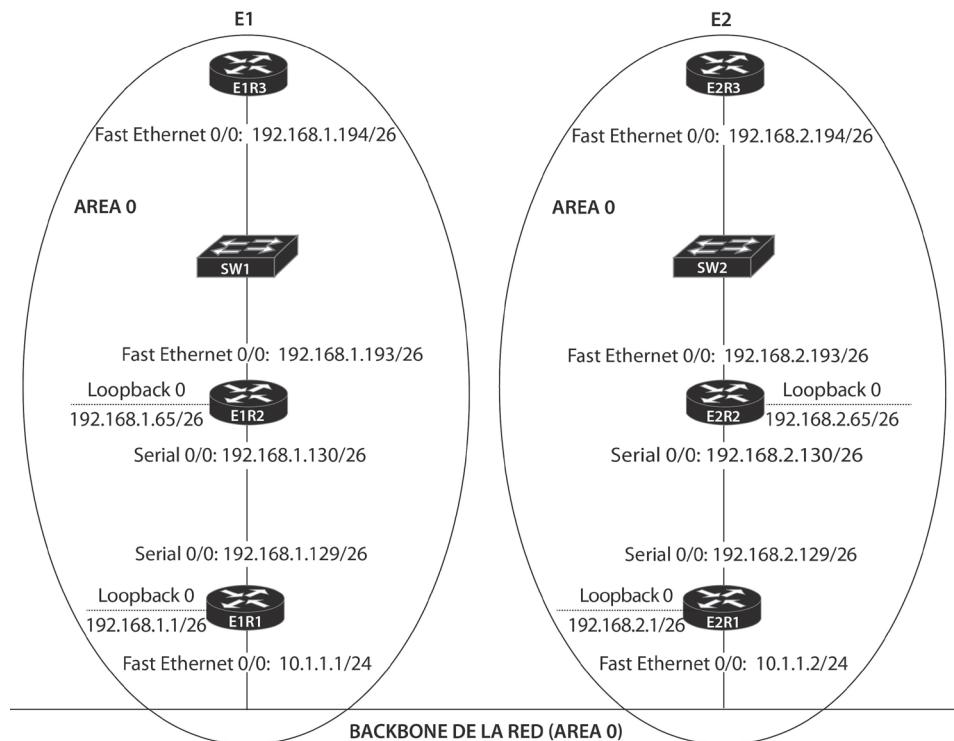


Figura 9.1 Red IP que ejecuta el protocolo de enrutamiento OSPF en el conjunto de equipos E1 (equipos administrados por usted) y E2 (equipos administrados por un compañero) en el área cero

Habilitar OSPF dentro de E1 (y de E2)

Usando equipos físicos del laboratorio, o el programa de simulación gráfica de red GNS3 (Graphical Network Simulator), o el software BOSON NETSIM Router Simulator, realizar el montaje y configuración del conjunto de equipos contenidos dentro del dominio de administración “E1” de

la red de la Figura 9.1; habilitar solamente OSPF como único protocolo de enrutamiento operando en el área cero. Esta parte del ejercicio de laboratorio supone que el conjunto de equipos contenidos dentro del dominio de administración “E2” serán configurados (por usted o por un compañero) con el protocolo OSPF, el cual también estará operando en el área cero.

Observación: en algunos puntos del procedimiento se presentan las respuestas y resultados esperados mediante el encabezado “//Respuesta:”.

1. Configurar las direcciones IP de las interfaces Ethernet, Serie y de Loopback involucradas en cada encaminador de la Figura 9.1, tanto en E1 como en E2. Habilitar dichas interfaces y configurar el nombre de cada equipo (hostname).
2. Los comandos para la configuración de OSPF de R1, R2 y R3 (en E1), es decir, para E1R1, E1R2 y E1R3, son.

Para E1R1:

```
E1R1(config)# router ospf 1
E1R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
E1R1(config-router)# network 10.1.1.0 0.0.0.255 area 0
```

Para E1R2:

```
E1R2(config)# router ospf 1
E1R2(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Para E1R3:

```
E1R3(config)# router ospf 1
E1R3(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Para E2R1, E2R2 y E2R3 se usan comandos similares a los anteriores, pero, en lugar de usar la dirección 192.168.1.0, en estos se utiliza la dirección 192.168.2.0. Realizar lo anterior para R1, R2 y R3 en E2.

3. Con el paso anterior se configura OSPF en los encaminadores R1, R2 y R3 (en E1 y E2) usando un “Proces ID” de “1” y se ponen todas las interfaces en el área cero (incluyendo las interfaces de loopback).
4. Para ver la tabla de enrutamiento en E1R1 y buscar el valor de la distancia administrativa de OSPF, utilizar el comando *show ip route*.

E1R1# show ip route

//Respuesta: el valor de la distancia administrativa de OSPF es 110.

5. Identifique el valor de la distancia administrativa o “Distance” y el “Router ID” de OSPF mediante el comando *show ip protocols*.

E1R1# *show ip protocols*

//Respuesta: Distance: (default is 110), Router ID 192.168.1.1.

Uso del comando *show ip ospf*

Desde el encaminador E1R1, digite el comando *show ip ospf*. Use la salida por pantalla para responder las siguientes preguntas y comparar el resultado con las respuestas sugeridas.

1. ¿Cuál es el “ID del proceso de enrutamiento OSPF” de R1?

Respuesta: Routing Process “ospf 1” with ID 192.168.1.1, el cual es igual al valor del Router ID.

2. ¿Por qué el encaminador seleccionó dicho valor para el “Router ID”?

Respuesta: El “Router ID” se usa para identificar al encaminador completo frente al protocolo OSPF. Por defecto, el valor que se escoge para el “Router ID” es la dirección de loopback más alta del encaminador (de varias posibles interfaces de loopback). En caso de no tener configurada al menos una interfaz de loopback en el encaminador, se escoge la dirección más alta de las interfaces activas del mismo. Esta dirección es importante para establecer relaciones de vecindad y coordinar mensajes entre copias del algoritmo “Primero el camino más corto” (Shorest Path First o SPF) que se esté ejecutando en la red. El “Router ID” también se usa para conseguir un desempate durante el proceso de elección del encaminador designado (Designated Router o DR) y del encaminador designado de respaldo (Backup Designated Router o BDR) cuando los valores de prioridad de la interfaz de los dos encaminadores que compiten son iguales.

3. ¿Cuántas veces ha ejecutado el algoritmo SPF el encaminador?

Respuesta: SPF algorithm executed 4 times.

4. ¿Cuántas interfaces hay en el área cero?

Respuesta: Number of interfaces in this area is 3 (1 loopback).

5. ¿En cuántas áreas participa R1?

Respuesta: Number of areas in this router is 1. Area BACKBONE(0).

Uso del comando `show ip ospf neighbor`

Desde el encaminador E1R1, digite el comando `show ip ospf neighbor`. Use la salida por pantalla para responder lo siguiente.

1. ¿Cuántos vecinos tiene R1?

Respuesta: dos.

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.65	0	FULL/ -	00:00:33	192.168.1.130	Serial1/0
192.168.2.1	1	FULL/DR	00:00:34	10.1.1.2	FastEthernet0/0

2. ¿Qué significado tiene la palabra “full” bajo la columna “state”?

Respuesta: el significado es que los vecinos han intercambiado la base de datos de los anuncios de estado de enlace (Link State Advertisement Database).

3. ¿Cuál de los vecinos de E1R1 sobre la interfaz FastEthernet0/0 es DR (Designated Router)?

Nota: si en E1R1 no se muestra el DR, es porque E1R1 es el DR. Consulte en E2R1.

Respuesta: en este caso es el 192.168.2.1.

4. ¿Por qué no hay DR/BDR en la interfaz Serial 0/0?

Respuesta: la elección del DR y el BDR no tiene lugar en redes punto a punto.

Uso del comando `show ip ospf database`

Desde el encaminador E1R1, digite el comando `show ip ospf database`. Use la salida por pantalla para responder lo siguiente.

1. ¿Cuántos tipos de Anuncios de estado de enlace (LSA) se muestran?

Respuesta: dos Tipos: Router Link States (Area 0) y Net Link States (Area 0).

OSPF Router with ID (192.168.1.1) (Process ID 1)**Router Link States (Area 0)**

Link ID	ADV Router	Age	Seq#	Checksum	Link count
192.168.1.1	192.168.1.1	718	0x80000005	0x00868B	4
192.168.1.65	192.168.1.65	737	0x80000005	0x00372A	4
192.168.1.194	192.168.1.194	889	0x80000004	0x007845	1
192.168.2.1	192.168.2.1	708	0x80000004	0x00010B	4
192.168.2.65	192.168.2.65	702	0x80000005	0x00DB7D	4
192.168.2.194	192.168.2.194	698	0x80000004	0x007C3D	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.2	192.168.2.1	708	0x80000003	0x00D14D
192.168.1.194	192.168.1.194	889	0x80000003	0x0004F1
192.168.2.194	192.168.2.194	698	0x80000003	0x0008E9

2. ¿Qué tipo de encaminador genera un “Router Link LSA”?

Respuesta: Internal Router o IR.

3. ¿Qué tipo de encaminador genera un “Network Link LSA”?

Respuesta: Designated Router o DR.

INFORME**Uso del comando show ip ospf interface**

Desde el encaminador E1R1, digite el comando *show ip ospf interface*. Use la salida por pantalla para responder las siguientes preguntas.

1. ¿Cuántas interfaces hay configuradas para OSPF?

Respuesta: tres.

2. ¿Cuál es el “Router ID” usado para cada interfaz?

Respuesta: Router ID 192.168.1.1.

3. ¿Qué tan frecuentes son enviados los mensajes de “Hello”?

Respuesta: Hello 10 “segundos”.

4. ¿Cuál es la dirección IP de la interfaz FastEthernet 0/0 de R1?

Respuesta: Internet Address 10.1.1.1/24.

5. ¿A cuál área pertenece la interfaz FastEthernet 0/0?

Respuesta: Area 0.

6. ¿Cuál es el costo de usar una interfaz FastEthernet 0/0?

Respuesta: Cost: 10.

7. ¿Cuál es la prioridad de la interfaz FastEthernet 0/0?

Respuesta: Priority 1.

8. ¿Cuál es el ID del “Designated Router”?

Respuesta: Designated Router (ID) 192.168.2.1.

9. ¿Cuál es la dirección IP de la interfaz del “Designated Router”?

Respuesta: Interface address 10.1.1.2.

10. ¿Cuál es el ID del “Backup Designated Router”?

Respuesta: Backup Designated router (ID) 192.168.1.1.

11. ¿Cuál es la dirección IP de la interfaz del “Backup Designated Router”?

Respuesta: Interface address 10.1.1.1.

12. ¿Cuál es la dirección IP de la interfaz Serial 0/0 de R1?

Respuesta: Internet Address 192.168.1.129/26.

13. ¿A cuál área pertenece la interfaz Serial 0/0?

Respuesta: Area 0.

14. ¿Cuál es el costo de usar una interfaz Serial 0/0?

Respuesta: Cost: 64.

15. ¿Cuál es la prioridad de la interfaz Serial 0/0?

Respuesta: no aplica.

EJERCICIOS DE LABORATORIO

En este ejercicio se debe configurar la red de la Figura 9.1 y tener en cuenta las siguientes consideraciones o cambios:

La red se ha dividido en tres áreas (área 0, área 1, y área 2) como lo representa la Figura 9.2.

El siguiente procedimiento hace referencia solamente a la configuración de los equipos del área 1 (E1); para efectos de asignación de direcciones se mantienen los valores del diseño de la Figura 9.1.

Se supone que los equipos que se encuentran en el área 2 (E2) también van a ser configurados (por usted o por su compañero).

Se habilita solamente OSPF como único protocolo de enrutamiento operando en la red.

No es necesaria la configuración del equipo denominado “Router” de la Figura 9.2, la configuración de dicho equipo se aborda en la sección “Problemas”.

Configurar OSPF en un ambiente multi-área

1. Remueva la configuración actual de OSPF para R1, R2 y R3 en E1 y E2 con el comando *no router ospf 1*.
2. Configure el protocolo de enrutamiento OSPF en los encaminadores de E1 (R1, R2 y R3) usando el área adecuada para cada una de sus interfaces (área 0 o área 1), tal como se muestra en la Figura 9.2. Permita que OSPF anuncie las interfaces de loopback de los encaminadores. Cuando se trate de un encaminador que involucre varias áreas (como R1 que es de tipo “Area Border Router” o ABR), se debe configurar cada interfaz del encaminador para el área a la cual dicha interfaz se conecta. Los comandos para configurar los encaminadores son los siguientes.

Para E1R1:

```
E1R1(config)# router ospf 1  
E1R1(config-router)# network 10.1.1.0 0.0.0.255 area 0  
E1R1(config-router)# network 192.168.1.0 0.0.0.255 area 1
```

Para E1R2:

```
E1R2(config)# router ospf 2  
E1R2(config-router)# network 192.168.1.0 0.0.0.255 area 1
```

Para E1R3:

```
E1R3(config)# router ospf 3  
E1R3(config-router)# network 192.168.1.0 0.0.0.255 area 1
```

Para E2R1:

```
E2R1(config)# router ospf 1  
E2R1(config-router)# network 10.1.1.0 0.0.0.255 area 0  
E2R1(config-router)# network 192.168.2.0 0.0.0.255 area 2
```

Para E2R2:

```
E2R2(config)# router ospf 2  
E2R2(config-router)# network 192.168.2.0 0.0.0.255 area 2
```

Para E2R3:

```
E2R3(config)# router ospf 3  
E2R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
```

3. Cuando haya terminado de configurar E1 (y E2), ejecute el comando *show ip route*.
¿Qué tipos de rutas hay en la tabla de enrutamiento (O; IA; E1; o E2)?
Respuesta: OSPF y OSPF Inter Area.
4. Usar los comandos telnet o ping para asegurarse de que hay conectividad a todas las áreas de la red.
5. En los encaminadores E1R1 y E1R2, ejecute los siguientes comandos “*show*” y explore la salida.

E1R1# *show ip ospf database*

Respuesta:

E1R1 tiene los siguientes tipos de LSA para el área 0

Tipo Router o “Tipo 1”

Tipo Network o “Tipo 2”

Tipo Summary o “Tipo 3 y 4”

E1R1 tiene los siguientes tipos de LSA para el área 1

Tipo Router o “Tipo 1”

Tipo Network o “Tipo 2”

Tipo Summary o “Tipo 3 y 4”

E1R2# *show ip ospf database*

Respuesta:

E1R2 tiene los siguientes tipos de LSA solamente para el área 1

Tipo Router o “Tipo 1”

Tipo Network o “Tipo 2”

Tipo Summary “Tipo 3 y 4”

E1R1# *show ip ospf interface*

E1R2# *show ip ospf interface*

Respuesta:

E1R1 tiene las siguientes interfaces operando en una de las dos áreas (área 0 o área 1)

FastEthernet0/0 en el Area 0

Loopback0 en el Area 1

Serial0/0 en el Area 1

E1R2 tiene las siguientes interfaces operando solamente en el área 1

FastEthernet0/0, Area 1

Loopback0, Area 1

Serial0/0, Area 1

E1R1# *show ip ospf*

Respuesta: Number of areas in this router is 2

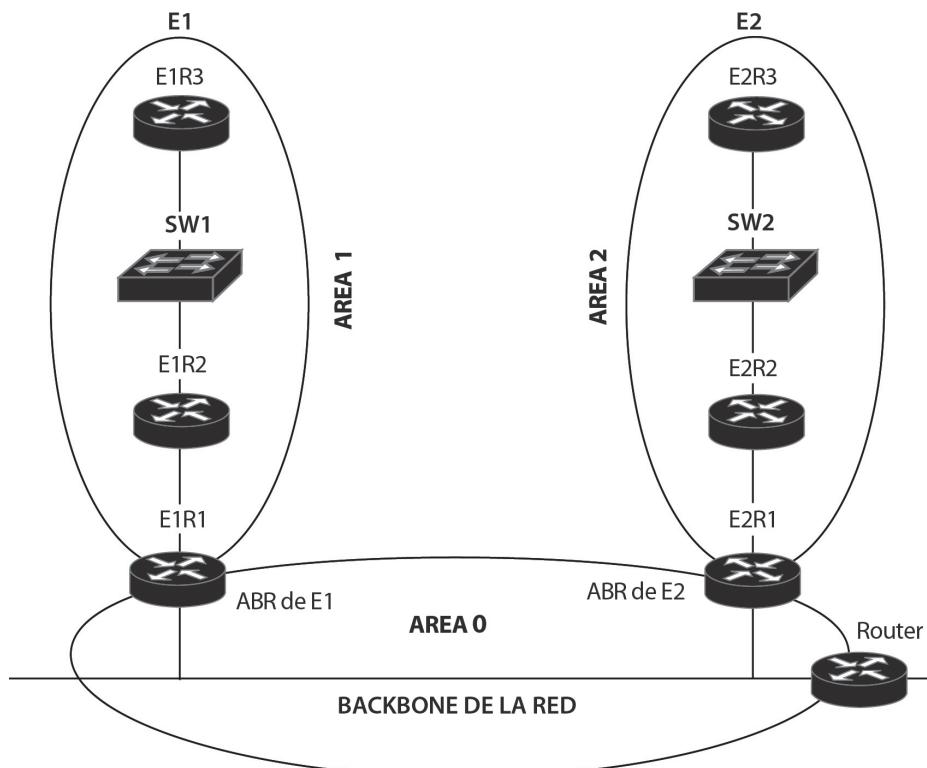


Figura 9.2. Red IP que usa el protocolo de enrutamiento OSPF y divide un sistema autónomo en tres áreas: el área cero que conforma el Backbone de la red, el área 1 (en E1) con equipos administrados por usted y el área 2 (en E2) con equipos administrados por un compañero

Resumen de rutas OSPF

- En el encaminador vecino E2R1 (o también R1 de E2) ejecute el comando *show ip route*. ¿Cuántas rutas del E1 se tienen en E2?
Respuesta: cuatro.
- E1 usa cuatro subredes /26 contiguas, la ruta 192.168.1.0/24 (que se va a utilizar en el siguiente punto) puede resumir las cuatro subredes /26.
- Configure la ruta resumen en el ABR de E1 (E1R1) y en el ABR de E2 (E2R1) de la siguiente manera:

```
E1R1(config)# router ospf 1
E1R1(config-router)# area 1 range 192.168.1.0 255.255.255.0
```

```
E2R1(config)# router ospf 1
E2R1(config-router)# area 2 range 192.168.2.0 255.255.255.0
```

- Ejecute el comando *show ip route* en E1R1 para verificar que las rutas del área 2 están resumidas. Los ABR deben tener rutas específicas para su respectiva área y para el área cero, y rutas resumidas para las otras áreas.

E1R1# *show ip route*

Gateway of last resort is not set

```
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, FastEthernet0/0
192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks
C 192.168.1.128/26 is directly connected, Serial1/0
O 192.168.1.192/26 [110/65] via 192.168.1.130, 00:05:28, Serial1/0
C 192.168.1.0/26 is directly connected, Loopback0
O 192.168.1.0/24 is a summary, 00:05:28, Null0
O 192.168.1.65/32 [110/65] via 192.168.1.130, 00:05:28, Serial1/0
192.168.2.0/24 is subnetted, 1 subnets
O IA 192.168.2.0 [110/2] via 10.1.1.2, 00:04:56, FastEthernet0/0
```

INFORMACIÓN COMPLEMENTARIA

Los encaminadores OSPF establecen una relación de vecindad y después intercambian información de enrutamiento mediante “Anuncios de estado

de enlace” o LSA (Link State Advertisements), para esto usan las direcciones IP Multicast 224.0.0.5 (para todos los encaminadores OSPF) y 224.0.0.6 (para el encaminador OSPF designado). Con esto, cada encaminador obtiene una topología precisa de la red, ello permite calcular su tabla de enrutamiento. Una red OSPF puede dividirse en varias áreas para que el intercambio de LSA quede confinado dentro de cada una de ellas, en dicho caso, la información de enrutamiento proveniente de otras áreas se inyecta de manera resumida por el encaminador de borde de área o ABR, el cual se encarga de conectar un área específica con las otras áreas de la red por medio del área cero (esto es fundamental, puesto que las otras áreas deben conectarse a ésta). Lo anterior permite que una red basada en OSPF tenga gran escalabilidad y un tiempo de convergencia bajo. Referirse a la obra de Douglas Comer referenciada en la bibliografía.

PROBLEMAS

1. Practique el siguiente código que permite que el equipo denominado “Router” (a través de cuya interfaz FastEthernet usted podría conectar al área cero de la Figura 9.2) propague la ruta por defecto a la red OSPF.

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip address 10.1.1.3 255.255.255.0
Router(config-if)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 200.1.1.1
Router(config)# router ospf 1
Router(config-router)# network 10.1.1.0 0.0.0.255 area 0
Router(config-router)# default-information originate metric 31 metric-type 1
```

2. Practique el siguiente código que permite que el equipo “Router” (del punto anterior) redistribuya dos rutas estáticas hacia la red OSPF.

```
Router(config)# ip route 192.168.3.0 255.255.255.0 12.2.2.2
Router(config)# ip route 9.1.1.0 255.255.255.0 13.3.3.3
Router(config)# router ospf 1
Router(config-router)# redistribute static
```

¿Cuál es el resultado en la tabla de enrutamiento de los otros encaminadores?

Adicionar la palabra clave “*subnet*” al comando “*redistribute static*” (*redistribute static subnet*).

Nuevamente ¿cuál es el resultado en la tabla de enrutamiento de los otros encaminadores?

3. Para controlar la selección del DR se utiliza el comando *ip ospf priority*. Suponiendo que un segmento LAN es compartido por tres encaminadores (RX, RY y RZ) con la siguiente configuración de sus interfaces Ethernet.

```
RX(config-if)# ip ospf priority 3
RY(config-if)# ip ospf priority 0
RZ(config-if)# ip ospf priority 5
```

¿Cuál encaminador asumirá el papel de DR del segmento?

¿Cuál encaminador asumirá el papel de BDR del segmento?

¿Cuál encaminador nunca asumirá el papel de DR o BDR del segmento?

4. Habilitar la autenticación MD5 OSPF en el área cero entre dos encaminadores (podría ser entre E1R1 y E2R1 de la Figura 9.2). El siguiente código sirve de guía para configurar los dos encaminadores. Probar el resultado con el comando *show ip ospf interface fasteternet 0/0*.

```
E1R1(config)# interface Fastethernet 0/0
E1R1(config-if)# ip ospf message-digest-key 1 md5 passcode
E1R1(config-if)# exit
E1R1(config)# router ospf 1
E1R1(config-router)# area 0 authentication message-digest
```

5. Revise las características de los siguientes cuatro tipos de área: Stubby Area, Totally Stubby Area, Not So Stubby Area (NSSA), Totally Stubby Not So Stubby Area.

GLOSARIO

Anuncio del estado del enlace (Link State Advertisement o LSA): el protocolo OSPF se basa en que cada encaminador tiene conocimiento de la topología de la red, dicho conocimiento se consigue mediante los anuncios del estado de los enlaces que provienen de otros encaminadores que estén dentro de la misma área.

Área cero o área de backbone: área común e indispensable de OSPF mediante la cual se puede intercambiar la información de enrutamiento proveniente de otras áreas.

Encaminador de borde de área (Area Border Router o ABR): equipo que se encarga de conectar un área específica con el área cero, dicho equipo puede enviar hacia el área específica la información resumida de enrutamiento que proviene de las otras áreas.

Respaldo del router designado: Previendo que el encaminador designado de una red puede fallar en algún momento, en el proceso de elección del router designado también se elige el respaldo del mismo.

Router designado: en las redes de acceso múltiple tipo difusión –Broadcast Multiple Access (BMA)–, como Ethernet, es necesario elegir uno de los encaminadores para que envíe los LSA relacionados con dicha red en representación de los otros, de tal manera que se evita la duplicidad innecesaria del mismo trabajo.

BIBLIOGRAFÍA

- COMER, D. (2005). *Internetworking with TCP/IP, Volumen 1: Principles, Protocols, and Architecture*. 5th Ed. Upper Saddle River, NJ: Pearson Prentice Hall.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOYLE, J.; CARROLL, J. (2007). *Routing TCP/IP*. 2nd Ed. Indianapolis, IN: Cisco Press. Vol. 1.
- KUROSE J. F.; ROSS, K. W. (2012). *Computer Networking: A Top-down Approach*. 7th Ed. Boston: Addison-Wesley.
- STEVENS, W. R. (1994). *TCP/IP Illustrated, Vol. 1: The Protocols*. Reading, MA: Addison-Wesley.

CAPÍTULO 10

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 Comutador 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.

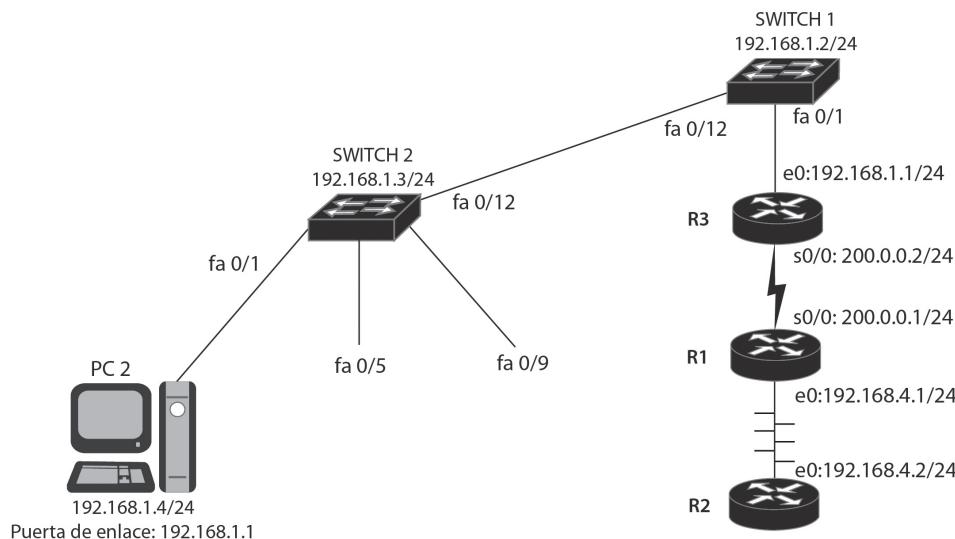


Figura 10.1. Diagrama de red para practicar conceptos alrededor de VLAN, NAT y PAT

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 [CRTL] 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”. Asígnele al conmutador la dirección IP 192.168.1.3 con máscara de subred 255.255.255.0. Asígnele 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 comutadores 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 comutador 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 comutadores. El costo que adiciona un comutador 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 comutador diferente al switch raíz, para cada segmento de la red se escoge un solo puerto de un comutador 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 comutador progresará 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 comutador). 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 comutador 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 commutadores 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 commutadores 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 commutadores 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 commutador 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 commutadores que tengan igual prioridad?, ¿cuál es el criterio de desempate para elegir el puerto raíz en un commutador 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 commutadores que anuncien hacia el segmento el mismo costo al switch raíz?
4. EtherChannel: revise las siguientes líneas de configuración que permiten interconectar dos commutadores 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.

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 commutada, creación e interconexión de VLAN, conexión de comutadores 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 comutador 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.

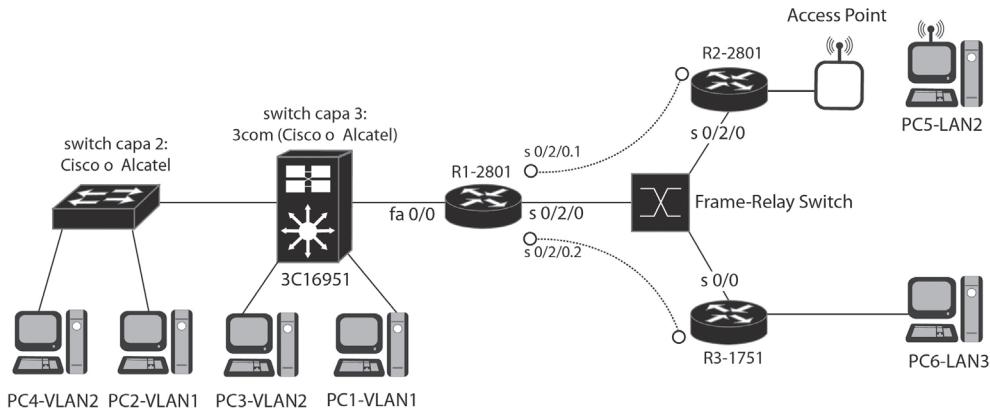


Figura 11.1 Esquema de la intranet del proyecto

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 IEEE802.3– 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	Número 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-

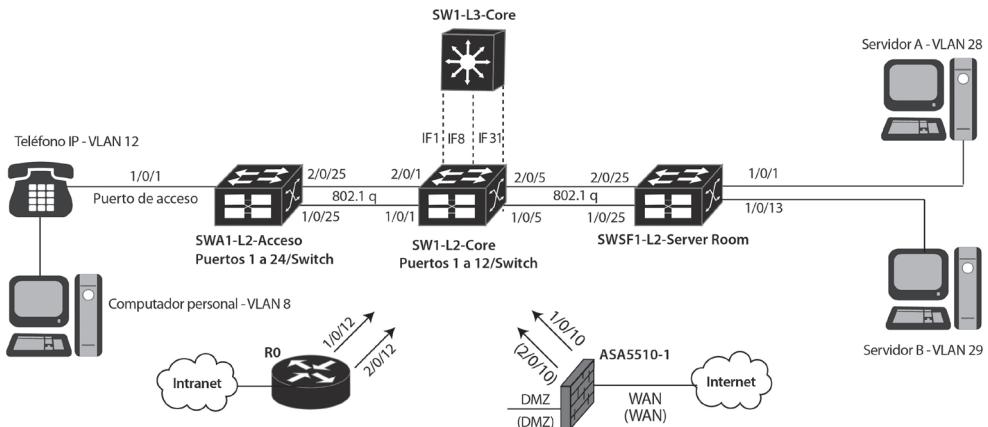


Figura 11.2 Infraestructura básica de la red “LAN1” de Dirección general “Headquarters”

rios de cableado para los commutadores de acceso; dos commutadores 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 commutadores apilados y se tienen dos armarios de cableado para commutadores de la granja de servidores. Observe que, en la nomenclatura usada, la letra “x” en los nombres de los commutadores 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 commutador 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 commutador de núcleo con mayor desempeño –por ejemplo, el commutador 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=Rendezvous Point). “ip multicast-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 commutador 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 commutador 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 commutador 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 commutadores 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-phone (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.

CAPÍTULO 12

REDES INALÁMBRICAS IEEE 802.11 A/B/G

Para que una estación cliente (inalámbrica) tenga acceso a la infraestructura de red, es necesario que ésta se asocie y autentique con el punto de acceso (Access Point) que se encuentre más cercano. Las soluciones de acceso inalámbrico IEEE 802.11, en general, pueden basarse en un conjunto de puntos de acceso autónomos o en un conjunto de puntos de acceso livianos (administrados por un controlador central), distribuidos estratégicamente en las áreas que requieran el servicio. La conexión entre la estación cliente y el punto de acceso (AP) puede ser abierta o proporcionar diferentes grados de seguridad: WEP, WPA o WPA2 (personal o empresarial). En el presente capítulo se aborda el aprovisionamiento de tres puntos de acceso autónomos (AP1, AP2 y AP3) que usan las normas IEEE802.11 b/g, y coexisten en la misma área de trabajo gracias a que operan en los canales 1, 6 y 11, respectivamente. También se aborda el aprovisionamiento de una red inalámbrica con mayor cobertura, en la cual se utiliza la interfaz de radio IEEE 802.11a para el enlace entre AP1 y AP2, y se reutiliza la interfaz de radio IEEE 802.11 b/g para el enlace entre el AP1 y AP3. La seguridad que se utiliza en los diferentes enlaces es: abierta, WEP, WPA personal y WPA2 personal.

OBJETIVO

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

- Configurar un punto de acceso inalámbrico y las estaciones clientes inalámbricas (IEEE 802.11 b/g) para que funcionen “sin seguridad” o con seguridad “WEP open”.
- Configurar un punto de acceso inalámbrico y las estaciones clientes inalámbricas (IEEE 802.11 b/g) para que funcionen con “WPA personal (TKIP o AES) usando clave compartida”.
- Realizar la interconexión de varias redes inalámbricas mediante puntos de acceso IEEE 802.11 a/b/g.

PROCEDIMIENTO

Configuración de los puntos de acceso inalámbricos y de las estaciones clientes inalámbricas IEEE 802.11 b/g

Identificación de los equipos a usar en el montaje

Un punto de acceso inalámbrico es un dispositivo que funciona en la capa 2, sus decisiones las basa en las direcciones MAC, presentes en las tramas Ethernt (o IEEE 802.3) de la parte cableada y en las tramas IEEE 802.11 del lado inalámbrico de la red. Después que la estación cliente inalámbrica, se haya asociado y autenticado con el AP, este último recibirá las tramas “unicast” de dicha estación (aquellas tramas que tengan como destino una estación en la red cableada) y las reenviará hacia la red alambrada. El AP también recibirá las tramas “unicast” de la red alambrada (que tengan como destino la estación inalámbrica) y las reenviará hacia a la estación inalámbrica. Para el caso de las tramas de difusión (broadcast), el AP se comporta como un dispositivo de capa 2 convencional.

Para el montaje, se dispone de los puntos de acceso relacionados en la Tabla 12.1. Es provechoso tomar nota de las direcciones MAC que tienen las interfaces alambradas y las interfaces de aire de cada dispositivo, puesto que esto facilita el entendimiento y verificación de los resultados. En la Tabla 12.1 se asigna una dirección IP a la interfaz BVI1 de cada AP con el propósito de habilitar su administración. El AP utilizado tiene la interfaz IEEE 802.11 b/g (antena de 2.4 Ghz) en el mismo lado que la interfaz FastEthernet (parte frontal de la Figura 12.1), mientras que la interfaz IEEE 802.11a (antenas de 5 Ghz) está en el lado opuesto (parte posterior de la Figura 12.1).

Tabla 12.1 Direcciones MAC correspondientes a las interfaces LAN y de aire de los puntos de acceso

Punto de acceso Modelo del AP Hostname del AP Dirección IP de BVII	Interfaz FastEthernet 0 Dirección MAC	Interfaz Dot11Radio0 IEEE 802.11 b/g Canal de operación Dirección MAC	Interfaz Dot11Radio1 IEEE 802.11a Canal de operación Dirección MAC
AIR-AP1242AG-AK9 ap1 192.168.55.150	0018:b9e9:4aaa	1 0018:7489:ec70	Dinámico 0018:748d:ec70
AIR-AP1242AG-AK9 ap2 192.168.55.151	0018.b9e9.4b7e	6 0018.7489.f310	Dinámico 0018.748d.f310
AIR-AP1231G-AK9 ap3 192.168.55.152	0018.19bd.b6a7	11 000a.b87e.b680	N/A N/A



Figura 12.1. Punto de acceso inalámbrico modelo AIR-AP1242AG-A-K9 de Cisco™

Una estación inalámbrica que se asocie a un AP puede recibir una dirección IP de parte de un servidor DHCP instalado en la red alambrada, o puede tener asignada la dirección IP de manera permanente. Para el montaje se dispone de las tarjetas inalámbricas USB relacionadas en la Tabla 12.2, cada interfaz inalámbrica tiene una dirección MAC asignada por el fabricante (la cual se puede administrar localmente).



Figura 12.2. Tarjeta USB inalámbrica WUSB54GC marca Linksys (Cisco)

Tabla 12.2. Direcciones MAC correspondientes a las tarjetas inalámbricas WUSB54GC

Nombre del equipo	Dirección MAC de la tarjeta inalámbrica
PC-A	0018:3917:91fd
PC-B	0018:3917:918f
PC-C	0018:3917:9180
PC-D	0018:3917:91ba

Instalar el driver de las tarjetas inalámbricas y la tarjeta WUSB54GC

Siga el siguiente procedimiento en estricto orden (no conecte la tarjeta WUSB54GC al computador personal antes de instalar el driver).

1. Usando el CD de las tarjetas WUSB54GC, instale el driver en los computadores personales: PC-A, PC-B, PC-C, PC-D.
2. Ahora ya puede conectar la tarjeta WUSB54GC a cada computador personal
3. Desconecte estos cuatro PC de la red local alambrada (Ethernet).

Configurar tres puntos de acceso con los valores por defecto, configurar la dirección IP en la interfaz BVI1, entrar a “Express Setup” por medio de un navegador Web, configurar un servidor DHCP, habilitar las interfaces de radio y configurar los canales de operación de la interfaz de radio 802.11 b/g

1. Manteniendo presionado el botón “mode” del “Access Point” (estando el AP apagado), simultáneamente conecte el adaptador a un tomacorriente durante 2 minutos. Repita este paso para cada uno de los tres AP.

2. Conecte el puerto COM1 del PC al puerto de consola del AP. Use un programa de emulación de terminal (por ejemplo, el programa Hyperterminal: 9600, 8, ninguno, 1, ninguno) para entrar a la interfaz de línea de comandos de cada AP (ap1, ap2 ó ap3) y verificar la configuración actual mediante el comando *show running-config*; constate que las interfaces de radio estén administrativamente deshabilitadas (shutdown).
3. Configure el “hostname” y la dirección IP de la interfaz BVII de cada AP de la siguiente manera (digite el usuario “Cisco” y la clave “Cisco”).

```

ap> enable
password: Cisco
ap# show running-config
ap# configure terminal
(config)# hostname ap1 !(o ap2 o ap3, nombre de acuerdo a la Tabla 12.1)
(config)# interface BVII
(config-if)# ip address 192.168.55.150 255.255.255.0 !(valor de acuerdo a la Tabla 12.1)

```

4. Conecte la interfaz FastEthernet 0 de cada AP (interfaz de LAN alambrada del AP) a los puertos de un conmutador Ethernet (puertos que pertenezcan a la VLAN 1, en el supuesto caso que el conmutador tenga configuradas varias VLAN). Mediante otro computador que se encuentre conectado al conmutador, ejecute un programa navegador Web (Mozilla Firefox o Internet Explorer) y acceda a cada AP (use la dirección URL <http://192.168.55.150> para el ap1, <http://192.168.55.151> para el ap2, <http://192.168.55.152> para el ap3), digite el usuario “Cisco” y la clave “Cisco”. Haga clic en la opción “Express Setup” y configure la puerta de enlace de cada AP con la dirección 192.168.55.106, hacer clic en “Apply”.
5. Configurar solamente el ap1 para que haga la función de servidor DHCP.

```

ap1(config)# ip dhcp excluded-address 192.168.55.1 192.168.55.220
ap1(config)# ip dhcp pool direcciones
ap1(config-pool)# network 192.168.55.0 255.255.255.0
ap1(config-pool)# default-router 192.168.55.106
ap1(config-pool)# lease 1
ap1(config-pool)# dns-server 192.168.18.10

```

6. Habilitar las interfaces de radio 802.11 b/g en cada AP (en ap1, ap2 y ap3).

```
(config)# interface Dot11Radio0  
(config-if)# no shutdown
```

7. Habilitar las interfaces de radio 802.11 a en cada AP (solamente en ap1 y ap2).

```
(config)# interface Dot11Radio1  
(config-if)# no shutdown
```

8. Para evitar interferencia entre las interfaces 802.11 b/g de los AP, hay que configurarlos para que el ap1 funcione utilizando el canal 1, el ap2 utilice el canal 6 y al el ap3 utilice el canal 11. Esto se consigue por medio del navegador Web, al hacer clic en la opción “Network Interfaces” (que permite observar la página resumen de interfaces); después, hacer clic en la interfaz de radio “Radio802.11B/G” (que permite observar la página que muestra el estado de la interfaz de radio), hacer clic en la pestaña “Settings” (que permite observar la página de configuración de la interfaz de radio), “seleccionar el canal” de la interfaz de radio 802.11 b/g (de acuerdo al nombre del AP en la Tabla 12.1) y hacer clic en “Apply”.

Configuración para operar en modo “No security”

1. Hacer clic en la opción “Express Security”, crear un SSID (Service set identifier) en cada AP con las siguientes características:

Nombre: ap1nosec (para el ap1), ap2nosec (para el ap2), ap3nosec (para el ap3).

- Que no pertenezca a ninguna VLAN.
- Que sea difundido en la trama de “Beacon”.
- Sin seguridad.

Cuando se usa la opción “Express Security”, por defecto, el SSID creado es aplicado a ambas interfaces de radio, a pesar que el usuario requiera aplicar el SSID a una sola interfaz de radio. En nuestro caso, nos interesa que el SSID sea aplicado a la interfaz de radio Dot11Radio0 (802.11 b/g). Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```

! El comando “guest-mode” difunde el SSID ap1nosec en la trama Beacon
dot11 ssid ap1nosec
authentication open
guest-mode
!
interface Dot11Radio0
!
ssid ap1nosec

```

2. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, hacer un barrido para buscar las redes inalámbricas anunciadas por los AP. Para uno de los SSID anunciados, modificar su perfil en el software de la tarjeta USB, haciendo que el nombre del SSID configurado coincida con el SSID anunciado por el AP al cual se desea conectar, y configurar la opción “security = disable”. Salvar la configuración y conectarse al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Verificar las asociaciones con el comando *show dot11 associations*. Por medio de “Express Security”, borrar el SSID en los tres AP.

Configuración para operar en modo “WEP Open”

1. Hacer clic en la opción “Express Security”, crear un “SSID” en cada AP con las siguientes características:

Nombre: ap1wepopen (para el ap1), ap2wepopen (para el ap2), ap3wepopen (para el ap3).

- Que no pertenezca a ninguna VLAN.
- Que el SSID sea difundido en la trama de Beacon.
- Seguridad WEP Mandatory.
- Clave en la ranura 1 para que tenga un tamaño de 40 bits con valor hexadecimal 0123456789 (Transmit Key).

Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1wepopen
authentication open
guest-mode
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption key 1 size 40bit 7 BD5A59824B7D transmit-key
encryption mode wep mandatory
!
ssid ap1wepopen
```

2. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, hacer un barrido para buscar las redes inalámbricas anunciadas por los AP. Para uno de los SSID anunciados, modificar su perfil en el software de la tarjeta USB, haciendo que el nombre del SSID configurado coincida con el SSID anunciado por el AP al cual se desea conectar, configurar la opción “security = WEP” y la clave con el valor 0123456789. Salvar la configuración y conectarse al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por “Express Security” borrar el SSID.

Configuración para operar en modo

“WPA Personal TKIP con clave compartida”

1. Hacer clic en la opción “Security” y en “Encryption Manager” realizar los siguientes pasos:
 - a. En “Encryption Mode” marcar “Cipher” y escoger “TKIP”.
 - b. Borrar el valor de la clave de cifrado 1.
 - c. Marcar la clave de cifrado 2 como clave de transmisión.
 - d. Aplicar lo anterior al radio Dot11Radio0.
2. En “SSID Manager” realizar los siguientes pasos:
 - e. SSID = ap1tkip (para el ap1), ap2tkip (para el ap2), ap3tkip (para el ap3).
 - f. Mediante el recuadro de selección aplicar el SSID al radio 802.11G.
 - g. Marcar el recuadro de selección “Open authentication” y seleccione “No addition”.

- h. En la opción “Client Authentication Key Management”, seleccionar “Key Management = Mandatory”, marcar el recuadro “WPA”.
- i. Llenar en “WPA Preshared Key” el valor “0123456789” y marcar el botón circular “ASCII”.
- j. Aplicar la configuración con el primer botón “Apply”.

Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1tkip
authentication open
authentication key-management wpa
wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
encryption mode ciphers tkip
!
ssid ap1tkip
```

3. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, crear un perfil haciendo que el nombre del SSID configurado coincida con el SSID del AP al cual se desea conectar (el SSID no es anunciado porque no tiene el comando *guest-mode*), configurar la opción “security = WPA-Personal” y la clave compartida con el valor 0123456789. Salve la configuración y conéctese al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por “Express Security” borrar el SSID en los tres AP.

Configuración para operar en modo

“WPA Personal AES con clave compartida”

1. Hacer clic en la opción “Security” y en “Encryption Manager” realizar los siguientes pasos:
 - a. En “Encryption Mode” marcar “Cipher” y escoger “AES-CCMP”.
 - b. Borrar el valor de la clave de cifrado 1.
 - c. Marcar la clave de cifrado 2 como clave de transmisión.
 - d. Aplicar lo anterior al radio Dot11Radio0.

2. En “SSID Manager” realizar los siguientes pasos:
 - e. SSID = ap1aes (para el ap1), ap2aes (para el ap2), ap3aes (para el ap3).
 - f. Mediante el recuadro de selección, aplicar el SSID al radio 802.11G.
 - g. Marcar el recuadro de selección “Open authentication” y seleccionar “No addition”.
 - h. En la opción “Client Authentication Key Management”, seleccionar “Key Management = Mandatory”, marcar el recuadro “WPA”.
 - i. Llenar en “WPA Preshared Key” el valor “0123456789” y marcar el botón circular “ASCII”.
 - j. Aplicar la configuración.

Lo anterior se traduce a las siguientes líneas del archivo de configuración en la interfaz Dot11Radio0 para el ap1.

```
dot11 ssid ap1aes
authentication open
authentication key-management wpa
wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
    encryption mode ciphers aes-ccm
    ssid ap1aes
```

3. En los computadores personales (PC-A, PC-B, PC-C, PC-D) con tarjetas WUSB54GC, crear el perfil, haciendo que el nombre del SSID configurado coincida con el SSID del AP al cual se desea conectar (el SSID no es anunciado porque no tiene el comando *guest-mode*), configurar la opción “security = PSK2” y la clave compartida con el valor 0123456789. Salve la configuración y conéctese al AP. Verificar que la tarjeta WUSB54GC del PC se asocia al AP correspondiente, recibe una dirección IP del servidor DHCP y puede comunicarse con otros equipos que se encuentran conectados a la red alambrada (mediante ping). Por “Express Security” borrar el SSID.

Interconexión de los Puntos de acceso IEEE 802.11 a/b/g

En el siguiente montaje se busca que los puntos de acceso ap1 y ap2 se interconecten en modo punto a punto usando la interfaz de radio Dot11Radio1 de cada uno de ellos (IEEE802.11a, la cual opera a 5 Ghz). Para ello el ap1 opera en modo “root bridge” sobre su interfaz de radio Dot11Radio1,

mientras que el ap2 opera en modo “non-root bridge” sobre su interfaz de radio Dot11Radio1. Además el ap1 opera en modo “root bridge wireless-clients” sobre su interfaz de radio Dot11Radio0 (IEEE 802.11 b/g de 2.4 Ghz), con el fin de recibir tanto a las estaciones clientes cercanas como al ap3 por dicha interfaz, mientras que el ap3 opera en modo “non-root bridge with wireless clients” sobre su interfaz de radio Dot11Radio0 para recibir estaciones clientes cercanas y para asociarse al ap1.

Realizar el siguiente procedimiento general en el ap1

1. Configurar los siguientes SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap1,
anunciarlo a los clientes del ap1 y ! recibir al ap3
dot11 ssid extendido
authentication open
guest-mode
!
! SSID para aplicarlo a la interfaz Dot11Radio1 del ap1 y recibir al ap2
dot11 ssid punto-a-punto
authentication open
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “0123456789”, que la clave 1 sea transmitida, aplicar el SSID “extendido” y que el papel de la interfaz sea “root bridge wireless-clients”.

```
interfaz Dot11Radio0
!
encryption key 1 size 40bit 7 BA94047C696A transmit-key
encryption mode wep mandatory
!
ssid extendido
!
station-role root bridge wireless-clients
```

3. Hacer que la interfaz Dot11Radio1 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “9876543210”, que la clave 1 sea transmitida, aplicar el SSID “punto-a-punto” y que el papel de la interfaz sea “root bridge”.

```
interfaz Dot11Radio1
!
encryption key 1 size 40bit 7 33072E76758A transmit-key
encryption mode wep mandatory
!
ssid punto-a-punto
!
station-role root bridge
```

Realizar el siguiente procedimiento general en el ap2

1. Configurar los siguientes SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap2 y anunciarlo a los clientes del
ap2
dot11 ssid remoto
authentication open
guest-mode
!
! SSID para aplicarlo a la interfaz Dot11Radio1 del ap2 y conectarse al ap1
dot11 ssid punto-a-punto
authentication open
infrastructure-ssid optional
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “1234512345”, que la clave 1 sea transmitida, aplicar el SSID “remoto” y que el papel de la interfaz sea “root”.

```
interface Dot11Radio0
!
encryption key 1 size 40bit 7 66061D6FD052 transmit-key
encryption mode wep mandatory
!
ssid remoto
!
station-role root
```

3. Hacer que la interfaz Dot11Radio1 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a

“9876543210”, que la clave 1 sea transmitida, aplicar el SSID punto-a-punto y que el papel de la interfaz sea “non-root bridge”.

```
interface Dot11Radio1
!
encryption key 1 size 40bit 7 EE6B241F059D transmit-key
encryption mode wep mandatory
!
ssid punto-a-punto
!
station-role non-root bridge
```

Realizar el siguiente procedimiento general en el ap3.

1. Configurar el siguiente SSID.

```
! SSID para aplicarlo a la interfaz Dot11Radio0 del ap3,
anunciarlo a los clientes del ap3 y ! conectarse al ap1
dot11 ssid extendido
authentication open
guest-mode
infrastructure-ssid optional
```

2. Hacer que la interfaz Dot11Radio0 funcione con WEP obligatorio, con la clave 1 de 40 bits de tamaño, valor hexadecimal de la clave igual a “0123456789”, que la clave 1 sea transmitida, aplicar el SSID “extendido” y que el papel de la interfaz sea “non-root bridge wireles-clients”.

```
interface Dot11Radio0
!
encryption key 1 size 40bit 7 66063D6FD042 transmit-key
encryption mode wep mandatory
!
ssid extendido
!
station-role non-root bridge wireles-clients
```

PROBLEMAS

1. Buscar una solución inalámbrica de un fabricante (Cisco, Meru Networks, Aruba Networks, Trapeze) que incluya los pasos necesarios para el aprovisionamiento de una red basada en puntos de acceso livianos manejados desde un controlador central o WLC (Wireless LAN Controller).
2. Leer sobre los aspectos generales y el estado actual del protocolo estándar de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP: Control And Provisioning of Wireless Access Points Protocol Specification, RFC 5415).

GLOSARIO

Asociarse: primer paso que se da en el establecimiento de la conexión entre una estación cliente inalámbrica y un punto de acceso (que emite uno o varios identificadores o SSID). El usuario de la estación cliente decide con cuál identificador desea asociarse para continuar con el establecimiento de la conexión.

Autenticarse: segundo paso que se da en el establecimiento de la conexión entre una estación cliente inalámbrica y un punto de acceso. En este paso, la estación presenta las credenciales para que el punto de acceso las valide y permita el flujo de tramas con datos hacia y desde la red cableada.

SSID (Service Set Identifier): identificador emitido por la interfaz de radio del punto de acceso (el AP puede emitir uno o varios SSID). El SSID tiene un perfil que define las características que tendrá la conexión de la estación cliente inalámbrica que se autentique en dicho identificador (VLAN, usuario, clave, etc.).

Trama Beacon: trama de gestión IEEE 802.11 que se emite con cierta periodicidad (100 milisegundos por lo general, o el valor configurado), anunciando la presencia de la red inalámbrica e información de la red.

Unicast: tramas o paquetes que van dirigidos a un solo destino.

WEP (Wired Equivalent Privacy): algoritmo de seguridad (frágil) usado para proteger un enlace IEEE 802.11, caracterizado por usar una clave con longitud de 40 bits o de 104 bits. Declarado obsoleto por la IEEE en el año 2004.

WPA (Wi-Fi Protected Access) Personal: algoritmo de seguridad (intermedio) usado para proteger un enlace IEEE 802.11, útil en equipos que no tengan hardware con soporte WPA2. WPA Personal está basado en el

protocolo de cifrado TKIP (Temporal Key Integrity Protocol) y en una clave compartida entre el punto de acceso y la estación cliente.

WPA2 Personal o Empresarial: algoritmo de seguridad (sucesor de WPA) usado para proteger un enlace IEEE 802.11. Está basado en un mecanismo de cifrado AES y usa el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

BIBLIOGRAFÍA

- GAST, M. (2002). *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, CA: O'Reilly.
- KOTFILA, D.; MOORHOUSE, J.; PRICE, C.; WOLFSON, R. (2008) *CCNP Building Multilayer Switched Networks (BCMSN 642-812) Lab Portfolio*. Indianapolis, IN: Cisco Press.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

ENCAPSULADO GENÉRICO DE ENCaminamiento Y SEGURIDAD IP (GRE/IPSEC)

GRE (Generic Routing Encapsulation) es un protocolo estándar abierto, documentado en los RFC 1701 y 1702, y actualizado en el RFC 2784. GRE es encapsulado directamente en la capa IP, la cual usa el valor 47 en el campo “número de protocolo” para identificarlo y transportarlo. GRE incluye sus propios campos en el encabezado y un campo de datos; en este último transporta diferentes protocolos de capa 3, incluyendo a IP. IPsec (IP security) es un conjunto de protocolos y algoritmos relacionados con la seguridad de los datagramas IP, documentado en los RFC 2401 a 2412, y en el RFC 2451. El marco de referencia IPsec proporciona las funciones de autenticación y cifrado del tráfico IP, y el intercambio seguro de las claves de autenticación y cifrado; siendo compatible con IPv4 e IPv6. En el presente capítulo se explora la interconexión de tres redes IP privadas de un suscriptor por medio de la Internet pública: se usa el protocolo GRE para transportar los datagramas IP de las redes privadas y al protocolo IPsec en modo transporte para proporcionar la protección y seguridad por ellos requeridas.

OBJETIVO

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

- Configurar los protocolos GRE e IPsec en los encaminadores de borde de tres redes de área local, con el propósito de interconectar dichas redes mediante el uso seguro de la infraestructura pública de Internet.
- Monitorizar las redes que usan los protocolos GRE e IPsec.

PROCEDIMIENTO

Red que permite emular una Internet pública básica

Montaje de emulación de la Internet pública básica

Llevar a cabo el montaje y la conexión de los encaminadores R1, R2, R3 e ISP de acuerdo con la Figura 13.1 (puede usar GNS3); los encaminadores R1, R2 y R3 representan a un suscriptor conectado a uno o varios ISP de la Internet pública, mientras que el encaminador ISP es una representación simplificada de la Internet pública (conformada por diferentes ISP).

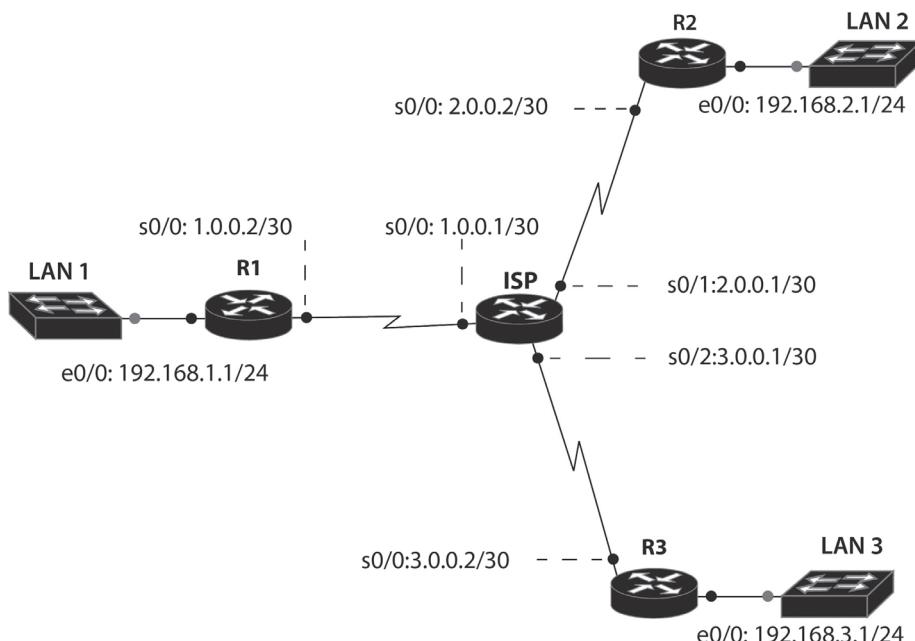


Figura 13.1. Representación básica de la conexión de tres redes privadas de un suscriptor a la Internet pública (ISP)

Configuración y prueba de la Internet pública

Configurar los encaminadores ISP, R1, R2 y R3 de acuerdo a las líneas de código de los archivos ISP-internet-cfg, R1-internet-cfg, R2-internet-cfg y R3-internet-cfg, relacionados a continuación. Estos archivos permiten establecer la funcionalidad de conexión de tres redes de área local con una Internet pública básica. Probar el funcionamiento de dicha red.

ISP-internet-cfg	R1-internet-cfg
<pre> hostname ISP ! interface Serial0/0 description *Recibe a R1* ip address 1.0.0.1 255.255.255.252 no shutdown ! interface Serial0/1 description *Recibe a R2* ip address 2.0.0.1 255.255.255.252 no shutdown ! interface Serial0/2 description *Recibe a R3* ip address 3.0.0.1 255.255.255.252 no shutdown !</pre>	<pre> ! hostname R1 ! interface Serial0/0 description *Conexión a Internet* ip address 1.0.0.2 255.255.255.252 no shutdown ! interface Fastethernet0/0 description * Conexión de R1 a Lan1* ip address 192.168.1.1 255.255.255.0 no shutdown ! ip route 0.0.0.0 0.0.0.0 1.0.0.1 !</pre>

R2-internet-cfg	R3-internet-cfg
<pre> hostname R2 ! interface Serial0/0 description *Conexión a Internet* ip address 2.0.0.2 255.255.255.252 no shutdown ! interface Fastethernet0/0 description * Conexión de R2 a Lan2* ip address 192.168.2.1 255.255.255.0 no shutdown ! ip route 0.0.0.0 0.0.0.0 2.0.0.1 !</pre>	<pre> hostname R3 ! interface Serial0/0 description *Conexión a Internet* ip address 3.0.0.2 255.255.255.252 no shutdown ! interface Fastethernet0/0 description * Conexión de R3 a Lan3* ip address 192.168.3.1 255.255.255.0 no shutdown ! ip route 0.0.0.0 0.0.0.0 3.0.0.1 !</pre>

Para probar el funcionamiento de la red anterior, se ejecutan los siguientes comandos desde el encaminador R1.

```
R1> ping ip 2.0.0.2 source 1.0.0.2  
R1> ping ip 3.0.0.2 source 1.0.0.2  
R1> ping ip 2.0.0.2 source 192.168.1.1  
R1> ping ip 3.0.0.2 source 192.168.1.1
```

Los primeros dos comandos deben funcionar, mientras que los dos últimos no, puesto que el encaminador ISP no conoce la red del origen del mensaje ICMP (192.168.1.0/24). Note que el encaminador ISP solamente conoce las tres redes directamente conectadas a él: 1.0.0.0/30; 2.0.0.0/30; y 3.0.0.0/30.

Túneles GRE funcionando sobre la Internet pública

Túneles GRE

Observar y tener en cuenta las direcciones IP (lógicas) de los túneles que se van a crear entre los encaminadores R1-R2 y R1-R3, representados en la Figura 13.2, dichos túneles permiten interconectar las tres redes de área local a través de Internet.

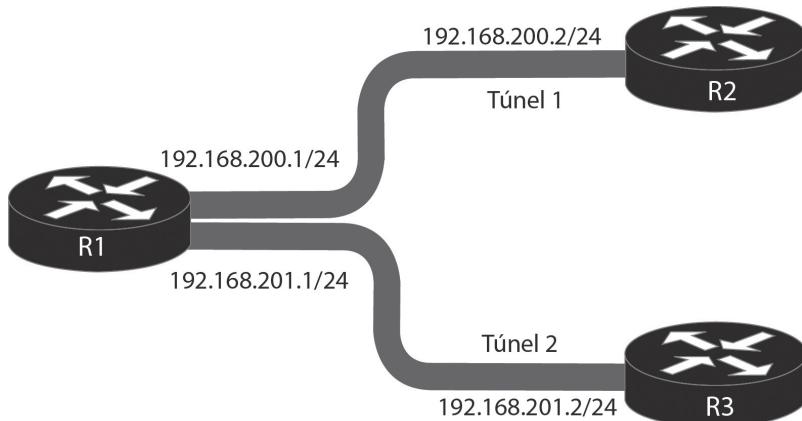


Figura 13.2. Representación de los dos túneles GRE en la Internet pública

Configuración y prueba de los túneles GRE

A la configuración de los encaminadores R1, R2 y R3 realizada anteriormente, adicionar la configuración que permite crear dos túneles mediante el protocolo GRE; los comandos correspondientes se encuentran en las líneas de código de los archivos R1-gre-conf, R2-gre-conf y R3-gre-conf. Probar el funcionamiento de la red configurada con GRE.

R1-gre-conf	R2-gre-conf
<pre> ! interface Tunnel1 description túnel GRE hacia router R2 ip address 192.168.200.1 255.255.255.0 tunnel source 1.0.0.2 tunnel destination 2.0.0.2 ! interface Tunnel2 description Túnel GRE hacia router R3 ip address 192.168.201.1 255.255.255.0 tunnel source 1.0.0.2 tunnel destination 3.0.0.2 ! router rip network 192.168.1.0 network 192.168.200.0 network 192.168.201.0 !</pre>	<pre> ! interface Tunnel1 description Túnel GRE hacia router R1 ip address 192.168.200.2 255.255.255.0 tunnel source 2.0.0.2 tunnel destination 1.0.0.2 ! router rip network 192.168.2.0 network 192.168.200.0 !</pre>

R3-gre-conf
<pre> ! interface Tunnel2 description Tunnel GRE hacia R1 ip address 192.168.201.2 255.255.255.0 tunnel source 3.0.0.2 tunnel destination 1.0.0.2 ! router rip network 192.168.3.0 network 192.168.201.0 !</pre>

Para probar el funcionamiento de la red anterior con el túnel GRE, desde el encaminador R1 se ejecutan los siguientes comandos:

```

R1# show ip route
R1# ping ip 192.168.2.1 source 192.168.1.1
R1# ping ip 192.168.3.1 source 192.168.1.1
```

El primer comando debe mostrar (en la tabla de enrutamiento) las redes aprendidas a través de los dos túneles que se han configurado. El segundo y tercer comando envían un ping extendido que prueba la conexión hacia la interfaz Ethernet de los encaminadores R2 y R3.

Cifrado de los túneles mediante IPsec

Configuración y prueba del cifrado de los túneles GRE mediante IPsec

A la configuración de los encaminadores R1, R2 y R3 realizada en el paso anterior, adicionar la configuración que permite cifrar los dos túneles mediante el protocolo IPsec, cuyos comandos se encuentran en las líneas de código de los archivos R1-ipsec-cfg, R2-ipsec-cfg y R3-ipsec-cfg. Nota: los comandos demasiado largos están precedidos por un asterisco (*) para indicar que continúan en la segunda línea.

R1-ipsec-cfg	R2-ipsec-cfg
<pre>! * access-list 101 permit gre host 1.0.0.2 host 2.0.0.2 * access-list 102 permit gre host 1.0.0.2 host 3.0.0.2 ! crypto isakmp policy 1 encryption aes authentication pre-share group 5 hash sha ! * crypto isakmp key 0 univalle1 address 2.0.0.2 * crypto isakmp key 0 univalle1 address 3.0.0.2 ! * crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac mode transport ! crypto map vpn 10 ipsec-isakmp description VPN from R1 to R2 set peer 2.0.0.2 set transform-set tunel-trans match address 101 !</pre>	<pre>! * access-list 100 permit gre host 2.0.0.2 host 1.0.0.2 ! ! crypto isakmp policy 1 encryption aes authentication pre-share group 5 hash sha ! * crypto isakmp key 0 univalle1 address 1.0.0.2 ! ! * crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac mode transport ! crypto map vpn 10 ipsec-isakmp description VPN from R2 to R1 set peer 1.0.0.2 set transform-set tunel-trans match address 100 !</pre>

Viene

crypto map vpn 11 ipsec-isakmp	!	
description VPN from R1 to R3	!	
set peer 3.0.0.2	!	
set transform-set tunel-trans	!	
match address 102	!	
!	!	
interface Tunnel1	interface Tunnel1	
ip mtu 1500	ip mtu 1500	
ip tcp adjust-mss 1400	ip tcp adjust-mss 1400	
keepalive	keepalive	
!	!	
interface Tunnel2	!	
ip mtu 1500	ip mtu 1500	
ip tcp adjust-mss 1400	ip tcp adjust-mss 1400	
keepalive	keepalive	
!	!	
interface Serial0/0	interface Serial0/0	
crypto map vpn	crypto map vpn	
!	!	

R3-ipsec-cfg

```
!
* access-list 100 permit gre host 3.0.0.2 host 1.0.0.2
!
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 5
  hash sha
!
* crypto isakmp key 0 univalle1 address 1.0.0.2
!
!
* crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac
  mode transport
!
crypto map vpn 10 ipsec-isakmp
  description VPN from R3 to R1
  set peer 1.0.0.2
  set transform-set tunel-trans
  match address 100
!
```

Continua

Viene

```
!
interface Tunnel2
ip mtu 1500
ip tcp adjust-mss 1400
keepalive
!
interface Serial0/0
crypto map vpn
!
```

Para probar el funcionamiento de la red anterior, configurada con dos túneles GRE cifrados con IPsec, se ejecutan los siguientes comandos desde el encaminador R1.

```
R1# show crypto engine connections active
R1# show crypto ipsec sa
R1# show ip route
```

PROBLEMAS

1. Por defecto, la interfaz “tunnel” opera encapsulando el protocolo GRE (*tunnel mode gre ip*). ¿Qué otros protocolos soporta dicha interfaz?, use el comando “*tunnel mode ?*”. Reconocer el propósito de los comandos “*tunnel path-mtu-discovery*” y “*tunnel path-mtu-discovery min-mtu 1000*” en el siguiente trozo de código.

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode ?
R1(config-if)# tunnel path-mtu-discovery
R1(config-if)# tunnel path-mtu-discovery min-mtu 1000
```

2. Por defecto, las conexiones IPsec usan el modo túnel. ¿Qué significa poner a IPsec a operar en modo de transporte? ¿Cuándo es necesario usar el modo túnel de IPsec?

```
R1(config-if)# crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac
R1(config-if)# mode transport
```

3. ¿Qué cambios son necesarios en la configuración de las dos conexiones protegidas por IPsec de la Figura 13.2 para que el modo de autenticación use claves RSA (Rivest, Shamir, and Adelman)? Implemente los cambios y verifique los resultados.

GLOSARIO

Cifrado: técnica que combina claves y algoritmos complejos para transformar los paquetes que transportan datos en texto claro a datos ininteligibles, con el fin de proporcionar seguridad.

Internet pública: la red de redes, está conformada por la interconexión de redes de los ISP de acuerdo a su jerarquía, caracterizada por usar direcciones IP públicas.

Mensaje ICMP: hace referencia al protocolo ICMP, el cual forma parte integral de IP. Sirve para reportar errores, realizar funciones de control y generar mensajes de prueba o depuración.

Túnel: conexión lógica superpuesta sobre otra conexión lógica. Por ejemplo, IP versión 4 encima de IP versión 4, o IP versión 6 encima de IP versión 4.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- COMER, D. (2005). *Internetworking with TCP/IP, Volumen 1: Principles, Protocols, and Architecture*. 5th Ed. Upper Saddle River, NJ: Pearson Prentice Hall.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™* 2nd Ed. Sebastopol, CA: O'Reilly.
- KUROSE J. F.; ROSS, K. W. (2012). *Computer Networking: A Top-down Approach*. 7th Ed. Boston: Addison-Wesley.

PÁGINA EN BLANCO
EN LA EDICIÓN IMPRESA

CAPÍTULO 14

VOZ SOBRE IP

El servicio de voz sobre IP le permite a las organizaciones tener mayor provecho de su infraestructura de red basada en IP, a continuación se exploran los pasos básicos para habilitar el servicio de voz sobre IP en encaminadores Cisco modelo 3725 y 2801, los cuales contienen un módulo software denominado “Call Manager Express”, o CME, que los habilita para ejercer su función como conmutadores de voz sobre IP. Como terminales de voz se usa el teléfono IP 7961GE de Cisco y el software X-Lite, este último habilita la función de teléfono IP en un computador personal. También se exploran ideas alrededor del tema de calidad de servicio en el contexto de voz sobre IP.

OBJETIVO

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

- Configurar un encaminador y un teléfono IP para obtener el servicio de Voz sobre IP (VoIP) mediante el uso del protocolo de inicio de sesión –Session Initiation Protocol (SIP).
- Monitorizar el proceso de registro SIP de los teléfonos IP en el enrutador.

PROCEDIMIENTO

Configurar la interfaz Ethernet de dos computadores personales

Conectar a una red de área local los dos computadores representados en la Figura 14.1. En el computador PC1 de esta Figura se puede emular, mediante el programa simulador gráfico de red –Graphical Network Simulator (GNS3)–, un conmutador de Voz sobre IP, para esto es necesario asignar una dirección IP a la interfaz Ethernet de dicho equipo, por ejemplo:

Dirección IP de PC1: 192.168.55.45
Máscara de red: 255.255.255.0

También es necesario usar un teléfono IP o un segundo computador –PC2 de la Figura 14.1– y configurar la interfaz Ethernet del mismo, por ejemplo:

Dirección IP de PC2: 192.168.55.46
Máscara de red: 255.255.255.0

Instalar el programa X-Lite 4

Descargar desde Internet e instalar el programa X-Lite 4 (de Counter-Path) en los computadores PC1 y PC2, dicho software permite tener un teléfono IP en el computador (también denominado Softphone).

Crear la topología básica de la red en el programa GNS3 y configurar los parámetros básicos

Crear en el programa emulador GNS3 la topología representada en la Figura 14.1. Crear el enrutador R0 –se puede trabajar con el sistema operativo del equipo 3725 de la plataforma 3700 de Cisco– y una Nube (cloud). Por la opción “Configure” de la nube, asociar la interfaz Ethernet del PC1 y aplicar el cambio. Conectar la interfaz fastEthernet 0/0 del enrutador R0 con la Nube.

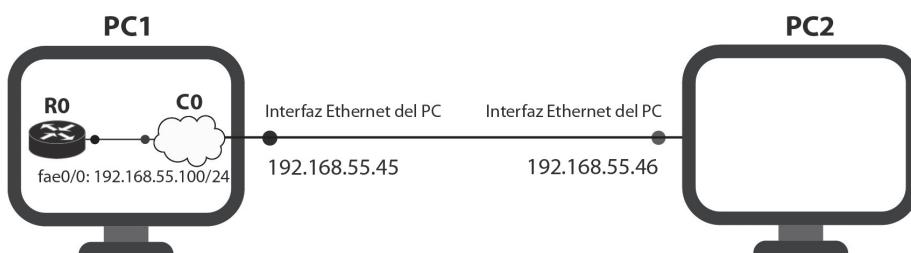


Figura 14.1. Conexión de fastEthernet 0/0 de R0 al PC1 por medio del objeto Nube (cloud)

Configurar los parámetros básicos del enrutador R0 y verificar la conectividad del mismo con la interfaz Ethernet de PC1 mediante el comando ping.

Configurar R0 y probar su conectividad con el PC:

```
(config)# hostname CME
(config)# interface fastethernet 0/0
(config-if)# ip address 192.168.55.100 255.255.255.0
(config-if)# no shutdown
(config-if)# do ping 192.168.55.45
```

Configurar el servicio de conmutador de voz sobre IP en el encaminador

A continuación se indican cinco pasos que permiten habilitar el servicio de voz sobre IP –usando el “Call Manager Express”– en el encaminador.

Configurar los parámetros del servicio de voz

Usar el comando global de configuración “voice service voip” para configurar los parámetros del servicio de voz, habilitar las conexiones SIP a SIP con el comando “allow-connections sip to sip”, y al servidor SIP Registra (servicio SIP Registra) con el comando “registrar server”, cuando se ejecuta este último comando, el encaminador acepta mensajes de registro SIP (entrantes). Si, para efectos de prueba, se desea cambiar el valor por defecto del tiempo con el que el teléfono IP vuelve a registrarse, el comando “registrar server” permite especificar dicho parámetro (el tiempo de vencimiento para registrarse está dado en segundos).

```
(config)# voice service voip
(conf-voi-serv)# allow-connections sip to sip
(conf-voi-serv)# sip
(conf-serv-sip)# registrar server expires max 600 min 300
(conf-serv-sip)# exit
(conf-voi-serv)# exit
(config)#
```

Especifique las preferencias de compresor y descompresor que desee (este paso es opcional, pero se recomienda)

Las preferencias de compresor-descompresor (codec) se especifican con el comando “voice class codec”. Posteriormente se puede hacer referencia a esta configuración de codec desde el comando de configuración “voice

register pool”. La configuración de codec se puede especificar también directamente desde el modo “voice register pool”.

```
(config)# voice class codec 1
(config-class)# codec preference 1 g729r8
(config-class)# codec preference 2 g711ulaw
(config-class)# codec preference 3 g711alaw
(config-class)# exit
(config)#

```

Configurar los parámetros globales de registro de voz

Uso de los comandos de “voice register global”. Los parámetros globales de registro de voz representan para SIP lo que los parámetros de configuración de “telephony-service” representan para el protocolo propietario de Cisco denominado Skinny Call Control Protocol (SCCP).

```
(config)# voice register global
(config-register-global)# mode cme           !pone el IOS SIP registrar en modo CME!
(config-register-global)# source 192.168.55.100 port 5060
!dirección IP para el registro de teléfonos SIP!
(config-register-global)# max-dn 5            !máximo número de extensiones!
(config-register-global)# max-pool 5          !máximo número de teléfonos IP!
(config-register-global)# timezone 13         !zona horaria -5 GMT!
(config-register-global)# time-format 24       !formato de tiempo militar de 24 horas!
(config-register-global)# hold-alert !        !específica la alerta de hold!
(config-register-global)# tftp-path flash:    !específica el camino para los archivos tftp!
(config-register-global)# create profile
!crea el perfil de configuración para los teléfonos IP!
(config-register-global)# exit
(config)#

```

Configurar dos extensiones y sus parámetros

El comando “voice register dn” –dn significa directory name– crea los números de extensión para el “pool de registros de voz”. Esto es similar a los “ephone-dn” generados para los “ephone” mediante la utilidad “telephony-setup” de Cisco.

En el modo dn de registro de voz se configura: el número de extensión, el nombre a mostrar en la pantalla, la etiqueta –label– y el desvío de llamada –si ésta no se contesta dentro de un tiempo límite.

```

(config)# voice register dn 1
(config-register-dn)# number 2001           !número de extensión 2001!
(config-register-dn)# name Pedro
(config-register-dn)# label Pedro-2001
(config-register-dn)# no-reg
(config-register-dn)# call-forward b2bua noan 2005 timeout 10

(config-register-dn)# exit
(config)#

(config)# voice register dn 2
(config-register-dn)# number 2002           !número de extensión 2002!
(config-register-dn)# name Ana
(config-register-dn)# label Ana-2002
(config-register-dn)# no-reg
(config-register-dn)# call-forward b2bua noan 2005 timeout 10

(config-register-dn)# exit
(config)#

```

Configurar los parámetros de los dos teléfonos SIP

Configurar los parámetros del pool de registro de voz para cada Softphone X-Lite –que están basados en el protocolo SIP– usando el comando “voice register pool”. El pool de registro de voz para los teléfonos SIP es idéntico al ephone generado para los teléfonos SCCP.

Se especifica la dirección capa 2 (MAC) de cada teléfono, se asigna el “dn con tag 1” a la línea 1 del teléfono 1 y el “dn con tag 2” a la línea 1 del teléfono 2, se configura el tipo de “dtmf-relay” (RFC2833), se especifica el “voice class codec”, se configura el usuario y la clave para el registro de cada teléfono SIP.

En este caso, el teléfono IP (Softphone X-Lite) se está implementado en el software, por lo tanto, adquiere la misma dirección MAC del PC donde se está ejecutando dicho programa. En el ejemplo se supone la dirección MAC 001E.C946.4B1F para el softphone que se ejecuta en el PC1 y la dirección MAC 0009.6B26.21A9 para el softphone que se ejecuta en el PC2. No obstante, dicha dirección puede variar de acuerdo al PC específico donde se ejecute el programa X-Lite.

```
(config)# voice register pool 1          !primer teléfono IP!
(config-register-pool)# id mac 001e.c946.4b1f   !MAC de PC1 donde corre softphone1!
(config-register-pool)# number 1 dn 1        !la línea 1 se asocia la extensión 2001!
(config-register-pool)# username 2001 password cisco
(config-register-pool)# voice-class codec 1
(config-register-pool)# dtmf-relay rtp-nte sip-notify

(config)# voice register pool 2          !segundo teléfono IP!
(config-register-pool)# id mac 0009.6b26.21a9   !MAC de PC2 donde corre softphone2!
(config-register-pool)# number 1 dn 2        !la línea 1 se asocia la extensión 2002!
(config-register-pool)# username 2002 password cisco
(config-register-pool)# voice-class codec 1
(config-register-pool)# dtmf-relay rtp-nte sip-notify
```

Configurar el X-Lite SIP phone

Para el PC1 con dirección IP 192.168.55.45, en el programa X-Lite se debe seleccionar la opción [Account settings] del menú “Softphone” y diligenciar las siguientes propiedades de la cuenta (ver Figura 14.2).

Configurar en la pestaña [Account].

Account name: Pedro

En la sección User Details:

User ID: 2001

Domain: 192.168.55.100

Password: cisco

Display name: Pedro

Authorization name: 2001

En la sección Domain Proxy:

Marcar el recuadro “Register with domain and receive calls”.

En “send outbound via:” marcar el círculo “Domain”

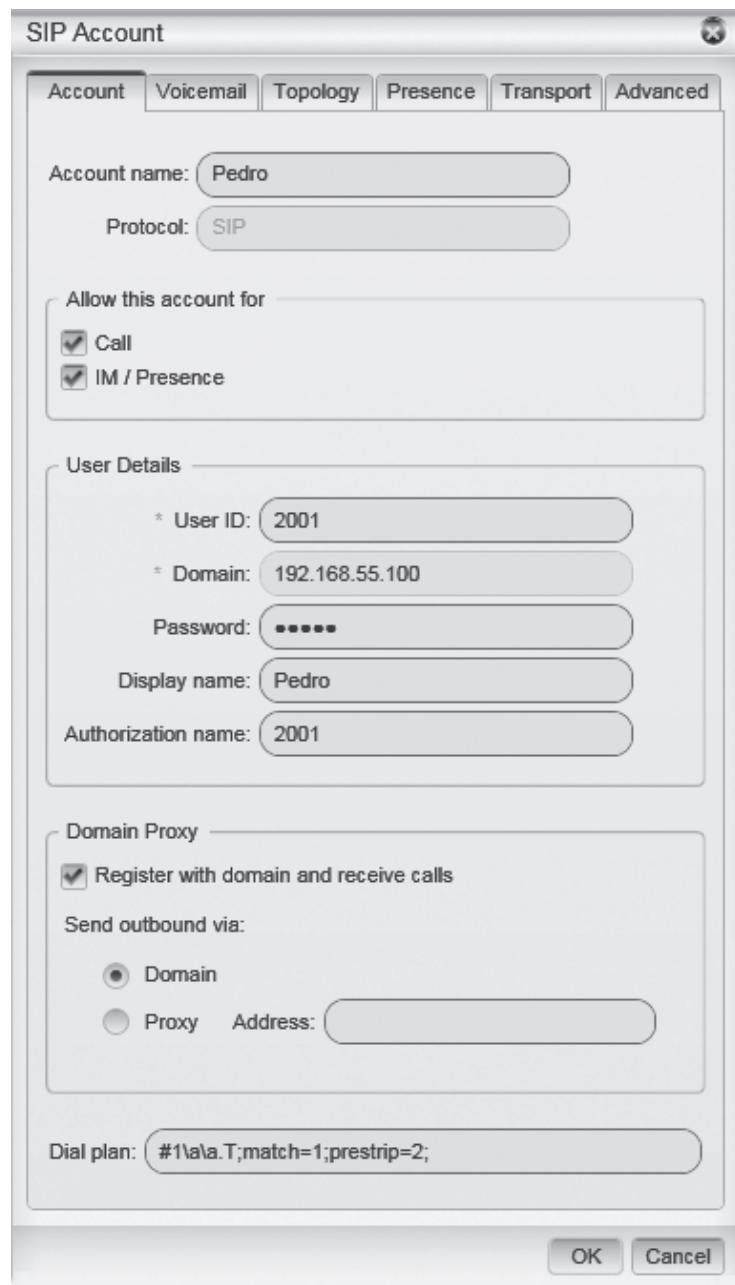


Figura 14.2. Propiedades de la cuenta SIP

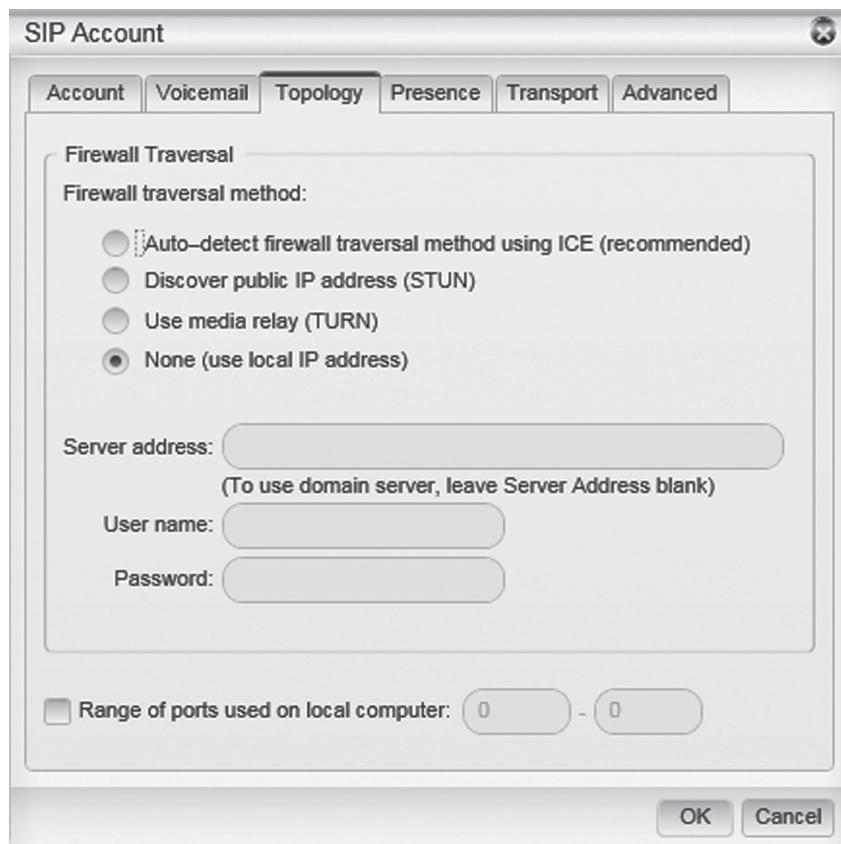


Figura 14.3. Pestaña Topology

Configurar en la pestaña [Topology] (ver Figura 14.3) el siguiente campo.

En la sección Firewall transversal method:
Marcar el círculo “None (use local IP address)”

Aplicar y aceptar los cambios. Repetir el paso anterior para el equipo PC2.

Monitorización del registro de los teléfonos IP

Para monitorear el registro correcto de los teléfonos IP, ejecutar el programa X-Lite en cada PC y usar los siguientes comandos en el encaminador R0 (dichos comandos permiten ver la información correspondiente al registro de los teléfonos IP).

```
# show voice register statistics  
# show voice register all  
# show voice register pool 1  
# show voice register pool 2
```

En lugar de usar el Softphone X-Lite, es posible utilizar un teléfono IP basado en hardware, como el IPtouch modelo 4028 de Alcatel-Lucent o el 7961GE de Cisco. Este último es presentado en la Figura 14.4 y será usado en la sección de ejercicios de laboratorio.



Figura 14.4. Teléfono IP 7961GE de Cisco

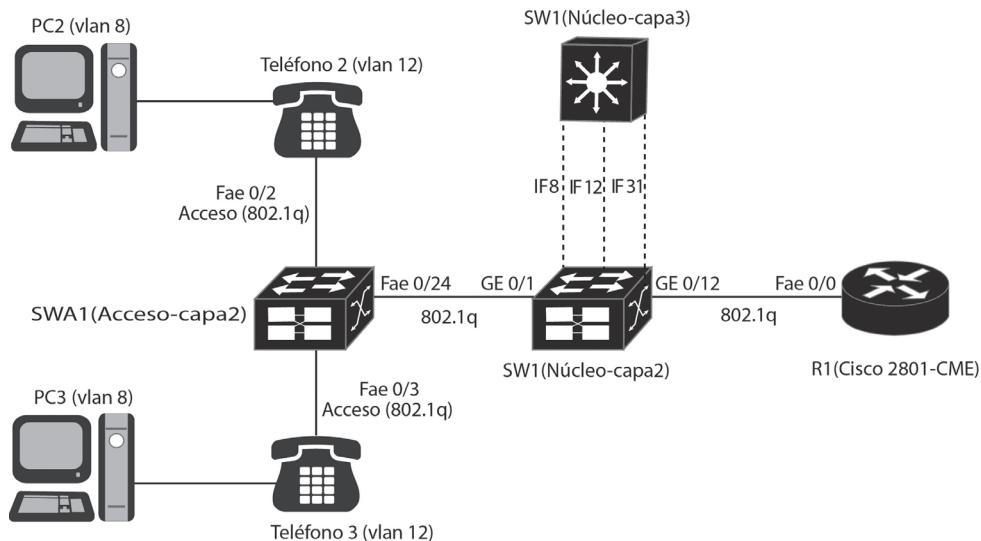
INFORME

Corroborar el funcionamiento del servicio de voz sobre IP, estableciendo una llamada desde la extensión 2001 hacia la extensión 2002 y viceversa; anotar la información obtenida con los comandos “show” de la lista de comandos indicada arriba. Capturar una traza de los protocolos involucrados en la operación del servicio de voz sobre IP –por ejemplo, usando Wireshark.

EJERCICIOS DE LABORATORIO

La Figura 14.5 presenta el bosquejo de una red de área local cuyas redes de datos y voz están definidas para operar en las VLAN 8 y 12, respectivamente. En esta topología, tanto el conmutador Ethernet de acceso (SWA1) como el encaminador 2801 (R1) se conectan al conmutador

Ethernet de núcleo (SW1) por medio de un enlace troncal 802.1Q. Con relación a la red de voz, el equipo R1 hace las veces de conmutador de voz IP (CME), éste se configura para soportar teléfonos IP de tipo softphone (extensión 101) y Cisco modelo 7961GE (extensiones 102 y 103). La configuración de la red con soporte VoIP se realiza mediante los siguientes diez pasos.



Nota: IF8= Interfaz de la VLAN 8. CME = Call Manager Express. Teléfono = Cisco 7961GE

Figura 14.5. Red de área local que soporta los servicios de voz y datos (VLAN 12 y VLAN 8) por medio de un conmutador de voz IP (encaminador Cisco 2801 con módulo Call Manager Express) y teléfonos IP Cisco 7961GE

Paso 1. Subir los archivos del firmware del teléfono Cisco 7961GE al equipo 2801 –este paso se realiza solamente la primera vez que se configura R1 o cada vez que se requiera actualizar el firmware de los teléfonos IP 7961GE. Se descomprime el archivo “cmterm-7941_7961-sip.8-5-2.cop” en la carpeta TFTP, el cual contiene los archivos correspondientes al firmware más actual del teléfono IP 7961GE; después se copian dichos archivos hacia la memoria flash de R1 usando el servidor TFTP. Hay que asegurarse de haber copiado los siguientes archivos a la memoria flash.

```
SIP41.8-5-2S.loads
apps41.8-5-2TH1-9.sbn
cnu41.8-5-2TH1-9.sbn
copstart.py
copstart.sh
cvm41sip.8-5-2TH1-9.sbn
dsp41.8-5-2TH1-9.sbn
jar41sip.8-5-2TH1-9.sbn
term41.default.loads
term61.default.loads
load115.txt
load308.txt
load309.txt
load30018.txt
XMLDefault.cnf.xml
```

El archivo “XMLDefault.cnf.xml” no viene incluido en el archivo “cmterm-7941_7961-sip.8-5-2.cop”, hay que crearlo y subirlo. El archivo “XMLDefault.cnf.xml” debe tener al menos las siguientes líneas.

```
<Default>
<callManagerGroup>
<members>
<member priority="0">
<callManager>
<ports>
<ethernetPhonePort>2000</ethernetPhonePort>
<mgcpPorts>
<listen>2427</listen>
<keepAlive>2428</keepAlive>
</mgcpPorts>
</ports>
<processNodeName></processNodeName>
</callManager>
</member>
</members>
</callManagerGroup>
<loadInformation30018 model="IP Phone 7961">SIP41.8-5-2S</loadInformation30018>
<loadInformation308 model="IP Phone 7961G-GE">SIP41.8-5-2S</loadInformation308>
<authenticationURL></authenticationURL>
<directoryURL></directoryURL>
<idleURL></idleURL>
<informationURL></informationURL>
<messagesURL></messagesURL>
<servicesURL></servicesURL>
</Default>
```

Paso 2. Configurar la interfaz FastEthernet 0/0, el servidor DHCP y el protocolo EIGRP en el equipo R1.

```
Router(config)# hostname CME-SIP
CME-SIP(config)# interface fastethernet 0/0
CME-SIP(config-if)# no shutdown
CME-SIP(config-if)# description Se conecta a GigabitEthernet0/12 (802.1Q) de SW1
CME-SIP(config-if)# interface fastethernet 0/0.31
CME-SIP(config-subif)# encapsulation dot1q 31
CME-SIP(config-subif)# ip address 192.168.31.2 255.255.255.0
CME-SIP(config-subif)# no shutdown
CME-SIP(config-subif)# exit

CME-SIP(config)# ip dhcp excluded-address 192.168.31.1 192.168.31.65
CME-SIP(config)# ip dhcp excluded-address 192.168.31.252 192.168.31.254
CME-SIP(config)# ip dhcp excluded-address 192.168.8.1 192.168.8.10
CME-SIP(config)# ip dhcp excluded-address 192.168.12.1 192.168.12.10

CME-SIP(config)# ip dhcp pool data
CME-SIP(dhcp-config)# network 192.168.8.0 255.255.255.0
CME-SIP(dhcp-config)# default-router 192.168.8.1
CME-SIP(dhcp-config)# exit

CME-SIP(config)# ip dhcp pool voice
CME-SIP(dhcp-config)# network 192.168.12.0 255.255.255.0
CME-SIP(dhcp-config)# default-router 192.168.12.1
CME-SIP(dhcp-config)# option 150 ip 192.168.31.2
CME-SIP(dhcp-config)# exit

CME-SIP(config)# router eigrp 1
CME-SIP(config-router)# network 192.168.31.0
CME-SIP(config-router)# exit
```

Paso 3. Configurar los parámetros del servicio de voz en R1.

```
CME-SIP(config)# voice service voip
CME-SIP(conf-voi-serv)# allow-connections sip to sip
CME-SIP(conf-voi-serv)# sip
CME-SIP(conf-serv-sip)# registrar server expires max 1200 min 300
CME-SIP(conf-serv-sip)# exit
CME-SIP(conf-voi-serv)# exit
```

Paso 4. Configurar los parámetros globales de registro de voz en R1. El comando “create profile” se debe volver a repetir después de haber realizado los pasos 5 y 6 para que R1 cree los perfiles de los teléfonos IP de acuerdo a la configuración realizada en dichos pasos –basada en la dirección MAC de los teléfonos IP. El comando “dialplan-pattern 1 5063344... extension-length 3” supone que la compañía de telefonía suministra el servicio de marcación interna directa –Direct Inward Dialing– por medio de troncales telefónicas que se conectan a R1 mediante un circuito primario.

```
CME-SIP(config)# voice register global
CME-SIP(config-register-global)# mode cme
CME-SIP(config-register-global)# source-address 192.168.31.2 port 5060
CME-SIP(config-register-global)# max-dn 20
CME-SIP(config-register-global)# max-pool 10
CME-SIP(config-register-global)# load 7961GE SIP41.8-5-2S
CME-SIP(config-register-global)# authenticate register
CME-SIP(config-register-global)# authenticate realm cisco.com
CME-SIP(config-register-global)# tftp-path flash:
CME-SIP(config-register-global)# create profile
CME-SIP(config-register-global)# dialplan-pattern 1 5063344... extension-length 3
CME-SIP(config-register-global)# exit
```

Paso 5. Configurar las extensiones y sus respectivos parámetros. La extensión 101 se asociará al softphone X-Lite y las extensiones 102 y 103 se asociarán cada una a su respectivo teléfono IP 7961GE.

```
CME-SIP(config)# voice register dn 1
CME-SIP(config-register-dn)# number 101
CME-SIP(config-register-dn)# call-forward b2bua noan 103 timeout 10
CME-SIP(config-register-dn)# name Phone1
CME-SIP(config-register-dn)# no-reg
CME-SIP(config-register-dn)# label 5063344101
CME-SIP(config-register-dn)# exit

CME-SIP(config)# voice register dn 2
CME-SIP(config-register-dn)# number 102
CME-SIP(config-register-dn)# call-forward b2bua noan 100 timeout 20
CME-SIP(config-register-dn)# call-forward b2bua busy 100
CME-SIP(config-register-dn)# name Phone2
CME-SIP(config-register-dn)# label 5063344102
CME-SIP(config-register-dn)# mwi
CME-SIP(config-register-dn)# allow watch
CME-SIP(config-register-dn)# exit

CME-SIP(config)# voice register dn 3
CME-SIP(config-register-dn)# number 103
CME-SIP(config-register-dn)# call-forward b2bua noan 100 timeout 20
CME-SIP(config-register-dn)# call-forward b2bua busy 100
CME-SIP(config-register-dn)# name Phone3
CME-SIP(config-register-dn)# label 5063344103
CME-SIP(config-register-dn)# mwi
CME-SIP(config-register-dn)# allow watch
CME-SIP(config-register-dn)# exit
```

Paso 6. Configurar los teléfonos IP para que operen con el protocolo SIP. Las direcciones MAC especificadas en el pool 1, pool 2 y pool 3 corresponden respectivamente a la dirección MAC del computador personal donde se ejecuta X-Lite y a los dos teléfonos IP Cisco 7961GE.

```
CME-SIP(config)# voice register pool 1
CME-SIP(config-register-pool)# id mac 0022.1915.72F2
CME-SIP(config-register-pool)# number 1 dn 1
CME-SIP(config-register-pool)# dtmf-relay rtp-nte sip-notify
CME-SIP(config-register-pool)# codec g711ulaw
CME-SIP(config-register-pool)# username user1 password cisco
CME-SIP(config-register-pool)# exit
```

Continua

Viene

```
CME-SIP(config)# voice register pool 2
CME-SIP(config-register-pool)# id mac 001d.45e9.4c8e
CME-SIP(config-register-pool)# number 1 dn 2
CME-SIP(config-register-pool)# dtmf-relay sip-notify
CME-SIP(config-register-pool)# codec g711ulaw
CME-SIP(config-register-pool)# username user2 password cisco
CME-SIP(config-register-pool)# type 7961GE
CME-SIP(config-register-pool)# exit

CME-SIP(config)# voice register pool 3
CME-SIP(config-register-pool)# id mac 001d.45e9.54ac
CME-SIP(config-register-pool)# number 1 dn 3
CME-SIP(config-register-pool)# dtmf-relay sip-notify
CME-SIP(config-register-pool)# codec g711ulaw
CME-SIP(config-register-pool)# username user3 password cisco
CME-SIP(config-register-pool)# type 7961GE
CME-SIP(config-register-pool)# exit
```

Paso 7. Configurar R1 para que permita activar el servicio TFTP para los archivos del firmware de los teléfonos IP y para el archivo XMLDefault.cnf.xml.

```
CME-SIP(config)# tftp-server flash:SIP41.8-5-2S.loads
CME-SIP(config)# tftp-server flash:term61.default.loads
CME-SIP(config)# tftp-server flash:term41.default.loads
CME-SIP(config)# tftp-server flash:apps41.8-5-2TH1-9.sbn
CME-SIP(config)# tftp-server flash:cnu41.8-5-2TH1-9.sbn
CME-SIP(config)# tftp-server flash:cvm41sip.8-5-2TH1-9.sbn
CME-SIP(config)# tftp-server flash:dsp41.8-5-2TH1-9.sbn
CME-SIP(config)# tftp-server flash:jar41sip.8-5-2TH1-9.sbn
CME-SIP(config)# tftp-server flash:XMLDefault.cnf.xml
```

Paso 8. Configurar el commutador de núcleo SW1 –Cisco 3560G– de modo que permita: el funcionamiento con las VLAN 8, 12 y 31; interconectar las VLAN anteriores por medio de sus interfaces de capa 3; que las interfaces de capa 3 hagan la función de Proxy DHCP; establecer una conexión 802.1Q con SWA1 y R1 mediante los puertos GigabitEthernet0/1 y GigabitEthernet0/12, respectivamente, y habilitar un protocolo de enrutamiento en la VLAN 31 que sea compatible con el protocolo de enrutamiento habilitado en R1.

```
Switch# vlan database
Switch(vlan)# vlan 8
Switch(vlan)# vlan 12
Switch(vlan)# vlan 31
Switch(vlan)# exit

Switch(config)# hostname SW1
SW1(config)# interface GigabitEthernet0/1
SW1(config-if)# description Se conecta a FastEthernet0/24 (802.1Q) de SWA1.
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan all
SW1(config-if)# spanning-tree link-type point-to-point
SW1(config-if)# ip arp inspection trust
SW1(config-if)# ip dhcp snooping trust
SW1(config-if)# exit

SW1(config)# interface GigabitEthernet0/12
SW1(config-if)# description Se conecta a FastEthernet0/0 (802.1Q) de R1.
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan all
SW1(config-if)# spanning-tree link-type point-to-point
SW1(config-if)# ip arp inspection trust
SW1(config-if)# ip dhcp snooping trust
SW1(config-if)# exit

SW1(config)# interface Vlan 8
SW1(config-if)# description Data VLAN
SW1(config-if)# ip address 192.168.8.1 255.255.255.0
SW1(config-if)# ip helper-address 192.168.31.2

SW1(config)# interface Vlan 12
SW1(config-if)# description Voice VLAN
SW1(config-if)# ip address 192.168.12.1 255.255.255.0
SW1(config-if)# ip helper-address 192.168.31.2

SW1(config)# interface Vlan 31
SW1(config-if)# description Routing VLAN
SW1(config-if)# ip address 192.168.31.1 255.255.255.0
SW1(config-if)# ip helper-address 192.168.31.2

SW1(config)# router eigrp 1
SW1(config-router)# network 192.168.0.0 0.0.255.255
SW1(config-router)# no auto-summary
SW1(config-router)# passive-interface default
SW1(config-router)# no passive-interface Vlan31
```

Paso 9. Configurar el comutador de acceso SWA1 –Cisco 3550G– de modo que permita: el funcionamiento con la VLAN 8 para datos y la VLAN 12 para voz; tener una conexión 802.1Q entre el puerto FastEthernet0/24 de SWA1 y el puerto GigabitEthernet0/1 de SW1, y disponer de los puertos de acceso FastEthernet0/2 y FastEthernet0/3 para la conexión de los teléfonos IP y de los computadores personales –note que estos dos últimos puertos proporcionan los mismos servicios, a pesar de diferir ligeramente en su configuración.

```
Switch# vlan database
Switch(vlan)# vlan 8
Switch(vlan)# vlan 12
Switch(vlan)# exit

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

SWA1(config)# interface FastEthernet0/24
SWA1(config-if)# description Se conecta a GigabitEthernet0/1 (802.1Q) de SW1.
SWA1(config-if)# switchport trunk encapsulation dot1q
SWA1(config-if)# switchport mode trunk
SWA1(config-if)# switchport trunk allowed vlan all
SWA1(config-if)# spanning-tree link-type point-to-point
SWA1(config-if)# ip arp inspection trust
SWA1(config-if)# ip dhcp snooping trust
SWA1(config-if)# exit

SWA1(config)# interface FastEthernet0/2
SWA1(config-if)# description 7961GE Phone and PC
SWA1(config-if)# switchport mode access
SWA1(config-if)# switchport access vlan 8
SWA1(config-if)# switchport voice vlan 12
SWA1(config-if)# spanning-tree portfast
SWA1(config-if)# spanning-tree bpduguard enable

SWA1(config-if)# interface FastEthernet0/3
SWA1(config-if)# description 7961GE Phone and PC
SWA1(config-if)# switchport trunk encapsulation dot1q
SWA1(config-if)# switchport mode trunk
SWA1(config-if)# switchport trunk native vlan 8
SWA1(config-if)# switchport voice vlan 12
SWA1(config-if)# spanning-tree portfast
SWA1(config-if)# spanning-tree bpduguard enable
```

Paso 10. Configurar R1 con el objetivo de que el equipo genere los respectivos archivos de operación para voz sobre IP.

```
CME-SIP(config)# voice register global  
CME-SIP(config-register-global)# no create profile  
CME-SIP(config-register-global)# create profile  
  
CME-SIP# show flash:
```

Verificar mediante el comando “show flash” que se han creado los siguientes archivos:

- SEP001D45E94C8E.cnf.xml
- SEP001D45E954AC.cnf.xml
- SIPDefault.cnf
- softkeyDefault_kpml.xml
- softkeyDefault.xml
- syncinfo.xml

Los archivos “SEP001D45E94C8E.cnf.xml” y “SEP001D45E954AC.cnf.xml” son los perfiles creados por el conmutador de voz –R1– para ser utilizados, respectivamente, por los teléfonos IP cuya dirección MAC es “001D45E94C8E” y “001D45E954AC”. Cada teléfono IP busca su respectivo archivo SEP\$MAC.cnf.xml –donde \$MAC es una variable que representa la dirección MAC específica del teléfono IP– y lo carga; posteriormente, el teléfono IP carga el archivo “softkeyDefault_kpml.xml” para hacer efectivas las funciones en él definidas con las respectivas teclas del teléfono IP.

Después de configurar los equipos R1, SW1 y SWA1, establezca una llamada entre los dos teléfonos IP 7961GE y monitoree su registro mediante los comandos “show” de la sección anterior: “Monitorización del registro de los teléfonos IP”.

INFORMACIÓN COMPLEMENTARIA

Calidad de servicio

IEEE 802.1Q e IP proporcionan mecanismos para que las diferentes aplicaciones –incluyendo VoIP– puedan solicitar una determinada prioridad acorde a sus necesidades, este hecho involucra el concepto de calidad de servicio. Se pueden encontrar los elementos que subyacen en el concepto de calidad de servicio en el apéndice B del libro de Kevin Dooley e Ian J. Brown referenciado en la bibliografía.

PROBLEMAS

1. Interconecte dos encaminadores Cisco mediante sus interfaces Serie 0/0 –puede usar GNS3–, configure las direcciones IP de dichas interfaces y el protocolo de enrutamiento RIP. Para que estos dos encaminadores Cisco generen automáticamente una política de calidad de servicio para el tráfico VoIP que cruza por las interfaces serie que los interconecta, configure dichas interfaces con el comando *auto qos voip*. Finalizada la configuración, use el comando *show auto qos* en modo privilegiado e interprete la política generada para el tráfico de voz sobre IP.
2. Familiarización con la característica AutoQoS de Cisco. Interconecte dos encaminadores Cisco mediante sus interfaces Serie 0/0 –puede usar GNS3–, configure las direcciones IP de dichas interfaces, el protocolo de enrutamiento RIP y la velocidad a 9600 bps –*clock rate 9600, bandwidth 9*. Conecte dos estaciones finales al lado LAN de los encaminadores. Para que estos dos encaminadores Cisco generen automáticamente una política de calidad de servicio para todo el tráfico corporativo –en general– que cruza por las interfaces serie que los interconecta, ejecute los siguientes pasos en ambos encaminadores:

Paso 1: configure las interfaces serie mediante el comando *auto discovery qos* –para habilitar la fase de recolección de información de los diferentes tipos de aplicación que usan la red.

Paso 2: genere o permita el flujo del tráfico de las aplicaciones corporativas por el periodo de tiempo que considere necesario para que los encaminadores puedan recolectar suficiente información para clasificar los diferentes tipos de tráfico. Mediante el comando *show auto discovery qos* monitoree la información recolectada –es necesario generar un promedio considerable de tráfico respecto a la velocidad configurada en las interfaces.

Paso 3: configure las interfaces serie mediante el comando *auto qos* –para configurar los encaminadores con la información previamente recolectada.

Paso 4: configure las interfaces serie mediante el comando *no auto discovery qos* –para deshabilitar la fase de recolección de información.

Finalmente, para verificar la configuración añadida a los encaminadores use el comando *show auto qos* o el comando *show running-config*.

GLOSARIO

Call Manager Express (CME): programa software licenciado de Cisco que permite tener la funcionalidad de un conmutador de voz sobre IP en un enrutador Cisco, por ejemplo, en los modelos 2801 o 3725 de Cisco. Existen programas similares de otros fabricantes que permiten dicha función (el programa licenciado OmniPCX Office de Alcatel-Lucent o el programa libre Asterisk) o la posibilidad de emular la plataforma Cisco en GNS3.

Pool de registros de voz: registros que integran una serie de propiedades (número de extensión, usuario, clave, dirección MAC) para asociar un número de extensión a un cliente SIP.

SIP registra: hace referencia a un equipo servidor que acepta y procesa las solicitudes de registro SIP, las cuales contienen el identificador de recursos uniforme (Uniform Resource Identifier o URI) de los equipos clientes. Dicho servidor también suministra información de localización, proporcionando las direcciones IP registradas en el URI.

Softphone: denominación que se le da al programa software de voz sobre IP que permite lograr la funcionalidad de tener un teléfono de voz sobre IP en el computador personal.

BIBLIOGRAFÍA

- BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.
- DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook™*. 2nd Ed. Sebastopol, CA: O'Reilly.
- HATTINGH, C.; SLADDEN, D.; ZAKARIA, A. (2010). *SIP Trunking*. Indianapolis, IN Cisco Press.
- MCQUERRY, S.; JANSEN, D.; HUCABY, D. (2009). *Cisco LAN Switching Configuration Handbook*. 2nd Ed. Indianapolis, IN: Cisco Press.
- SINNREICH, H.; JOHNSTON, A. (2006). *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*. 2nd Ed. Indianapolis, IN: Wiley.



Universidad
del Valle

Programa *E*ditorial