UNIVERSIDAD ORT
Uruguay
Facultad de Ingeniería
Bernard Wand - Polak

INTRODUCCIÓN A LA CONFIGURACIÓN DE ROUTERS CISCO

GUÍA PARA LABORATORIOS DE REDES

Escuela de Tecnología

Gerardo Matturro, MC
Docente, Redes de Datos

Con la colaboración de
Guzmán Barrio
Técnico en Electrónica Informática
Cisco Certified Network Associate (CCNA)

Año 2007

Universidad ORT Uruguay
Facultad de Ingeniería
Bernard-Wand-Polak

Escuela de Tecnología

Introducción a la Configuración de Routers Cisco

Gerardo Matturro, MC

con la colaboración de

Guzmán Barrio
Técnico en Electrónica Informática
Cisco Certified Network Associate (CCNA)

Corrector Técnico: Ing. Daniel Baccino

Corrector Ortográfico: Escuela de Tecnología

Diciembre 2007

Dedicatoria

A Daniella y Oriana

Agradecimientos

Deseo expresar mi agradecimiento a las personas que, de diferentes maneras, me brindaron su apoyo y colaboración en la realización de este trabajo.

Menciono así al Decano de la Facultad de Ingeniería Mario Fernández, al Secretario Docente de la Escuela de Tecnología Víctor Paulós, al Coordinador de la Escuela de Tecnología Armando Gervaz y al Coordinador Académico de Electrónica Marcos Delgado, quienes recibieron con beneplácito la propuesta de realizar este trabajo y me alentaron a llevarlo a cabo.

También deseo expresar mi gratitud al Ing. Daniel Baccino, corrector técnico de este trabajo, quien dedicó muchas horas de su escaso tiempo a la revisión técnica del texto y cuyos aportes y sugerencias ciertamente contribuyeron a mejorar la calidad del mismo.

En relación con el trabajo de armado y de edición final de este libro va mi agradecimiento a Erica Yac y a Sandra Leal del Departamento de Publicaciones, quienes realizaron su labor con la dedicación y profesionalidad que las caracteriza.

Finalmente, deseo destacar la importante labor realizada por Guzmán Barrio, quien colaboró y trabajó intensamente en el Laboratorio de Redes de la Facultad de Ingeniería de la Universidad ORT en los aspectos relativos al armado de las redes, la configuración de los routers y en la captura de las pantallas que ilustran los resultados de la ejecución de los comandos que se estudian en el libro.

Prefacio

La idea de escribir un libro de introducción a la configuración de *routers* Cisco surgió a partir de la incorporación, en el año 2002, de este tema en las asignaturas Redes 1 y Redes 2 de la carrera de Técnico en Electrónica Informática que se imparte en la Escuela de Tecnología de la Universidad ORT Uruguay. Estas asignaturas, en conjunto, incluyen en sus programas los aspectos más importantes y novedosos acerca de las principales tecnologías de redes de área local y de redes de área extensa, así como el estudio en profundidad del conjunto de protocolos TCP/IP.

Los aspectos teóricos de esas tecnologías y protocolos se llevan a la práctica en el diseño e implementación de interredes basadas en TCP/IP. Elementos esenciales en ese diseño e implementación lo constituyen los dispositivos de red denominados encaminadores o *routers*. El Laboratorio de Redes de la Facultad de Ingeniería de la Universidad ORT Uruguay cuenta, entre otros elementos, con *routers*, *switches* y otro equipamiento de Cisco de última generación, de modo que los alumnos puedan realizar sus prácticas de laboratorio con equipamiento real desarrollado por una de las principales empresas en el área de las tecnologías de redes y comunicaciones de datos y voz.

¿En qué se diferencia este libro de otros que tratan el mismo tema de configuración de *routers* de Cisco? Básicamente en el ordenamiento de los temas y en el enfoque con el cual se exponen los mismos, aspectos ambos que son el resultado de las experiencias previas del dictado del curso. La práctica docente (tanto en el aula como en el laboratorio) y el seguimiento constante de la manera en que los alumnos captan y asimilan los nuevos conceptos y también de las dificultades que en este sentido han encontrado y cómo se han superado, condujo a estructurar el contenido del libro y su enfoque de presentación de modo tal que se maximice la oportunidad de aplicación práctica de los conceptos que se introducen y, en particular, de los comandos del sistema operativo IOS de los *routers* de Cisco. La forma más adecuada de aprender a configurar un *router* de Cisco (y en realidad cualquier *router* de cualquier fabricante) es trabajando directamente sobre hardware "real" en situaciones que, si bien se plantean y se desarrollan en un laboratorio, se asemejan en mucho a la realidad. La aplicación práctica de los conceptos y de los comandos facilita la comprensión de los mismos y la familiarización con su sintaxis básica al tiempo que hace innecesario el esfuerzo, a la postre inútil, de memorización.

Si bien la audiencia primaria de este libro la constituyen los alumnos de las asignaturas mencionadas al comienzo, se ha tratado de generalizar la exposición de modo que también sea de utilidad para técnicos y administradores de redes que estén interesados o necesitados de una introducción rápida y práctica a los principales conceptos y procedimientos de configuración y mantenimiento de un *router*.

Gerardo Matturro, MC
Primavera 2006

Nota preliminar

El presente trabajo cubre los routers de CISCO correspondientes a las series 800, 2500, 2600, 3600 y 3700. Al momento de impresión de este libro, Cisco ha lanzado al mercado una nueva generación de routers, plasmada en las series 1800, 2800 y 3800, y que ha de sustituir en el futuro a los routers de la generación anterior, excepto la línea 800.

Esta nueva generación de routers presenta una renovación sustantiva en su arquitectura de hardware que cambia algunos conceptos vigentes hasta ahora tales como, por ejemplo, el clásico puerto serial de consola, el cual es ahora implementado mediante un puerto del tipo USB, presente en todos los modelos de routers de la nueva generación. Otras innovaciones son la compresión de datos y la incorporación a la motherboard de los puertos de voz.

Mayor información sobre esta nueva generación de routers de Cisco puede obtenerse en el sitio web de Cisco: http://www.cisco.com.

Tabla de Contenido

1. Componentes de un router

Un router o encaminador es un dispositivo de red que permite la interconexión de redes al nivel de la capa de Red del Modelo de Referencia OSI.

Desde el punto de vista funcional, un router puede concebirse como una computadora de propósito específico, en contraposición a una computadora personal a la que suele caracterizarse como de "propósito general". En efecto, en una computadora personal podemos ejecutar software tan variado como un procesador de texto, programas para el tratamiento de imágenes o de sonido, aplicaciones que accedan a bases de datos, programas de contabilidad e incluso juegos.

En un router no es posible ejecutar este tipo de software; en particular, en un router de Cisco solo se ejecuta un software específicamente diseñado para el mismo. Se trata del sistema operativo IOS, Internetwork Operating System, que realiza todas las funciones lógicas del router como ser el encaminamiento de paquetes, registro de tráfico de datagramas, actualización de tablas de encaminamiento a otras redes, etc.

Por este motivo, configurar un router significa establecer los valores de una serie de parámetros de funcionamiento de este sistema operativo tales como, por ejemplo, el nombre de host del router o las direcciones IP de sus interfaces de red, habilitar la ejecución de ciertos procesos como, por ejemplo, el encaminamiento de datagramas IP mediante los protocolos de encaminamiento RIP o IGRP, entre otros.

Considerado el router, entonces, como una computadora especial, entre sus componentes de hardware principales se encuentran un procesador, encargado de la ejecución de tareas y procesos, una placa madre y distintos tipos de memorias, así como ranuras o "slots" de expansión y dispositivos para la entrada y salida de datos. Lo que no suele tener un router es monitor y teclado, ni unidades de almacenamiento secundarias de datos como lo son las unidades de disquetes y de discos duros. En el Capítulo 3 veremos de qué manera, aunque no estén presentes estos elementos, es posible acceder al router para ver y modificar su configuración.

De los elementos de hardware que sí están presentes, vamos a analizar aquellos con los cuales el usuario responsable de la configuración del router interactúa más habitualmente.

Memorias

Un router de Cisco normalmente consta de cuatro tipos de memoria, cada uno destinado a almacenar, en forma temporal o permanente, diferentes tipos de información.

Estos cuatro tipos de memoria se denominan:

- RAM
- ROM
- NVRAM
- FLASH

En la memoria **RAM** se almacena, entre otros elementos, las tablas de encaminamiento del router, la *caché* del protocolo ARP, los datagramas entrantes y también las colas de datagramas salientes. Es, en esencia, la memoria de trabajo del router.

En esta memoria también se encuentra un archivo con los parámetros de ejecución del router; este archivo se denomina RUNNING-CONFIG, el cual se va a tratar mas adelante.

En la memoria RAM, por otra parte, es donde se carga el sistema operativo IOS para su ejecución, de modo similar a como ocurre con el sistema operativo de una computadora personal que se carga desde disco a la memoria RAM en el proceso de arranque.

La memoria **ROM** contiene el código de arranque del router, encargado de realizar las tareas de inicialización y carga del sistema operativo IOS. También en esta memoria se encuentra una versión "reducida" del sistema operativo a la cual se accede en caso que se necesite realizar alguna tarea de mantenimiento del router o en caso en que no se encuentre la imagen "normal" del sistema operativo. En el capítulo 10 se tratará mas en detalle este punto.

La memoria **NVRAM** es un tipo especial de memoria que tiene la particularidad de que su contenido no se borra cuando se apaga el router. NV significa Non-Volatile, es decir no volátil. En esta memoria se almacenan dos elementos muy importantes para la operativa del router: el archivo de configuración de arranque, denominado STARTUP-CONFIG y el registro de configuración, denominado CONFIG-REGISTER.

Finalmente, en la memoria **FLASH**, que también es una memoria no volátil, se almacena la imagen del sistema operativo, pudiéndose almacenar más de una imagen si el tamaño de la memoria FLASH instalada resulta suficiente.

Dispositivos de Entrada y Salida

Los routers de Cisco disponen principalmente de dos tipos de dispositivos para entrada y salida de datos: **puertos** e **interfaces de red**.

Puertos

A través de los puertos es que el Administrador accede al router para ver y modificar su configuración y también para ver sus estadísticas de funcionamiento.

Todos los routers de Cisco disponen de un puerto denominado CONSOLA (CONSOLE) y la mayoría de ellos también disponen de un puerto denominado AUXILIAR (AUX). Ambos puertos suelen estar ubicados en el panel posterior del router aunque en algunos modelos, como los de la serie 3600, se encuentran ubicados en el panel frontal

El puerto de **CONSOLA** proporciona una conexión serial asincrónica del tipo EIA/TIA-232 (anteriormente denominada RS-232). El tipo de conector depende del modelo del router; algunos tienen un conector del tipo DB25 y otros tienen un conector del tipo RJ-45.

Puesto que un router no tiene ni teclado ni monitor, se debe utilizar una computadora personal para suplir esta ausencia. Mediante un cable especial se conecta la computadora a través de uno de sus puertos seriales (COM1, por ejemplo) a este puerto. En el Capítulo 3 se detalla este procedimiento.

El tipo de cable a utilizar depende del tipo de conector de consola que tenga el router. Si el conector es del tipo RJ-45, el cable a utilizar debe ser del tipo "rollover" y si el conector es DB25,

se ha de utilizar un cable serial. El cable, cualquiera sea su tipo, es provisto por el fabricante junto con el router.

El puerto **AUXILIAR** también proporciona una conexión serial asincrónica del tipo EIA/TIA-232. Este puerto se utiliza principalmente para acceder al router en forma remota a través de un modem y su correspondiente línea telefónica. Esta forma de acceso es útil cuando no se tiene acceso físico directo al router. Este puerto también puede utilizarse como una interfaz de red, por ejemplo, para respaldo discado ("dial backup") o discado bajo demanda ("dial on-demand").

Interfaces de red

Las interfaces de red se utilizan para conectar físicamente el router a las redes que el router va a interconectar. Es a través de estas interfaces que los paquetes de datos entran y salen del router.

Habitualmente los routers tienen una interface de tipo LAN y una o más interfaces del tipo WAN. La cantidad y tipos de interfaces de red dependerán del modelo de router de que se trate. Incluso, algunos modelos de Cisco tienen ranuras de expansión que permiten insertar módulos de hardware con interfaces LAN o WAN adicionales.

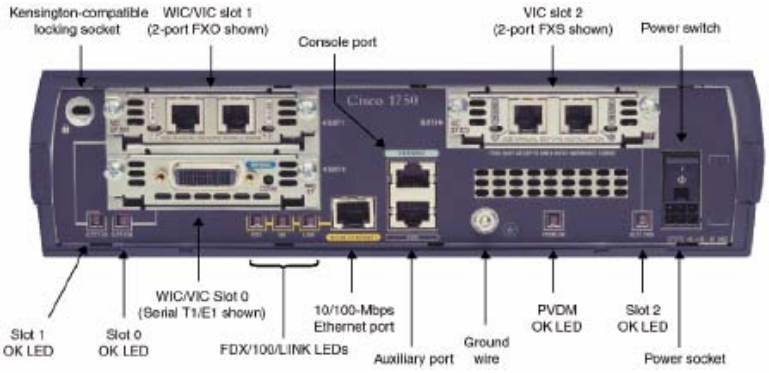
Mediante una interfaz LAN se conecta el router a la red local y las interfaces WAN se utilizan para conectar el router a redes remotas.

Cisco ha definido una forma normalizada para identificar cada interfaz de un router; la forma general es TIPO #RANURA/#INTERFACE. TIPO hace referencia al tipo de interface, tal como Ethernet, FastEthernet, Token-Ring, Serial, etc. y #RANURA/#INTERFACE hace referencia al número de identificación de una interface específica (#INTERFACE) del módulo de expansión inserto en la ranura #RANURA. La numeración de las ranuras de expansión y de las interfaces en cada ranura comienza en 0, es decir, la primera interface será la 0, la segunda la 1, etc. Por ejemplo, para hacer referencia a la primera interface LAN de tipo FastEthernet de la primera ranura se indica como fastethernet 0/0 y la identificación de la primera interface serial de la segunda ranura es serial 1/0.

Para aquellos modelos de routers que no tengan ranuras de expansión la forma de identificar las interfaces es simplemente TIPO #INTERFACE; por ejemplo, ethernet 0 identifica a la primera interface LAN de tipo Ethernet.

Los routers de este libro

Los routers con los que vamos a trabajar en este libro pertenecen a la serie 1700 de Cisco; en particular, serán del modelo 1751. En la figura siguiente se muestra el panel posterior, donde podemos apreciar las distintas interfaces y conectores.



Este modelo dispone de un puerto de consola y de un puerto auxiliar, ambos con conectores del tipo RJ-45, y una interface de red Ethernet de 10/100 Mbps., también del tipo RJ-45. Asimismo, dispone de tres ranuras de expansión en las que pueden insertarse tarjetas de hardware con interfaces WAN (WIC, WAN Interface Card) o con interfaces para voz (VIC, Voice Interface Card). Las interfaces WAN permiten conectar el router a redes de área extensa basadas en las principales tecnologías de uso actual tales como Frame Relay, ISDN, DSL de banda ancha y enlaces dedicados punto a punto. Por su parte, las interfaces de voz permiten digitalizar el tráfico de voz para luego encapsularlo en paquetes de datos y priorizarlos sobre el tráfico de datos normal.

En cuanto a las capacidades de memoria, el modelo base 1751 tiene 16 MB de memoria FLASH y 32 de memoria RAM en forma predeterminada.

Entre las varias funcionalidades que brinda el modelo 1751 podemos destacar el soporte para VLANs (LANs virtuales) IEEE 802.1Q, soporte para la creación de VPNs (Virtual Private Network) y capacidades de firewall (mediante el paquete de IOS firewall), así como de administración basadas en el protocolo SNMP.

En el sitio web de Cisco, en http://www.cisco.com, puede encontrarse información mas detallada sobre la serie 1700, así como de las otras series y modelos de routers provistos por este fabricante.

2. La Interfaz de Línea de Comandos

Tal como hemos mencionado en el Capítulo 1, configurar un router implica, entre otras tareas, establecer valores para una serie de parámetros de funcionamiento de su sistema operativo, así como habilitar o deshabilitar ciertas funcionalidades del mismo. La forma habitual de hacer esto en un router de Cisco es a través de una interface de usuario basada en caracteres denominada Interfaz de Línea de Comandos o CLI (Command Line Interface).

Esta interfaz es la parte "visible" de un componente del sistema operativo IOS que se denomina Intérprete de Comandos. La Interfaz de Línea de Comandos presenta al usuario un indicador de sistema o "prompt" donde escribir los comandos, de modo similar a como se escriben comandos en una "ventana de DOS" de Windows. Cuando se ingresa un comando y se presiona la tecla **Intro**, el Intérprete de Comandos verifica que el texto ingresado sea un comando válido para el sistema operativo y que se haya utilizado la sintaxis correcta del mismo. En caso que el texto ingresado no sea un comando o que el mismo esté incompleto, el Intérprete de Comandos desplegará un mensaje de error.

Modos

La Interface de Línea de Comandos de IOS está organizada en lo que Cisco denomina Modos. En cada uno de los modos están disponibles una serie de comandos, los cuales solo pueden ejecutarse en el modo correspondiente. Estos modos se denominan:

- Usuario
- Privilegiado
- Configuración Global
- Sub-Modos de Configuración (varios)
- Monitor ROM
- Setup

Modo Usuario

Cuando se inicia una sesión en el router mediante la Interface de Línea de Comandos, habitualmente se accede al modo Usuario, a menos que el router haya sido configurado para acceder directamente al modo Privilegiado.

El modo Usuario es el modo más básico de la Interface de Línea de Comandos. Cuando se está en este modo, el indicador del sistema consiste del nombre de host del router seguido del símbolo ">". En forma predeterminada, el nombre de host es "Router":

```
Router>
```

Los comandos disponibles en el modo Usuario son un subconjunto de los comandos disponibles en el modo Privilegiado. Para ver la lista de los comandos disponibles se utiliza el caracter "?":

```
Router> ?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  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
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  ssh              Open a secure shell client connection
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  voice            Voice Commands
  where            List active connections
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD
```

Los comandos disponibles en este modo no permiten modificar la configuración del router; solamente se pueden ver algunos elementos de su configuración, en particular de sus componentes de hardware y de su sistema operativo. El Capítulo 4 estará dedicado a ver algunos de los comandos de uso habitual que están disponibles en este modo.

Para salir del modo Usuario y terminar una sesión en el router se pueden utilizar los comandos `logout`, `exit` o `quit`.

```
Router> logout
```

Modo Privilegiado

En el modo Privilegiado no solamente están disponibles los comandos del modo Usuario, sino también un conjunto adicional de comandos que solo pueden ser ejecutados en este modo.

El modo Privilegiado es el ámbito desde el cual se puede acceder al modo de Configuración Global, en el cual se encuentran aquellos comandos que permiten modificar la configuración del router y, por lo tanto, su funcionamiento. Por este motivo es que el acceso al modo Privilegiado suele estar protegido mediante una contraseña. En el capítulo 7 veremos el procedimiento para establecer esta y otras contraseñas de acceso.

Cuando la contraseña del modo Privilegiado haya sido establecida, el sistema operativo solicitará al usuario que ingrese la misma antes de permitir el acceso. Cuando se escriba esta contraseña, la misma no aparece visualizada en la pantalla.

Para acceder al modo Privilegiado se debe ejecutar el comando de modo Usuario `enable`:

```
Router> enable
Password: <....>
Router#
```

Una vez en el modo Privilegiado, el indicador del sistema cambia y consiste del nombre de host del router seguido del símbolo "#".

Al igual que en el modo Usuario, para obtener la lista de los comandos disponibles en el modo Privilegiado se utiliza el símbolo "?":

```
Router# ?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS subsystem
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
 --More--
```

En la última línea vemos el mensaje `--More--`; la Interface de Línea de Comandos muestra este mensaje cada vez que, al desplegar varias líneas de información, se llena una pantalla. Para continuar y ver las siguientes líneas se presiona la tecla de barra espaciadora:

```
  isdn             Run an ISDN EXEC command on a BRI interface
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  monitor          Monitoring different system events
  more             Display the contents of a file
  mrinfo           Request neighbor and version information from a multicast
                   router
  mrm              IP Multicast Routing Monitor Test
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  ncia             Start/Stop NCIA Server
  no               Disable debugging functions
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  pwd              Display current working directory
  reload           Halt and perform a cold restart
  rename           Rename a file
  restart          Restart Connection
  resume           Resume an active network connection
 --More--
  rlogin           Open an rlogin connection
  rsh              Execute a remote command
  sdlc             Send SDLC test frames
  send             Send a message to other tty lines
  setup            Run the SETUP command facility
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  ssh              Open a secure shell client connection
  start-chat       Start a chat-script on a line
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  test             Test subsystems, memory, and interfaces
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  undebug          Disable debugging functions (see also 'debug')
  verify           Verify a file
  voice            Voice Commands
  where            List active connections
```

```
  write            Write running configuration to memory, network, or
                   terminal
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD
Router#
```

Para salir del modo Privilegiado y volver al modo Usuario se utiliza el comando `disable`:

```
Router# disable
Router>
```

Observe que el indicador del sistema ha vuelto a cambiar, para indicar que ahora estamos nuevamente en el modo Usuario.

Para terminar la sesión estando en el modo Privilegiado se pueden utilizar los comandos `logout`, `exit` o `quit`, como en el modo Usuario.

Modo de Configuración Global

El modo de Configuración Global permite configurar parámetros del router que modifican globalmente su funcionamiento y también permite acceder a sub-modos de configuración específicos para configurar elementos tales como interfaces de red y protocolos de encaminamiento.

Todos los comandos que se ejecuten en el modo de Configuración Global modifican la configuración en ejecución del router y toman efecto inmediatamente después de ser ejecutados desde la línea de comandos. En virtud de esto, solo puede accederse a este modo de configuración desde el modo Privilegiado al que, como hemos mencionado anteriormente, suele controlarse su acceso mediante una contraseña.

Para acceder al modo de Configuración Global se utiliza el comando de modo Privilegiado `configure terminal`:

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

Una vez en el modo de Configuración Global el indicador del sistema cambia y consiste del nombre de host del router, seguido de la palabra “config” entre paréntesis y del símbolo #. Nuevamente, para obtener la lista de comandos disponibles, se utiliza el símbolo “?”.

```
Router(config)# ?
Configure commands:
  aaa                      Authentication, Authorization and Accounting.
  boot                     Modify system boot parameters
  clock                    Configure time-of-day clock
  config-register          Define the configuration register
  default                  Set a command to its defaults
  do                       To run exec commands in config mode
```

```
  downward-compatible-config  Generate a configuration compatible with older
                              software
  enable                      Modify enable password parameters
  hostname                    Set system's network name
  ip                          Global IP configuration subcommands
  logging                     Modify message logging facilities
  memory-size                 Adjust memory size by percentage
  netbios                     NETBIOS access control filtering
  no                          Negate a command or set its defaults
  parser                      Configure parser
  regexp                      regexp commands
  rif                         Source-route RIF cache
  service                     Modify use of network based services
  tdm                         TDM configurations
  track                       Object tracking configuration commands
 --More--
```

Para salir del modo de Configuración Global y volver al modo Privilegiado pueden utilizarse los comandos `end` o `exit` y también presionando la combinación de teclas Control-Z.

```
Router(config)# end
Router#
```

Al salir del modo de Configuración Global, el indicador del sistema vuelve a indicar que ahora se está en el modo Privilegiado.

Sub-Modos de Configuración

Los Submodos de Configuración permiten acceder a la configuración de componentes y procesos más específicos del router, como ser las interfaces y/o subinterfaces de red o los protocolos de encaminamiento de IP.

Los Submodos de Configuración que tiene IOS son más de veinte. Como ejemplo, vamos a tratar ahora el submodo de Configuración de Interface, dejando para capítulos posteriores el tratamiento de otros submodos de uso habitual en la configuración de un router de Cisco.

Sub-Modo de Configuración de Interface

Este submodo permite acceder a la configuración de las interfaces de red del router, tales como FastEthernet o Serial. Puesto que en un router hay varias interfaces de red, es necesario indicar en la Línea de Comandos cual es la interface que se va a configurar; para ello se utiliza el formato general de identificación de interfaces visto en el Capítulo 1. Así, para acceder al submodo de configuración de la interface `FastEthernet 0/0` se utiliza el comando de Configuración Global `interface fastethernet 0/0`:

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

Observe que el indicador del sistema ha cambiado para indicar que ahora se está en el submodo de Configuración de Interface (`config-if`). Como anteriormente, para obtener la lista de comandos disponibles, se utiliza el símbolo de interrogación "?".

```
Router(config-if)# ?
Interface configuration commands:
  access-expression       Build a bridge boolean access expression
  appletalk               Appletalk interface subcommands
  arp                     Set arp type (arpa, probe, snap) or timeout
  backup                  Modify backup parameters
  bandwidth               Set bandwidth informational parameter
  bridge-group            Transparent bridging interface parameters
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  cmns                    OSI CMNS
  crypto                  Encryption/Decryption commands
  custom-queue-list       Assign a custom queue list to an interface
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  dlsw                    DLSw interface subcommands
  dspu                    Down Stream PU
  exit                    Exit from interface configuration mode
  fair-queue              Enable Fair Queuing on an Interface
  fras                    DLC Switch Interface Command
  full-duplex             Configure full-duplex operational mode
  h323-gateway            Configure H323 Gateway
 --More--
  half-duplex             Configure half-duplex and related commands
  help                    Description of the interactive help system
  hold-queue              Set hold queue depth
  ip                      Interface Internet Protocol config commands
  ipv6                    IPv6 interface subcommands
  ipx                     Novell/IPX interface subcommands
  keepalive               Enable keepalive
  lan-name                LAN Name command
  llc2                    LLC2 Interface Subcommands
  load-interval           Specify interval for load calculation for an
                          interface
  locaddr-priority        Assign a priority group
  logging                 Configure logging for interface
  loopback                Configure internal loopback on an interface
  mac-address             Manually set interface MAC address
  max-reserved-bandwidth  Maximum Reservable Bandwidth on an Interface
  media-type              Interface media type
  mtu                     Set the interface Maximum Transmission Unit (MTU)
  multilink-group         Put interface in a multilink bundle
```

```
  netbios                 Use a defined NETBIOS access list or enable
                          name-caching
  no                      Negate a command or set its defaults
  ntp                     Configure NTP
 --More--
  priority-group          Assign a priority group to an interface
  random-detect           Enable Weighted Random Early Detection (WRED) on an
                          Interface
  rate-limit              Rate Limit
  sap-priority            Assign a priority group
  service-policy          Configure QoS Service Policy
  shutdown                Shutdown the selected interface
  smrp                    Simple Multicast Routing Protocol interface
                          subcommands
  sna                     SNA pu configuration
  snapshot                Configure snapshot support on the interface
  snmp                    Modify SNMP interface parameters
  speed                   Configure speed operation.
  standby                 HSRP interface configuration commands
  timeout                 Define timeout values for this interface
  traffic-shape           Enable Traffic Shaping on an Interface or
                          Sub-Interface
  transmit-interface      Assign a transmit interface to a receive-only
                          interface
  trunk-group             Configure interface to be in a trunk group
  tx-ring-limit           Configure PA level transmit ring limit
```

En el Capítulo 8 vamos a utilizar extensamente este comando cuando configuremos las interfaces de nuestros routers.

Para salir del submodo de Configuración de Interface y volver al modo de Configuración Global se utiliza el comando `exit`. Si se desea volver directamente al modo Privilegiado puede utilizarse el comando `end` o la combinación de teclas Control-Z.

Modo ROM Monitor

El modo ROM Monitor (ROMMON) ejecuta una versión reducida del sistema operativo IOS, localizada en la memoria ROM del router. Se utiliza particularmente para realizar una carga manual del sistema operativo cuando, por ejemplo, no es posible que se cargue en forma automática desde la memoria FLASH. El modo Monitor ROM también se utiliza en circunstancias especiales para realizar pruebas de diagnóstico del router.

En la mayoría de los sistemas puede accederse a este modo ejecutando el comando de modo Privilegiado `reload` (que provoca la reinicialización del router) y luego presionando la tecla Break o la combinación de teclas Control-C dentro de los primeros 60 segundos de arranque del router. Otra forma de acceder a este modo es estableciendo un valor específico en el registro de configuración `CONFIG-REGISTER` mencionado en el Capítulo 1, lo cual ocasiona que el router ingrese automáticamente en este modo cuando se reinicia. En el Capítulo 10 estudiaremos el registro de configuración y su relación con el proceso de arranque de un router

de Cisco y veremos cómo interactuar con el modo Monitor ROM y en qué situaciones es necesario hacerlo.

Modo Setup

El modo Setup es un modo interactivo que se ejecuta automáticamente cuando se enciende el router por primera vez, y que permite establecer una configuración mínima inicial en un router que no tenga ya un archivo de configuración de arranque en su memoria NVRAM. Este modo presenta al usuario una serie de preguntas que, al irlas respondiendo una a una, van construyendo esa configuración inicial mínima.

Las primeras líneas que despliega el modo Setup se muestran a continuación:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-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]:
```

En el Capítulo 8 utilizaremos este modo para establecer una configuración inicial a uno de los routers con los cuales vamos a trabajar en ese capítulo y en los siguientes.

Resumen de Modos

En la tabla siguiente se resumen los cuatro primeros modos de la Interface de Línea de Comandos. Estos cuatro modos son los que de manera más frecuente vamos a utilizar a lo largo del resto del libro.

Usuario	Acceso:
	Indicador:
	Salida:
		Inicio de sesión
		`Router>`
		`logout`

Privilegiado	Acceso:
	Indicador:
	Salida:
		`enable`
		`Router#`
		`disable`

Configuración Global	Acceso:
	Indicador:
	Salida:
		`configure terminal`
		`Router(config)#`
		`end` o `<CNTL/Z>`

Configuración de Interface	Acceso: Indicador: Salida:	`interface` <id. de interface> `Router(config-if)#` `exit` para volver al modo de Configuración Global `end` para volver al modo Privilegiado

El Sistema de Ayuda

El sistema operativo IOS cuenta con cientos de comandos, muchos de los cuales requieren que también se especifique el valor de uno o mas parámetros o de palabras claves adicionales que completan la sintaxis. Un ejemplo es el comando `interface fastethernet 0/0` que vimos anteriormente, donde el comando `interface` requiere de la palabra clave `fastethernet` y del parámetro `0/0`.

La Interface de Línea de Comandos de IOS ofrece un sistema de ayuda que es sensible al contexto y que permite obtener ayuda específica al modo de configuración en que nos encontremos y también sobre la sintaxis de los comandos disponibles en cada modo.

Veremos ahora algunas de las facilidades que ofrece este sistema de ayuda y dejaremos otras para capítulos posteriores, que introduciremos a medida que se presente la oportunidad.

Ya hemos visto anteriormente que para obtener la lista de comandos disponibles en un modo podemos utilizar el signo de interrogación "?". Este signo tiene también otras funciones mas específicas; veamos dos de ellas.

El primer lugar, para obtener la lista de comandos que comienzan con una secuencia específica de caracteres podemos escribir esos caracteres seguidos del signo "?", sin espacio entre medio:

```
Router# co?
  configure   connect   copy
```

En el ejemplo podemos ver que, en el modo Privilegiado (#) hay tres comandos que comienzan con las letras "co": `configure`, `connect` y `copy.`

La otra función de signo "?" permite obtener la lista de argumentos (parámetros) o de palabras claves de un comando. Para esto, se escribe el comando seguido del signo "?", separados por un espacio en blanco. Veamos un ejemplo de uso en el modo Privilegiado:

```
Router# configure ?
  memory              Configure from NV memory
  network             Configure from a TFTP network host
  terminal            Configure from the terminal
  <cr>
```

El ejemplo anterior nos muestra que el comando `configure` admite tres opciones o variantes: `configure memory`, `configure network` y `configure terminal`.

Otro ejemplo, esta vez en el modo de Configuración Global, es el comando `interface` que vimos anteriormente:

```
Router(config)# interface ?
  Async               Async interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
```

```
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Group-Async        Async Group interface
  Lex                Lex interface
  Loopback           Loopback interface
  MFR                Multilink Frame Relay bundle interface
  Multilink          Multilink-group interface
  Null               Null interface
  Serial             Serial
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  range              interface range command
```

En este caso el comando `interface` requiere la especificación del tipo de interface que se va a configurar. La lista desplegada puede variar en función de los tipos de interfaces que tenga el router con el que se está trabajando.

Dependiendo del comando de que se trate, esta última facilidad puede utilizarse repetidas veces hasta completar el comando con todos sus parámetros y palabras clave. Como ejemplo, veamos el comando de modo Privilegiado `clock` que permite establecer la fecha y hora del sistema:

```
Router# clock ?
  set       Set the time and date
Router# clock
```

La salida anterior indica que el comando `clock` debe ir seguido de la palabra clave `set` para establecer la hora y la fecha. Vemos además que la Interface de Línea de Comandos escribe a continuación el comando inicial por nosotros. Utilicemos nuevamente la facilidad de ayuda para ver que debemos escribir a continuación de `set`:

```
Router# clock set ?
  hh:mm:ss    Current time
Router# clock set
```

De acuerdo a lo que indica la ayuda, lo que debemos escribir a continuación de `clock set` es la hora, en el formato hora:minutos:segundos. Escribamos la hora y presionemos la tecla **Intro**:

```
Router# clock set 12:00:00
% Incomplete command.
```

El mensaje de error anterior es desplegado por el Intérprete de Comandos y nos indica que algo está faltando en el comando anterior, es decir, que además de especificar la hora, hay algo mas que debemos escribir para completar el comando. Sigamos pidiendo ayuda:

```
Router# clock set 12:00:00 ?
  <1-31>    Day of the month
  January   Month of the year
  February
  March
  April
  May
  June
  July
  August
  September
  October
  November
  December
Router# clock set 12:00:00
```

Lo que está faltando indicar es la fecha; ingresémosla a continuación de la hora:

```
Router# clock set 12:00:00 30 March 05
                                     ^
% Invalid input detected at "^" marker.
```

El símbolo "^" marca el lugar donde el Intérprete de Comandos ha detectado un error de sintaxis en el comando escrito. En este caso, nos está indicando que hay un problema al indicar el año como "05". Usemos nuevamente la facilidad de ayuda para ver la forma correcta de especificarlo:

```
Router# clock set 12:00:00 30 March ?
 <1993-2035>  Year
Router# clock set 12:00:00 30 March
```

La ayuda nos dice que el año debe especificarse con sus cuatro dígitos y que el rango válido va de 1993 a 2035. Tenemos ahora, entonces, el comando completo:

```
Router# clock set 12:00:00 30 March 2005
Router#
```

Si luego de ejecutar un comando no aparece ningún mensaje en la línea de comandos, significa que el comando está correcto y fue aceptado como válido por el Intérprete de Comandos.

Otra característica de la Interfaz de Línea de Comandos es que los comandos y palabras claves pueden ser abreviados a una cantidad de letras que lo hagan único, es decir, no ambiguo. Por ejemplo, en lugar de escribir el comando completo `enable`, es suficiente con escribir `ena`

puesto que no hay ningún otro comando que comience con esas tres letras. Lo mismo ocurre, por ejemplo, para especificar una interface; en lugar de escribir `interface ethernet 0` alcanza con escribir `int eth 0` e incluso `int e 0` ya que el único tipo de interface que comienza con la letra "e" es ethernet.

En caso que la abreviación utilizada no corresponda a un único comando, la Interface de Línea de Comandos despliega un mensaje de error:

```
Router# dis
% Ambiguous command: "dis"
```

Para el Intérprete de Comandos, la palabra `dis` es ambigua; veamos por qué:

```
Router# dis?
 disable disconnect
```

En el ejemplo anterior hay, entonces, dos comandos de modo Privilegiado que comienzan con "`dis`": `disable` y `disconnect`. Si el comando que queremos ejecutar es `disable`, podemos abreviarlo a `disa`, con lo cual el Intérprete de Comandos no podrá confundirlo con `disconnect`:

```
Router# disa
Router>
```

También con esta facilidad de comandos abreviados puede utilizarse la tecla TAB (tabulador) para que la Interface de Línea de Comandos complete el nombre del comando. Así, si se escribe el comando abreviado `en` y se presiona la tecla TAB, la Interface de Línea de Comandos completará el comando y desplegará `enable`:

```
Router> en<TAB>
Router> enable
```

Historia de comandos

La Interface de Línea de Comandos mantiene en memoria, en forma predeterminada, una lista de los diez últimos comandos que han sido ejecutados. Utilizando las teclas de **Flecha hacia Arriba** y **Flecha hacia Abajo** o, respectivamente, las combinaciones de teclas **Control-P** (Previous) y **Control-N** (Next) se puede recorrer la lista y volver a ejecutar o a editar un comando ya ejecutado sin tener que escribirlo nuevamente.

Para desplegar la lista completa de esos diez últimos comandos se utiliza el comando `show history`:

```
Router# show history
  enable
  configure terminal
  dis
  show history
Router#
```

La cantidad de comandos que IOS mantiene en la lista es configurable, así como también es posible deshabilitar y volver a habilitar esta facilidad de historia de comandos. El comando `show history` puede ejecutarse tanto en modo Usuario como en modo Privilegiado.

3. Acceso al router

Para poder ver o modificar la configuración de un router es necesario, en primer término, conectarse físicamente al mismo. Las dos formas más habituales de conectarse a un router de Cisco para iniciar una sesión de administración en el mismo son:

- A través del puerto Consola, utilizando una computadora personal y un software de emulación de terminal.
- A través de la red, accediendo por una de sus interfaces de red mediante la aplicación Telnet de TCP/IP.

Con cualquiera de estas dos formas se accede a la misma Interface de Línea de Comandos que hemos descrito en el Capítulo 2 y es posible realizar "casi" las mismas tareas de configuración con ambas; mas adelante veremos el por qué de la expresión "casi".

Acceso por el puerto Consola

El acceso por el puerto Consola se utiliza cuando se tiene acceso físico directo al router y es, por otra parte, la primera forma a utilizar cuando se va a configurar un router por primera vez o cuando el router, por algún motivo, ha perdido su archivo de configuración de arranque.

Tal como mencionamos en el Capítulo 1, para conectarse físicamente al router a través del puerto de Consola se requiere disponer de una computadora personal o un "portable" y de un cable serial o "rollover", según el tipo de conector que tenga el router para ese puerto.

Dependiendo del modelo de router con el que se esté trabajando, el puerto Consola puede ser del tipo RJ-45 o del tipo DB25. En la tabla siguiente se muestran algunas series de modelos de routers de Cisco y los correspondientes tipos de conector para el puerto Consola y los tipos de cables requeridos:

Serie	Conector Consola	Cable de conexión
700, 800, 1000, 1600, 1700, 2500, 2600, 3600	RJ-45	Rollover
4000, 4500, 4700, 7000, 7200, 7500, 12000	DB25	Serial directo

Los routers con los que vamos a trabajar en este libro pertenecen a la serie 1700 que, como lo indicamos en la tabla anterior, tienen su puerto Consola del tipo RJ-45 y requieren, en consecuencia, del uso de un cable "rollover" para conectarnos a él. Este cable tiene conectores RJ-45 en sus dos extremos.

Para establecer, entonces, la conexión física al router, uno de los extremos del cable "rollover" se conecta al puerto Consola y el otro extremo se conecta a uno de los puertos seriales, COM1 o COM2, de la computadora personal. Para esta última conexión se requerirá un adaptador RJ-45 a DB9 puesto que los puertos COM son del tipo DB9.

Una alternativa al cable "rollover" es el cable denominado "cable de gestión", el cual tiene un conector RJ-45 en uno de sus extremos y un conector DB-9 "hembra" en el otro.

En este caso el extremo RJ-45 se conecta al puerto de Consola del router y el otro extremo va directamente conectado al puerto COM de la computadora personal, sin necesidad de utilizar un adaptador.

Los procedimientos anteriores nos permiten, pues, la conexión física al router. Para acceder ahora a la Interface de Línea de Comandos debemos utilizar cualquier software de emulación de terminal como, por ejemplo, HyperTerminal de Windows 95/98.

Ya sea que utilicemos este software o algún otro, para iniciar una sesión en el router es necesario configurar en el software sus parámetros de comunicación. Los valores apropiados para la comunicación serial al puerto Consola de un router de Cisco son los siguientes:

Parámetro	Valor
Emulación de terminal	VT100
Velocidad	9.600
Paridad	No
Bits de datos	8
Bits de parada	1
Control de flujo	Ninguno

El procedimiento para configurar estos parámetros en HyperTerminal de Windows 95/98 es el siguiente:

1. Iniciar la ejecución de HyperTerminal: en el menú de **Inicio** de Windows seleccionamos **Programas**, luego **Accesorios**, luego **Comunicaciones** y finalmente **HyperTerminal**.

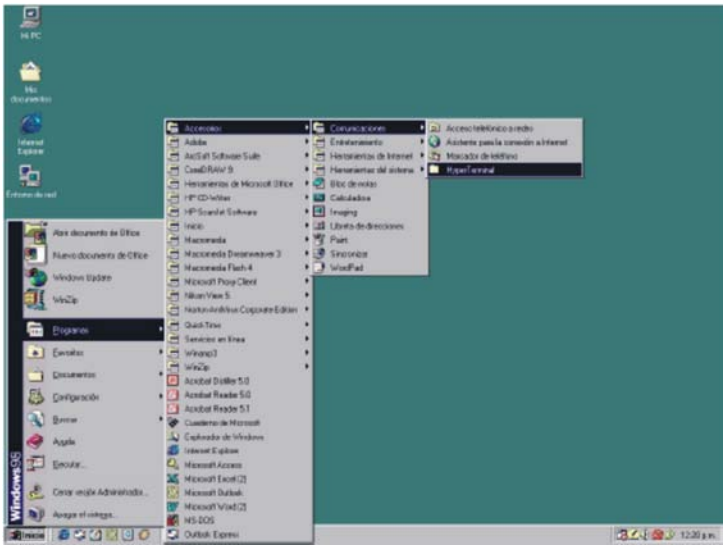


Fig. 3 - 1

2. En la primera ventana que aparece asignamos un nombre a la nueva conexión, por ejemplo "Router Cisco", y presionamos el botón **Aceptar**:

Fig. 3 - 2

3. En la siguiente ventana seleccionamos el puerto de comunicaciones COM1 o COM2, según a cual de los puertos COM de la computadora personal hayamos conectado el cable de Consola:

Fig. 3 - 3

4. La siguiente pantalla es la que nos permite configurar los parámetros de comunicación del puerto COM seleccionado en el paso anterior. Asignamos entonces los valores de la tabla anterior:

Fig. 3 - 4

Luego de ajustar los parámetros, presionamos el botón **Aceptar**. Si todo funciona correctamente, al cabo de unos instantes veremos en pantalla el siguiente mensaje:

```
Router Con0 is now available


Press RETURN to get started.
```

Si presionamos la tecla **Intro** aparece el indicador del sistema ("prompt") para indicar que se está en el modo Usuario de la Interface de Línea de Comandos:

```
Router>
```

A partir de este momento podemos comenzar a ejecutar comandos de IOS para ver o modificar la configuración actual del router o para establecer su configuración inicial si el router aún no ha sido configurado por primera vez. En el Capítulo 4 veremos los primeros comandos que podemos ejecutar en el modo Usuario y en los capítulos siguientes veremos nuevos comandos, disponibles en los otros modos de la Interface de Línea de Comandos.

Acceso con Telnet

Telnet es una aplicación estándar de TCP/IP que permite iniciar una sesión en un host remoto mediante una conexión TCP al puerto 23. Telnet es una aplicación del tipo "cliente/servidor"; la parte "servidor" ejecuta en el host remoto (en nuestro caso, el router) y la parte "cliente" está disponible en todas las versiones de Windows, así como también en las diferentes distribuciones de Linux y UNIX.

Para ejecutar el cliente Telnet en Windows vamos al menú de **Inicio**, seleccionamos la opción **Ejecutar**, escribimos TELNET en la ventana de diálogo y presionamos el botón **Aceptar**. Aparece entonces la ventana principal de Telnet:

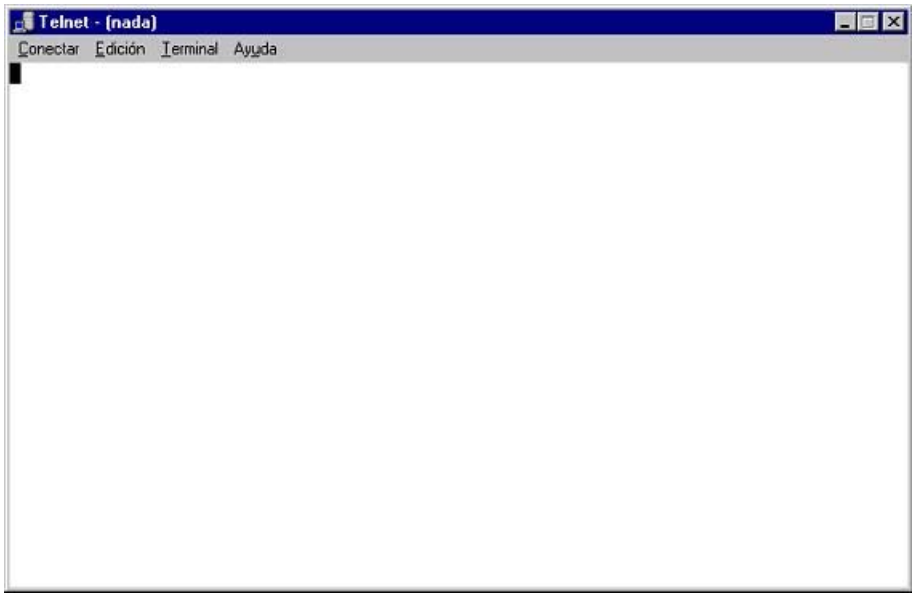


Fig. 3 - 5

Para poder iniciar una sesión Telnet en el router, éste debe estar accesible a través de la red, ya sea en la red local o a través de un enlace WAN. Por lo tanto, la interface de red que conecta el router a esa red debe estar previamente configurada en una dirección IP válida y esta configuración debió hacerse previamente mediante el acceso por Consola. El acceso por Telnet es útil cuando no se tiene acceso físico directo al router y es necesario hacer alguna tarea de mantenimiento en la configuración del mismo.

Supongamos que somos los administradores de la red de una organización que tiene sus instalaciones distribuidas en varios sitios distantes unos de otros, por ejemplo, una empresa que tiene sucursales en distintos puntos de la ciudad y que en cada sucursal hay una red local y que todos los sitios están interconectados mediante enlaces WAN formando una sola interred privada. Si en algún momento es necesario ver o modificar la configuración de alguno de los routers, una alternativa es desplazarse físicamente hasta el sitio donde está el router y, estando allí, conectarnos al mismo a través del puerto de Consola para hacer esas tareas. Sin embargo, si el router está funcionando correctamente y está accesible a través de la interred, es más sencillo y eficiente acceder al mismo a través de la red IP e iniciar una sesión con Telnet desde donde estemos, en lugar de desplazarnos hasta el lugar donde está instalado el router.

Supongamos por el momento que el router que queremos configurar está accesible en la red local donde también está conectada nuestra estación de trabajo, tal como se muestra en la figura 3-6.

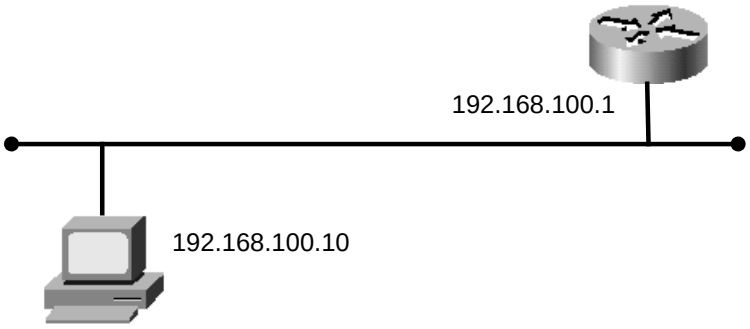


Fig. 3 - 6

Para iniciar la sesión Telnet debemos especificar al cliente Telnet la dirección IP del router o, alternativamente, su nombre de host. Para que esto último funcione, debe haber en la red un servidor DNS que permita la resolución de nombres y configurar en el router la dirección IP de éste, para luego poder obtener a partir de él la dirección IP del router. Asumamos que no tenemos un servidor DNS en la red e indiquemos la dirección IP del router. Para ello, en el cliente Telnet seleccionamos la opción **Conectar** del menú **Conectar** y en la ventana de diálogo especificamos la dirección IP del router y presionamos el botón **Aceptar**.

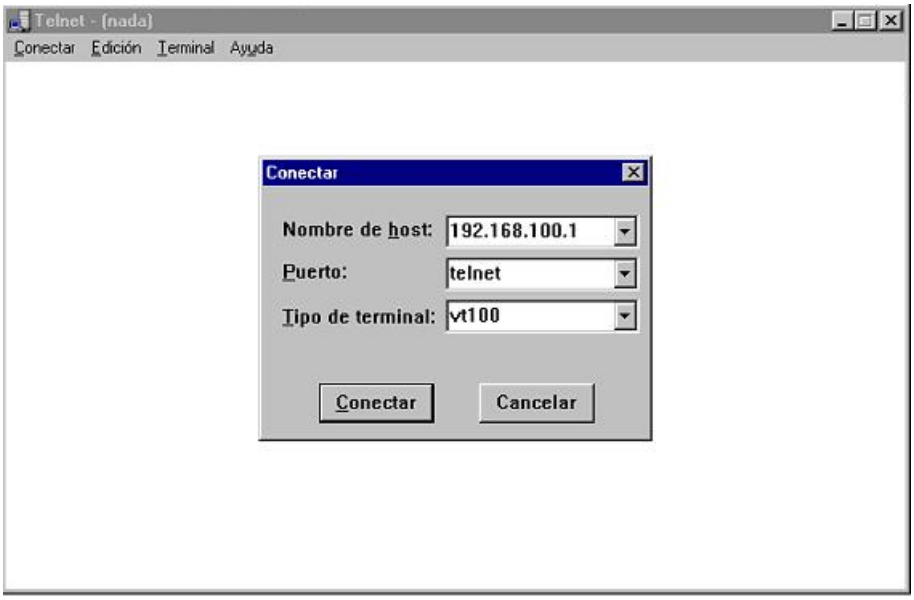


Fig. 3 - 7

Puesto que para acceder al router usando Telnet se debe especificar su dirección IP, la interface de red del router a través de la cual se hace la conexión debe estar previamente configurada con una dirección IP válida y esta configuración previa debe hacerse, como dijimos antes, a través de la Consola. Por este motivo es que mas arriba dijimos que con una conexión Telnet puede hacer "casi" lo mismo que a través de la Consola. Si estamos conectados vía Telnet y modificamos, por ejemplo, la dirección IP de la interface a través de la cual estamos accediendo, perderemos de inmediato la conexión al router.

Un requisito imprescindible para poder iniciar la sesión con Telnet es haber configurado una contraseña de acceso remoto, lo cual debe hacerse también previamente a través de una conexión de Consola. Si el acceso por Telnet no está protegido por una contraseña, el router

rechaza el intento de inicio de sesión. En el Capítulo 7 veremos los comandos para establecer ésta y otras contraseñas que controlan el acceso al router como, por ejemplo, las que controlan el acceso al modo Privilegiado y también las que pueden establecerse para controlar el acceso a través de los puertos Consola y Auxiliar.

Asumamos por el momento que la contraseña de acceso por Telnet ha sido establecida; un mensaje en la terminal indicará que debemos ingresarla:

```
User Access Verification

Password: < .. .. >
```

Una vez ingresada la contraseña e iniciada la conexión, lo que se ve en la pantalla de la estación de trabajo es exactamente lo mismo que se ve con la conexión por el puerto de Consola, es decir, el indicador del sistema de la Interface de Línea de Comandos:

```
Router>
```

En el ejemplo anterior ejecutamos el cliente Telnet desde una estación de trabajo con Windows 98. El sistema operativo IOS proporciona también un comando `telnet` que puede ser ejecutado en los modos Usuario y Privilegiado. Este comando es útil cuando se ha iniciado una sesión en un router, por ejemplo a través de la Consola, y se necesita acceder a un router remoto a través de la red.

4. Comandos de modos Usuario y Privilegiado

El sistema operativo IOS tiene cientos de comandos, muchos de los cuales requieren, a su vez, de la especificación de palabras claves para completar su sintaxis. La discusión en detalle de todos ellos, con sus opciones y parámetros, está documentada en forma completa en los manuales del sistema operativo que Cisco provee, tanto en la caja junto con el router como en su sitio web denominado CCO (Cisco Connection Online).

En este capítulo solamente vamos a repasar algunos de los comandos de uso más habitual en los modos Usuario y Privilegiado de la Interface de Línea de Comandos.

Modo Usuario

Tal como hemos mencionado en el Capítulo 2, el modo Usuario es el modo más básico que presenta la Interface de Línea de Comandos y es al que normalmente se accede cuando se inicia una sesión en el router.

Si nos conectamos al router, por ejemplo a través del puerto de Consola (siguiendo el procedimiento que vimos en el capítulo anterior) veremos inicialmente el indicador del sistema del modo Usuario:

```
Router>
```

Recordemos que para ver la lista de los comandos de IOS disponibles en este modo podemos utilizar la facilidad de ayuda de la Interface de Línea de Comandos:

```
Router> ?
```

Recordemos también que los comandos de IOS disponibles en este modo permiten ver pero no modificar la configuración del router.

Los comandos SHOW

Veremos a continuación algunos de estos comandos que son de uso frecuente para inspeccionar el estado de diferentes componentes del hardware y del software del router y también de algunos parámetros de la configuración del mismo. Estos comandos comienzan con la palabra clave `show`; usemos la facilidad de ayuda para desplegar la lista de opciones:

```
Router> show ?
  aaa               Show AAA values
  backup            Backup status
  bgp               BGP information
  c1700             Show c1700 information
  call              Show call
  caller            Display information about dialup connections
  cca               CCA information
  cdapi             CDAPI information
```

```
  cef               Cisco Express Forwarding
  class-map         Show QoS Class Map
  clock             Display the system clock
  cns               CNS subsystem
  compress          Show compression statistics
  connection        Show Connection
  controllers       Interface controller status
  cops              COPS information
  crm               Carrier Resource Manager info
  crypto            Encryption module
  dial-peer         Dial Plan Mapping Table for, e.g. VoIP Peers
  dialer            Dialer parameters and statistics
  drip              DRiP DB
  exception         exception informations
 --More--
  flash:            display information about flash: file system
  fras-host         FRAS Host Information
  gateway           Show status of gateway
  h323              Show H.323 VoIP information
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host table
  ip                IP information
  ipv6              IPv6 information
  kerberos          Show Kerberos Values
  location          Display the system location
  modemcap          Show Modem Capabilities database
  ncia              Native Client Interface Architecture
  num-exp           Number Expansion (Speed Dial) information
  policy-map        Show QoS Policy Map
  ppp               PPP parameters and statistics
  qdm               Show information about QoS Device Manager
  queue             Show queue contents
  queueing          Show queueing configuration
  radius            Shows radius information
  rmon              rmon statistics
  rpms-proc         RPMS Process Information
  rtr               Service Assurance Agent (SAA)
  sessions          Information about Telnet connections
 --More--
  snmp              snmp statistics
  srcp              Display SRCP Protocol information
  ssh               Status of SSH server connections
  ssl               Show SSL command
  tacacs            Shows tacacs+ server statistics
  tdm               Show tdm related information
  template          Template information
  terminal          Display terminal configuration parameters
  traffic-shape     traffic rate shaping configuration
```

```
  translation-rule  Show translation rule table
  trunk             Trunk info
  users             Display information about terminal lines
  version           System hardware and software status
  voice             Voice port configuration & stats
  vpdn              VPDN information
```

show clock

Este comando despliega en pantalla la fecha y hora interna actual del router:

```
Router> show clock
*12:45:56.396 UTC Mon Mar 17 2005
```

El formato de hora es: hora:minutos:segundos.milisegundos. UTC hace referencia a la zona horaria; en este caso indica el Tiempo Universal Coordinado (Coordinated Universal Time), también conocido como Hora del Meridiano de Greenwich (GMT – Greenwich Meridian Time).

Algunos modelos de routers de Cisco disponen de un reloj interno (hardware) alimentado por baterías, los cuales mantienen la fecha y hora establecidas entre rearranques del router. Para aquellos modelos que no tengan un reloj de este tipo, la fecha y hora se pierde cuando se apaga el router. Cuando se vuelve a encender, el reloj del sistema se establece a la hora 0 del 1 de Marzo de 1993. Cuando esto ocurre, es necesario establecer manualmente la hora correcta utilizando el comando de modo Privilegiado `clock set` que vimos en el Capítulo 2.

show hosts

Este comando muestra información sobre el nombre de dominio predeterminado, el estilo en uso para la resolución de nombres y las direcciones IP de los servidores de DNS que hayan sido configurados en el router:

```
Router> show hosts
Default domain is not set
Name/address lookup uses domain service
Name servers are 207.3.115.130, 207.3.115.131, 206.99.44.254
```

show users

Este comando despliega los usuarios actualmente conectados al router para tareas de administración del mismo.

```
Router> show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00

  Interface      User        Mode                 Idle     Peer Address
```

Como vemos en la salida del comando, hay una sola conexión activa y es a través de la línea `con,` que corresponde a la consola.

show version

Este comando despliega gran cantidad de información sobre la configuración del hardware del router, la versión del software de IOS y los nombres y orígenes del archivo de configuración y de la imagen de arranque del sistema operativo.

```
Router> show version
 1 Cisco Internetwork Operating System Software
 2 IOS(tm) C1700 Software (C1700-BK8NO3R2SV3Y7-M),Version 12.2(11)T,RELEASE SOFTWARE
(fc1)
 3 TAC Support: http://www.cisco.com/tac
 4 Copyright (c) 1986-2002 by cisco Systems, Inc.
 5 Compiled Wed 31-Jul-02 10:34 by ccai
 6 Image text-base: 0x80008124, data-base: 0x813ACC18
 7 ROM: System Bootstrap, Version 12.1(5r)T1, RELEASE SOFTWARE (fc1)
 8 ROM: C1700 Software (C1700-BK8NO3R2SV3Y7-M),Version 12.2(11)T,RELEASE SOFTWARE
(fc1)
 9 Router uptime is 8 minutes
10 System returned to ROM by power-on
11 System image file is "flash:c1700-bk8no3r2sv3y7-mz.122-11.T.bin"
12 cisco 1751 (MPC860P) processor (revision 0x101) with 55706K/9830K bytes of memory
13 Processor board ID JAD052212GV (390108165), with hardware revision 653413.
14 MPC860P processor: part number 5, mask 2
15 Bridging software
16 X.25 software, Version 3.0.0
17 1 FastEthernet/IEEE 802.3 interface(s)
18 2 Serial(sync/async) network interface(s)
19 4 Voice FXS interface(s)
20 32K bytes of non-volatile configuration memory
21 32768K bytes of processor board System flash (Read/Write)
22
23 Configuration register is 0x2102
```

Veamos qué significa la información desplegada en algunas de las líneas anteriores. La línea 1 muestra el nombre del sistema operativo que está ejecutando en el router, mientras que la línea 2 muestra la versión del mismo y la línea 4 la fecha en que fue compilado. Las líneas 7 y 8 muestran la versión del software de la memoria ROM.

La línea 9 indica el tiempo que ha transcurrido desde la última vez que se ha reinicializado el router; la línea 10 dice que el router se reinició por haber sido apagado y reencendido y la línea 11 muestra el nombre del archivo que contiene la imagen del sistema operativo IOS que se cargó a la memoria RAM desde la memoria FLASH.

La línea 13 proporciona información sobre el hardware de la placa de procesador y la línea 14 indica el tipo de procesador con el que está equipado. Las líneas 17 a 19 indican que este router tiene una interface de red del tipo FastEthernet, dos interfaces de red de tipo Serial y cuatro interfaces de voz para telefonía IP. Las líneas 20 y 21 indican, respectivamente, que el router tiene 32 KBytes de memoria NVRAM y 32 Mbytes de memoria RAM, y que el contenido de esta última se puede modificar (Read/Write).

Finalmente, la línea 23 muestra el valor del Registro de Configuración cuyo valor indica al router desde donde debe cargar el sistema operativo. En el Capítulo 10 volveremos sobre este parámetro.

Otros comandos SHOW

Las opciones del comando `show` que aparecen en el listado inicial no son las únicas posibles para este comando, sino que son las que la Interface de Línea de Comandos despliega en forma predeterminada.

Estando en el modo Usuario, y también en el modo Privilegiado, podemos configurar la sesión actual para que la facilidad de ayuda despliegue, no solamente todos los comandos disponibles en esos modos, sino también, para el ejemplo del comando `show`, todas sus opciones. Para esto se utiliza el comando `terminal full-help`:

```
Router> terminal full-help
```

Si ahora utilizamos nuevamente la facilidad de ayuda sobre el comando `show`, veremos que la lista de opciones es mayor:

```
Router> show ?
  aaa                 Show AAA values
  access-expression   List access expression
  access-lists        List access lists
  adjacency           Adjacent nodes
  aliases             Display alias commands
  appletalk           AppleTalk information
  arp                 ARP table
  async               Information on terminal lines used as router interfaces
  backup              Backup status
  bgp                 BGP information
  bridge              Bridge Forwarding/Filtering Database [verbose]
  bsc                 BSC interface information
  bstun               BSTUN interface information
  buffers             Buffer pool statistics
  c1700               Show c1700 information
  call                Show call
  caller              Display information about dialup connections
  cca                 CCA information
  cdapi               CDAPI information
  cdp                 CDP information
  cef                 Cisco Express Forwarding
  class-map           Show QoS Class Map
  clock               Display the system clock
  cls                 DLC user information
  cns                 CNS subsystem
  compress            Show compression statistics
  connection          Show Connection
  controllers         Interface controller status
  cops                COPS information
  crm                 Carrier Resource Manager info
  crypto              Encryption module
  debugging           State of each debugging option
```

```
  diag              Show diagnostic information for port adapters/modules
  dial-peer         Dial Plan Mapping Table for, e.g. VoIP Peers
  dialer            Dialer parameters and statistics
  dlsw              Data Link Switching information
  dnsix             Shows Dnsix/DMDP information
  drip              DRiP DB
  dspu              Display DSPU information
  dxi               atm-dxi information
  entry             Queued terminal entries
  exception         exception informations
  flash:            display information about flash: file system
  frame-relay       Frame-Relay information
  fras              FRAS Information
  fras-host         FRAS Host Information
  gateway           Show status of gateway
  h323              Show H.323 VoIP information
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host
                    table
  interfaces        Interface status and configuration
  ip                IP information
  ipv6              IPv6 information
  ipx               Novell IPX information
  kerberos          Show Kerberos Values
  line              TTY line information
  llc2              IBM LLC2 circuit information
  lnm               IBM LAN manager
  local-ack         Local Acknowledgement virtual circuits
  location          Display the system location
  logging           Show the contents of logging buffers
  memory            Memory statistics
  modemcap          Show Modem Capabilities database
  ncia              Native Client Interface Architecture
  netbios-cache     NetBIOS name cache contents
  ntp               Network time protocol
  num-exp           Number Expansion (Speed Dial) information
  policy-map        Show QoS Policy Map
  ppp               PPP parameters and statistics
  privilege         Show current privilege level
  processes         Active process statistics
  protocols         Active network routing protocols
  qdm               Show information about QoS Device Manager
  qllc              Display qllc-llc2 and qllc-sdlc conversion information
  queue             Show queue contents
  queueing          Show queueing configuration
  radius            Shows radius information
  registry          Function registry information
  reload            Scheduled reload information
```

```
  rif                RIF cache entries
  rmon               rmon statistics
  route-map          route-map information
  rpms-proc          RPMS Process Information
  rtr                Service Assurance Agent (SAA)
  sdllc              Display sdlc - llc2 conversion information
  sessions           Information about Telnet connections
  smds               SMDS information
  smrp               Simple Multicast Routing Protocol (SMRP) information
  sna                Display SNA host information
  snapshot           Snapshot parameters and statistics
  snmp               snmp statistics
  sntp               Simple network time protocol
  source-bridge      Source-bridge parameters and statistics
  spanning-tree      Spanning tree topology
  srcp               Display SRCP Protocol information
  ssh                Status of SSH server connections
  ssl                Show SSL command
  stacks             Process stack utilization
  standby            Hot Standby Router Protocol (HSRP) information
  stun               STUN status and configuration
  subsys             Show subsystem information
  tacacs             Shows tacacs+ server statistics
  tcp                Status of TCP connections
  tdm                Show tdm related information
  tech-support       Show system information for Tech-Support
  template           Template information
  terminal           Display terminal configuration parameters
  track              Tracking information
  traffic-shape      traffic rate shaping configuration
  translation-rule   Show translation rule table
  trunk              Trunk info
  users              Display information about terminal lines
  version            System hardware and software status
  vlans              Virtual LANs Information
  voice              Voice port configuration & stats
  vpdn               VPDN information
  whoami             Info on current tty line
  x25                X.25 information
  x29                X.29 information
```

Para deshabilitar esta facilidad de "ayuda completa" podemos utilizar el comando `terminal no full-help`:

```
Router> terminal no full-help
```

De la lista "completa" de opciones del comando `show` vamos a ver algunas de ellas que muestran información de importancia para el administrador del router.

show flash

Este comando muestra información acerca del contenido de la memoria FLASH del router.

```
Router> show flash
System flash directory:
File  Length   Name/status
  1   11327932  c1700-bk8no3r2sv3y7-mz.122-11.T.bin
[11327996 bytes used, 22226436 available, 33554432 total]
32768K bytes of processor board System flash (Read/Write)
```

En este ejemplo vemos que en la memoria FLASH hay un solo archivo de nombre c1700-bk8no3r2sv3y7-mz.122-11.T.bin, cuyo tamaño es de 11.327.932 bytes. Este archivo es el que contiene la imagen del sistema operativo IOS que se carga a la memoria RAM del router para su ejecución. La línea siguiente indica las cantidades de memoria FLASH ocupada, libre y total, todas expresadas en bytes.

show interfaces

Este comando permite ver el estado de las interfaces de red del router, sus parámetros de configuración y sus estadísticas de tráfico y de errores:

```
Router> show interfaces
 1 FastEthernet0/0 is administratively down, line protocol is down
 2  Hardware is PQUICC_FEC, address is 0004.c14e.8067 (bia 0004.c14e.8067)
 3  Internet address is 17.0.0.1/8
 4  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 252/255, txload 1/255, rxload 1/255
 5  Encapsulation ARPA, loopback not set
 6  Keepalive set (10 sec)
 7  Auto-duplex, 10Mb/s, 100BaseTX/FX
 8  ARP type: ARPA, ARP Timeout 04:00:00
 9  Last input never, output 00:08:40, output hang never
10  Last clearing of "show interface" counters never
11  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
12  Queueing strategy: fifo
13  Output queue :0/40 (size/max)
14  5 minute input rate 0 bits/sec, 0 packets/sec
15  5 minute output rate 0 bits/sec, 0 packets/sec
16     0 packets input, 0 bytes
17     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
18     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 watchdog
19     0 input packets with dribble condition detected
20     9 packets output, 1098 bytes, 0 underruns
21     9 output errors, 0 collisions, 0 interface resets
```

```
22     0 babbles, 0 late collision, 0 deferred
23     9 lost carrier, 0 no carrier
24     0 output buffer failures, 0 output buffers swapped out
25 Serial0/0 is administratively down, line protocol is down
26  Hardware is PowerQUICC Serial
27  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
28     reliability 255/255, txload 1/255, rxload 1/255
29  Encapsulation HDLC, loopback not set
30  Keepalive set (10 sec)
31  Last input never, output never, output hang never
32  Last clearing of "show interface" counters 00:08:51
33  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
34  Queueing strategy: fifo
35  Output queue :0/40 (size/max)
36  5 minute input rate 0 bits/sec, 0 packets/sec
37  5 minute output rate 0 bits/sec, 0 packets/sec
38     0 packets input, 0 bytes, 0 no buffer
39     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
40     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
41     0 packets output, 0 bytes, 0 underruns
42     0 output errors, 0 collisions, 1 interface resets
43     0 output buffer failures, 0 output buffers swapped out
44     0 carrier transitions
45     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
46 Serial0/1 is administratively down, line protocol is down
47  Hardware is PowerQUICC Serial
48  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
49     reliability 255/255, txload 1/255, rxload 1/255
50  Encapsulation HDLC, loopback not set
51  Keepalive set (10 sec)
52  Last input never, output never, output hang never
53  Last clearing of "show interface" counters never
54  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
55  Queueing strategy: weighted fair
56  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
57     Conversations  0/0/256 (active/max active/max total)
58     Reserved Conversations 0/0 (allocated/max allocated)
59     Available Bandwidth 1158 kilobits/sec
60  5 minute input rate 0 bits/sec, 0 packets/sec
61  5 minute output rate 0 bits/sec, 0 packets/sec
62     0 packets input, 0 bytes, 0 no buffer
63     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
64     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65     0 packets output, 0 bytes, 0 underruns
66     0 output errors, 0 collisions, 0 interface resets
67     0 output buffer failures, 0 output buffers swapped out
68     0 carrier transitions
69     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

Las líneas 1, 25 y 46 muestran el estado operacional de las interfaces del router; la línea 1 para la interface `fastethernet 0/0` y las líneas 25 y 46 para las interfaces `serial 0/0` y `serial 0/1`. El estado de una interface comprende dos aspectos: uno al nivel de la capa Física del Modelo de Referencia OSI y el otro al nivel de la capa de Enlace.

El estado al nivel de la capa Física indica si la interface está recibiendo la señalización eléctrica a través del medio de transmisión al cual está conectada, es decir, la señal de portadora ("carrier"). En una interface Ethernet, por ejemplo, esta señalización indica si hay conexión física con el Hub o Switch al cual el router está conectado.

El estado al nivel de la capa de Enlace, referido en las líneas 1, 25 y 46 como "line protocol" indica si la interface está recibiendo los paquetes de estado de enlace que son periódicamente transmitidos por un dispositivo para indicar su presencia al dispositivo de red al cual está directamente conectado.

En la tabla siguiente se muestran las combinaciones comunes de estos dos aspectos del estado de una interface:

Estado capa Física	Estado capa Enlace	Descripción
Up	Up	La interface está operacional.
Up	Down	La conexión física está correcta, pero no se están recibiendo los paquetes de estado de enlace. La interface no está operacional.
Down	Down	La conexión física de la interface no está funcionando bien o la interface está desconectada.
Administratively Down	Down	La interface ha sido manualmente deshabilitada o nunca ha sido habilitada luego de su configuración inicial.

Veamos ahora con mas detalle los principales datos desplegados para la interface `fastethernet 0/0`. La línea 2 muestra el tipo de hardware de la interface y su dirección física o MAC. La línea 3 indica la dirección IP configurada en la interface. El "/8" que aparece a continuación de la dirección IP indica el valor de la máscara de subred; tiene ocho unos, es decir, la máscara de subred es 255.0.0.0. Si esta interface no tuviera una dirección IP configurada, se mostraría el mensaje `Internet address is not set`.

La línea 4 muestra los valores de los parámetros MTU (Maximun Transmission Unit) de la interface, el ancho de banda (BW – bandwidth) en Kbytes, el retardo de la línea (DLY – delay) en microsegundos, la confiabilidad del enlace (RELY – reliability) y la carga de tráfico (LOAD). Veamos que significan estos parámetros:

- **MTU**: es el tamaño máximo de las tramas de datos que pueden ser recibidas o transmitidas por la interfaz.
- **BW**: en general, indica la velocidad de transferencia de datos de la interfaz. Algunos procesos que pueden ejecutar en el router utilizan este valor para ciertos cálculos como, por ejemplo, el protocolo de encaminamiento IGRP para determinar la mejor ruta hacia otra red. El valor de este parámetro se fija con el comando de interfaz `bandwith`.

- **DLY**: indica cuanto tiempo demora la señal en llegar a la interfaz desde el otro extremo del enlace.
- **RELY**: es un valor calculado por el router basándose en los errores de transmisión de datos detectados e indica cuan confiable o estable es la interfaz. El valor se presenta como una fracción de 255, donde 255 indica un 100% de confiabilidad.
- **LOAD**: es un valor, también calculado por el router, que mide el nivel de utilización o carga de tráfico que entra y sale por la interfaz. También se presenta como una fracción de 255, donde 255 indica un 100% de utilización.

Continuemos ahora con la línea 5; ésta indica que el formato de encapsulamiento de las tramas de datos a nivel de la capa de Enlace es ARPA, también conocido como Ethernet_II.

Finalmente, las líneas 11 a 24 muestran estadísticas de tráfico de la interfaz, que son recolectadas por el router en tiempo real.

A partir de la línea 25 y hasta la línea 45 se despliega información análoga a la anterior para la interfaz `serial 0/0` y lo mismo desde la línea 47 a la 69 para la interfaz `serial 0/1`.

Si se desea restringir la información desplegada por el comando `show interfaces` a una interfaz en particular, se puede poner el nombre de esa interfaz como parámetro del comando:

```
Router> show interface fastethernet 0/0
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is PQUICC_FEC, address is 0004.c14e.8067 (bia 0004.c14e.8067)
  Internet address is 17.0.0.1/8
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 252/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:08:40, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  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
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     9 packets output, 1098 bytes, 0 underruns
     9 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     9 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

show protocols

Este comando muestra información sobre los protocolos configurados y habilitados en el router.

```
Router> show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 17.0.0.1/8
Serial0/0 is up, line protocol is up
  Internet address is 200.10.10.5/30
Serial0/1 is up, line protocol is up
  Internet address is 200.10.30.5/30
```

Modo Privilegiado

Tal como mencionamos en el Capítulo 2, en el modo Privilegiado está disponible un conjunto mayor de comandos que los que encontramos en el modo Usuario. Puesto que varios de estos comandos permiten modificar algunos de los parámetros de funcionamiento del router, el acceso a este modo suele estar protegido por una contraseña.

Recordemos del Capítulo 2 que para acceder al modo Privilegiado se utiliza el comando `enable`; asumamos por el momento que no se ha establecido una contraseña de acceso:

```
Router> enable
Router#
```

Veamos la lista de comandos utilizando la facilidad de ayuda de la Interfaz de Línea de Comandos:

```
Router# ?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS subsystem
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
```

```
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
erase            Erase a filesystem
exit             Exit from the EXEC
help             Description of the interactive help system
isdn             Run an ISDN EXEC command on a BRI interface
lock             Lock the terminal
login            Log in as a particular user
logout           Exit from the EXEC
monitor          Monitoring different system events
more             Display the contents of a file
mrinfo           Request neighbor and version information from a multicast
                 router
mrm              IP Multicast Routing Monitor Test
mstat            Show statistics after multiple multicast traceroutes
mtrace           Trace reverse multicast path from destination to source
name-connection  Name an existing network connection
ncia             Start/Stop NCIA Server
no               Disable debugging functions
pad              Open a X.29 PAD connection
ping             Send echo messages
ppp              Start IETF Point-to-Point Protocol (PPP)
pwd              Display current working directory
reload           Halt and perform a cold restart
rename           Rename a file
restart          Restart Connection
resume           Resume an active network connection
rlogin           Open an rlogin connection
rsh              Execute a remote command
sdlc             Send SDLC test frames
send             Send a message to other tty lines
setup            Run the SETUP command facility
show             Show running system information
slip             Start Serial-line IP (SLIP)
ssh              Open a secure shell client connection
start-chat       Start a chat-script on a line
systat           Display information about terminal lines
telnet           Open a telnet connection
terminal         Set terminal line parameters
test             Test subsystems, memory, and interfaces
traceroute       Trace route to destination
tunnel           Open a tunnel connection
udptn            Open an udptn connection
undebug          Disable debugging functions (see also 'debug')
verify           Verify a file
voice            Voice Commands
where            List active connections
```

```
  write            Write running configuration to memory, network, or
                   terminal
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD
Router#
```

Como podemos ver, la lista de comandos es mas larga que la del modo Usuario y podría ser mas larga aún si habilitamos la "ayuda completa" con el comando `terminal full-help` que mencionamos anteriormente.

Analicemos ahora algunos comandos interesantes de la lista anterior y que son específicos del modo Privilegiado.

configure

Con este comando se accede al modo de Configuración Global y permite cambiar la configuración en ejecución del sistema desde la memoria o desde un host en el que se esté ejecutando un software de servidor TFTP.

```
Router# configure ?
  memory             Configure from NV memory
  network            Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal           Configure from the terminal
  <cr>
```

En el siguiente capítulo utilizaremos este comando, en particular `configure terminal` para comenzar a utilizar los primeros comandos de configuración.

copy

Este comando permite copiar archivos entre dispositivos del router como, por ejemplo, entre las memorias RAM y NVRAM, o entre el router y un host externo, como ser un servidor FTP.

```
Router# copy ?
  /erase          Erase destination file system.
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  null:           Copy from null: file system
  nvram:          Copy from nvram: file system
  rcp:            Copy from rcp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
  system:         Copy from system: file system
  tftp:           Copy from tftp: file system
  xmodem:         Copy from xmodem: file system
  ymodem:         Copy from ymodem: file system
```

En los capítulos 6 y 11 veremos cómo utilizar este comando y sus variantes para hacer copias de respaldo de los archivos de configuración de IOS y de los archivos de imagen del sistema operativo.

erase

Este comando permite borrar el contenido de las memorias FLASH y NVRAM.

```
Router# erase ?
  /all           Erase all files(in NVRAM)
  flash:         Filesystem to be erased
  nvram:         Filesystem to be erased
  startup-config Erase contents of configuration memory
```

Veamos como ejemplo el comando `erase flash` que elimina todo el contenido de la memoria Flash del router:

```
Router# erase flash
Erasing the flash filesystem will remove all files! Continue? [confirm] y
Erasing device … eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee… erased
Erase of flash: complete
Router#
```

reload

Este comando permite reinicializar el router sin tener que apagarlo. Es útil cuando se está administrando un router remoto y no se tiene acceso físico al mismo y no es posible utilizar el interruptor de encendido/apagado para reinicializarlo.

```
Router# reload ?
  LINE    Reason for reload
  at      Reload at a specific time/date
  cancel  Cancel pending reload
  in      Reload after a time interval
  <cr>
```

La ejecución sin parámetros de este comando provoca la reinicialización del router en forma inmediata:

```
Router# reload
Proceed with reload? [confirm] y
```

Existen dos variantes de este comando que permiten fijar el momento de la reinicialización para un tiempo posterior al ingreso del comando, es decir, permite calendarizar la reinicialización. Las formas generales de estas dos variantes son las siguientes:

```
Router# reload in hh:mm
```

```
Router# reload at hh:mm month day
```

La primera variante permite indicar que la reinicialización se lleve a cabo dentro de la cantidad de horas y minutos especificados en el comando. Por ejemplo, para que la reinicializacion se efectúe dentro de 1 hora y 15 minutos, el comando toma la siguiente forma:

```
Router# reload in 01:15
Router#
```

La segunda variante del comando permite fijar la fecha y hora exactas en que se quiere que se produzca la reinicialización. Por ejemplo, para que la reinicializacion se efectúe el día 6 de enero a las 10:00, el comando toma la siguiente forma

```
Router# reload at 10:00 Jan 06
Router#
```

La fecha y hora que se indique con esta variante del comando no puede estar mas allá de 24 días a partir de la fecha del reloj interno del router.

Para ver el estado de una reinicialización programada se utiliza el comando show reload:

```
Router# show reload
```

Para cancelar una reinicialización programada con el comando `reload`, se utiliza el comando de modo Privilegiado `reload cancel`:

```
Router# reload cancel
Router#
* * *
* * * - - - SHUTDOWN ABORTED - - - * * *
***
```

setup

Este comando permite acceder al modo de configuración Setup que describimos en el Capítulo 2 y que utilizaremos en detalle en el Capítulo 8 cuando configuremos un router usando las facilidades de este modo de configuración.

5. Primeros comandos de Configuración Global

Tal como hemos mencionado en el Capítulo 2, los comandos que se ejecuten en el modo de Configuración Global son tales que modifican el funcionamiento del router como un todo.

Estando en el modo Privilegiado, se accede al modo de Configuración Global con el comando `configure terminal`:

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

Nombre de host

Todos los routers basados en IOS deben tener un nombre de host. El nombre predeterminado es "Router", pero es buena práctica asignar al router un nombre más significativo. Para asignar o cambiar el nombre de host de un router se utiliza el comando `hostname`, que requiere como parámetro el nombre de host que se ha de asignar al router:

```
Router(config)# hostname RouterA
RouterA(config)#
```

Como podemos ver en el indicador del sistema ("prompt"), el comando toma efecto inmediatamente; en lugar de "Router" aparece el nombre de host que acabamos de asignar.

El nombre de host puede tener un largo máximo de 63 caracteres, debe comenzar con una letra y puede contener letras, dígitos y guión ("-").

Resolución de nombres

La resolución de nombres es el proceso por el cual, dado el nombre de un host, se obtiene su dirección IP. Hay dos formas de llevar a cabo este proceso de resolución; mediante el servicio de nombres de dominio (DNS) o por medio de una tabla estática de nombres de hosts.

Cuando en la línea de comandos, ya sea que estemos en el modo Usuario o en el Privilegiado, se escribe una palabra, IOS asume de forma predeterminada que se trata de un comando. Si el Intérprete de Comandos determina que no se trata de un comando válido, entonces asume que esa palabra es el nombre de un host con el cual se quiere establecer una sesión de Telnet y tratará de obtener su dirección IP consultando alguno de los servidores de DNS que hayan sido configurados.

Si no se ha configurado ningún servidor de DNS, IOS utilizará la dirección de broadcast 255.255.255.255, enviando la consulta DNS por todas sus interfaces en busca de ese tal servidor.

Puesto que los router bloquean los paquetes de broadcast, la resolución de nombres por este método de broadcast no se hará, a menos que haya un servidor de DNS conectado en la misma red que el router. En tal caso, IOS devolverá un mensaje de error:

```
Router# disavle
Translating "DISAVLE" ... domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

Para la resolución de nombres mediante DNS es necesario configurar el router con la dirección IP de uno o más servidores de DNS a los cuales consultar. IOS permite configurar hasta siete servidores de DNS y el comando de Configuración Global para ello es `ip name-server`:

```
Router# configure terminal
 Enter configuration commands, one per line. End with CNTL/Z
Router(config)# ip name-server 206.99.44.254
Router(config)# ip name-server 206.99.44.245
Router(config)# end
Router#
```

IOS coloca estas direcciones en la configuración en ejecución en el mismo orden en que son ingresadas y es en este orden en el cual el router los consulta para resolver un nombre.

Para anular cualquier comando ejecutado, la forma genérica de hacerlo es anteponiendo "`no`" al comando ejecutado. Por ejemplo, si se desea eliminar alguna de estas direcciones de la lista, debemos utilizar la forma "`no`" del mismo comando:

```
Router# configure terminal
 Enter configuration commands, one per line. End with CNTL/Z
Router(config)# no ip name-server 206.99.44.254
Router(config)# end
Router#
```

IOS permite deshabilitar la funcionalidad de resolución de nombres mediante el comando `no ip domain-lookup`:

```
Router# configure terminal
 Enter configuration commands, one per line. End with CNTL/Z
Router(config)# no ip domain-lookup
Router(config)# end
Router#
```

Para habilitar nuevamente esta funcionalidad se utiliza el mismo comando, pero sin el "`no`" delante:

```
Router# configure terminal
 Enter configuration commands, one per line. End with CNTL-Z
Router(config)# ip domain-lookup
Router(config)# end
```

```
Router#
```

La resolución de nombres también puede realizarse mediante una tabla local de hosts, que es simplemente una tabla que el router mantiene en memoria y que contiene los nombres de hosts a los que se suele acceder en forma mas frecuente y sus respectivas direcciones IP. Esta tabla debe construirse y mantenerse manualmente y para agregar entradas en la misma se utiliza el comando de Configuración Global `ip host`:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# ip host RouterB 200.10.10.6
Router(config)# end
Router#
```

Como vemos, el comando `ip host` requiere dos parámetros: el nombre de host y su dirección IP. IOS siempre utiliza esta tabla antes de usar DNS para tratar de resolver un nombre. Si el nombre buscado no figura en la tabla, IOS intentará resolver el nombre mediante la consulta a alguno de los servidores de DNS que tenga configurados.

Para eliminar de la tabla algún host, se utiliza la forma "`no`" del mismo comando:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# no ip host RouterB 200.10.10.6
Router(config)# end
Router#
```

IOS proporciona un comando para ver el contenido de la tabla de hosts y que puede ser ejecutado en el modo Privilegiado; se trata del comando `show hosts` que vimos en el capítulo anterior.

Banners

Los "banners" o carteles permiten a IOS enviar y desplegar mensajes informativos a la consola o terminal cuando el administrador inicia una sesión en el router.

Vamos a ver tres tipos de "banners" que pueden establecerse; éstos se denominan:

- MOTD (Message of the Day)
- Login
- Exec

El banner MOTD se envía a la terminal en el momento en que se activa una conexión en la misma y el banner Login también es enviado a la terminal cuando ésta se activa, pero se despliega después del MTOD en caso en que éste se haya establecido. Por su parte, el banner Exec se despliega en la terminal inmediatamente después que se haya iniciado la sesión de administración en el router.

Para crear cualquiera de estos tres banners se utiliza el comando de Configuración Global `banner`; su formato general es el siguiente:

```
Router(config)# banner  { exec | login | motd } delim mensaje delim
```

El comando `banner` debe incluir una de las tres opciones `exec`, `login` o `motd`; para crear los tres tipos de banners debemos ejecutar tres comandos `banner` separados, uno por vez, especificando en cada uno la opción requerida.

El texto del mensaje a desplegar debe escribirse entre caracteres delimitadores del texto. El delimitador a usar puede ser cualquier carácter que no esté incluido en el propio texto del mensaje a desplegar.

Veamos un ejemplo de creación del banner "mtod"; utilicemos como delimitador el carácter %:

```
Router(config)# banner mtod % Mantenimiento del sistema hoy a las 14 hs. %
```

Un mensaje de banner puede estar formado por varias líneas de texto. Para ello se escribe el comando hasta el primer delimitador y se presiona la tecla **Intro**. Luego se escribe cada línea del mensaje, presionando la tecla **Intro** al final de cada una y se termina el mensaje escribiendo el delimitador final y presionando nuevamente la tecla **Intro**.

```
Router(config)# banner mtod %
Enter TEXT message. End with the character '%'
Mantenimiento del sistema hoy a las 14 hs.
Volverá a estar disponible a las 14:15 aprox.
%
Router(config)#
```

Los banners Login y Exec se crean de la misma manera que el banner MTOD, especificando la palabra `login` o `exec` según el caso.

6. Los archivos de configuración de IOS

Archivos de Configuración

En los routers de Cisco encontramos dos archivos muy importantes para su funcionamiento: el archivo de configuración de arranque y el archivo de configuración en ejecución.

El archivo de configuración en ejecución, denominado RUNNING-CONFIG, contiene la configuración actual con la cual el router está ejecutando. Este archivo se mantiene en la memoria RAM y se modifica cada vez que se ejecuta un comando de Configuración.

Por su parte, el archivo de configuración de arranque, denominado STARTUP-CONFIG, contiene la configuración que IOS utiliza inicialmente cuando se enciende el router. Este archivo se almacena en la memoria NVRAM cuyo contenido, como ya vimos, no se borra cuando se apaga el router.

Durante el proceso normal de arranque del router, el sistema operativo IOS busca en la memoria NVRAM este archivo y lo carga en la memoria RAM con el nombre RUNNING-CONFIG.

El archivo RUNNING-CONFIG siempre existe en el router, mientras que el archivo STARTUP-CONFIG puede no existir, tal como ocurre, por ejemplo, en un router nuevo aún sin configurar.

Para ver el contenido del archivo RUNNING-CONFIG se utiliza el comando de modo Privilegiado `show running-config`:

```
Router# show running-config
  Building configuration ...
```

De modo similar, para ver el contenido del archivo STARTUP-CONFIG se utiliza el comando de modo Privilegiado `show startup-config`:

```
Router# show startup-config
```

Durante la operativa normal del router, estos dos archivos suelen ser iguales. Sin embargo, tal como mencionamos anteriormente, cuando se ejecuta algún comando de Configuración para cambiar el valor de algún parámetro de la configuración del router, este cambio se refleja en el archivo RUNNING-CONFIG. Si luego de estos cambios se apaga el router, los mismos se pierden puesto que el archivo RUNNING-CONFIG se mantiene en la memoria RAM.

Si se desea que los cambios realizados en la configuración se mantengan luego de reiniciar el router, debemos copiar el contenido del archivo RUNNING-CONFIG en el archivo STARTUP-CONFIG ya que es desde este archivo que IOS toma la configuración inicial cuando el router se enciende o se reinicializa. Para realizar esta copia se utiliza el comando de modo Privilegiado `copy running-config startup-config`:

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

IOS puede demorar uno o dos minutos en generar el archivo de configuración y salvarlo a la memoria NVRAM. Una vez que la configuración haya sido salvada, aparece el siguiente mensaje:

```
[OK]
Router#
```

En algunas circunstancias puede ocurrir que se hayan realizado varios cambios en la configuración en ejecución del router y que esos cambios hayan afectado su funcionamiento de modo que no funcione como debe y se desee volver a la configuración inicial. Hay, básicamente, tres formas de volver el router a su configuración previa.

La primera es deshacer manualmente cada uno de los cambios realizados, volviendo a ejecutar cada comando con el o los parámetros originales. Sin embargo, si se han realizado muchos cambios y los mismos no están adecuadamente documentados, puede resultar difícil recordarlos.

Una alternativa es apagar y reencender el router o, de manera equivalente, ejecutar el comando `reload` que provoca la reinicialización del mismo. En ambos casos, el sistema operativo IOS se vuelve a cargar a memoria y se vuelve a la configuración inicial almacenada en el archivo STARTUP-CONFIG. Este método, aunque efectivo, provoca que el router salga de funcionamiento por unos minutos, durante los cuales se pierde la conectividad con las otras redes a las cuales el router está conectado.

El tercer método, menos disruptivo que el anterior para volver a la configuración original del router, es copiar su configuración de arranque sobre la configuración en ejecución. Para esto, se utiliza el comando de modo Privilegiado `copy startup-config running-config`:

```
Router# copy startup-config running-config
```

Este comando, entonces, provoca que IOS sustituya la configuración en ejecución del router por su configuración original de arranque guardada en la memoria NVRAM.

Mencionamos anteriormente el comando de modo Privilegiado `reload,` el cual provoca la reinicialización del router. En el caso en que se haya modificado el archivo RUNNING-CONFIG pero no se hayan salvado los cambios al STARTUP-CONFIG, ante la ejecución de este comando, IOS pregunta si se desean salvar esos cambios antes de proceder a reinicializar el router:

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

Si le indicamos a IOS que no salve la configuración, procederá con la reinicialización y el router arrancará con la configuración de arranque anterior sin incluir los cambios que hayamos realizado.

Gestión de los archivos de configuración

Llevar a cabo la configuración de un router es una tarea compleja que requiere planificación, tiempo y esfuerzo y todo este tiempo y esfuerzo se refleja en la información de parámetros y comandos que luego aparecen en los archivos de configuración anteriores.

Hemos visto en el Capítulo 1 que un router contiene varios elementos de hardware los cuales no están libres de fallar en su funcionamiento, al igual que ocurre con la memoria RAM o el disco duro de una computadora personal.

Hemos mencionado anteriormente que el archivo STARTUP-CONFIG se mantiene almacenado en la memoria NVRAM del router y es desde esta memoria desde donde IOS lee este archivo para obtener los parámetros de configuración inicial con los cuales el router se pone en funcionamiento luego de haberlo reinicializado. Si por algún motivo esta memoria falla y su contenido queda ilegible, habremos perdido el archivo STARTUP-CONFIG y, en consecuencia, toda la configuración del router. Ante esta situación habría que reemplazar la memoria defectuosa y volver a configurar manualmente el router como si fuera la primera vez para retornarlo a su estado operacional anterior.

Si bien no es habitual que la memoria NVRAM falle, siempre es conveniente prever una situación de este tipo y disponer de una copia de respaldo de la configuración del router.

Cuando trabajamos en una computadora personal redactando, por ejemplo, un documento importante, una forma habitual de tener una copia de respaldo del mismo es copiando el archivo a un disquete.

Puesto que los routers no disponen de unidades de disquetes, no es posible hacer lo mismo con sus archivos de configuración. Sin embargo, IOS proporciona un mecanismo alternativo para generar y almacenar copias de respaldo de los archivos de configuración, que consiste en copiar esos archivos a otro host en la red, en particular a un servidor TFTP o a un servidor FTP.

Usando TFTP

TFTP, Trivial File Transfer Protocol, es una aplicación cliente/servidor estándar de TCP/IP que permite la transferencia de archivos desde y hacia otro host.

A diferencia de lo que ocurre si se utiliza FTP, que requiere de una cuenta de usuario y una contraseña para poder iniciar una sesión en el servidor, TFTP no requiere autenticación de usuario para transferir archivos.

El servidor TFTP debe estar corriendo en algún host de la red y el sistema operativo IOS proporciona comandos para copiar los archivos de configuración hacia o desde el servidor.

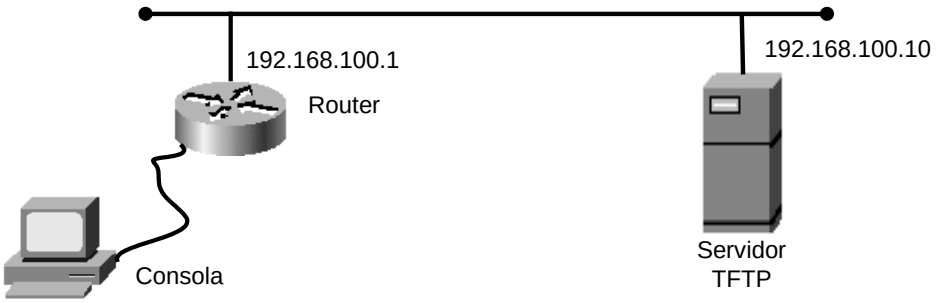


Fig. 6 - 1

Para copiar el archivo RUNNING-CONFIG a un servidor TFTP se utiliza el comando de modo Privilegiado `copy running-config tftp`:

```
Router# copy running-config ftfp
1 Remote host []? 197.168.100.10
2 Name of configuration file to write [Router-confg]? RouterA-conf.txt
3 Write file RouterA-conf.txt on host 197.168.100.10? [confirm] y
4 Building configuration ...

5 Writing RouterA-conf.txt  !!!!! [OK]
6 Router#
```

La ejecución del comando provoca un diálogo en el que deben especificarse una serie de parámetros requeridos por el mismo. En la línea 1 debe identificarse el host en el que está corriendo el servidor TFTP y al cual se va a copiar el archivo de configuración. Puede indicarse aquí la dirección IP del servidor o su nombre host siempre que su dirección pueda resolverse usando DNS o una tabla de hosts local. En nuestro ejemplo, el servidor TFTP está ejecutando en el host con dirección IP 197.168.100.10.

La línea 2 requiere indicar el nombre con el cual quiere almacenarse el archivo en el host remoto; IOS presenta entre paréntesis rectos el nombre predeterminado que asignará si no se especifica otro. Este nombre predeterminado consiste del nombre de host del router, seguido de "-confg". En el ejemplo de arriba cambiamos ese nombre predeterminado por RouterA-config.txt.

En la línea 3, IOS solicita la confirmación de la acción de copia a realizarse, ante lo cual respondemos presionando la tecla "`y`" (de "yes"). En la línea 4, IOS indica que está generando el archivo de configuración y en la línea 5 muestra el mensaje que indica que la copia se está realizando, presentando signos "!" a medida que se van transfiriendo bloques de texto, y terminar con un `[OK]` para indicar que la copia se realizó correctamente.

Una vez transferido al servidor TFTP, el archivo puede posteriormente copiarse a disquete desde el host, de modo de tener una copia de respaldo adicional en un medio magnético removible. El archivo generado en la transferencia es simplemente un archivo de texto cuyo contenido puede verse e incluso editarse con un procesador de textos.

Si en algún momento es necesario restaurar el archivo RUNNING-CONFIG al router, IOS proporciona un comando análogo al anterior que permite copiar el archivo de respaldo desde el

servidor TFTP a la memoria RAM del router. Este comando, de modo Privilegiado es `copy tftp startup-config`:

```
Router# copy tftp running-config
1 Host o network configuration file [host]? host
2 IP address of remote host [255.255.255.255]? 197.168.100.10
3 Name of configuration file [Router-confg]? RouterA-config.txt
4 Configure using RouterA-config.txt from 197.168.100.10? [confirm] y
5 Loading RouterA-config.txt from 197.168.100.10 (via Ethernet0): !!!
6 [OK]
7 Router#
```

La pregunta de la línea 1 puede ser respondida con las palabras clave "host" o "network". El archivo a transferir será un archivo "host" si contiene comandos que son específicos a un router individual y será un archivo "network" si contiene comandos comunes a varios routers. La respuesta que indiquemos se utiliza para generar los nombres predeterminados de los archivos. Un archivo host tiene como nombre predeterminado el nombre de host del router seguido de "-confg" y un archivo "network" tiene como nombre predeterminado "network-confg"

La pregunta de la línea 2 es para indicar la dirección IP del servidor TFTP desde el cual se hará la transferencia; alternativamente puede indicarse el nombre de host del servidor en caso en que esté activa la funcionalidad de resolución de nombres, ya sea mediante DNS o por medio de la tabla de hosts local.

En la línea 4 se solicita la confirmación de la acción a realizarse y en la línea 5 se muestra el estado del proceso de transferencia.

En relación con el archivo STARTUP-CONFIG, IOS proporciona comandos similares a los anteriores, tanto para transferir ese archivo hacia un servidor TFTP, como para realizar el proceso inverso de transferencia desde el servidor TFTP al router. En ambos casos, los diálogos que se presentan son iguales a los respectivos presentados por los comandos para copiar el archivo RUNNING-CONFIG; lo único que cambia es el nombre del archivo a transferir.

Así, para transferir el archivo STARTUP-CONFIG a un servidor TFTP se utiliza el comando `copy startup-config tftp`:

```
Router# copy startup-config tftp
```

De manera análoga, para transferir el archivo STARTUP-CONFIG a la memoria NVRAM del router, el comando a utilizar es `copy tftp startup-config`:

```
Router# copy tftp startup-config
```

Usando FTP

FTP, File Transfer Protocol, también es una aplicación cliente/servidor estándar de TCP/IP, tal vez mas conocida que TFTP, que permite la transferencia de archivos desde y hacia otro host y si se dispone de un tal servidor en la red, puede utilizarse como alternativa a TFTP para mantener almacenadas copias de respaldo de los archivos de configuración.

A diferencia de TFTP, para acceder al servidor FTP y poder transferir archivos, se requiere disponer de una cuenta de usuario y una contraseña en ese servidor para poder iniciar una sesión en él. Para poder copiar un archivo hacia el servidor FTP, la cuenta de usuario que se utilice debe tener permisos de escritura (write) en el servidor mientras que para poder transferir un archivo desde el servidor, esa cuenta de usuario debe tener al menos permisos de lectura (read).

Hay dos formas de especificar la cuenta de usuario y la contraseña a utilizar para establecer una sesión con el servidor FTP. Una de estas formas es indicando esos parámetros en el propio comando de copia y la otra es predefiniendo los valores de esos parámetros con los comandos de Configuración Global que veremos en un momento.

Para la primera forma, la sintaxis general del comando es la siguiente:

```
Router# copy archivo ftp://nombre_de_usuario@contraseña
```

donde *archivo* es el nombre del archivo a transferir, es decir, RUNNING-CONFIG o STARTUP-CONFIG.

Supongamos que el nombre de usuario a utilizar es *admin*, que su contraseña es *secreto* y que vamos a transferir el archivo RUNNING-CONFIG. El comando a ejecutar toma, entonces, la siguiente forma:

```
Router# copy running-config ftp://admin@secreto
```

La segunda forma para realizar la copia hacia un servidor FTP permite especificar la cuenta de usuario y la contraseña que el comando `copy` utilizará en forma predeterminada; esta alternativa evita tener que especificar esos parámetros cada vez que quiera copiar el archivo al servidor. IOS proporciona dos comandos de Configuración Global para configurar estos parámetros: `ip username` para configurar el nombre de usuario e `ip password` para especificar la contraseña. Supongamos nuevamente que el nombre de usuario a utilizar es *admin* y que su contraseña es *secreto*:

```
Router# configure terminal
  Enter configuration commands, one per line. End with CNTL/Z
Router(config)# ip username admin
Router(config)# ip password secreto
Router(config)# <CNTL-Z>
Router#
```

Una vez definidos estos parámetros, el comando de copia se simplifica:

```
Router# copy running-config ftp
```

La práctica común entre los administradores es utilizar TFTP ya que el programa servidor es pequeño y puede ejecutarse en cualquier portable (“notebook”) o PC común.

7. Contraseñas

El uso de contraseñas permite proteger al router de accesos no autorizados. Vamos a ver a continuación cómo se establecen las contraseñas que permiten controlar el acceso a los modos Usuario y Privilegiado.

Estas no son las únicas contraseñas que IOS permite establecer, pero sin dudas, son las primeras que deberían configurarse para controlar el acceso inicial al router.

Contraseñas para el modo Usuario

Tal como vimos en el Capítulo 3, hay esencialmente tres formas de acceder al router: a través del puerto CONSOLA, a través del puerto AUX y usando la aplicación Telnet.

Las conexiones al router a través de las opciones anteriores se realizan por medio de lo que Cisco denomina "líneas" y la configuración de sus parámetros se realiza accediendo a un nuevo submodo de configuración denominado submodo de Configuración de Línea. Estando en el modo de Configuración Global, para acceder al submodo de Configuración de Línea se utiliza el comando `line`:

```
RouterA> enable
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# line ?
  <0-10>   First Line number
  aux      Auxiliary line
  console  Primary terminal line
  tty      Terminal controller
  vty      Virtual terminal
```

Puerto Consola

Para el comando `line` anterior, la palabra clave `console` permite especificar que es esta línea la que se va a configurar y, puesto que el router tiene un solo puerto de Consola, su número de identificación es 0:

```
RouterA(config)# line console 0
RouterA(config-line)#
```

Como vemos, el indicador del sistema ha cambiado a `(config-line)#` para indicar que hemos ingresado al submodo de Configuración de Línea. Los comandos disponibles en este submodo pueden verse utilizando la facilidad de ayuda:

```
RouterA(config-line)# ?
```

Para establecer la contraseña de acceso se utiliza el comando `password` y para provocar que IOS verifique la contraseña antes de permitir el acceso se utiliza el comando `login`:

```
RouterA(config-line)# password cisco
```

```
RouterA(config-line)# login
```

Recordemos que para salir de este submodo y volver al modo de Configuración Global se utiliza el comando `exit:`

```
RouterA(config)# exit
RouterA(config)#
```

Para regresar al modo Privilegiado desde el modo de Configuración Global, volvemos a ejecutar el comando `exit`:

```
RouterA(config-line)# exit
RouterA#
*Mar  17 00:01:43.183: %SYS-5-CONFIG_I: Configured from console by console
```

Puerto AUX

La configuración de la contraseña de acceso por el puerto Auxiliar es completamente análoga a la del puerto Consola. Puesto que en caso en que el router tiene puerto Auxiliar, éste será único, su número de identificación es 0:

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# line aux 0
RouterA(config-line)# password cisco
RouterA(config-line)# login
```

Para salir de este submodo y volver directamente al modo de Privilegiado utilizamos el comando `end`.

```
RouterA(config-line)# end
RouterA#
*Mar  1 00:03:17.113: %SYS-5-CONFIG_I: Configured from console by console
```

Telnet

El acceso al router mediante Telnet se realiza por medio de lo que se conocen como "puertos virtuales", en contraposición con los puertos "reales" como lo son CONSOLE y AUX. Todos los routers de Cisco tienen definidos en forma predeterminada cinco puertos virtuales, denominados VTY y numerados de 0 a 4. Si bien es posible establecer una contraseña diferente para cada uno de ellos, lo habitual es definir una sola contraseña común para todos. La razón para esto es que cuando se realiza una conexión vía Telnet, IOS asigna una de las VTYs disponibles, pero no es posible saber, de antemano, cual de ellas será. En consecuencia, al no saberse cual VTY se va a utilizar, tampoco es posible saber cual contraseña ha de utilizarse para el acceso.

Un detalle importante respecto a las contraseñas de las VTYs es que si las mismas no están configuradas, no es posible el acceso al router usando Telnet. Dicho de otro modo, si las terminales VTY no están protegidas por contraseñas, el acceso al router usando Telnet está deshabilitado en forma predeterminada.

El procedimiento para establecer las contraseñas de las VTYs es similar al empleado para las contraseñas de los puertos CONSOLA y AUX:

```
RouterA(config)# line vty 0 4
RouterA(config-line)# password cisco
RouterA(config-line)# login
```

Para permitir conexiones Telnet sin requerir contraseña de acceso (algo no recomendado) puede utilizarse el comando `no login`:

```
RouterA(config)# line vty 0 4
RouterA(config-line)# no login
```

Contraseñas en secreto

Las contraseñas vistas hasta ahora, esto es, la de los puertos de Consola y Auxiliar y las de las terminales VTY se guardan en el archivo `running-config` en la misma forma en que fueron escritas, es decir, en forma totalmente legible. Si un usuario puede ejecutar el comando `enable` y acceder al modo Privilegiado, podrá conocer estas contraseñas viendo el contenido de ese archivo y leyendo las respectivas contraseñas:

```
RouterA> enable
RouterA# show running-config
 1 Building configuration...

 2 Current configuration : 724 bytes
 3 !
 4 version 12.2
 5 service timestamps debug datetime msec
 6 service timestamps log datetime msec
 7 no service password-encryption
 8 !
 9 hostname RouterA
10 !
11 memory-size iomem 15
12 ip subnet-zero
13 !
14 ip audit notify log
15 ip audit po max-events 100
16 !
17 voice call carrier capacity active
18 !
19 interface FastEthernet0/0
20  no ip address
```

```
21  shutdown
22  speed auto
23 !
24 interface Serial0/0
25  no ip address
26  shutdown
27  no fair-queue
28 !
29 interface Serial0/1
30  no ip address
31 shutdown
32 !
33 ip classless
34 no ip http server
35 !
36 call rsvp-sync
37 !
38 voice-port 1/0
38 !
40 voice-port 1/1
41 !
42 voice-port 2/0
43 !
44 voice-port 2/1
45 !
46 dial-peer cor custom
47 !
48 line con 0
49  password cisco
50  login
51 line aux 0
52  password cisco
53  login
54 line vty 0 4
55  login
56 !
57 end
```

Como podemos ver en la salida anterior, en las líneas 49 y 52 aparecen, en forma completamente legibles, las contraseñas que hemos establecido anteriormente para las líneas consola y auxiliar. Para que en el archivo `running-config` las contraseñas aparezcan ilegibles (encriptadas) puede configurarse a IOS para que lo haga. El servicio de encriptación de contraseñas se habilita con el comando de Configuración Global `service password-encription`:

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# service password-encryption
RouterA(config)# end
```

Si vemos ahora el contenido del archivo `running-config`, las contraseñas en las líneas 49 y 52 se muestran encriptadas:

```
RouterA# show running-config
 1 Building configuration...

 2 Current configuration : 730 bytes
 3 !
 4 version 12.2
 5 service timestamps debug datetime msec
 6 service timestamps log datetime msec
 7 service password-encryption
 8 !
 9 hostname RouterA
10 !
11 memory-size iomem 15
12 ip subnet-zero
13 !
14 ip audit notify log
15 ip audit po max-events 100
16 !
17 voice call carrier capacity active
18 !
19 interface FastEthernet0/0
20  no ip address
21  shutdown
22  speed auto
23 !
24 interface Serial0/0
25  no ip address
26  shutdown
27  no fair-queue
28 !
29 interface Serial0/1
30  no ip address
31  shutdown
32 !
33 ip classless
34 no ip http server
35 !
36 call rsvp-sync
37 !
38 voice-port 1/0
```

```
39 !
40 voice-port 1/1
41 !
42 voice-port 2/0
43 !
44 voice-port 2/1
45 !
46 dial-peer con custom
47 !
48 line con 0
49  password 7 104D000A0618
50  login
51 line aux 0
52  password 7 104D000A0618
53 line vty 0 4
54  login
55 !
56 end
```

Contraseñas para el modo Privilegiado

Ya hemos visto que cualquier usuario que acceda al modo Privilegiado puede hacer lo que desee con la configuración del router como, por ejemplo, reiniciarlo, deshabilitar una interfaz e incluso cambiar las contraseñas de acceso que se hayan establecido. Es por esta razón que es conveniente proteger el acceso al modo Privilegiado, lo cual también se hace mediante el establecimiento de contraseñas.

Dos comandos del modo de Configuración Global que permiten establecer contraseñas de acceso a este modo son `enable password` y `enable secret`:

```
RouterA(config)# enable password cisco

RouterA(config)# enable secret ort
```

La diferencia entre uno y otro comando es que la contraseña que se establece con `enable password` se guarda en el archivo `running-config` tal cual fue escrita, es decir, sin encriptar, a menos que se haya habilitado el servicio `service password-encription`. Sin embargo, aún cuando este servicio no esté habilitado, la contraseña establecida con `enable secret` sí se guarda encriptada.

En la siguiente salida vemos en la línea 11 que la contraseña establecida con el comando `enable secret` se despliega en forma completamente irreconocible. Por su parte, la contraseña establecida con el comando `enable password` se muestra, en la línea 12, tal cual fue ingresada.

```
RouterA# show running-config
 1 Building configuration...

 2 Current configuration : 802 bytes
 3 !
```

```
 4 version 12.2
 5 service timestamps debug datetime msec
 6 service timestamps log datetime msec
 7 no service password-encryption
 8 !
 9 hostname RouterA
10 !
11 enable secret 5 $1$5bij$XOpWIpVbz9dd0L4zOE1kp0
12 enable password cisco
13 !
14 memory-size iomem 15
15 ip subnet-zero
16 !
17 ip audit notify log
18 ip audit po max-events 100
19
20 !
21 voice call carrier capacity active
22 !
23 interface FastEthernet0/0
24  no ip address
25  shutdown
26  speed auto
27 !
28 interface Serial0/0
29  no ip address
30  shutdown
31  no fair-queue
32 !
33 interface Serial0/1
34  no ip address
35  shutdown
36 !
37 ip classless
39 no ip http server
40 !
41 call rsvp-sync
42 !
43 voice-port 1/0
44 !
45 voice-port 1/1
46 !
47 voice-port 2/0
48 !
49 voice-port 2/1
50 !
51 dial-peer con custom
52 !
```

```
53 line con 0
54  password 7 104D000A0618
55  login
56 line aux 0
57  password 7 104D000A0618
58 line vty 0 4
59  login
60 !
61 end
```

Un aspecto importante en relación con estas dos contraseñas es que si se ha establecido una con `enable secret`, es ésta la que IOS utiliza para controlar el acceso al modo Privilegiado en lugar de la establecida con `enable password`.

En caso de establecer ambas contraseñas, las mismas deben ser diferentes entre si, puesto que si son iguales, la "`enable secret`" ya no sería secreta dado que la "`enable password`" se muestra tal cual en el archivo `running-config`. Si queremos intentar que sean iguales, IOS nos mostrará un mensaje al respecto:

```
RouterA(config)# enable secret cisco
RouterA(config)# enable password cisco
The enable password you have choosen is the same as your enable secret. This
is not recommended. Re-enter your enable password.
RouterA(config)#
```

8. Configuración IP en las interfaces de red

En este capítulo vamos a abordar los aspectos relativos a la configuración de las interfaces de red del router para funcionar en un ambiente de interredes basado en TCP/IP.

Vamos a tomar como base para nuestro trabajo una configuración de interredes como la que se muestra en la figura 8-1:

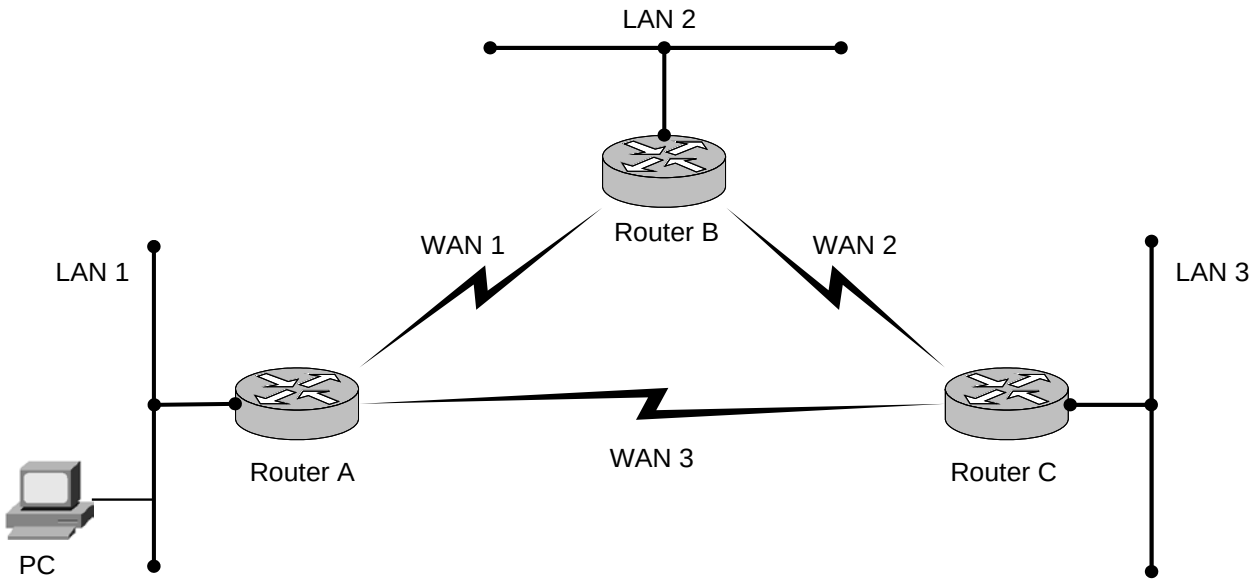


Fig. 8 - 1

En nuestra configuración de trabajo tenemos tres redes de área local, identificadas como LAN1, LAN2 y LAN3 y tres enlaces WAN identificados como WAN1, WAN2 y WAN3. Los tres routers en nuestra interred tiene las mismas características físicas; cada uno tiene una interfaz LAN tipo FastEthernet y dos interfaces WAN tipo Serial. La interfaz LAN conecta cada router a su red local y las interfaces WAN permiten interconectar los router entre sí.

Esta topología en forma de anillo tiene la particularidad de que, desde cada red LAN hay dos caminos posibles para llegar hasta cada una de las otras redes locales. Por ejemplo, desde la red local LAN1 se puede llegar hasta la red LAN3 directamente por el enlace WAN3 o indirectamente por los enlaces WAN1 y WAN2, pasando por el router B. La configuración de IP en las interfaces de los tres router en este capítulo nos va a preparar el camino para, en el capítulo siguiente, configurar los protocolos de encaminamiento dinámico y ver cómo, ante la falla de uno de los enlaces, se actualizan en forma dinámica las tablas de encaminamiento en cada router y la conectividad entre las redes LAN se mantiene.

Las redes LAN

Vamos a considerar que las redes LAN de nuestra interred son redes del tipo IEEE 802.3. Si bien en el diagrama están representadas por segmentos, en una instalación real seguramente

tendrán una topología de estrella centrada en un HUB o en un SWITCH. En consecuencia, la interfaz FastEthernet de cada router estará físicamente conectada a uno de los puertos de su respectivo hub o switch, bien directamente o, lo que es mas habitual, indirectamente a través de una conexión a la "patchera" de la infraestructura física del respectivo sitio.

Esquemáticamente, podemos representar esta conexión local de la siguiente manera:

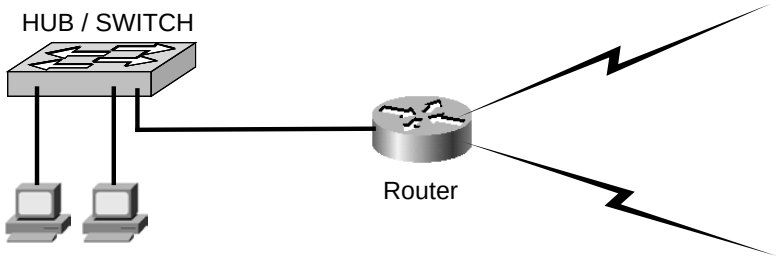


Fig. 8 - 2

Los enlaces WAN

Para los enlaces WAN de nuestra interred vamos a considerar, por el momento, que los mismos son enlaces punto a punto, es decir, cada enlace conecta exactamente dos dispositivos, uno en cada extremo del enlace. Un diagrama de un enlace de este tipo se muestra en la figura siguiente:

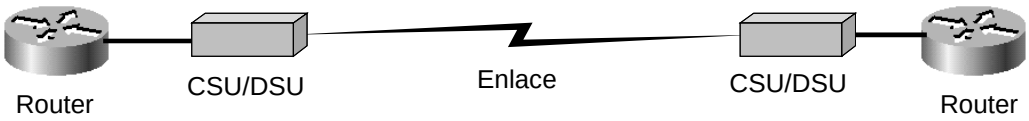


Fig. 8 - 3

En la figura, el "enlace" es habitualmente provisto por un Proveedor de Servicios o Compañía Telefónica, junto con los equipos de telecomunicaciones, denominados genéricamente CSU/DSU, Channel Service Unit/Data Service Unit. Estos equipos realizan la conversión de formatos de tramas y señales de comunicaciones entre el puerto en el router y el enlace WAN y viceversa. El componente CSU recibe y transmite las señales desde y hacia el enlace, mientras que el componente DSU maneja el control de la línea y los formatos apropiados de las tramas de datos.

El router de cada sitio, a su vez, está conectado a su respectivo CSU/DSU. El tipo de cable que se utiliza para esta conexión local depende del tipo de CSU/DSU que, a su vez, depende del tipo de enlace WAN que se tenga.

Uno de los extremos de este cable es un conector DB60 (60 pines) que se conecta a la interface Serial sincrónica del router, por ejemplo a la Serial 0. El otro extremo del cable tiene un conector del tipo V.35 que se conecta al puerto correspondiente del CSU/DSU.

La mayoría de los dispositivos utilizados para el procesamiento de datos tienen un alcance limitado en cuanto a la distancia a la que pueden transmitir datos. Ejemplos de estos

dispositivos son las terminales, las computadoras personales y también los routers. Para transmitir datos a distancias mayores, estos equipos requieren el uso de dispositivos diseñados para este propósito específico. Ejemplos de estos dispositivos son los modems y también los CSU/DSU que hemos mencionado anteriormente.

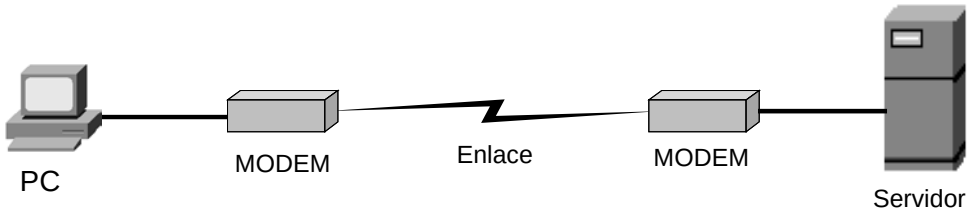


Fig. 8 - 4

En términos generales, un dispositivo de procesamiento de datos recibe el nombre genérico de Equipo Terminal de Datos o DTE, Data Terminal Equipment y un dispositivo de transmisión de datos recibe el nombre de Equipo de Terminación del Circuito de Datos o DCE, Data Circuit-terminating Equipment. Con estas definiciones, entonces, podemos decir que un router es típicamente un dispositivo DTE, mientras que el CSU/DSU es un DCE.

En un ambiente de laboratorio puede no disponese de un enlace WAN "verdadero" ni de dispositivos del tipo CSU/DSU. Sin embargo, es posible simular un enlace WAN punto a punto utilizando dos cables especiales, similares a los de la figura 8-4. Estos cables se denominan "cable DCE" y "cable DTE". Ambos tipos de cables tienen en uno de sus extremos un conector del tipo DB60 mientras que en el otro extremo el cable DTE tiene un conector V.35 "macho" y el cable DCE un conector V.35 "hembra".

Estos cables están formados por una serie de conductores internos, uno de los cuales se utiliza para la transmisión de datos (Tx) y el otro para la recepción de datos (Rx). La diferencia entre un cable DTE y uno DCE es, básicamente, que el cable DTE es un cable "directo" mientras que el cable DCE es un cable "cruzado" en el que las posiciones de los pines correspondientes a los conductores de transmisión y de recepción están intercambiadas:

De este modo, cuando el router con el cable DCE envía datos por el pin Tx de transmisión, la señal eléctrica de ese pin entra por el pin Rx de recepción del otro router y lo mismo ocurre cuando el que transmite es el router del otro extremo.

Para establecer la conexión física directa entre los dos routers, los extremos DB60 de cada cable se conectan a la interfaz Serial de su router y los extremos V.35 se conectan entre sí para simular el enlace punto a punto entre ambos routers. Este tipo de conexión generalmente se denomina "back-to-back". En la figura siguiente se muestra esta configuración:

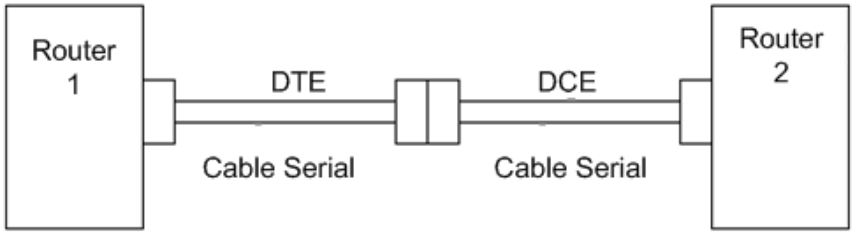


Fig. 8 - 5

Puesto que en esta configuración no tenemos un CSU/DSU que provea el sincronismo para el enlace, será necesario configurar a uno de los routers del enlace para que lo provea. Más específicamente, lo que deberemos configurar para este propósito es la interface serial utilizada en el enlace. Para ello utilizaremos en comando de submodo de Configuración de Interfaz `clock rate`:

```
Router(config-if)# clock rate ?
   Speed (bits per second)
1200
2400
4800
9600
19200
38400
[texto omitido]
<1200 – 4000000> Choose clockrate from list above
```

Este comando solo es aplicable a la interfaz que actúe como DCE. Si quisiéramos aplicarlo, por ejemplo, a una interfaz FastEthernet obtendríamos un mensaje de error:

```
Router(config)# interface fastethernet 0
Router(config-if)# clock rate 64000
%Error: This command applies only to DCE interfaces
Router(config-if)#
```

En nuestra interred vamos a considerar que el router A proporciona el sincronismo para los enlaces WAN1 y WAN2 y que el router B lo proporciona para el enlace WAN3. Resumamos esto en la siguiente tabla:

Un extremo ...				**El otro extremo ...**		
Router	**Interface**	**Rol**	**Enlace**	**Rol**	**Interface**	**Router**
A	Serial 0/0	DCE	WAN1	DTE	Serial 0/0	B
A	Serial 0/1	DCE	WAN3	DTE	Serial 0/1	C
B	Serial 0/1	DCE	WAN2	DTE	Serial 0/0	C

La figura 8-6 muestra la misma interred de la figura 8-1 con los nombres de las interfaces de red:

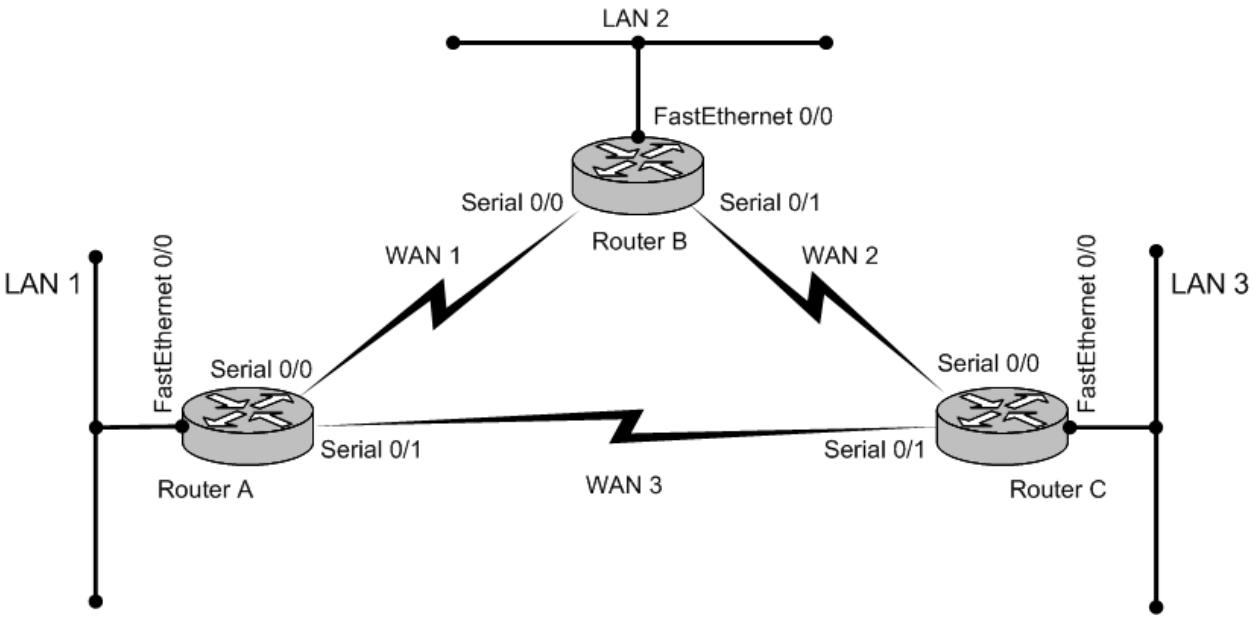


Fig. 8 - 6

Esquema de direccionamiento

Antes de comenzar con las tareas de configuración de cada interfaz debemos definir un esquema de direccionamiento para cada una de las seis redes de nuestra interred. Para las redes LAN 1, LAN 2 y LAN 3 vamos a seleccionar direcciones de clases A, B y C respectivamente, de acuerdo al siguiente esquema:

Red	Dirección	Máscara de subred
LAN1	17.0.0.0	255.0.0.0
LAN2	177.16.0.0	255.255.0.0
LAN3	197.168.100.0	255.255.255.0

En cuanto a los enlaces WAN, asignemos para ellos direcciones IP públicas:

Red	Dirección	Máscara de subred
WAN1	200.10.10.0	255.255.255.252
WAN2	200.10.20.0	255.255.255.252
WAN3	200.10.30.0	255.255.255.252

Definamos ahora las direcciones IP específicas a utilizar en las interfaces de cada router. Comencemos por definir las direcciones IP para las interfaces del router A de nuestra interred. Este router tiene una de sus interfaces, la `FastEthernet`, conectada a la red local LAN1, de modo que esa interfaz deberá tener una dirección IP en el rango definido para esa red. Una práctica habitual al definir una dirección IP para una interfaz de un router es asignarle, cuando sea posible, una dirección que sea la primera o la última del rango; esto facilita posteriormente

recordar cual es su dirección. Definamos, entonces, para la interfaz `FastEthernet` la dirección IP 17.0.0.1, con máscara de subred 255.0.0.0.

En relación con las interfaces de tipo Serial, una de ellas, la `serial 0/0` conecta el router al enlace WAN1 y la otra, la `serial 0/1`, al enlace WAN3, de modo que cada interfaz deberá tener una dirección IP en el rango respectivo definido para cada enlace. Definamos entonces las siguientes direcciones: para la interfaz `serial 0/0` la dirección 200.10.10.5 y para la `serial 0/1` la dirección 200.20.30.5, ambas con máscara de subred 255.255.255.252.

Resumamos entonces, en la siguiente tabla, las definiciones anteriores para el Router A:

Interfaz	Enlace	Dirección	Máscara de subred
FastEthernet	LAN1	17.0.0.1	255.0.0.0
Serial 0/0	WAN1	200.10.10.5	255.255.255.252
Serial 0/1	WAN3	200.10.30.5	255.255.255.252

Un razonamiento similar nos lleva a definir las direcciones IP para las interfaces de los otros dos router.

Para el **router B** tenemos:

Interfaz	Enlace	Dirección	Máscara de subred
FastEthernet	LAN2	177.16.0.1	255.255.0.0
Serial 0/0	WAN1	200.10.10.6	255.255.255.252
Serial 0/1	WAN2	200.10.20.5	255.255.255.252

Y para el **router C** definamos las siguientes direcciones:

Interfaz	Enlace	Dirección	Máscara de subred
FastEthernet	LAN2	197.168.100.1	255.255.255.0
Serial 0/0	WAN2	200.10.20.6	255.255.255.252
Serial 0/1	WAN3	200.10.30.6	255.255.255.252

Configuración del router A

Con nuestro esquema de direccionamiento definido, podemos comenzar ahora con las tareas de configurar las interfaces del router A. Para ello debemos conectarnos al router a través de su puerto de consola, tal como fue descrito en el Capítulo 3.

Configuración de la interfaz FastEthernet

Sigamos ahora la secuencia de comandos, comenzando en el modo Usuario, hasta llegar al punto en que podamos ingresar los comandos de configuración de IP en esta interfaz. En resumen, los pasos a seguir son: pasar al modo Privilegiado, luego ingresar al modo de Configuración Global y finalmente acceder al submodo de Configuración de la Interfaz

FastEthernet. Puesto que nuestro router A tiene una sola interfaz FastEthernet, su número de identificación será el 0.

En el modo Usuario, el indicador del sistema es:

```
Router>
```

Ingresemos al modo Privilegiado con el comando `enable` e ingresemos la contraseña de acceso si la misma está configurada:

```
Router> enable
Password: <...>
Router#
```

Estando en el modo Privilegiado podemos ejecutar el comando de IOS que nos permite ver el estado actual de la interfaz `FastEthernet 0/0`; este comando es: `show interface fastethernet 0/0`:

```
Router# show interface fastethernet 0/0
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is PQUICC_FEC, address is 0004.c14e.8067 (bia 0004.c14e.8067)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:52, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     16 packets output, 5982 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

La salida anterior nos indica que la interfaz está deshabilitada (“administratively down”) y que no tiene asignada una dirección IP.

Ingresemos ahora al modo de Configuración Global; el comando para ello es `configure terminal`:

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

Observe que el indicador del sistema ha cambiado, para indicar ahora que estamos en el modo de Configuración Global.

En este momento podemos asignar a nuestro router un nombre de host, de modo de poder referirnos a él de manera más fácil en el futuro. El comando para ello es `hostname` y el nombre que vamos a asignarle a este router es, simplemente, "RouterA":

```
Router(config)# hostname RouterA
RouterA(config)#
```

Observe que el indicador del sistema ha cambiado nuevamente, para reflejar ahora el nombre de host que acabamos de asignar al router.

Tal como vimos en el Capítulo 2, para poder configurar una interfaz de red en el router, debemos acceder al submodo de Configuración de Interfaces, indicando cual es la interfaz que vamos a configurar. El comando para ello es `interface fastethernet 0/0`:

```
RouterA(config)# interface fastethernet 0/0
RouterA(config-if)#
```

Observe que el indicador del sistema ha cambiado otra vez, ahora para indicar que estamos en el submodo de Configuración de Interface.

Veamos ahora cuales son los comandos de IOS disponibles en este submodo; utilicemos para ello la facilidad de ayuda que ofrece la Interfaz de Línea de Comandos:

```
RouterA(config-if)# ?
Interface configuration commands:
  access-expression   Build a bridge boolean access expression
  arp                 Set arp type (arpa, probe, snap) or timeout
  backup              Modify dial-backup parameters
  bandwidth           Set bandwidth informational parameter
  bridge-group        Transparent bridging interface parameters
  cdp                 CDP interface subcommands
  cmns                OSI CMNS
  custom-queue-list   Assign a custom queue list to an interface
  delay               Specify interface throughput delay
  description         Interface specific description
  exit                Exit from interface configuration mode
  fair-queue          Enable Fair Queuing on an Interface
  frame-relay         Set frame relay parameters
  help                Description of the interactive help system
  hold-queue          Set hold queue depth
```

```
  ip                  Interface Internet Protocol config commands
  keepalive           Enable keepalive
  llc2                LLC2 Interface Subcommands
  load-interval       Specify interval for load calculation for an interface
  loopback            Configure internal loopback on an interface
  mac-address         Manually set interface MAC address
  mtu                 Set the interface Maximum Transmission Unit (MTU)
  no                  Negate a command or set its defaults
  priority-group      Assign a priority group to an interface
  shutdown            Shutdown the selected interface
  snapshot            Configure snapshot support on the interface
  snmp                Modify SNMP interface parameters
  standby             Hot standby interface subcommands
  transmit-interface  Assign a transmit interface to a receive-only interface
  tx-queue-limit      Configure card level transmit queue limit
```

De la lista anterior vemos que el comando `ip` está relacionado con la configuración de ese protocolo en la interfaz. Veamos la ayuda nuevamente:

```
RouterA(config-if)# ip ?
Interface IP configuration subcommands:
  access-group        Specify access control for packets
  accounting          Enable IP accounting on this interface
  address             Set the IP address of an interface
  bandwidth-percent   Set EIGRP bandwidth limit
  broadcast-address   Set the broadcast address of an interface
  directed-broadcast  Enable forwarding of directed broadcasts
  gdp                 Gateway Discovery Protocol
  hello-interval      Configures IP-EIGRP hello interval
  helper-address      Specify a destination address for UDP broadcasts
  hold-time           Configures IP-EIGRP hold time
  irdp                ICMP Router Discovery Protocol
  mask-reply          Enable sending ICMP Mask Reply messages
  mobile              Mobile Host Protocol
  mtu                 Set IP Maximum Transmission Unit
  probe               Enable HP Probe support
  proxy-arp           Enable proxy ARP
  rarp-server         Enable RARP server for static arp entries
  redirects           Enable sending ICMP Redirect messages
  rip                 Router Information Protocol
  route-cache         Enable fast-switching cache for outgoing packets
  security            DDN IP Security Option
  split-horizon       Perform split horizon
  summary-address     Perform address summarization
  tcp                 TCP header compression parameters
  unnumbered          Enable IP processing without an explicit address
  unreachables        Enable sending ICMP Unreachable messages
```

El comando para configurar la dirección IP de la interfaz es, entonces, `ip address`; veamos que nos dice la ayuda acerca de cómo usar este comando:

```
RouterA(config-if)# ip address ?
  A.B.C.D  IP address
  dhcp     IP Address negotiated via DHCP
  pool     IP Address autoconfigured from a local DHCP pool
```

La ayuda nos dice que, como parámetro, debemos especificar la dirección IP a asignar en notación decimal con puntos:

```
RouterA(config-if)# ip address 17.0.0.1
% Incomplete command
```

El mensaje de error nos indica que el comando está incompleto; veamos qué nos está faltando indicar:

```
RouterA(config-if)# ip address 17.0.0.1 ?
  A.B.C.D   IP subnet mask
RouterA(config-if) ip address 17.0.0.1
```

Indiquemos entonces la máscara de subred:

```
RouterA(config-if)# ip address 17.0.0.1 255.0.0.0
RouterA(config-if)# exit
RouterA(config)# exit
RouterA#
```

Bien; la interfaz `fastethernet 0/0` ha quedado configurada con su dirección IP y su correspondiente máscara de subred. Veamos ahora el estado de la interfaz:

```
RouterA# show interface fastethernet 0/0
1 FastEthernet0/0 is administratively down, line protocol is down
2  Hardware is PQUICC_FEC, address is 0004.c14e.8067 (bia 0004.c14e.8067)
3  Internet address is 17.0.0.1/8
[texto omitido]
```

En la línea 3 vemos la dirección IP configurada en el siguiente formato: 17.0.0.1/8. El "/8" indica que la máscara de subred tiene ocho 1s; es la forma abreviada que utiliza IOS para indicar que la máscara de subred es, en este caso, 255.0.0.0.

En la línea 1 vemos que el estado de la interfaz es "administratively down". En forma predeterminada, las interfaces del router vienen deshabilitadas. Esto significa que, aunque estén configuradas, no procesarán ningún paquete de datos que reciban ni enviarán ningún paquete de datos hacia en otro extremo del enlace. El comando de submodo de Configuración de Interfaz para habilitar una interfaz es `no shutdown`, es decir, la negación del comando `shutdown`, el cual lo que hace es, precisamente, deshabilitar una interfaz.

```
Router# configure terminal
  Enter configuration commands, one per line. End with CNTL/Z
```

```
RouterA(config)# interface fastethernet 0/0
RouterA(config-if)# no shutdown
```

Antes de finalizar la configuración de la interfaz podemos agregar una descripción a la misma para documentarla; el comando para ello es `description`:

```
RouterA(config-if)# description Conexión a la LAN1
RouterA(config-if)# exit
RouterA(config)# exit
RouterA#
```

Luego de ejecutado el último comando `exit` para salir del modo de Configuración Global, veremos en la pantalla los siguientes mensajes de IOS:

```
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

Veamos ahora, nuevamente, el estado de la interfaz:

```
RouterA# show interface fastethernet 0/0
1.FastEthernet0/0 is up, line protocol is up
2.  Hardware is PQUICC_FEC, address is 0004.c14e.8067 (bia 0004.c14e.8067)
3.  Internet address is 17.0.0.1/8
[texto omitido]
```

Bien; la interfaz `fastethernet 0/0` está configurada con su dirección IP y está habilitada; en la línea 1 vemos ahora que el estado de la interfaz es "up". Recordemos que esta configuración está contenida en el archivo `RUNNING-CONFIG`; si queremos preservarla aún cuando se apague y reencienda el router debemos salvarla al archivo `STARTUP-CONFIG`:

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

Configuración de las interfaces Seriales

Hay dos parámetros que son particularmente importantes para la configuración de una interfaz Serial: el "ancho de banda" y el "encapsulamiento".

Ancho de banda

Los routers de Cisco vienen, de fábrica, con una configuración predeterminada de 1544 Mbps para el ancho de banda o "bandwidth" de sus interfaces seriales. El valor de este parámetro, en realidad, no tiene mucho que ver con la velocidad real a la que se transfieren datos por la interfaz. El valor de ancho de banda de un enlace serial es utilizado por los

protocolos de encaminamiento tales como IGRP, EIGRP y OSPF para calcular la mejor ruta a una red remota en una interred. En el próximo capítulo, cuando veamos la configuración del encaminamiento IP, veremos estos protocolos y cómo utilizan estos parámetros.

Para configurar el ancho de banda de una interfaz serial se utiliza el comando de submodo de Configuración de Interfaz `bandwidth`:

```
Router(config-if)# bandwidth ?
  <1 – 10000000>   Bandwidth in kilobits
```

Encapsulamiento

El método de encapsulamiento en una interfaz determina el formato de las tramas de datos al nivel de la capa de Enlace del Modelo de Referencia OSI.

Una interfaz serial puede soportar un solo tipo de encapsulamiento, el cual depende del tipo de dispositivo con el cual la interfaz se comunica a nivel de la capa de Enlace. Si la interface se comunica con un switch Frame Relay, el encapsulamiento debe ser Frame Relay y si se comunica con un switch X.25, el encapsulamiento debe ser X.25. Si el router se comunica directamente con otro router a nivel de la capa 2, el encapsulamiento puede ser HDLC, LAPB o PPP.

HDLC es el encapsulamiento predeterminado para todas las interfaces seriales en un router de Cisco. Como regla general, si el enlace WAN es una línea dedicada y el router del otro extremo es también un router de Cisco, se puede dejar el encapsulamiento como HDLC. Sin embargo, puesto que la implementación de Cisco de HDLC es propietaria, se deberá utilizar un encapsulamiento PPP en caso en que el router del otro extremo sea un router de otro fabricante.

Para establecer el encapsulamiento de una interfaz serial se utiliza el comando de submodo de Configuración de Interface `encapsulation`:

```
RouterA(config-if)# encapsulation ?
  atm-dxi         ATM-DXI encapsulation
  bstun           Block Serial tunneling (BSTUN)
  frame-relay     Frame Relay networks
  hdlc            Serial HDLC synchronous
  lapb            LAPB (X.25 Level 2)
  ppp             Point-to-Point protocol
  sdlc            SDLC
  sdlc-primary    SDLC (primary)
  sdlc-secondary  SDLC (secondary)
  smds            Switched Megabit Data Service (SMDS)
  stun            Serial tunneling (STUN)
  x25             X.25
```

Con estos elementos, entonces, podemos comenzar a configurar las interfaces seriales del router. Comencemos por la interfaz `serial 0/1`, recordando que esta interfaz ha de proveer el sincronismo para el enlace WAN1, por lo que deberemos utilizar el comando `clock rate`.

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
```

```
RouterA(config)#  interface serial 0/0
RouterA(config-if)# ip address 200.10.10.5 255.255.255.252
RouterA(config-if)# description Enlace 128K al router B
RouterA(config-if)# bandwidth 128
RouterA(config-if)# clock rate 128
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# exit
RouterA# copy running-config startup-config
```

Veamos cómo ha quedado el estado de esta interfaz:

```
RouteAr# show interface serial 0/0
 Serial0/0 is up, line protocol is down
   Hardware is PowerQUICC Serial
  Description: Enlace 128K al router B
  Internet address is 200.10.10.5/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP REQsent, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:00:56
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/2/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  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 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3 packets output, 42 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

En la primera línea de la salida anterior vemos que el estado de la interfaz dice "line protocol is down". Lo que ocurre es que la interfaz `serial 0/0` del router B (la del otro extremo del enlace) aún no ha sido configurada ni habilitada con el comando `no shutdown`. Cuando configuremos esta interfaz, volveremos al router A para verificar que ha quedado habilitada y operativa.

Configuremos ahora la interfaz `serial 0/1` de nuestro router A, la cual también ha de proporcionar el sincronismo para el enlace WAN3:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)#  interface serial 0/1
RouterA(config-if)# ip address 200.10.30.5 255.255.255.252
RouterA(config-if)# description Enlace 256K al router C
RouterA(config-if)# bandwidth 256
RouterA(config-if)# clock rate 256000
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# exit
RouterA# copy running-config startup-config
Building configuration …
[OK]
```

Configuración del router B

Los pasos para configurar el router B son análogos a los que hemos seguido para configurar el router A. Accedamos a este router a través de su puerto de consola, tal como lo hicimos con el router A.

Comencemos por la interfaz `fastethernet 0/0`:

```
Router> enable
Password: <...>
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# hostname RouterB
RouterB(config)# interface fastethernet 0/0
RouterB(config-if)# description Conexión a la LAN2
RouterB(config-if)# ip address 177.16.0.1 255.255.0.0
RouterB(config-if)# no shutdown
RouterB(config-if)# exit
RouterB(config)
```

Configuremos ahora la interfaz `serial 0/0` del enlace WAN1 al router A; recordemos que en este enlace es el router A el que proporciona el sincronismo, de modo que para esta interfaz no debemos utilizar el comando `clock rate`:

```
RouterB(config)#  interface serial 0/0
RouterB(config-if)# ip address 200.10.10.6 255.255.255.252
RouterB(config-if)# description Enlace 128K al router A
RouterB(config-if)# bandwidth 128
RouterB(config-if)# encapsulation ppp
RouterB(config-if)# no shutdown
```

```
RouterB(config-if)# exit
RouterB(config)#
```

Configuremos ahora la interfaz `serial 0/1` del enlace WAN2 al router C; recordemos que esta interfaz ha de proveer el sincronismo del enlace:

```
RouterB(config)#  interface serial 0/1
RouterB(config-if)# ip address 200.10.20.5 255.255.255.252
RouterB(config-if)# description Enlace 128K al router C
RouterB(config-if)# bandwidth 128
RouterB(config-if)# clock rate 128000
RouterB(config-if)# encapsulation ppp
RouterB(config-if)# no shutdown
RouterB(config-if)# exit
RouterB(config)#
```

Vayamos ahora el modo Privilegiado y veamos el estado de las interfaces:

```
RouterB(config)# exit
RouterB#
RouterB# show interfaces
 1 FastEthernet0/0 is up, line protocol is up
 2  Hardware is PQUICC_FEC, address is 0004.c14e.7ff4 (bia 0004.c14e.7ff4)
 3  Description: Enlace a la LAN 2
 4  Internet address is 177.16.0.1/16
 5  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
 6     reliability 255/255, txload 1/255, rxload 1/255
 7  Encapsulation ARPA, loopback not set
 8  Keepalive set (10 sec)
 9  Auto-duplex, 10Mb/s, 100BaseTX/FX
10  ARP type: ARPA, ARP Timeout 04:00:00
11  Last input never, output 00:00:05, output hang never
12  Last clearing of "show interface" counters never
13  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
14  Queueing strategy: fifo
15  Output queue: 0/40 (size/max)
16  5 minute input rate 0 bits/sec, 0 packets/sec
17  5 minute output rate 0 bits/sec, 0 packets/sec
18     0 packets input, 0 bytes
19     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
20     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
21     0 watchdog
22     0 input packets with dribble condition detected
23     369 packets output, 181000 bytes, 0 underruns
24     0 output errors, 0 collisions, 2 interface resets
25     0 babbles, 0 late collision, 0 deferred
26     0 lost carrier, 0 no carrier
27     0 output buffer failures, 0 output buffers swapped out
```

```
Serial0/0 is up, line protocol is up
 Hardware is PowerQUICC Serial
 Description: Enlace 128 K al router A
 Internet address is 200.10.10.6/30
 MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation PPP, LCP Open
 Open: CDPCP, IPCP, loopback not set
 Last input 00:00:05, output 00:00:02, output hang never
 Last clearing of "show interface" counters 00:02:02
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    30 packets input, 1108 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    1 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
    29 packets output, 1094 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
Serial0/1 is up, line protocol is down
 Hardware is PowerQUICC Serial
 Description: Enlace 128K al router C
 Internet address is 200.10.20.5/30
 MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 253/255, txload 1/255, rxload 1/255
 Encapsulation PPP, LCP Listen, loopback not set
 Last input 00:00:08, output 00:00:26, output hang never
 Last clearing of "show interface" counters 00:00:52
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: weighted fair
 Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations  0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 96 kilobits/sec
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    7 packets input, 168 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    1 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
    10 packets output, 140 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Finalmente, salvemos la configuración en ejecución en la configuración de arranque:

```
RouterB# copy running-config startup-config
Building configuration …
[OK]
RouterB# disable
RouterB>
```

Configuración del router C

Para comenzar a configurar el router C vamos a hacer algo distinto a lo que hemos hecho para los routers A y B; vamos a utilizar el modo de Configuración Setup que mencionamos en el Capítulo 2. Recordemos que este modo es mas frecuentemente utilizado cuando arranca el router y no tiene un archivo de configuración de arranque en la memoria NVRAM. A este modo puede igualmente ingresarse mediante el comando de modo Privilegiado `setup`.

Vamos a hacer de cuenta que nuestro router C es un router nuevo, recién sacado de su caja y que solo tiene precargada la imagen del sistema operativo IOS en su memoria FLASH. Para esto vamos a conectarnos al router C por su puerto de Consola, accederemos al modo Privilegiado, borraremos el contenido de su memoria NVRAM con el comando `erase nvram` y reiniciaremos el router con el comando `reload`:

```
Router> enable
Router# erase nvram
Erasing the nvram filesystem will remove all files! Continue? [confirm] y
[OK]
Erase of nvram: complete
*Mar  1 00:22:31.003: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router# reload
Proceed with reload? [confirm] y
*Mar  1 00:22:38.775: %SYS-5-RELOAD: Reload requested by console.
```

Luego de unos instantes veremos desplegarse en pantalla la serie de mensajes correspondientes a la reinicialización del router

```
System Bootstrap, Version 12.1(5r)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
RSR = 0xE8000000
C1700 platform with 65536 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0xacd8c8

Self decompressing the image :
################################################################################
################################################################################
################################################## [OK]
```

```
                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK8NO3R2SV3Y7-M), Version 12.2(11)T,  RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 31-Jul-02 10:34 by ccai
Image text-base: 0x80008124, data-base: 0x813ACC18

Compliance with U.S. Export Laws and Regulations - Encryption

This product performs encryption and is regulated for export
by the U.S. Government.

This product is not authorized for use by persons located
outside the United States and Canada that do not have prior
approval from Cisco Systems, Inc. or the U.S. Government.

This product may not be exported outside the U.S. and Canada
either by physical or electronic means without PRIOR approval
of Cisco Systems, Inc. or the U.S. Government.

Persons outside the U.S. and Canada may not re-export, resell,
or transfer this product by either physical or electronic means
without  prior approval of Cisco Systems, Inc. or the U.S.
Government.

cisco 1751 (MPC860P) processor (revision 0x101) with 55706K/9830K bytes of
memory.
Processor board ID JAD052212D4 (2101109953), with hardware revision 6534
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 FXO interface(s)
```

```
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
```

Una vez reinicializado el router veremos en la pantalla un mensaje indicando de que el contenido de la memoria NVRAM no es válido (recordemos que eliminamos su contenido con el comando `erase nvram`)y a continuación la pregunta de si queremos entrar al modo de configuración inicial, a lo cual responderemos que **Si** (yes):

```
NOTICE: NVRAM invalid, possibly due to write erase

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

A continuación, el modo Setup despliega una serie de instrucciones de uso:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

Luego nos pregunta si queremos acceder a la configuración básica (mínima) de gestión, a lo cual respondemos que No:

```
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]: no
```

A continuación la pregunta es si queremos ver un sumario de la configuración actual de las interfaces; respondemos que **Si**.

```
First, would you like to see the current interface summary? [yes]:
Any interface listed with OK? value "NO" does not have a valid configuration
Interface          IP-Address     OK?  Method    Status    Protocol
FastEthernet0/0    unassigned     NO   unset     up        down
Serial0/0          unassigned     NO   unset     down      down
Serial0/1          unassigned     NO   unset     down      down
```

Llegados a este punto, el modo Setup nos permite configurar algunos parámetros globales del router: su nombre de host y las contraseñas de modo Privilegiado y de acceso por Telnet (virtual terminal password):

```
Configuring global parameters:
Enter host name [Router]: RouterC
 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: cisco
```

```
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: routerC
The virtual terminal password is used to protect access to the router over a
network interface.
Enter virtual terminal password: cisco
```

A continuación, una serie de preguntas nos dan la oportunidad de configurar distintos protocolos, así como acceder a la configuración de SNMP. Respondamos "Si" solamente para acceder a la configuración del protocolo IP:

```
Configure SNMP Network Management? [yes]: no
Configure AppleTalk? [no]:
Configure bridging? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]: no
Configure RIP routing? [no]: no
```

Llegamos así al paso de configuración de IP en las tres interfaces del router:

```
Configuring interface parameters:
Do you want to configure FastEthernet0/0 interface? [yes]:
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: 197.168.100.1
Subnet mask for this interface [255.255.255.0]: 255.255.255.0
Class C network is 197.168.100.0, 24 subnet bits; mask is /24

Do you want to configure Serial0/0 interface? [yes]:
  Some supported encapsulations are
     ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
  Choose encapsulation type [hdlc]: ppp
Configure IP on this interface? [yes]:
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 200.10.20.6
Subnet mask for this interface [255.255.255.0]: 255.255.255.252
Class C network is 200.10.20.0, 30 subnet bits; mask is /30

Do you want to configure Serial0/1 interface? [yes]:
  Some supported encapsulations are
     ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
  Choose encapsulation type [hdlc]: ppp
Configure IP on this interface? [yes]:
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 200.10.30.6
```

```
Subnet mask for this interface [255.255.255.0]: 255.255.255.252
Class C network is 200.10.30.0, 30 subnet bits; mask is /30
```

Observe que únicamente hemos podido configurar las direcciones IP de cada interfaz y el método de encapsulamiento para las interfaces de tipo Serial. En particular, para las interfaces de tipo Serial deberemos posteriormente configurar en forma manual sus demás parámetros mediante los comandos apropiados.

Por último, el diálogo de Setup nos muestra la configuración ha crear y nos da la opción de salvarla a la memoria NVRAM en el archivo `startup-config`, para lo cual seleccionamos, al final, la opción 2:

```
The following configuration command script was created:
hostname RouterC
enable secret 5 $1$gXHU$blL9yGVDJsMmjvLCFVP6J/
enable password routerC
line vty 0 4
password secreto
no snmp-server
!
no appletalk routing
no bridge 1
no ipx routing
ip routing
!
interface FastEthernet0/0
media-type 100BaseX
half-duplex
ip address 197.168.100.1 255.255.255.0
!
interface Serial0/0
encapsulation ppp
ip address 200.10.20.6 255.255.255.252
!
interface Serial0/1
encapsulation ppp
ip address 200.10.30.6 255.255.255.252
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
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
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

```
Press RETURN to get started!
```

Si ahora presionamos la tecla **Intro**, veremos una serie de mensajes relativos a las interfaces y pasamos al modo Usuario:

```
*Mar  1 00:00:04.843: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar  1 00:00:05.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Mar  1 00:00:12.539: %LINK-3-UPDOWN: Interface Serial0/0, changed state to
up
*Mar  1 00:00:12.543: %LINK-3-UPDOWN: Interface Serial0/1, changed state to
up
*Mar  1 00:00:13.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
*Mar  1 00:00:13.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to up
*Mar  1 00:00:13.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Mar  1 00:00:39.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to down
*Mar  1 00:01:01.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to down
*Mar  1 00:01:03.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
*Mar  1 00:01:29.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to down
*Mar  1 00:05:22.283: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0,
changed state to up
*Mar  1 00:05:22.283: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/1,
changed state to up
*Mar  1 00:05:22.283: %LINK-3-UPDOWN: Interface Foreign Exchange Station 2/0,
changed state to up
*Mar  1 00:05:22.287: %LINK-3-UPDOWN: Interface Foreign Exchange Station 2/1,
changed state to up
*Mar  1 00:05:24.695: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK8NO3R2SV3Y7-M), Version 12.2(11)T,  RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 31-Jul-02 10:34 by ccai
*Mar  1 00:05:24.739: %SNMP-5-COLDSTART: SNMP agent on host RouterC is
undergoing a cold start
*Mar  1 00:05:27.795: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to up
```

```
*Mar  1 00:05:27.795: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
RouterC>
```

Lo que resta hacer ahora es completar las configuraciones de las interfaces seriales, proceso análogo al que hemos realizado anteriormente en los otros dos routers:

```
RouterC> enable
Password:
RouterC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterC(config)# interface serial 0/0
RouterC(config-if)# description Enlace 128K al router B
RouterC(config-if)# bandwidth 128
RouterC(config-if)# no shutdown
RouterC(config-if)# exit

RouterC(config)# interface serial 0/1
RouterC(config-if)# description Enlace 256 al router A
RouterC(config-if)# bandwidth 256
RouterC(config-if)# no shutdown
RouterC(config-if)# exit
RouterC(config)# exit
*Mar  1 00:07:34.963: %SYS-5-CONFIG_I: Configured from console by console
RouterC# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RouterC#
```

Pruebas de conectividad

Ahora que nuestros tres routers tienen su configuración IP básica en sus interfaces, vamos a ver si funciona.

Vayamos al router A y veamos primeramente un nuevo comando de modo Privilegiado que nos muestra, en forma resumida, la configuración de las interfaces:

```
RouterA# show ip interfaces brief
Interface          IP-Address    OK?  Method   Status    Protocol
FastEthernet0/0    17.0.0.1      YES  manual   up        up
Serial0/0          200.10.10.5   YES  manual   up        up
Serial0/1          200.10.30.5   YES  manual   up        up
```

Otro comando interesante de modo Privilegiado para ver la configuración IP del router es `show protocols`:

```
RouterA# show protocols
```

```
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 17.0.0.1/8
Serial0/0 is up, line protocol is up
  Internet address is 200.10.10.5/30
Serial0/1 is up, line protocol is up
  Internet address is 200.10.30.5/30
```

Un comando básico, pero muy útil, para verificar la conectividad en un entorno TCP/IP es el comando `ping`. IOS proporciona dos versiones de este comando; una es el comando `ping` básico, que puede ejecutarse en el modo Usuario y la otra es el comando `ping` extendido que solo puede ejecutarse en el modo Privilegiado.

Comencemos verificando la conectividad entre los routers A y B a través del enlace WAN1. Estando en la consola del router A ejecutamos el comando `ping` a la interface `serial 0/0` del router B:

```
RouterA# ping 200.10.10.6
1 Type escape secuence to abort
2 Sending 5, 100-byte ICMP Echos to 200.10.10.6, timeout is 2 seconds:
3 !!!!!
4 Success rate is 100 percent (5/5), round-trip min/avg/max = 32/46/104 ms
RouterA#
```

La línea 2 nos dice que el comando va a enviar cinco paquetes al destino especificado en la línea de comandos y en la línea 3 nos muestra un signo de admiración por cada respuesta recibida desde ese destino La línea 4 finalmente nos indica el resultado global de la ejecución del comando, así como los tiempos mínimo, promedio y máximo de ida y vuelta.

Los signos de admiración de la línea 3 son uno de los varios códigos que IOS utiliza para indicar el estado de la ejecución del comando. Los otros códigos posibles son:

Código	Descripción. La respuesta recibida fue ...
.	no se recibe respuesta
U	destino inalcanzable (Unrecheable)
N	red inalcanzable (Network unrecheable)
P	puerto inalcanzable (Port unrecheable)
Q	source Quench
M	no se puede fragmentar
?	Paquete desconocido

Lo que hemos verificado con el comando `ping` anterior es la conectividad entre los routers. Esto es importante y un buen síntoma de que estamos haciendo las cosas bien. Sin embargo, lo que verdaderamente nos interesa es verificar la conectividad entre las redes LAN de nuestra interred; en particular, en este momento, que un host de la LAN1 pueda comunicarse con un host en la LAN2.

Hay dos formas de verificar esta conectividad host a host. Una de ellas es ejecutando el comando `ping` de Windows desde un host conectado a la LAN1 y destinado a un host en la LAN2. La otra forma de hacerlo es utilizando el comando `ping` extendido de IOS, el cual permite, entre otras cosas, modificar la dirección IP de origen de los paquetes ICMP echo request. Como vimos anteriormente, el comando `ping` básico utiliza la dirección IP de la interface `serial 0/0` como dirección de origen, pero si queremos probar la conectividad entre las redes LAN, la dirección de origen debe ser una dirección IP en la LAN1.

El comando `ping` extendido se ejecuta en el modo Privilegiado, escribiendo simplemente `ping` en la línea de comandos y respondiendo a las preguntas que nos hace:

```
RouterA# ping
 1 Protocol [ip]:
 2 Target IP address: 200.10.10.6
 3 Repeat count [5]:
 4 Datagram size [100]:
 5 Timeout in seconds [2]:
 6 Extended commands [n]: y
 7 Source address or interface: 17.0.0.1
 8 Type of service [0]:
 9 Set DF bit in IP header? [no]:
10 Validate reply data? [no]:
11 Data patterns [0xABCD]:
12 Loose, Strict, Record, Timestamp, Verbose [none]:
13 Sweep range of sizes [n]:
14 Type escape sequence to abort.
15 Sending 5, 100-byte ICMP Echos to 200.10.10.6, timeout is 2 seconds:
16 .....
17 Success rate is 0 percent (0/5)
RouterA#
```

Como podemos ver en las líneas 16 y 17, el comando ha fallado. Lo que ocurre es que el router B no conoce la existencia de la red LAN1, es decir, no sabe como encaminar de regreso los paquetes ICMP "echo replan". La palabra clave aquí es, precisamente, "encaminar"; router B no sabe hacia donde enviar los paquetes destinados a la dirección IP 17.0.0.1.

Esto lo podemos verificar viendo el contenido de la tabla de encaminamiento del router B. Para ello utilizamos el comando de modo Privilegiado `show ip route`:

```
RouterB# 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, 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

     200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C       200.10.20.6/32 is directly connected, Serial0/1
C       200.10.20.4/30 is directly connected, Serial0/1
C    177.16.0.0/16 is directly connected, FastEthernet0/0
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.5/32 is directly connected, Serial0/0
RouterB#
```

Como puede verse en la salida anterior, la tabla de encaminamiento de router B no tiene información sobre la red 17.0.0.0.

En el capítulo siguiente resolveremos este problema configurando el encaminamiento IP en cada router de modo que cada uno conozca la existencia de las otras redes a las cuales no está directamente conectado.

9. Configuración del encaminamiento IP

La configuración del encaminamiento IP es lo que permite al router hacer efectivamente su principal trabajo en una interred, esto es, poder encaminar los datagramas entrantes hacia sus destinos finales determinando la mejor ruta para ello en cada caso.

Cuando un router recibe un datagrama destinado a otro host, debe decidir hacia donde reenviarlo para que el mismo llegue hasta ese host. Para ello, el router se basa en la información contenida en lo que se denomina "tabla de encaminamiento" la cual contiene, básicamente, las direcciones IP de las demás redes de la interred y la identificación de las interfaces por las cuales reenviar los datagramas para llegar a cada una de ellas.

IOS tiene tres fuentes de las cuales obtener información acerca de las rutas hacia otras redes a incluir en su tabla de encaminamiento:

- Las redes a las cuales está directamente conectado
- Las rutas estáticas, ingresadas manualmente por el administrador
- Los protocolos de encaminamiento

IOS puede ejecutar varios protocolos de encaminamiento en forma simultánea. Cada protocolo utiliza una métrica diferente para indicar el largo de los caminos hacia las redes que está publicitando. Cuando para una red IOS aprende varios caminos posibles, seleccionará el "mejor" de ellos como aquél que tenga la menor métrica y es ese camino el que incorpora a su tabla de encaminamiento.

Cuando se presenta la situación de haber varios caminos hacia una red y esa información es obtenida basándose en distintos protocolos de encaminamiento, IOS utiliza lo que se denomina "distancia administrativa" para seleccionar el mejor de ellos. La distancia administrativa es un valor numérico entre 0 y 255 que representa la fiabilidad del origen de la información de encaminamiento. Cada tipo de ruta y de protocolo de encaminamiento tiene asociado un valor particular de distancia administrativa. Cuanto más bajo su valor, más fiable es el origen de la información.

En la tabla siguiente se resumen los valores de distancia administrativa para los diferentes protocolos de encaminamiento:

Fuente	Distancia
Directamente conectada	0
Ruta estática	1
Resumen EIGRP	5
EIGRP	90
IGRP	100
OSPF	110
RIP	120
Desconocida	255

Estos son los valores predeterminados que IOS maneja para las distancias administrativas de las distintas fuentes de información de encaminamiento e IOS proporciona un comando, `distance`, que permite modificar estos valores predeterminados.

Cuando para dos o mas caminos hacia una red la distancia administrativa es la misma, es decir, cuando la información sobre esas rutas se obtuvo de una misma fuente o protocolo de encaminamiento, IOS selecciona como la mejor de ellas aquella cuya métrica sea la menor. Si varios caminos hacia una red tienen la misma distancia administrativa y la misma métrica, entonces IOS coloca todas las rutas, hasta seis, en su tabla de encaminamiento.

Encaminamiento estático

El encaminamiento estático implica establecer manualmente en las tablas de encaminamiento de caca router las rutas a las redes destino que el router no conoce.

Para una referencia rápida, en la figura 9-1 se muestra nuevamente nuestra interred con las direcciones asignadas a cada red:

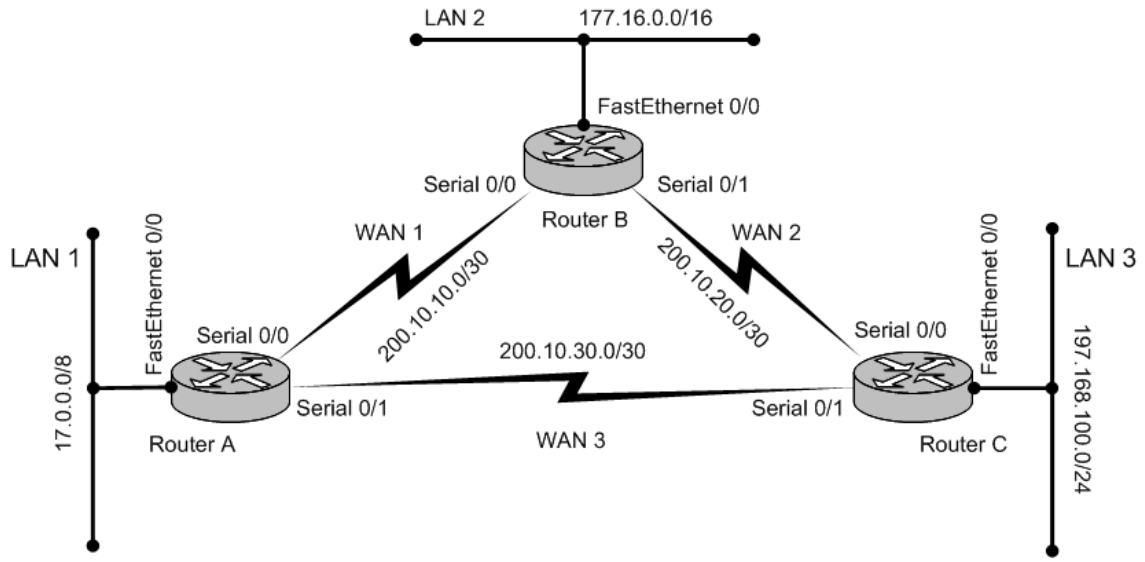


Figura 9 - 1

Lo que nosotros queremos en nuestra interred es que cualquier paquete de datos originado, por ejemplo, en un host de la red LAN1 pueda llegar a su destino, por ejemplo, un host en las redes LAN2 o LAN3.

Rutas estáticas en el router A

Comencemos por ver el contenido actual de la tabla de encaminamiento del router A. Para ello utilizamos el comando de modo Privilegiado `show ip route`:

```
RouterA# 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, 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    17.0.0.0/8 is directly connected, FastEthernet0/0
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.6/32 is directly connected, Serial0/1
C       200.10.30.4/30 is directly connected, Serial0/1
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.6/32 is directly connected, Serial0/0
```

Como podemos ver, el router A tiene información únicamente sobre las tres redes a las cuales está directamente conectado. En consecuencia, si desde LAN1 el router recibe un paquete de datos destinado a la LAN2 o a la LAN3, no sabrá hacia donde encaminarlo, simplemente porque desconoce la existencia de esas redes.

La forma de hacerle saber al router A cómo encaminar correctamente esos datagramas es incorporando a su tabla de encaminamiento información sobre esas redes y cómo llegar hasta ellas, es decir, debemos hacerle saber de la existencia de las redes 177.16.0.0 y 197.168.100.0 y hacia dónde reenviar los datagramas para llegar a las mismas.

Para esto se utiliza el comando de Configuración Global `ip route`. Para ver cómo utilizar este comando utilicemos, como lo hemos hecho anteriormente con otros comandos, la facilidad de ayuda de la Interface de Línea de Comandos:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# ip route ?
  A.B.C.D  Destination prefix
  profile  Enable IP routing table profile
  static   Allow static routes
  vrf      Configure static route for a VPN Routing/Forwarding instance
```

Como primer parámetro, entonces, debemos indicar la dirección de la red de destino. Comencemos por la red LAN 2, cuya dirección IP es 177.16.0.0

```
RouterA(config)# ip route 177.16.0.0
% Incomplete command
```

El mensaje de "comando incompleto" nos indica que el comando `ip route` reqiere algún parámetro adicional a a dirección IP de la red de destino. Continuemos entonces utilizando la facilidad de ayuda para ver cómo es la sintaxis completa del comando:

```
RouterA(config)# ip route 177.16.0.0 ?
  A.B.C.D  Destination prefix mask
```

El siguiente parámetro es, entonces, la máscara de subred en uso en la red de destino. Agreguemos este parámetro y veamos qué sucede:

```
RouterA(config)#ip route 177.16.0.0 255.255.0.0
% Incomplete command.
```

Como vemos, aún sigue faltando algo. Veamos qué es:

```
RouterA(config)#ip route 177.16.0.0 255.255.0.0 ?
 1  A.B.C.D            Forwarding router's address
 2  Async              Async interface
 3  BVI                Bridge-Group Virtual Interface
 4  CTunnel            CTunnel interface
 5  Dialer             Dialer interface
 6  FastEthernet       FastEthernet IEEE 802.3
 7  Lex                Lex interface
 8  Loopback           Loopback interface
 9  MFR                Multilink Frame Relay bundle interface
10  Multilink          Multilink-group interface
11  Null               Null interface
12  Serial             Serial
13  Tunnel             Tunnel interface
14  Vif                PGM Multicast Host interface
15  Virtual-TokenRing  Virtual TokenRing
```

La línea 1 indica que el parámetro que está faltando especificar es la dirección IP del router al cual reenviar los datagramas para llegar a la red de destino. De acuerdo con la configuración de nuestra interred, para llegar a la red 177.16.0.0 los datagramas deben pasar por el router B y el camino adecuado para llegar hasta él es a través del enlace WAN 1. El router B está conectado a este enlace por la interface cuya dirección IP es 200.10.10.6, de modo que el tercer parámetro para el comando `ip route` debe ser esta dirección IP.

Como alternativa, la línea 12 nos indica que puede especificarse la interface del router A por la cual deben salir los datagramas para llegar al router B. De todos modos, utilicemos la dirección IP del router B en ese enlace.

```
RouterA(config)#ip route 177.16.0.0 255.255.0.0 200.10.10.6
RouterA(config)#
```

Puesto que ahora no hemos obtenido ningún mensaje de error, nuestro comando ha sido aceptado. Para verificarlo, veamos ahora el nuevo estado de la tabla de encaminamiento del router A:

```
RouterA(config)#exit
RouterA#
*Mar  1 00:39:05.051: %SYS-5-CONFIG_I: Configured from console by console

RouterA# 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, 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

1 S    177.16.0.0/16 [1/0] via 200.10.10.6
2 C    17.0.0.0/8 is directly connected, FastEthernet0/0
3      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
4 C       200.10.30.6/32 is directly connected, Serial0/1
5 C       200.10.30.4/30 is directly connected, Serial0/1
6      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
7 C       200.10.10.4/30 is directly connected, Serial0/0
8 C       200.10.10.6/32 is directly connected, Serial0/0
```

En la línea 1 de la salida anterior vemos la información correspondiente a la ruta recién ingresada. La expresión 1/0 entre paréntesis indica que la distancia administrativa de esa ruta es 1 (por ser una ruta estática) y que la métrica de esa ruta es 0.

El comando `ip route` tiene dos opciones adicionales que no hemos utilizado y que se establecen mediante las palabras claves `distance` y `permanent`.

La palabra clave `distance` permite modificar el valor predeterminado de la distancia administrativa de una ruta que, para el caso de rutas estáticas es, como vimos antes, igual a 1. Por su parte, la palabra clave `permanent` tiene el siguiente uso. Si la interface del router asociada con una determinada ruta se deshabilita (con el comando shutdown) o el router no puede comunicarse con el del otro extremo, la ruta es automáticamente eliminada de la tabla de encaminamiento. Agregando la palabra clave `permanent` a esa ruta, la misma se mantendrá en la tabla de encaminamiento aunque se dé alguna de esas situaciones. En tal caso, cuando el enlace se restablezca o la interface se vuelva a habilitar, la ruta ya estará en la tabla de encaminamiento pues, de lo contrario sería necesario volver a ingresarla. Recordemos que estamos hablando de rutas estáticas que se deben ingresar y actualizar en forma manual.

Agreguemos ahora a la tabla de encaminamiento del router A la entrada correspondiente a la red LAN3:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# ip route 197.168.100.0 255.255.255.0 200.10.30.6
RouterA(config)# exit
RouterA#
*Mar  1 00:40:04.751: %SYS-5-CONFIG_I: Configured from console by console
```

Veamos nuevamente el contenido de la tabla de encaminamiento:

```
RouterA# 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, 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

1 S    177.16.0.0/16 [1/0] via 200.10.10.6
2 C    17.0.0.0/8 is directly connected, FastEthernet0/0
3      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
4 C       200.10.30.6/32 is directly connected, Serial0/1
5 C       200.10.30.4/30 is directly connected, Serial0/1
6      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
7 C       200.10.10.4/30 is directly connected, Serial0/0
8 C       200.10.10.6/32 is directly connected, Serial0/0
9 S    197.168.100.0/24 [1/0] via 200.10.30.6
```

Como podemos ver en la salida anterior, la línea 9 contiene la información de la nueva ruta ecién incorporada.

Resumamos entonces la información de rutas incorporada en la siguiente tabla:

Red	Destino	Máscara de subred	A dónde ....
LAN2	177.16.0.0	255.255.0.0	200.10.10.6
LAN3	197.168.100.0	255.255.255.0	200.10.30.6

Para terminar con la configuración del router A, no olvidemos salvar la nueva configuración al archivo STARTUP-CONFIG:

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

Rutas estáticas en el router B

Para configurar el encaminamiento estático en el router B debemos incorporar a su tabla de encaminamiento las rutas hacia las redes LAN1 y LAN3:

Red	Destino	Máscara de subred	A dónde....
LAN1	17.0.0.0	255.0.0.0	200.10.10.5
LAN3	197.168.100.0	255.255.255.0	200.10.20.6

Hagamos, entonces, lo siguiente: veamos el contenido actual de la tabla de encaminamiento del router B, incorporemos las rutas hacia aquellas redes y veamos finalmente el nuevo contenido de su tabla de encaminamiento. Comencemos pro ver el estado de la tabla de encaminamiento:

```
RouterB# 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, 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

     200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.20.6/32 is directly connected, Serial0/1
C       200.10.20.4/30 is directly connected, Serial0/1
C    177.16.0.0/16 is directly connected, FastEthernet0/0
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.5/32 is directly connected, Serial0/0
```

Como vemos, solo aparecen las redes a las cuales el router B está directamente conectado. Configuremos ahora las rutas estáticas hacia las redes LAN 1 y LAN 3:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterB(config)# ip route 17.0.0.0 255.0.0.0 200.10.10.6
RouterB(config)# ip route 197.168.100.0 255.255.255.0 200.10.20.6
RouterB(config)# exit
RouterB#
*Mar  1 00:44:37.731: %SYS-5-CONFIG_I: Configured from console by console
```

Veamos ahora el nuevo contenido de la tabla de encaminamiento:

```
RouterB# 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, 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

1      200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
2 C       200.10.20.6/32 is directly connected, Serial0/1
```

```
3 C       200.10.20.4/30 is directly connected, Serial0/1
4 C    177.16.0.0/16 is directly connected, FastEthernet0/0
5 S    17.0.0.0/8 [1/0] via 200.10.10.5
6      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
7 C       200.10.10.4/30 is directly connected, Serial0/0
8 C       200.10.10.5/32 is directly connected, Serial0/0
9 S    197.168.100.0/24 [1/0] via 200.10.20.6
```

En las líneas 5 y 9 de la salida anterior aparecen las rutas estáticas recién ingresadas; son las que comienzan con la letra "S".

```
RouterB# copy runing-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RouterB#
```

Rutas estáticas en el router C

Configuremos ahora el router C son la información de rutas estáticas de la siguiente tabla:

Red	Destino	Máscara de subred	A dónde....
LAN1	17.0.0.0	255.0.0.0	200.10.30.5
LAN2	177.16.0.0	255.255.0.0	200.10.20.5

```
RouterC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterC(config)# ip route 17.0.0.0 255.0.0.0 200.10.30.5
RouterC(config)# ip route 172.18.0.0 255.255.0.0 200.10.20.5
Routerc(config)# exit
RouterC#
*Mar  1 00:21:28.471: %SYS-5-CONFIG_I: Configured from console by console
```

Si ahora inspeccionamos el contenido de la tabla de encaminamiento tenemos, en las líneas 4 y 5 las rutas estáticas recién ingresadas:

```
Routerc# 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
```

```
1      200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
2 C       200.10.20.0/24 is directly connected, Serial0/0
3 C       200.10.20.5/32 is directly connected, Serial0/0
4 S    177.16.0.0/16 [1/0] via 200.10.20.5
5 S    17.0.0.0/8 [1/0] via 200.10.30.5
6      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
7 C       200.10.30.4/30 is directly connected, Serial0/1
8 C       200.10.30.5/32 is directly connected, Serial0/1
9 C    197.168.100.0/24 is directly connected, FastEthernet0/0

RouterC# copy runing-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RouterC#
```

Pruebas de conectividad

Para probar la conectividad entre las redes LAN de nuestra interred podemos utilizar nuevamente el comando `ping` que utilizamos en el capítulo anterior.

```
RouterA# ping 197.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

RouterA# ping
Protocol [ip]:
Target IP address: 197.168.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
```

Veamos ahora otro comando de modo Privilegiado. Se trata del comando `trace`, el cual despliega en pantalla la ruta que siguen los datagramas desde el host en el cual se ejecuta el comando hasta el host de destino especificado en el mismo. Utilicemos la facilidad de ayuda de la Interface de Línea de Comandos para averiguar la sintaxis de este comando:

```
RouterA# trace ?
  WORD       Trace route to destination address or hostname
  appletalk  AppleTalk Trace
```

```
  clns       ISO CLNS Trace
  ip         IP Trace
  ipv6       IPv6 Trace
  ipx        IPX Trace
  <cr>
```

La primera opción indica que puede especificarse la dirección IP de destino hasta la cual quiere trazarse la ruta. Indiquemos entonces la dirección IP de un host en la red LAN 3:

```
RouterA# trace 197.168.100.11
1 Type escape sequence to abort.
2 Tracing the route to 197.168.100.11
3
4   1 200.10.30.6 16 msec 16 msec 16 msec
5   2 197.168.100.11 16 msec 16 msec 16 msec
RouterA#
```

En la línea 4 vemos que los datagramas "pasan" por la interface del router C cuya dirección IP es 200.10.30.6, para llegar al destino, indicado en la línea 5.

Encaminamiento dinámico

A diferencia del encamminamiento estático que vimos recién, el encaminamiento dinámico se basa en la utilización de algún protocolo de encaminamiento, de modo que los routers de nuestra interred se intercambien información sobre las redes y rutas que cada uno conoce.

Veremos a continuación la configuración básica de los siguientes protocolos de encaminamiento, en el orden mostrado desde el más sencillo al más complejo:

- RIP
- IGRP
- EIGRP
- OSPF

Para configurar un protocolo de encaminamiento debemos seguir básicamente dos pasos:

1. Indicar, con el comando de Configuración Global `router`, cual protocolo de encaminamiento va a ser configurado.
2. Iniciar el protocolo en las interfaces del router mediante el comando de submodo de Configuración de Router `network`.

Antes de comenzar esta tarea, vamos a eliminar de los tres routers las rutas estáticas que establecimos antes. Para ello se utiliza la forma "no" del comando `ip route`:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# no ip route
```

```
% Incomplete command.
```

El comando `no ip route` para eliminar una ruta estática requiere exactamente los mismos parámetros que se utilizaron para agregar esa misma ruta:

```
RouterA(config)# no ip route 177.16.0.0 255.255.0.0 200.10.10.6
RouterA(config)# no ip route 197.168.100.0 255.255.255.0 200.10.30.6
RouterA(config)# exit
RouterA#
*Mar  1 00:53:40.035: %SYS-5-CONFIG_I: Configured from console by console
```

La tabla de encaminamiento, ahora, contendrá únicamente las rutas a las redes a las cuales el router está directamente conectado:

```
RouterA# 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, 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    17.0.0.0/8 is directly connected, FastEthernet0/0
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.6/32 is directly connected, Serial0/1
C       200.10.30.4/30 is directly connected, Serial0/1
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.6/32 is directly connected, Serial0/0
RouterA#
```

Pasemos ahora al router B y quitemos las rutas estáticas que incorporamos anteriormente al mismo:

```
RouterB> enable
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterB(config)# no ip route 17.0.0.0 255.0.0.0 200.10.10.5
RouterB(config)# no ip route 197.168.200.0 255.255.255.0 200.10.20.6
RouterB(config)# exit
RouterB#
*Mar  1 00:56:58.055: %SYS-5-CONFIG_I: Configured from console by console
```

La tabla de encaminamiento de router B contendrá, ahora, la siguiente información:

```
RouterB# 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, 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

     200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.20.6/32 is directly connected, Serial0/1
C       200.10.20.4/30 is directly connected, Serial0/1
C    177.16.0.0/16 is directly connected, FastEthernet0/0
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.5/32 is directly connected, Serial0/0
RouterB#
```

Finalmente, quitemos las rutas estáticas del router C, de manera similar a como lo hicimos en los otros dos routers:

```
RouterC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterC(config)# no ip route 17.0.0.0 255.0.0.0 200.10.30.5
RouterC(config)# no ip route 177.16.0.0 255.255.0.0 200.10.20.5
RouterC(config)# exit
RouterC#
*Mar  1 00:32:01.127: %SYS-5-CONFIG_I: Configured from console by console
```

La tabla de encaminamiento de router C contendrá, ahora, la siguiente información:

```
RouterC# 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
```

```
     200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.20.0/24 is directly connected, Serial0/0
C       200.10.20.5/32 is directly connected, Serial0/0
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.4/30 is directly connected, Serial0/1
C       200.10.30.5/32 is directly connected, Serial0/1
C    197.168.100.0/24 is directly connected, FastEthernet0/0
RouterC#

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

El protocolo RIP

El protocolo RIP, Routing Information Protocol (Protocolo de Información de Ruteo), es un protocolo de encaminamiento del tipo vector-distancia que utiliza una métrica sencilla para determinar el mejor camino hacia una red. Esta métrica es la cantidad de "saltos" o routers intermedios entre el router que está ejecutando el proceso RIP y la red destino. La cantidad máxima de saltos que soporta el protocolo es 15, lo cual solo permite utilizarlo como protocolo de encaminamiento en interredes relativamente pequeñas. Esta métrica que utiliza RIP no le permite distinguir entre enlaces rápidos y lentos, y tampoco toma en consideración otros posibles parámetros como pueden serlo la tasa de errores de transmisión del enlace o el MTU (Maximun Transfer Unit) de los enlaces.

Existen dos versiones de este protocolo, denominadas simplemente Versión 1 y Versión 2. La versión 1 está especificada en el RFC 1058 y la versión 2 en el RFC 1723 y ambas están soportadas por el sistema operativo IOS de Cisco. En la siguiente tabla se muestra un resumen de las similitudes y diferencias entre ambas versiones:

Característica	Versión 1	Versión 2
Tipo	Vector-distancia	Vector-distancia
Métrica	Cantidad de saltos	Cantidad de saltos
Máximo de saltos	15	15
Actualizaciones	Broadcast: 255.255.255.255	Multicast: 224.0.0.9
Máscara de subred de largo variable	No	Si
Autenticación	No	Si

Configuración de RIP, versión 1

El proceso RIP versión 1 en cada router envía, cada 30 segundos, actualizaciones de sus tablas de encaminamiento a la dirección de broadcast 255.255.255.255 que solo son procesadas por sus router vecinos, es decir, por aquél conectado al otro extremo de cada enlace. Cuando un router recibe una actualización de su vecino, recalcula su propia tabla de encaminamiento, seleccionando como mejor ruta a una red aquella cuya cantidad de saltos sea menor.

Comencemos por configurar el protocolo de encaminamiento RIP en el router A. En primer lugar, utilicemos el comando de Configuración Global `router` para indicarle a IOS que los siguientes comandos van a ser utilizados por un proceso de encaminamiento. Veamos que nos dice la ayuda sobre este comando:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# router ?
  bgp       Border Gateway Protocol (BGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)
```

El comando para iniciar la configuración del protocolo RIP es, entonces, `router rip`:

```
RouterA(config)# router rip
RouterA(config-router)#
```

Observe que el indicador del sistema ha cambiado a `(config-router);` estamos, pues, en un nuevo submodo de configuración, el submodo de Configuración de Router. Una vez en este submodo debemos indicar a IOS las redes por las cuales las interfaces conectadas a las mismas enviarán y recibirán las actualizaciones periódicas de RIP. Recordemos que RIP no maneja subredes; por lo tanto hemos de indicar una dirección de red clase A, B o C completa, aún en el caso de que se traten de subredes.

Nuestro router A debe enviar las actualizaciones a los routers B y C y ha de recibir las actualizaciones que ellos envíen. En consecuencia, debemos indicar las redes por las cuales se llega a estos dos routers. Para ello se utiliza el comando de submodo de Configuración de Router `network`:

```
RouterA(config-router)# ?
Router configuration commands:
  address-family          Enter Address Family command mode
  auto-summary            Enable automatic network number summarization
  default                 Set a command to its defaults
  default-information     Control distribution of default information
  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
  flash-update-threshold  Specify flash update threshold in second
  help                    Description of the interactive help system
  input-queue             Specify input queue depth
  maximum-paths           Forward packets over multiple paths
  neighbor                Specify a neighbor router
```

```
  network                 Enable routing on an IP network
  no                      Negate a command or set its defaults
  offset-list             Add or subtract offset from RIP metrics
  output-delay            Interpacket delay for RIP updates
  passive-interface       Suppress routing updates on an interface
  redistribute            Redistribute information from another routing
                          protocol
  timers                  Adjust routing timers
  traffic-share           How to compute traffic share over alternate paths
  validate-update-source  Perform sanity checks against source address of
                          routing updates
  version                 Set routing protocol version

RouterA(config-router)# network ?
  A.B.C.D  Network number
```

Como vemos, el comando `network` requiere como parámetro una dirección de red. Puesto que el router A está conectado a tres redes, debemos especificar cada una de ellas con un comando `network`:

```
RouterA(config-router)# network 17.0.0.0
RouterA(config-router)# network 200.10.10.0
RouterA(config-router)# network 200.10.30.0
RouterA(config-router)# exit
RouterA(config)# exit
RouterA#
*Mar  1 00:58:38.747: %SYS-5-CONFIG_I: Configured from console by console
```

Como siempre, salvemos la nueva configuración en ejecución en la configuración de arranque:

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

Utilicemos ahora el comando de modo Privilegiado `shop ip protocols` para ver cómo ha quedado configurado el protocolo RIP:

```
RouterA# show ip protocols
 1 Routing Protocol is "rip"
 2   Sending updates every 30 seconds, next due in 10 seconds
 3   Invalid after 180 seconds, hold down 180, flushed after 240
 4   Outgoing update filter list for all interfaces is not set
 5   Incoming update filter list for all interfaces is not set
 6   Redistributing: rip
 7  Default version control: send version 1, receive any version
 8   Interface             Send  Recv  Triggered RIP  Key-chain
```

```
 9   FastEthernet0/0        1     1 2
10    Serial0/0             1     1 2
11    Serial0/1             1     1 2
12  Automatic network summarization is in effect
13  Maximum path: 4
14  Routing for Networks:
15    17.0.0.0
16    200.10.10.0
17    200.10.30.0
18  Routing Information Sources:
19    Gateway         Distance      Last Update
20  Distance: (default is 120)
```

La línea 1 nos dice que el protocolo de encaminamiento que está ejecutando el router es, precisamente, RIP. La línea 2 muestra que RIP envía sus actualizaciones cada 30 segundos y que la próxima actualización se enviará dentro de 10 segundos. Ese valor de 30 segundos corresponde a uno de los cuatro temporizadores o "timers" que regulan el funcionamiento del proceso RIP. Los otros tres temporizadores son los que se muestran en la línea 3 de la salida anterior y sus significados son los siguientes:

- INVALID: indica el tiempo que debe transcurrir antes de que el router determine que una ruta ya no es válida. RIP considera que una ruta ya no es válida si no ha recibido información sobre la misma en las actualizaciones que haya recibido de sus routers vecinos durante ese tiempo.

- HOLD DOWN: cuando el router determina que una ruta hacia una red ha fallado, debe ignorar cualquier información sobre una ruta alternativa a esa misma red durante el período de tiempo indicado por este temporizador.

- FLUSHed: establece el tiempo que debe transcurrir entre que una ruta se determina como no válida y su eliminación de la tabla de encaminamiento.

La línea 7 indica que el router envía actualizaciones RIP versión 1 y que es capaz de recibir y procesar actualizaciones RIP de cualquier versión. Las líneas 9 a 11 muestran, para cada una de las interfaces del router, las versiones de RIP de las actualizaciones que se envían y que se pueden recibir. Finalmente, las líneas 15 a 17 muesttran las direcciones de red de las redes a las cuales este router está directamente conectado

Vamos ahora a configurar RIP en los otros dos routers y luego inspeccionaremos las tablas de encaminamiento de los tres para ver en cada uno cómo se han actualizado automáticamente con la información proporcionada por los otros dos.

Vayamos en primer término al router B:

```
RouterB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)# router rip
RouterB(config-router)# network 177.16.0.0
```

```
RouterB(config-router)# network 200.10.10.0
RouterB(config-router)# network 200.10.20.0
RouterB(config-router)# exit
RouterB(config)# exit
RouterB#
*Mar  1 01:02:15.067: %SYS-5-CONFIG_I: Configured from console by console
```

Veamos el estado de la configuración de RIP en este router:

```
RouterB# show ip protocols
 1 Routing Protocol is "rip"
 2   Sending updates every 30 seconds, next due in 4 seconds
 3   Invalid after 180 seconds, hold down 180, flushed after 240
 4   Outgoing update filter list for all interfaces is not set
 5   Incoming update filter list for all interfaces is not set
 6   Redistributing: rip
 7   Default version control: send version 1, receive any version
 8     Interface             Send  Recv  Triggered RIP  Key-chain
 9     FastEthernet0/0       1     1 2
10     Serial0/0             1     1 2
11     Serial0/1             1     1 2
12   Automatic network summarization is in effect
13   Maximum path: 4
14   Routing for Networks:
15     177.16.0.0
16     200.10.10.0
17     200.10.20.0
18   Routing Information Sources:
19     Gateway         Distance      Last Update
20     200.10.10.5           120      00:00:23
21   Distance: (default is 120)
```

La salida anterior es similar a la que analizamos antes para el router A, pero ésta contiene información adicional. En la línea 20 tenemos información acerca de una fuente u origen desde la que este router ha recibido información de encaminamiento. Se trata del router A (donde ya hemos habilitado y configurado RIP), que envía sus actualizaciones al router B por la interface cuya dirección IP es 200.10.10.5. Vemos también en esta misma línea que la distancia administrativa de las rutas recibidas desde esa fuente es 120 (el valor de distancia administrativa para el protocolo RIP) y que la última actualización se recibió hace 23 segundos.

Inspeccionemos ahora la tabla de encaminamiento utilizando el comando `show ip route`:

```
RouterB# 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, 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

1      200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
2 C       200.10.20.6/32 is directly connected, Serial0/1
3 C       200.10.20.4/30 is directly connected, Serial0/1
4 C    177.16.0.0/16 is directly connected, FastEthernet0/0
5 R    17.0.0.0/8 [120/1] via 200.10.10.5, 00:00:09, Serial0/0
6 R    200.10.30.0/24 [120/1] via 200.10.10.5, 00:00:09, Serial0/0
7      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
8 C       200.10.10.4/30 is directly connected, Serial0/0
9 C       200.10.10.5/32 is directly connected, Serial0/0
```

Como vemos, además de las redes a las cuales el router está directamente conectado, en las líneas 5 y 6 aparecen las rutas aprendidas mediante RIP: la línea 5 es la ruta a la LAN 1 y la línea 6 es la ruta al enlace WAN 3.

Salvemos la configuración en ejecución en la configuración de arranque:

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

Pasemos ahora al router C y procedamos de igual forma que anteriormente:

```
RouterC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterC(config)# router rip
RouterC(config-router)# network 197.168.100.0
RouterC(config-router)# network 200.10.20.0
RouterC(config-router)# network 200.10.30.0
RouterC(config-router)# exit
RouterC(config)# exit
RouterC#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Utilicemos nuevamente el comando de modo Privilegiado `show ip protocols` para ver el estado del protocolo RIP en el router C:

```
RouterC# show ip protocols
 1 Routing Protocol is "rip"
 2   Sending updates every 30 seconds, next due in 25 seconds
 3   Invalid after 180 seconds, hold down 180, flushed after 240
```

```
 4   Outgoing update filter list for all interfaces is not set
 5   Incoming update filter list for all interfaces is not set
 6   Redistributing: rip
 7   Default version control: send version 1, receive any version
 8     Interface             Send  Recv  Triggered RIP  Key-chain
 9     FastEthernet0/0       1     1 2
10     Serial0/0             1     1 2
11     Serial0/1             1     1 2
12   Automatic network summarization is in effect
13   Maximum path: 4
14   Routing for Networks:
15     197.168.100.0
16     200.10.20.0
17     200.10.30.0
18   Routing Information Sources:
19     Gateway         Distance      Last Update
20     200.10.30.5          120      00:00:08
21     200.10.20.5          120      00:00:05
22   Distance: (default is 120)
```

En la salida anterior vemos, en las líneas 20 y 21, las dos fuentes desde las cuales el router C está recibiendo información de encaminamiento; estas son el router A (línea 20) y el router B (línea 21).

Veamos ahora el contenido de la tabla de encaminamiento:

```
RouterC# 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

 1      200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
 2 C       200.10.20.0/24 is directly connected, Serial0/0
 3 C       200.10.20.5/32 is directly connected, Serial0/0
 4 R    177.16.0.0/16 [120/1] via 200.10.20.5, 00:00:24, Serial0/0
 5 R    17.0.0.0/8 [120/1] via 200.10.30.5, 00:00:28, Serial0/1
 6      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
 7 C       200.10.30.4/30 is directly connected, Serial0/1
 8 C       200.10.30.5/32 is directly connected, Serial0/1
 9 R    200.10.10.0/24 [120/1] via 200.10.20.5, 00:00:25, Serial0/0
10                     [120/1] via 200.10.30.5, 00:00:00, Serial0/1
11 C    197.168.100.0/24 is directly connected, FastEthernet0/0
```

```
RouterC#
```

Las líneas 4, 5 y 9 muestras las rutas aprendidas mediante RIP a las redes LAN 2 (línea 4), LAN 1 (línea 5) y LAN 3 (línea 9). En consecuencia, router C ha aprendido en forma automática acerca de la existencia de esas tres redes y cómo llegar hasta ellas, es decir, hacia donde reenviar los datagramas destinados a algún host en las mismas.

Verificación de RIP

Volvamos ahora al router A y veamos otra vez su tabla de encaminamiento:

```
RouterA# 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, 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

 1 R    200.10.20.0/24 [120/1] via 200.10.10.6, 00:00:16, Serial0/0
 2                     [120/1] via 200.10.30.6, 00:00:11, Serial0/1
 3 R    177.16.0.0/16 [120/1] via 200.10.10.6, 00:00:16, Serial0/0
 4 C    17.0.0.0/8 is directly connected, FastEthernet0/0
 5      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
 6 C       200.10.30.6/32 is directly connected, Serial0/1
 7 C       200.10.30.4/30 is directly connected, Serial0/1
 8      200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
 9 C       200.10.10.4/30 is directly connected, Serial0/0
10 C       200.10.10.6/32 is directly connected, Serial0/0
11 R    197.168.100.0/24 [120/1] via 200.10.30.6, 00:00:12, Serial0/1
```

En la línea 1 de la salida anterior tenemos una nueva entrada, correspondiente a la red 200.10.20.0. Esta red es el enlace entre los routers B y C, y router A "aprendió" como llegar a esta red mediante el proceso RIP, lo cual está indicado por la letra "R" al comienzo de la línea. La información contenida en esta línea puede leerse así: "a la red 200.10.20.0 se llega enviando los datagramas a la dirección 200.10.10.6, saliendo por la interface `serial 0/0`". Recordemos que esa dirección IP es la de la interface del router B en el otro extremo del enlace.

La línea 2 muestra una ruta alternativa para llegar a la misma red y es a través de la dirección 200.10.30.6, "saliendo" por la interface `serial 0/1`. Por aquí se llega al router C y, a través de él, a la red de destino 200.10.20.0.

El router A también "aprendió" como llegar a las otras redes LAN; esto está indicado en las líneas 3 y 11.

Veamos ahora un nuevo comando de modo privilegiado: `debug ip rip`. Este comando provoca que la información de las actualizaciones que RIP envía y recibe se desplieguen en la consola.

```
RouterA# debug ip rip
RIP protocol debugging is on
RouterA#
```

Una vez activada esta funcionalidad, veremos desplegarse en pantalla la información que el proceso RIP envía por sus interfaces:

```
 1 *Mar  1 01:03:27.959: RIP: sending v1 update to 255.255.255.255 via
   FastEthernet0/0 (17.0.0.1)
 2 *Mar  1 01:03:27.959: RIP: build update entries
 3 *Mar  1 01:03:27.959:    network 177.16.0.0 metric 2
 4 *Mar  1 01:03:27.959:    network 197.168.100.0 metric 2
 5 *Mar  1 01:03:27.959:    network 200.10.10.0 metric 1
 6 *Mar  1 01:03:27.959:    network 200.10.20.0 metric 2
 7 *Mar  1 01:03:27.959:    network 200.10.30.0 metric 1
 8 *Mar  1 01:03:27.959: RIP: sending v1 update to 255.255.255.255 via
   Serial0/0 (200.10.10.5)
 9 *Mar  1 01:03:27.959: RIP: build update entries
10 *Mar  1 01:03:27.963:    network 17.0.0.0 metric 1
11 *Mar  1 01:03:27.963:    network 197.168.100.0 metric 2
12 *Mar  1 01:03:27.963:    network 200.10.30.0 metric 1
13 *Mar  1 01:03:27.963: RIP: sending v1 update to 255.255.255.255 via
   Serial0/1 (200.10.30.5)
14 *Mar  1 01:03:27.963: RIP: build update entries
15 *Mar  1 01:03:27.963:    network 17.0.0.0 metric 1
16 *Mar  1 01:03:27.963:    network 177.16.0.0 metric 2
17 *Mar  1 01:03:27.963:    network 200.10.10.0 metric 1
18 *Mar  1 01:03:30.271: RIP: received v1 update from 200.10.10.6 on
   Serial0/0
19 *Mar  1 01:03:30.271:      177.16.0.0 in 1 hops
20 *Mar  1 01:03:30.271:      197.168.100.0 in 2 hops
21 *Mar  1 01:03:30.271:      200.10.20.0 in 1 hops
22 *Mar  1 01:03:35.563: RIP: received v1 update from 200.10.30.6 on
   Serial0/1
23 *Mar  1 01:03:35.563:      177.16.0.0 in 2 hops
24 *Mar  1 01:03:35.567:      197.168.100.0 in 1 hops
25 *Mar  1 01:03:35.567:      200.10.20.0 in 1 hops
RouterA#
```

Analicemos la salida anterior. La línea 1 indica que RIP está enviando actualizaciones versión 1 (que es la versión de RIP habilitada) a la dirección de broadcast 255.255.255.255 a través de la interfaz `FastEthernet 0/0`. En las líneas 3 a 7 se muestran las cinco redes que router A conoce y, para cada una de ellas, la distancia a la misma. Vemos que para las redes

directamente conectadas la métrica es 1 (líneas 5 y 7) y que para las otras tres la métrica es 2 puesto que para llegar a ellas es necesario pasar por un router intermedio.

De manera similar, en las líneas 8 a 12 y 13 a 17 aparece la información enviada por las otras dos interfaces. En las líneas 18 a 21 se ve la información recibida desde router B a través de la interface `serial 0/0` y en las líneas 22 a 25 la recibida desde router C a través de la interface `serial 0/1`.

Aproximadamente 30 segundos después de desplegada la información anterior (tiempo entre actualizaciones que envía y recibe RIP) veremos desplegarse nuevamente información similar:

```
RouterA#
*Mar  1 01:03:56.267: RIP: received v1 update from 200.10.10.6 on Serial0/0
*Mar  1 01:03:56.267:      177.16.0.0 in 1 hops
*Mar  1 01:03:56.267:      197.168.100.0 in 2 hops
*Mar  1 01:03:56.267:      200.10.20.0 in 1 hops
*Mar  1 01:03:57.559: RIP: sending v1 update to 255.255.255.255 via
FastEthernet0/0 (17.0.0.1)
*Mar  1 01:03:57.559: RIP: build update entries
*Mar  1 01:03:57.559:   network 177.16.0.0 metric 2
*Mar  1 01:03:57.559:   network 197.168.100.0 metric 2
*Mar  1 01:03:57.559:   network 200.10.10.0 metric 1
*Mar  1 01:03:57.559:   network 200.10.20.0 metric 2
*Mar  1 01:03:57.559:   network 200.10.30.0 metric 1
*Mar  1 01:03:57.559: RIP: sending v1 update to 255.255.255.255 via Serial0/0
(200.10.10.5)
*Mar  1 01:03:57.559: RIP: build update entries
*Mar  1 01:03:57.563:   network 17.0.0.0 metric 1
*Mar  1 01:03:57.563:   network 197.168.100.0 metric 2
*Mar  1 01:03:57.563:   network 200.10.30.0 metric 1
*Mar  1 01:03:57.563: RIP: sending v1 update to 255.255.255.255 via Serial0/1
(200.10.30.5)
*Mar  1 01:03:57.563: RIP: build update entries
*Mar  1 01:03:57.563:   network 17.0.0.0 metric 1
*Mar  1 01:03:57.563:   network 177.16.0.0 metric 2
*Mar  1 01:03:57.563:   network 200.10.10.0 metric 1
```

Para, posteriormente deshabilitar esta funcionalidad de "debugging", se utiliza la forma "no" del mismo comando:

```
RouterA# no debug ip rip
RIP protocol debugging is off
RouterA#
```

Pruebas de conectividad

Probemos ahora, nuevamente, la conectividad entre las redes LAN de nuestra interred, utilizando el comando `ping` extendido de IOS:

```
RouterA# ping
Protocol [ip]:
Target IP address: 197.168.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
RouterA#
```

Utilicemos ahora nuevamente el comando de modo Privilegiado `trace`, el cual despliega en pantalla la ruta seguida por los datagramas hasta el destino especificado en el mismo.

```
RouterA# trace 197.168.100.11
1 Type escape sequence to abort.
2 Tracing the route to 197.168.100.11
3   1 200.10.30.6 16 msec 16 msec 16 msec
4   2 197.168.100.11 16 msec 16 msec 16 msec
RouterA#
```

Hagamos ahora una última prueba. Probemos desconectar uno de los enlaces WAN, por ejemplo WAN1 y veamos cómo reaccionan los router a este cambio. Lo que debe ocurrir es que las tablas de encaminamiento de los router A y B deben cambiar, para reflejar el hecho de que la ruta entre las redes LAN1 y LAN2 ya no es a través del enlace entre estos dos routers sino a través del router C. Tanto en el router A como en el B, al desconectar el enlace, el sistema operativo despliega los siguientes mensajes:

```
Dec 18 16:59:41.207: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
Dec 18 16:59:42.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,changed
state to down
```

Quitado entonces en enlace WAN 1, veamos cómo se han actualizado las tablas de encaminamiento de los tres routers. Comencemos por el router A:

```
RouterA# 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, 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
```

```
1 R    200.10.20.0/24 [120/1] via 200.10.30.6, 00:00:09, Serial0/1
2 R    177.16.0.0/16 [120/2] via 200.10.30.6, 00:00:09, Serial0/1
3 C    17.0.0.0/8 is directly connected, FastEthernet0/0
4      200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
5 C       200.10.30.4/30 is directly connected, Serial0/1
6 C       200.10.30.6/32 is directly connected, Serial0/1
7 R    197.168.100.0/24 [120/1] via 200.10.30.6, 00:00:09, Serial0/1
RouterA#
```

En la línea 1 de la salida anterior vemos que, ahora, a la red 200.10.20.0 se llega a través de la interfaz 200.10.30.6. Esto contrasta con la información desplegada por este mismo comando cuando lo ejecutamos antes de quitar el enlace, tal como se ve en las tres siguientes líneas:

```
1 R    200.10.20.0/24 [120/1] via 200.10.10.6, 00:00:16, Serial0/0
2                     [120/1] via 200.10.30.6, 00:00:11, Serial0/1
3 R    177.16.0.0/16 [120/1] via 200.10.10.6, 00:00:16, Serial0/0
```

La línea 1 era la ruta hacia la red 200.10.20.6 "aprendida" con RIP y la línea 2 muestra una ruta alternativa hacia la misma red de destino. Si comparamos esto con la salida previa marcada en gris, vemos que ya no hay una ruta alternativa, sino que "la" ruta es a través de la interfaz 200.10.30.6.

En relación con la red 177.16.0.0 podemos ver, marcada en gris, que la métrica para esa red es 2 en lugar de 1 como se muestra en la salida previa.

Veamos ahora la tabla de encaminamiento del router B:

```
RouterB# 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, 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

1      200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
2 C       200.10.20.6/32 is directly connected, Serial0/1
3 C       200.10.20.4/30 is directly connected, Serial0/1
4 C    177.16.0.0/16 is directly connected, FastEthernet0/0
5 R    17.0.0.0/8 [120/2] via 200.10.20.6, 00:00:22, Serial0/1
6 R    200.10.30.0/24 [120/1] via 200.10.20.6, 00:00:22, Serial0/1
7 R    197.168.100.0/24 [120/1] via 200.10.20.6, 00:00:22, Serial0/1
RouterB#
```

Aquí también las rutas se han modificado. Por ejemplo, en la línea 5 vemos que la distancia a la red 17.0.0.0 es de 2 y para legar hasta ella hay que pasar por el router C a través de su interfaz 200.10.20.6.

Por otra parte, tampoco hay aquí referencias a las red 200.10.10.0, que es precisamente la que hemos desconectado.

Finalmente si observamos la tabla de encaminamiento del router C podemos apreciar que la misma ha cambiado solamente para reflejar que la red 200.10.10.0 ya no existe.

```
RouterC# 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, 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

     200.10.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.20.4/30 is directly connected, Serial0/0
C       200.10.20.5/32 is directly connected, Serial0/0
R    177.16.0.0/16 [120/1] via 200.10.20.5, 00:00:23, Serial0/0
R    17.0.0.0/8 [120/1] via 200.10.30.5, 00:00:09, Serial0/1
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.4/30 is directly connected, Serial0/1
C       200.10.30.5/32 is directly connected, Serial0/1
C    197.168.100.0/24 is directly connected, FastEthernet0/0
RouterC#
```

Configuración de una interface como "pasiva"

Como vimos anteriormente, las actualizaciones que RIP envía periódicamente son dirigidas a la dirección IP de "broadcast" configurada en cada interfaz; su valor predeterminado es 255.255.255.255. En nuestra interred RIP enviará sus actualizaciones por las dos interfaces seriales de cada router y también por sus respectivas interfaces `FastEthernet`. Tomemos, por ejemplo, el router A. Las actualizaciones que envía por sus interfaces seriales llegan a los routers B y C pero las actualizaciones que envía por su interfaz `FastEthernet` no llegan a ningún router porque en la LAN 1 no hay otro router conectado a la misma. Esta actualización genera, entonces, cada 30 segundos, tráfico en la red LAN 1 que, en realidad, es innecesario.

Para deshabilitar que RIP envíe sus actualizaciones por una determinada interfaz puede configurarse la misma como "pasiva". Para ellos se utiliza el comando de submodo de Configuración de Router `passive-interface`. Apliquemos este comando a la interfaz `fastethernet 0/0` del router A:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# router rip
RouterA(config-router)# passive-interface ?
  Async              Async interface
```

```
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Group-Async        Async Group interface
  Lex                Lex interface
  Loopback           Loopback interface
  MFR                Multilink Frame Relay bundle interface
  Multilink          Multilink-group interface
  Null               Null interface
  Serial             Serial
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  default            Suppress routing updates on all interfaces
  <cr>
```

Este comando requiere, entonces, como parámetro, la identificación de la interface que se quiere establecer como pasiva:

```
RouterA(config-router)# passive-interface fastethernet 0/0
RouterA(config-router)# exit
RouterA(config)# exit
RouterA#
*Mar  1 01:06:11.139: %SYS-5-CONFIG_I: Configured from console by console
```

Cuando se configura una interfaz como pasiva, IOS no transmite actualizaciones por esa interfaz pero sí puede recibir las actualizaciones que lleguen por la misma. Este no es el caso para nuestra interred pero, si por ejemplo, configuráramos como pasiva la interfaz `serial 0/0`, el router A no enviaría sus actualizaciones por esa interfaz pero sí recibiría las que el router B envía y que le llegan por la misma.

Configuración de RIP, versión 2

IOS puede ejecutar en forma simultánea RIP 1 y RIP 2, pero ambos no pueden estar habilitados en la misma interfaz. Cuando las dos versiones están habilitadas en un router, se cumplen las siguientes reglas relativas a las actualizaciones enviadas y recibidas:

- Las interfaces con RIP 1 habilitado envían actualizaciones versión 1 y pueden recibir y procesar actualizaciones de versiones 1 y 2. Si reciben una actualización de versión 2, el router ignorará los campos de máscara de subred y de autenticación.
- Las interfaces con RIP 2 habilitado envían y reciben solo actualizaciones de versión 2.

Para configurar un router con la versión 2 de RIP se utiliza el comando de submodo de Configuración de Router `version`. Así, por ejemplo, para usar RIP 2 en todas las interfaces del router A de nuestra interred, la secuencia de comandos es:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with <CNTL-Z>
RouterA(config)# router rip
RouterA(config)# version 2
RouterA(config)# <CNTL-Z>
RouterA#
```

Para habilitar la versión 1 de RIP en una de las interfaces del router, por ejemplo, en la interface `serial 0/0`, de modo que por esa interface se envíen actualizaciones de versión 1 y se reciban y procesen actualizaciones de versiones 1 y 2 se utilizan los comandos de submodo de Configuración de Interface `ip rip send version` e `ip rip receive version`:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with <CNTL-Z>
RouterA(config)# interface serial 0/0
RouterA(config-if)# ip rip send version 1
RouterA(config-if)# ip rip receive version 1 2
RouterA(config)# exit
RouterA#
*Mar  1 01:08:25.103: %SYS-5-CONFIG_I: Configured from console by console

RouterA# 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, 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

R    200.10.20.0/24 [120/1] via 200.10.10.6, 00:00:06, Serial0/0
                    [120/1] via 200.10.30.6, 00:01:41, Serial0/1
R    177.16.0.0/16 [120/1] via 200.10.10.6, 00:00:06, Serial0/0
C    17.0.0.0/8 is directly connected, FastEthernet0/0
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.6/32 is directly connected, Serial0/1
C       200.10.30.4/30 is directly connected, Serial0/1
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.6/32 is directly connected, Serial0/0
R    197.168.100.0/24 [120/1] via 200.10.30.6, 00:01:42, Serial0/1
```

Veamos el estado del proceso RIP:

```
RouterA# show ip protocols
 1 Routing Protocol is "rip"
```

```
 2   Sending updates every 30 seconds, next due in 23 seconds
 3   Invalid after 180 seconds, hold down 180, flushed after 240
 4   Outgoing update filter list for all interfaces is not set
 5   Incoming update filter list for all interfaces is not set
 6   Redistributing: rip
 7   Default version control: send version 2, receive version 2
 8     Interface             Send  Recv  Triggered RIP  Key-chain
 9     Serial0/0             1     1 2
10     Serial0/1             2     2
11  Automatic network summarization is in effect
12  Maximum path: 4
13  Routing for Networks:
14    17.0.0.0
15    200.10.10.0
16    200.10.30.0
17  Passive Interface(s):
18    FastEthernet0/0
19  Routing Information Sources:
20    Gateway         Distance      Last Update
21    200.10.10.6         120      00:00:14
22    200.10.30.6         120      00:01:48
23  Distance: (default is 120)
```

En las líneas 9 y 10 vemos que para el caso particular de la `serial 0/0`, esta interface envía actualizaciones RIP versión 1 y puede recibir y procesar actualizaciones de versiones 1 y 2, mientras que la interface `serial 0/1` solo tiene habilitada la versión 2.

Por otra parte, podemos observar que la interface `fastethernet 0/0` no aparece en la salida; esto se debe a que, anteriormente, establecimos esa interface como "pasiva".

Remover RIP

Para remover el proceso RIP se utiliza el comando de Configuración Global `no router rip`. Hagámoslo en el router A:

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# no router rip
RouterA(config)# exit
RouterA#
*Mar  1 01:09:40.811: %SYS-5-CONFIG_I: Configured from console by console

RouterA# 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, 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    17.0.0.0/8 is directly connected, FastEthernet0/0
     200.10.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.30.6/32 is directly connected, Serial0/1
C       200.10.30.4/30 is directly connected, Serial0/1
     200.10.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.10.10.4/30 is directly connected, Serial0/0
C       200.10.10.6/32 is directly connected, Serial0/0
```

El protocolo IGRP

El protocolo IGRP, Interior Gateway Routing Protocol (Protocolo de Encaminamiento de Pasarela Interior), es un protocolo de encaminamiento del tipo vector-distancia propietario de Cisco, similar en muchos aspectos a RIP. IGRP maneja direcciones de red completas, envía actualizaciones periódicas a sus routers vecinos cada 90 segundos y no incluye las máscaras de subred en esas actualizaciones.

Una diferencia importante entre IGRP y RIP es que IGRP utiliza una métrica compuesta para indicar las distancias a las redes remotas. RIP utiliza una métrica simple; la cantidad de saltos o routers intermedios mientras que IGRP utiliza, en forma predeterminada, cuatro parámetros para calcular su métrica. Estos cuatro parámetros son:

- Ancho de banda (bandwidth)
- Retardo (delay)
- Confiabilidad (reliability)
- Carga (load)

Estos cuatro parámetros son medidos en forma permanente por IOS para cada interface de red del router. Estos parámetros ya fueron comentados en el Capítulo 4 cuando aplicamos el comando `show interfaces` a la interface Serial y sus valores pueden verse, precisamente, con ese comando:

```
RouterA# show interface serial 0/0
.................
[texto omitido]
```

Configuración de IGRP

La configuración del protocolo IGRP es muy similar a la configuración del protocolo RIP y consiste en especificar el proceso IGRP mediante el comando de Configuración `Global router igrp` y luego habilitar IGRP en las interfaces del router mediante el comando del submodo de Configuración de Router `network`.

La diferencia con RIP es que IGRP requiere especificar, además, un número de sistema autónomo o ASN, Autonomous System Number. Un Sistema Autónomo es un conjunto de routers bajo una administración común. Este conjunto de routers se puede restringir a un grupo de routers que utilizan los mismos protocolos de encaminamiento interiores para compartir información de encaminamiento.

Vamos a considerar que nuestros tres routers pertenecen a un mismo sistema autónomo, por lo cual todos deberán tener el mismo ASN en sus configuraciones de IGRP para que puedan compartir información de encaminamiento entre ellos. El Número de Sistema Autónomo es un valor de 16 bits, de modo que podemos seleccionar un número entre 0 y 65.535; elijamos el número 100 para nuestro Sistema Autónomo. IOS puede soportar múltiples sistemas autónomos en forma simultánea ejecutando distintos procesos IGRP, cada uno con un ASN distinto.

Configuremos entonces IGRP en los tres routers. Puesto que el procedimiento es análogo al empleado para configurar RIP, lo haremos sin explicar cada paso. Comencemos por el router A:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# router igrp 100
RouterA(config-router)# network 17.0.0.0
RouterA(config-router)# network 200.10.10.0
RouterA(config-router)# network 200.10.30.0
RouterA(config)# exit
RouterA#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Pasemos ahora al router B:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterB(config)# router igrp 100
RouterB(config-router)# network 177.16.0.0
RouterB(config-router)# network 200.10.10.0
RouterB(config-router)# network 200.10.20.0
RouterB(config-router)# exit
RouterB(config)# exit
RouterB#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Configuremos ahora IGRP en el router C:

```
RouterC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterC(config)# router igrp 100
RouterC(config-router)# network 197.168.100.0
RouterC(config-router)# network 200.10.20.0
RouterC(config-router)# network 200.10.30.0
RouterC(config-router)# exit
RouterC(config)# exit
RouterC#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Verificación de IGRP

Para verificar la configuración y el funcionamiento del proceso IGRP podemos utilizar los mismos comandos de modo Privilegiado `show ip protocols` y `show ip route` que utilizamos para el protocolo RIP.

Para este último comando, la tabla de encaminamiento creada por IGRP tiene exactamente las mismas rutas que la tabla creada por RIP. Las diferencias están en los valores de las distancias administrativas y la métrica asociada a cada ruta.

Por otra parte, las rutas aprendidas con IGRP aparecerán precedidas de la letra "I", la distancia administrativa es 100 y la métrica es una métrica compuesta. Esta métrica no nos da una buena idea de cuan cerca o lejos está una red, excepto que un valor muy grande indica generalmente la presencia de un enlace WAN "lento".

Cuando configuramos RIP utilizamos el comando `debug ip rip` para ver las actualizaciones de las tablas de encaminamiento; podemos hacer lo mismo para IGRP, recordando especificar el número de Sistema Autónomo:

```
RouterA# debug ip igrp 100
```

Luego, para deshabilitar esta funcionalidad, utilizamos la forma "no" del mismo comando:

```
RouterA# no debug ip igrp 100
RouterA#
```

Remover IGRP

Para remover el proceso IGRP se utiliza el comando de Configuración `Global no router igrp`. Hagámoslo en el router A:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# no router igrp 100
RouterA(config)# exit
RouterA#
```

El protocolo EIGRP

El protocolo EIGRP, Enhanced Interior Gateway Routing Protocol (Protocolo Mejorado de Encaminamiento de Pasarela Interior), es un protocolo de encaminamiento desarrollado por Cisco y mantiene varias de las características que ya hemos mencionado para IGRP. Por ejemplo, EIGRP utiliza la misma métrica compuesta que IGRP y también requiere el uso de un Número de Sistema Autónomo para su configuración.

El modo de operación de EIGRP es mas complejo que el de los protocolos de encaminamiento que vimos anteriormente; tiene un mecanismo mas complejo de administración de rutas y vecinos, pero resulta en un tiempo de convergencia mucho menor.

Cuando se configura EIGRP en una interfaz de un router, lo primera que hace el proceso EIGRP es iniciar un procedimiento para descubrir sus routers vecinos. Un router vecino es

aquél que está conectado al otro extremo del enlace y que está ejecutando EIGRP con el mismo Número de Sistema Autónomo. Los routers vecinos se descubren enviando un tipo especial de paquete de datos denominado "Hello" a la dirección IP de multidifusión 224.0.0.10. Cuando un router que está ejecutando EIGRP recibe un paquete Hello, colocará la dirección IP del router de origen en una tabla denominada "tabla de vecinos"; de este modo, los routers que son vecinos entre sí forman lo que se denomina "una adyacencia". Estos paquetes Hello son transmitidos por los procesos EIGRP cada cinco segundos, de modo de mantener actualizadas sus tablas de vecinos.

Al igual que los otros protocolos de encaminamiento, EIGRP envía actualizaciones de sus tablas de encaminamiento a sus router vecinos pero, en lugar de hacerlo en forma periódica, solo las envía cuando se establece una adyacencia y cuando hay un cambio en la topología de la red. En el primer caso se envía la tabla de encaminamiento completa, mientras que en el segundo caso solo se envía la información relativa a los cambios ocurridos.

Cuando un router recibe una actualización de alguno de sus vecinos, coloca la información recibida en una tabla denominada "tabla de topología". Esta tabla contiene todas las rutas aprendidas de cada router vecino y dos métricas para cada una. La primera métrica, denominada "distancia avisada", es la reportada por el router vecino y es la métrica calculada por ese vecino a la red de destino. La segunda métrica es la calculada por el propio router considerando el camino hacia la red de destino que pasa por el router vecino que comunicó la ruta. Esta segunda métrica se denomina "distancia factible".

Todas las rutas a una red destino se comparan y aquella con la menor distancia factible se incorpora a la tabla de encaminamiento. Si hubiera dos o más rutas con igual distancia factible, IOS incorpora hasta seis de ellas en la tabla.

El router vecino a través del cual se tiene el mejor camino hacia un destino se denomina "sucesor" y el router a través del cual se tiene la segunda mejor ruta se denomina "sucesor factible". Una vez que todas las rutas a un destino fueron agregadas a la tabla de topología y que se han seleccionado los routers sucesor y sucesor factible, se dice que la ruta está en un estado "pasivo".

Cuando ocurre que el router designado sucesor sale de servicio, el sucesor factible se convierte en el router sucesor y la ruta a través de él pasa a ser la mejor ruta. Para el caso en que no haya un sucesor factible, el router debe buscar un nuevo sucesor. La ruta cambia, entonces, su estado a "activa" y el router envía a sus routers vecinos una consulta solicitando nueva información sobre esa ruta. Los routers vecinos devuelven la información solicitada y si existe un camino alternativo, se vuelven a seleccionar los routers sucesor y sucesor factible y la ruta vuelve a su estado pasivo. Si no hay un camino alternativo, entonces la ruta se elimina de la tabla de topología y de la tabla de encaminamiento.

Configuración de EIGRP

El procedimiento para configurar EIGRP es idéntico al empleado para configura IGRP, de modo que configuraremos los tres routers de nuestra interred sin extendernos en explicar cada paso.

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# router eigrp 100
RouterA(config-router)# network 17.0.0.0
RouterA(config-router)# network 200.10.10.0
```

```
RouterA(config-router)# network 200.10.30.0
RouterA(config)# exit
RouterA#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Pasemos ahora al router B:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterB(config)# router eigrp 100
RouterB(config-router)# network 177.16.0.0
RouterB(config-router)# network 200.10.10.0
RouterB(config-router)# network 200.10.20.0
RouterB(config-router)# exit
RouterB(config)# exit
RouterB#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

Configuremos ahora EIGRP en el router C:

```
RouterC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterC(config)# router eigrp 100
RouterC(config-router)# network 197.168.100.0
RouterC(config-router)# network 200.10.20.0
RouterC(config-router)# network 200.10.30.0
RouterC(config-router)# exit
RouterC(config)# exit
RouterC#
*Mar  1 00:38:25.311: %SYS-5-CONFIG_I: Configured from console by console
```

La característica de configurar una interfaz como pasiva que vimos para el protocolo RIP es igualmente aplicable a EIGRP. Configuremos, entonces, la interfaz FastEthernet del router A como pasiva:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)# router eigrp 100
RouterA(config-router)# passive-interface fastethernet 0/0
RouterA(config-router)# exit
RouterA(config)# exit
RouterA#
```

Verificación de EIGRP

Dos de los comandos de IOS que nos permiten verificar la configuración y el funcionamiento de EIGRP son los ya conocidos `show ip protocols` y `show ip route`; que hemos utilizado para verificar RIP.

Para EIGRP en particular (y también para OSPF que vemos a continuación) existen otros comandos que permiten ver información específica sobre este protocolo. Estos comandos de modo Privilegiado son los que aparecen en la tabla siguiente:

Comando	Descripción
`show ip eigrp neighbors`	Despliega información sobre los "vecinos" descubiertos por el proceso EIGRP
`show ip eigrp topology`	Despliega el contenido de la tabla de topología
`show ip eigrp traffic`	Despliega la cantidad de paquetes EIGRP enviados y recibidos

Estos tres comandos admiten como parámetro adicional un Número de Sistema Autónomo.

Remover EIGRP

Para remover el proceso IGRP se utiliza el comando de Configuración `Global no router eigrp`. Hagámoslo en el router A; el procedimiento para deshabilitarlo en los otros dos routers es completamente análogo:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# no router eigrp 100
RouterA(config)# exit
RouterA#
```

El protocolo OSPF

OSPF, Open Shortest Path First (Primero el Camino Abierto mas Corto) es un protocolo de encaminamiento del tipo estado de enlace, cuya especificación de su versión 2 está en el RFC 2328.

Una interred basada en OSPF tiene una estructura lógica jerárquica conformada por áreas, donde cada área es un conjunto de routers y redes. Un router puede pertenecer a varias áreas adyacentes, pero una red solo puede pertenecer a un área.

Cada área se identifica por un número de 32 bits y siempre debe existir un área identificada por el número 0 y denominada "área de backbone" compuesta por los routers del "backbone", cuya principal función es realizar el tráfico de información de encaminamiento entre las demás áreas. Los routers conectados a más de un área se denominan "routers de frontera" y los routers que solo pertenecen a un área se denominan "routers internos".

Cada router envía a los otros routers de su área información de actualización de sus rutas conocidas. Esta información se envía en paquetes denominados "avisos de estado de enlace" y son enviados a la dirección de multidifusión 224.0.0.5 en forma periódica cada 30 segundos o cuando ha ocurrido un cambio en la topología de la interred. Cuando un router recibe un aviso de estado de enlace de alguno de los routers de su área, guarda la información recibida en lo que se denomina "base de datos de estado de enlace". Con la información recibida de los otros routers, cada router construye un árbol de caminos mas cortos hacia las redes conocidas, colocándose él como raíz de ese árbol. De esta forma, cada router OSPF tiene información de la topología de toda la red.

OSFP utiliza una métrica simple denominada "costo", el cual se calcula a partir del ancho de banda ("bandwidth") asignado a una interfaz. Estos costos que utiliza OSPF son aditivos, es decir, para determinar el costo a una red remota, OSPF suma los costos individuales de todos los enlaces por los cuales debe pasar hasta llegar a esa red. Los costos a las redes conocidas son recalculados cada vez que se recibe una actualización de otro router, lo cual provoca la reconstrucción del árbol de caminos mas cortos y la correspondiente actualización de la tabla de encaminamiento. El algoritmo utilizado para este recálculo se conoce con el nombre de algoritmo de Dijkstra. Para este protocolo existe también el concepto de Sistema Autónomo mencionado anteriormente para los protocolos IGRP y EIGRP.

Configuración de OSPF

El tamaño y la simplicidad de nuestra interred no amerita el uso de un protocolo como OSPF pero, a efectos didácticos, vamos a implementarlo para poder ver el procedimiento de configuración y los comandos que permiten verificar su funcionamiento.

Antes de comenzar con la configuración debemos definir las áreas en las que vamos a agrupar las redes y los routers de nuestra interred. Definamos, entonces, dos áreas de la siguiente manera:

Area	Router	Interface
0	A	FastEthernet, Serial 0/0, Serial 0/1
	B	FastEthernet, Serial 0/0
1	B	Serial 0/1
	C	Fastethernet, Serial 0/0, Serial 0/1

Con esta estructura, los routers A y C serán routers internos en las áreas 0 y 1 respectivamente y el router B será un router frontera de área, tal como se muestra en la Figura 9-2:

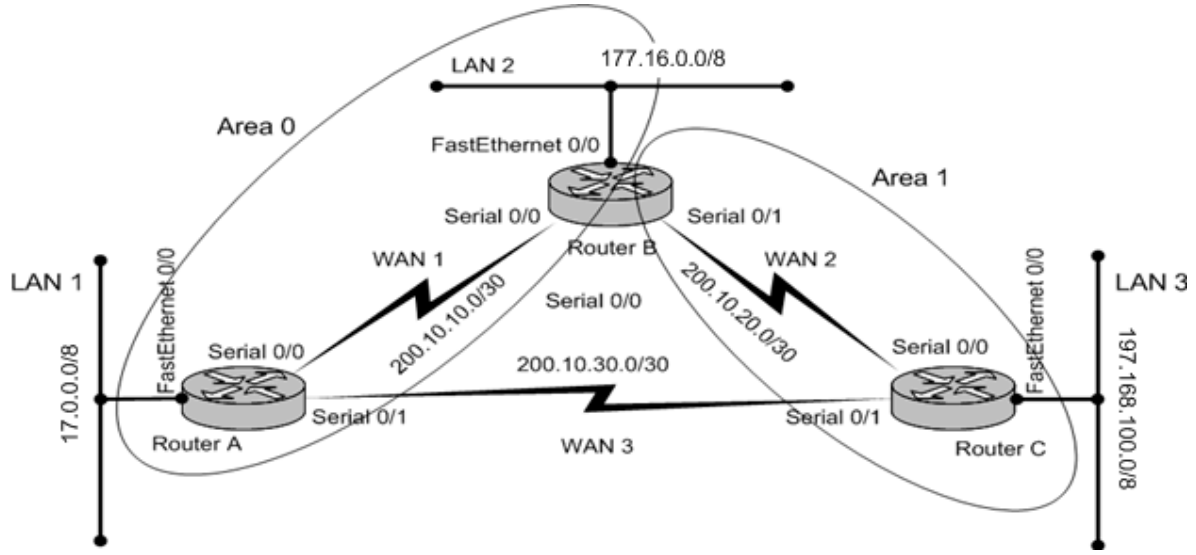


Figura 9 - 2

Para crear un proceso OSPF en un router se utiliza el comando de Configuración Global `router ospf`, el cual requiere como parámetro un número de proceso. Este número no tiene por que ser el mismo en todos los routers que utilizan OSPF.

El siguiente paso es especificar el área a la cual pertenece cada interfaz. Para esto se utiliza el comando de Configuración de Router `network`, cuya sintaxis en este caso es la siguiente:

`network direccion-ip mascara-comodín área número-de-área`

La pareja *`direccion-ip máscara-comodín`* permite definir cual o cuales interfaces van a pertenecer a un área determinada utilizando un solo comando `network`. Una máscara comodín tiene la misma estructura que una dirección IP o una máscara de subred, es decir, tiene un largo de 32 bits, agrupados en cuatro grupos de ocho bits cada uno. Los bits en 0 de la máscara comodín significan que IOS debe verificar los correspondientes bits en la dirección IP en busca de una coincidencia y los bits en 1 significan que IOS no debe verificar los correspondientes bits.

Veamos a continuación algunos ejemplos de máscaras comodín para aclarar el uso de las mismas:

	En decimal	**En binario**
Máscara comodín	0.0.0.0	00000000.00000000.0000000.00000000
Comentario	La dirección IP entera debe coincidir, es decir, deben examinarse los 32 bits en busca de una coincidencia	
Máscara comodín	0.0.0.255	00000000.00000000.00000000.11111111
Comentario	Solamente los primeros 24 bits de la dirección IP deben coincidir, es decir, solo deben examinarse los primeros 24 bits en busca de una coincidencia.	
Máscara comodín	0.0.15.255	00000000.00000000.00001111.11111111
Comentario	Solamente los primeros 20 bits de la dirección IP deben coincidir, es decir, solo deben examinarse los primeros 20 bits en busca de una coincidencia.	

Comencemos, entonces, por configurar OSPF en el router A asignando el número 100 como número de proceso y recordando que sus tres interfaces pertenecen al área 0

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# router ospf 100
RouterA(config-router)# network 17.0.0.1 0.0.0.0 area 0
RouterA(config-router)# network 200.10.10.5 0.0.0.0 area 0
RouterA(config-router)# network 200.10.30.5 0.0.0.0 area 0
RouterA(config-router)# exit
RouterA(config)# exit
RouterA#
```

Configuremos ahora OSPF en el router B, cuyas interfaces f`astethernet` y s`erial 0/0` pertenecen al área 0 y su interface `serial 0/1` al área 1:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterB(config)# router ospf 200
```

```
RouterB(config-router)# network 177.16.0.1 0.0.255.255 area 0
RouterB(config-router)# network 200.10.10.6 0.0.0.0 area 0
RouterB(config-router)# network 200.10.20.5 0.0.0.0 area 0
RouterB(config-router)# exit
RouterB(config)# exit
RouterB#
```

Finalmente, configuremos OSPF en el router C; todas sus interfaces pertenecen al área 1:

```
RouterC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterC(config)# router ospf 300
RouterC(config-router)# network 197.168.100.1 0.0.0.0 area 1
RouterC(config-router)# network 200.10.0.0 0.0.255.255 area 1
RouterC(config-router)# exit
RouterC(config)# exit
RouterC#
```

Verificación de OSPF

Al igual que para los otros protocolos de encaminamiento, dos de los comandos de IOS que nos permiten verificar la configuración y el funcionamiento de EIGRP son los ya conocidos `show ip protocols` y `show ip route` que hemos utilizado para verificar RIP.

Existen otros comandos que permiten ver información específica sobre este protocolo. Estos comandos de modo Privilegiado son los que aparecen en la tabla siguiente:

Comando	Descripción
`show ip ospf`	Despliega información general sobre los procesos de encaminamiento OSPF
`Show ip ospf database`	Despliega información sobre la base de datos del proceso OSPF
`show ip eigrp interface`	Despliega información sobre OSPF para una interface, la cual debe especificarse como parámetro
`show ip eigrp neighbor`	Despliega información sobre los routers vecinos

Remover OSPF

Para remover el proceso OSPF se utiliza el comando de Configuración `Global no router ospf`. Hagámoslo en el router A:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# no router ospf 100
RouterA(config)# exit
RouterA#
```

10. El proceso de arranque del router

Cuando se enciende un router de Cisco o cuando se lo reinicializa mediante el comando `reload`, el router realiza básicamente el mismo proceso de arranque que una computadora personal. Este proceso puede resumirse en los siguientes pasos:

1. El router realiza la autoprueba de encendido o POST, power-on self-test, para verificar el estado funcional de sus componentes de hardware, en particular, la CPU, la memoria y las interfaces de red.
2. El router carga y ejecuta el código de arranque (bootstrap) desde la memoria ROM.
3. El router localiza el archivo con la imagen del sistema operativo IOS, habitualmente en la memoria FLASH, y lo carga en la memoria RAM.
4. El router localiza en la memoria NVRAM el archivo de configuración de arranque `STARTUP-CONFIG` y lo carga en la configuración en ejecución, es decir, en el archivo `RUNNING-CONFIG` en la memoria RAM.

Todos los router siguen estos cuatro pasos cada vez que son encendidos o reinicializados. El código ejecutable del POST no puede ser cambiado por el administrador del router, pero sí pueden serlo las ubicaciones predeterminadas del código de arranque (bootstrap), del archivo de configuración de arranque (STARTUP-CONFIG) y de la imagen del sistema operativo. Lo habitual es, para los dos primeros elementos, utilizar la ubicación predeterminada que viene de fábrica y, en algunas circunstancias, lo que suele modificarse en la ubicación u origen del sistema operativo o software a cargar.

Hay tres tipos de software que pueden cargarse en un router de Cisco al momento de su arranque; estos son:

1. La versión completamente funcional de IOS, usada normalmente en un ambiente de producción que suele residir en la memoria FLASH, y que es la que hemos estado viendo hasta ahora.
2. Una versión "reducida" o de funcionalidad limitada que reside en la memoria ROM y que se denomina RXBOOT. Esta versión limitada proporciona conectividad IP básica y se utiliza cuando la memoria FLASH está dañada y se requiere cargar una imagen del IOS desde otro host, por ejemplo, desde un servidor TFTP disponible en la red.
3. Un software que proporciona acceso a un modo de configuración de bajo nivel denominado ROM Monitor y que se ejecuta desde la memoria ROM del router.

En los routers de Cisco hay dos elementos que permiten controlar cual de estos tres tipos de software se carga cuando se reinicializa el router. Estos elementos son el "registro de configuración" y el comando de Configuración Global `boot system`, que reside en el archivo de configuración.

El registro de configuración

El registro de configuración es un registro de software de 16 bits cuyo valor indicará al router, entre otras cosas, cual de los tres tipos de software mencionados debe cargar cuando se lo reinicialize. Los 16 bits de este registro están numerados de 0 a 15 y organizados en cuatro grupos de cuatro bits cada uno:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_

Con los cuatro bits de cada grupo podemos representar valores decimales de 0 a 15, pero en lugar de indicar el valor de cada grupo usando números decimales o binarios, se utilizan dígitos del sistema numérico hexadecimal. Este sistema numérico, de base 16, utiliza 16 dígitos: los números 0 a 9 para los valores decimales 0 a 9 y las letras A a F para los valores decimales 10 a 15. En la tabla siguiente se muestra la correspondencia entre los dígitos hexadecimales y sus respectivos valores decimales:

Decimal	Hexadecimal
0 - 9	0 – 9
10	A
11	B
12	C
13	D
14	E
15	F

Para distinguir entre un dígito hexadecimal y un dígito decimal o una letra, los valores en hexadecimal se escriben precedidos de “0x”; así, el valor hexadecimal 2 se escribe como 0x2 y el valor hexadecimal F se escribe como 0xF.

De la discusión anterior vemos que el valor de cada grupo de bits puede, entonces, representarse mediante un dígito hexadecimal. Por ejemplo, si el registro de configuración tiene el valor 0x2102, esto significa que los valores de cada grupo de bits son los siguientes:

Grupo	Bits	Valor hexadecimal
1	15 a 12	0x2
2	11 a 8	0x1
3	7 a 4	0x0
4	3 a 0	0x2

Si vamos al valor individual de cada bit, tenemos lo siguiente:

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Valor	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0
Hexa	2				1				0				2			

Este valor 0x2102, además de ser un ejemplo, es el valor predeterminado del registro de configuración, es decir, el valor con el que este registro viene de fábrica.

De los 16 bits de este registro, los cuatro bits de menor orden (3 a 0) conforman el denominado "campo de arranque" o "boot field" y es el valor de este campo el que controla cual de los tres tipos de software va a cargar el router cuando se reinicializa.

Si el valor de este campo es 0x0, el router procederá a cargar el Monitor ROM, mientras que si su valor es 0x1 se cargará la versión limitada de IOS que reside en la memoria ROM (RXBOOT). Para cualquier otro valor de este campo (0x2 a 0xF) el router buscará en el archivo STARTUP-CONFIG la presencia de algún comando `boot system` que le indique desde dónde cargar el sistema operativo IOS, es decir, desde la memoria ROM, desde la memoria FLASH o desde un servidor TFTP disponible en la red.

El comando `boot system`

Hay cuatro variantes del comando de Configuración Global `boot system`, que permiten indicar al router qué sistema operativo cargar y desde dónde hacerlo:

Comando	Resultado: se carga ....
`boot system ROM`	desde la memoria ROM, la versión limitada de IOS.
`boot system FLASH`	desde la memoria FLASH, el primer archivo de imagen de IOS que se encuentre.
`boot system FLASH` *archivo*	desde la memoria FLASH, el archivo de imagen de IOS de nombre *archivo*
`Boot system tftp` *archivo dir_ip*	desde un servidor TFTP, el archivo de imagen de IOS de nombre *archivo.*

Si se quiere establecer algún mecanismo de tolerancia a fallos para el proceso de carga de IOS, podemos especificar más de un comando `boot system` en el archivo de configuración de arranque. En tal caso, el router intentará la carga de IOS basándose en el valor del primer comando encontrado. Si este falla, intentará con el segundo y así sucesivamente hasta que uno resulte exitoso o hasta que se terminen los comandos `boot system`. El o los comandos `boot system` se ejecutarán a posteriori del registro de configuración.

Por ejemplo, podemos configurar el router para que, en primer término, intente cargar la imagen normal de IOS desde la memoria FLASH. Si esto falla, entonces que intente cargar un archivo de imagen de IOS desde un servidor TFTP y si esto también falla, que cargue la versión reducida de IOS que reside en la memoria ROM. Para esto, debemos establecer el valor del campo de arranque del registro de configuración en un valor distinto de 0x0 y de 0x1 y luego indicar los comandos `boot system` en la secuencia deseada de intentos:

```
Router# configure terminal
Enter configuration commands, one por line. End with CNTL/Z
Router(config)# config-register 0x0102
Router(config)# boot system flash
Router(config)# boot system tftp c1700-bk9no3r2sy7-mz.0412 197.168.100.10
Router(config)# boot system rom
```

```
Router(config)# end
Router# copy running-config startup-config
```

No debemos olvidar ejecutar el último comando, de modo que la nueva configuración sea la que utilice el router cuando se reinicialize.

Para ver el valor establecido en el registro de configuración se utiliza el comando de modo Privilegiado `show version`:

```
Router# show version
[texto omitido]
Configuration register is 0x2102 (will be 0x0101 at next reload)
```

La última línea muestra el valor actual del registro de configuración y el valor que tendrá luego de la reinicialización del router.

El modo ROM Monitor

El modo ROM Monitor, también denominado "programa de bootstrap" se ejecuta en el paso 2 del proceso de arranque del router que describimos anteriormente. En su operación normal, este programa inicializa el hardware del router y carga la imagen del sistema operativo IOS. Si en el router no hay cargada una imagen del sistema operativo IOS que pueda ejecutarse, es este programa de *bootstrap* el que se ejecuta.

Este modo también permite realizar ciertas tareas de configuración y de mantenimiento del router tales como la recuperación de contraseñas perdidas o la carga de software a través del puerto de Consola.

Una de las formas de acceder a este modo es interrumpir el proceso normal de arranque del router presionando la tecla Break dentro de los primeros 60 segundos de ejecución del proceso. La otra forma de hacerlo es estableciendo el valor 0x0 en el campo de arranque del registro de configuración. Esto provoca que, al reinicializarse el router, ingrese directamente al modo de ROM Monitor.

En el modo ROM Monitor, el indicador del sistema es la palabra `rommon` seguida del símbolo de mayor:

```
rommon # >
```

El símbolo # representa el número de línea y se incrementa secuencialmente con cada nueva línea que se ejecute.

Para obtener la lista de comandos disponibles en este modo se utiliza la facilidad de ayuda similar a la disponible en la Interfaz de Línea de Comandos:

```
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
context     display the context of a loaded image
cookie      display contents of cookie PROM in hex
dev         list the device table
dir         list files in the file system
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
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
```

Veamos, de manera concisa, algunos de los comandos disponibles en este modo.

`boot:`

Este comando permite cargar desde la memoria Flash una imagen del sistema operativo para su ejecución:

Comando	Descripción
`boot`	Carga la primera imagen disponible en la memoria Flash.
`boot flash` *archivo*	Carga la imagen de nombre *archivo* que se encuentre en la memoria Flash.

`confreg:`

Este comando permite modificar el valor del registro de configuración del router:

Comando	Descripción
`confreg`	Se ingresa al modo interactivo del comando.
`confreg` *numero*	Asigna al registro de configuración el valor *número* expresado en hexadecimal

La forma interactiva de este comando permite modificar el valor de los bits del registro de configuración sin tener que calcular y escribir el valor hexadecimal:

```
rommon 4 > confreg
Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]: y
enable "use net in IP bcast address"? y/n [n]:
enable "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]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 0
change the boot characteristics? y/n [n]: y
enter to boot:
0 = ROM Monitor
1 = the boot helper image
2-15 = boot system
[0]: 0
Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: y
You must reset or power cycle for new config to take effect
```

dir:

Este comando muestra el directorio de archivos de un dispositivo, por ejemplo, de la memoria Flash:

```
rommon 4 > dir flash:
File size     Checksum   File name
7729736 bytes (0x75f248) 0xb86d c1700-bk9no3r2sy7-mz.0412
```

reset:

Estando en el modo Monitor ROM, este comando reinicializa el router, de manera similar al comando de modo Privilegiado `reload`.

tftpdnld:

Este comando permite descargar en el router una imagen del sistema operativo IOS desde un servidor TFTP accesible a través de la red y la imagen descargada es almacenada, en forma predeterminada, en la memoria Flash del mismo.

Si por algún desperfecto en la memoria Flash del router fue necesario sustituir el módulo correspondiente por uno nuevo, este comando permite cargar una nueva copia de la imagen de IOS para que sea ésta la que se cargue y ejecute posteriormente en la operativa normal del router.

En el próximo capítulo describiremos el procedimiento para utilizar este comando en esas circunstancias.

11. Gestión de los archivos de imagen de IOS

El término “imagen de IOS” se utiliza para hacer referencia al archivo que contiene el código ejecutable del software del sistema operativo IOS.

La gestión de estos archivos implica, entre otras tareas, la realización de copias de respaldo de las mismas así como la carga de una imagen en la memoria Flash del router ya sea para actualizar la versión del software o para restaurar una imagen cuando la memoria Flash ha sido borrada o sustituida por un módulo nuevo.

Copia de una imagen hacia un servidor TFTP

Para hacer una copia de respaldo de la imagen actual de IOS residente en la memoria Flash del router a un servidor TFTP se utiliza el comando de modo Privilegiado `copy flash tftp`. Este comando es en realidad una variante del comando `copy startup-config tftp` que vimos en el Capítulo 6.

```
Router> enable
Password: <contraseña>
Router#
Router# copy flash tftp
Source filename []? c1700-bnr2sy-mz.070298
Address or name of remote host []? 197.168.100.10
Destination filename [c1700-bnr2sy-mz.070298]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
4501480 bytes copied in 56.88 secs (80383 bytes/sec)
```

El proceso de copia puede tardar varios minutos dependiendo del tamaño del archivo de imagen y de la velocidad de transmisión de la red. Los signos de admiración (“!”) indican que el proceso de copia se está realizando correctamente; IOS despliega un signo por cada diez paquetes de datos que se han transferido exitosamente.

Descarga de una imagen desde un servidor TFTP

Para descargar una nueva imagen de IOS desde un servidor TFTP a la memoria Flash del router se utiliza el comando de modo privilegiado `copy tftp flash`.

En caso en que en la memoria Flash no haya espacio libre suficiente para almacenar la nueva imagen de IOS, el comando solicitará una confirmación antes de proceder a eliminar todo el contenido de la memoria.

```
Router> enable
Password: <contraseña>
Router# copy tftp flash
```

```
Address or name of remote host []? 197.168.100.10
Source filename []? c1700-bnr2sy-mz.070298
Destination filename [c1700-bnr2sy-mz.070298]? y
Accessing tftp://197.168.100.10/ c1700-bnr2sy-mz.070298...
Erase flash: before copying? [confirm] y
!---If there is not enough memory available, erase the Flash
Erasing the flash filesystem will remove all files! Continue? [confirm] y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeee ...erased
Erase of flash: complete
Loading c1700-bnr2sy-mz.070298 from 197.168.100.10 (via Ethernet0/0): !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4501480/9001984 bytes]
Verifying checksum... OK (0xAC8A)
4501480 bytes copied in 56.88 secs (80383 bytes/sec)
router#
```

Para ejecutar la nueva imagen de IOS debemos apagar y encender el router o reinicializarlo con el comando de modo Privilegiado `reload`.

Descarga de una imagen en el modo ROM Monitor

En el modo ROM Monitor hay dos formas de transferir un archivo de imagen de IOS al router: a través de la red desde un servidor TFTP utilizando el comando `tftpdnld` o a través del puerto de Consola utilizando el comando `xmodem`.

Usando el comando `tftpdnld`

Si la memoria Flash ha sido borrada o el módulo de memoria ha sido sustituido por uno nuevo que se encuentra vacío, el router iniciará por sí mismo el modo Monitor ROM.

Para realizar la descarga de un archivo de imagen de IOS a la memoria Flash desde un servidor TFTP es necesario configurar ciertos parámetros para que la descarga pueda realizarse. Esta información incluye establecer la dirección IP de la interface de red a través de la cual se accede al servidor TFTP y el nombre del archivo de imagen a descargar. Esto se hace estableciendo los valores adecuados a ciertas "variables de entorno" del modo Monitor ROM en la siguiente forma general:

```
rommon 1 > NOMBRE_DE_VARIABLE=valor
rommon 2 >
```

Los nombres de las variables deben escribirse en mayúsculas y no debe haber espacios en blanco entre el nombre de la variable, el signo de igual y el valor que se asigne. Las variables de entorno cuyos valores deben establecerse son las siguientes:

Variable	Descripción
IP_ADDRESS	Dirección IP del router.
IP_SUBNET_MASK	Máscara de subred del router.
DEFAULT_GATEWAY	Puerta de enlace predeterminada del router en caso en que el router y el servidor TFTP no están en la misma subred
TFTP_SERVER	Dirección IP del servidor TFTP desde el cual se va a descargar el archivo de imagen.
TFTP_FILE	Nombre del archivo de imagen a descargar.

Para simplificar, asumamos que el servidor TFTP y el router están en la misma red 197.168.100.0/24, de modo que no necesitemos establecer un valor para la variable `DEFAULT_GATEWAY`.

```
rommon 1 > IP_ADDRESS=197.168.100.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > TFTP_SERVER=197.168.100.10
rommon 4 > TFTP_FILE= c1700-bnr2sy-mz.070298
```

Para verificar el valor de las variables se puede utilizar el comando `set`. Los valores que se establezcan para estas variables son temporarios y se pierden cuando se reinicializa el router. Una vez establecidos los valores de las variables, se ejecuta el comando `tftpdnld` que mencionamos en el capítulo anterior para proceder a la descarga del archivo:

```
rommon 5 > tftpdnld
IP_ADDRESS: 197.168.100.1
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 197.168.100.1
TFTP_SERVER: 197.168.100.10
TFTP_FILE: c1700-bnr2sy-mz.070298
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y
```

Una vez finalizada la descarga podemos ejecutar el comando `reset` para reinicializar el router y utilizar la imagen recién descargada.

Usando el comando `xmodem`

El modo Monitor ROM proporciona también una funcionalidad que permite descargar en el router un archivo de imagen de IOS a través del puerto de Consola. Esta funcionalidad es útil cuando no se dispone de un servidor TFTP accesible en la red y el archivo de imagen a descargar está almacenado localmente en la estación de trabajo con la cual se está accediendo a la consola.

Puesto que este procedimiento se basa en las velocidades de transmisión de datos del puerto de Consola y del puerto COM de la estación de trabajo, el proceso de transferencia del archivo puede tardar un tiempo prolongado, tal vez 30 minutos o más con una velocidad de

transferencia de 38.400 bps. Algunos modelos de routers de Cisco soportan velocidades de transferencia de hasta 115.000 bps

Para realizar la transferencia de un archivo de imagen se utiliza el comando de modo Monitor ROM `xmodem`. Este comando solo puede utilizarse para transferir archivos desde la estación de trabajo hacia el router y no para hacerlo desde el router a la estación de trabajo.

```
rommon 5 > xmodem c1700-ny-mz.bin

    Do not start the sending program yet...
```

El comando `xmodem` no realiza la transferencia del archivo sino que prepara al router para recibirlo. La transferencia del archivo debe iniciarse manualmente utilizando el software de emulación de terminal con el cual estemos realizando la sesión de consola.

Cuando el router esté preparado para recibir el archivo, desplegará un mensaje indicando que podemos iniciar la transferencia:

```
    Ready to receive file c1700-ny-mz.bin
```

Si estamos trabajando con HyperTerminal, para iniciar la transferencia del archivo seleccionamos la opción **Enviar Archivo...** del menú **Transferir**. En la ventana que aparece seleccionamos el archivo a transferir y luego XMODEM como protocolo.

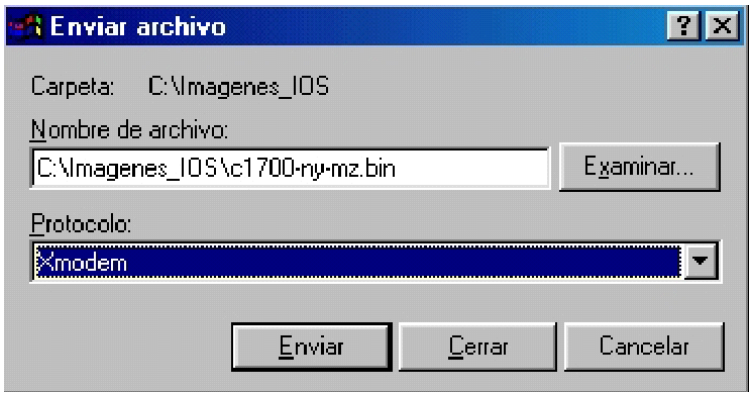


Fig. 11 - 1

Para iniciar la transferencia del archivo, presionamos el botón **Enviar**. Aparece entonces una ventana en la que puede verse el progreso de la transferencia.

Fig. 11 - 2

Una vez finalizada la transferencia, el Monitor ROM desplegará el siguiente mensaje:

```
Download Complete!
```

12. Registro de eventos

El registro de eventos o "logging" permite a IOS enviar mensajes a destinos designados cuando ha ocurrido un evento de importancia en el router. Estos mensajes reciben el nombre genérico de "mensajes de syslog" y el destino predeterminado de los mismos es la terminal de consola.

Además de desplegar los mensajes en pantalla, IOS mantiene en la memoria RAM del router una lista o "buffer" con los últimos mensajes generados. Puesto que el área de memoria destinada a almacenarlos es limitada, los mensajes más antiguos se van eliminando para hacer lugar a los nuevos mensajes que se van generando. Sin embargo, IOS dispone de mecanismos para mantener un registro histórico de todos los eventos reportados, los cuales veremos mas adelante en este capítulo.

Severidad y destinos

IOS dispone de ocho niveles de eventos a registrar, numerados de 0 a 7 y donde los niveles de numeración inferior corresponden a las condiciones o eventos de mayor severidad reportados. Estos ocho niveles se detallan en la tabla siguiente:

Nivel	Nombre	Descripción
0	Emergencias	El sistema está inutilizable
1	Alertas	Requiere acción inmediata
2	Crítico	Condiciones críticas
3	Errores	Condiciones de error
4	Advertencias	Condiciones de advertencia
5	Notificaciones	Condiciones normales pero significativas
6	Informativo	Mensajes informativos
7	Registro	Mensajes de registro (logging)

Ejemplos de mensajes de syslog son los siguientes:

```
% LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet 0, changed state to
up
% LINK-3-UPDOWN: Interface Ethernet 0, changed state to up
```

Los mensajes generados comienzan con un signo de porcentaje (%) y un código que indica el dispositivo o proceso al cual refiere el mismo. Luego viene el número que indica el nivel de severidad (0 a 7) de la situación reportada por el mensaje, un código mnemotécnico que identifica el mensaje particular para el dispositivo o proceso y finalmente el mensaje descriptivo del error o condición.

La funcionalidad de registro de eventos de IOS es muy flexible y permite configurar varios parámetros relativos al mismo, tales como:

- El nivel de severidad de los mensajes a registrar
- El destino a donde enviar los mensajes generados

- La cantidad de mensajes que IOS mantiene en la tabla en memoria (buffer)
- Deshabilitar y volver a habilitar el registro de mensajes

El registro de mensajes está habilitado en forma predeterminada y los destinos predeterminados a los cuales enviarlos son la consola y el buffer interno. IOS permite establecer otros destinos a los cuales también enviar los mensajes; entre ellos a un servidor de syslog, a una terminal virtual Telnet y también a una estación de gestión SNMP.

Para establecer el destino de los mensajes, así como el nivel de severidad de los mismos que se quieran registrar se utiliza el comando de Configuración Global `logging`, el cual tiene varias opciones posibles. El formato general de este comando es el siguiente:

```
Router(config)# logging destino nivel_de_severidad
```

El parámetro *destino* puede ser uno de los siguientes:

Destino	Descripción
`console`	Consola
`buffered`	Buffer interno
`monitor`	Terminal virtual VTY (Telnet)
`trap`	Servidor de syslog

Un "servidor de syslog" es un host en la red en el cual se esté ejecutando un proceso de servidor de syslog. Habitualmente se tratará de un host UNIX ejecutando un proceso de nombre *syslogd*, pero también puede ser un host Linux o Windows puesto que para estos sistemas operativos existen también aplicaciones de servidor de syslog.

El parámetro *nivel_de_severidad* permite establecer que los mensajes del nivel especificado y los de numeración inferior sean los que se registren. Para establecer el nivel de severidad no se especifica su número sino una palabra clave que lo identifica, de acuerdo a la siguiente tabla:

Nivel	Palabra clave
0	`emergencies`
1	`alerts`
2	`critical`
3	`errors`
4	`warnings`
5	`notifications`
6	`informational`
7	`debugging`

Este parámetro es opcional y si el mismo no se especifica en la línea de comandos IOS registrará en forma predeterminada los mensajes de niveles 4 e inferiores, es decir, `warning`, `errors`, `critical`, `alerts` y `emergencies`.

Veamos, como primer ejemplo, cómo indicar a IOS que envíe los mensajes de syslog de nivel 3 e inferiores a una terminal virtual Telnet. Para esto, en primer término es necesario configurar la terminal virtual y la sesión actual como "monitor". Esto se hace mediante el comando de modo Privilegiado `terminal monitor`. Este comando provoca que los mensajes

efectivamente se desplieguen en la terminal. Luego, en el modo de Configuración Global se ejecuta el comando `logging monitor` que habilita el envío de mensajes a la misma.

Asumiendo entonces que hemos iniciado una sesión Telnet en el router, los comandos para enviar los mensajes de nivel de severidad 4 o menor a la terminal son:

```
Router# terminal monitor
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# logging monitor errors
Router(config)# end
Router#
```

Si posteriormente se desea deshabilitar el despliegue de mensajes se utiliza el comando de modo Privilegiado `terminal no monitor` y si se quiere deshabilitar el envío de mensajes entonces se utiliza el comando de Configuración Global `no logging monitor`.

Como segundo ejemplo, configuremos nuestro router para enviar los mensajes de syslog generados de todos los niveles a un servidor de syslog accesible en la red. Para esto se necesitan ejecutar dos comandos, el primero de los cuales es para indicar a IOS la dirección IP del host en el cual está corriendo el proceso de syslog al cual debe enviar los mensajes. El segundo comando es para habilitar el envío de los mensajes al servidor de syslog indicado:

```
Router(config)# logging 197.168.100.20
Router(config)# logging trap debugging
```

En el ejemplo anterior, el servidor de syslog está corriendo en el host con dirección IP 197.168.100.20. Si se dispone de varios servidores de syslog en la red y se quiere que los mensajes se registren en todos ellos, se debe ejecutar un comando `logging` por cada uno de ellos:

```
Router(config)# logging 197.168.100.20
Router(config)# logging 177.16.100.100
Router(config)# logging trap debugging
```

Para eliminar alguno de los servidores de syslog de la lista se utiliza la forma "no" del mismo comando:

```
Router(config)# no logging 177.16.100.100
```

Para deshabilitar el envío de mensajes a los servidores de syslog que se hayan especificado, se utiliza la forma "no" del respectivo comando de Configuración Global, es decir, `no logging trap`.

Otros comandos de configuración

Es posible deshabilitar completamente la funcionalidad de envío de mensajes, de manera que incluso no se envíen a la consola ni al buffer interno. Para ello se utiliza el comando de Configuración Global `no logging on`. Si posteriormente se desea volver a habilitar la funcionalidad, entonces el comando adecuado es `logging on`.

Mencionamos anteriormente que, en forma predeterminada, los últimos mensajes de syslog generados son almacenados temporalmente en un buffer en memoria y que la cantidad de memoria destinada para esto es limitada. Para cambiar el tamaño del buffer de mensajes se utiliza el comando `logging buffered`, el cual debe recibir como parámetro el tamaño, en bytes, del área de memoria a reservar para este uso. El tamaño predefinido varía según el tipo y modelo de router, pero el valor que puede especificarse debe estar en el rango de 4.096 a 4.294.976.295 bytes:

```
Router(config)# logging buffered 9182
```

Para establecer la cantidad de mensajes que IOS mantiene en el buffer se utiliza el comando de Configuración Global `logging history size`, el cual debe recibir como parámetro la cantidad de mensajes a almacenar. Este valor es un número entre 1 y 500.

```
Router(config)# logging history size 25
```

Para eliminar todos los mensajes almacenados en el buffer interno se utiliza el comando de modo Privilegiado `clear logging`:

```
Router# clear logging
Clear logging buffer? [confirm] y
Router#
```

Finalmente, para ver el estado del registro de eventos podemos utilizar el commando de modo Usuario `show logging`:

```
Router> show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 8 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 12 message lines logged
```

Este último comando admite la palabra clave adicional `history`, que provoca que se despliegue, además de la información anterior, la lista de mensajes almacenados en el buffer interno.

13. Listas de Control de Acceso

Las Listas de Control de Acceso constituyen el mecanismo que proporciona IOS para realizar un filtrado básico de los paquetes de datos que llegan o salen del router.

Una Lista de Control de Acceso es una secuencia de instrucciones o reglas que aplican a las interfaces del router y donde cada regla está formada por un criterio de comparación y la acción correspondiente que IOS debe tomar con los paquetes de datos que cumplen con la condición establecida.

Los criterios de comparación de las reglas se basan en los campos de datos de los encabezados IP, TCP y UDP, tales como:

- Dirección IP de origen del datagrama
- Dirección IP de destino del datagrama
- Protocolo (ICMP, TCP, UDP, etc.)
- Puerto TCP o UDP de origen
- Puerto TCP o UDP de destino

Las acciones que pueden aplicarse sobre los paquetes de datos son básicamente dos: permitir el pasaje del paquete o no permitirlo, en función de que se cumpla o no la condición a evaluar.

Una Lista de Control de Acceso puede estar formada por una o varias reglas y la lógica de su funcionamiento es la siguiente. Cuando llega un paquete de datos a la interfaz del router sobre la que se aplicó la lista, IOS toma la primera regla de la lista y aplica el criterio de comparación. Si el criterio se verifica, entonces se ejecuta la acción definida para esa regla y el resto de las reglas de la lista se ignoran. Si el criterio de comparación no se verifica, entonces IOS toma la segunda regla y aplica el criterio de comparación. Si para esta segunda regla el criterio se verifica, se ejecuta la acción correspondiente y si no se verifica, se toma la tercera regla y así sucesivamente. Si luego de ejecutadas todas las reglas, el paquete de datos no verifica ninguno de los criterios, entonces el paquete se descarta.

Esto último implica que cada Lista de Control de Acceso tiene, como última regla y de manera implícita, una regla que descarta los paquetes de datos que no cumplan con ninguna de las reglas anteriores de la lista.

Por otra parte, cuando una regla se verifica, el resto de las reglas de la lista se ignoran. En consecuencia, el orden en que se establezcan las reglas en una lista es muy importante puesto que, si por ejemplo, la primera regla es tal que todos los paquetes de datos la verifican y la acción definida en la misma es descartarlos, entonces se estará bloqueando todo el tráfico.

Para establecer una Lista de Control de Acceso se deben seguir básicamente dos pasos:

1. Definir la lista, utilizando el comando de Configuración Global `access-list`.
2. Aplicar la lista a la interface de interés del router, utilizando el comando de submodo de Configuración de Interface `ip access-group`.

El formato general para definir una Lista de Control de Acceso es el siguiente:

```
Router(config)# access-list número acción condición
```

Los tres componentes del comando anterior significan lo siguiente:

- *número*: es un número que identifica a la Lista de Control de Acceso que se está definiendo.
- *acción*: es la acción que debe tomarse si la condición que viene a continuación se cumple. Esta acción puede ser: permitir el pasaje del paquete de datos, lo cual se indica con la palabra clave `permit`, o denegar el pasaje del paquete, lo cual se indica con la palabra clave `deny`.
- *condición*: es la condición que la regla debe evaluar

Para aplicar una Lista de Control de Acceso a una interface del router, el formato general es el siguiente:

```
Router(config-if)# ip access-group número sentido
```

Los dos componentes de este último comando significan lo siguiente:

- *número*: es el número que identifica a la Lista de Control de Acceso que se está aplicando a la interface.
- *sentido*: es el sentido de transmisión del paquete de datos y puede ser cuando llega a la interface, lo cual se indica con la palabra clave `in`, o cuando el paquete de datos va a salir por la interface, lo cual se indica con la palabra clave `out`.

Cuando se utiliza la palabra clave `in`, el paquete de datos ingresa al router por la interface y luego se le aplican las reglas de la lista asociada a esa interface. En cambio, cuando se utiliza la palabra clave `out`, las reglas de la lista de aplican antes de que el paquete de datos vaya a ser transmitido hacia afuera por la interface.

Hay algunas consideraciones importantes a tener en cuenta cuando se crean e implementan listas de control de acceso:

- Solo puede asignarse una lista de control de acceso por interface, protocolo y dirección de tráfico.
- Cuando se agrega una regla a una lista, la regla se ubica al final de la misma. Si se quiere agregar una regla en otra posición, es necesario editar la lista completa, es decir, crearla nuevamente ingresando todas las reglas en el orden deseado.
- Las Listas de Control de Acceso se implementan para filtrar el tráfico que pasa a través del router y no para filtrar paquetes de datos originados por el propio router.

IOS permite definir dos clases de Listas de Control de Acceso para IP: estándares y extendidas. Las Listas de Control de Acceso estándares se identifican por un número de 1 a 99 y la condición de cada regla es tal que permite exclusivamente verificar toda o parte de la dirección IP de origen del datagrama.

Por su parte, las Listas de Control de Acceso extendidas son más flexibles, se identifican por un número de 100 a 199 y en la condición de cada regla se pueden especificar otros parámetros, tales como la dirección IP de destino del datagrama, el tipo de protocolo y los números de puerto de origen y de destino, entre otros.

Listas de Control de Acceso estándares

Tal como mencionamos recién, las listas estándares solo utilizan la dirección IP de origen de los datagramas como elemento de comparación para determinar si los mismos deben permitirse o bloquearse. Esto habilita a bloquear o permitir el tráfico IP que provenga de un host en particular, de una subred o de una red completa.

Para establecer el criterio de comparación, IOS se vale de lo que se denomina "máscara comodín" o "wildcard mask". Una máscara comodín es un parámetro que define la parte de la dirección IP que IOS debe examinar en busca de una coincidencia que verifique la regla.

Recordemos del capítulo 9 que una máscara comodín tiene la misma estructura que una dirección IP o una máscara de subred, es decir, tiene un largo de 32 bits, agrupados en cuatro grupos de ocho bits cada uno. Los bits en 0 de la máscara comodín significan que IOS debe verificar los correspondientes bits en la dirección IP en busca de una coincidencia y los bits en 1 significan que IOS no debe verificar esos bits.

Veamos a continuación algunos ejemplos de máscaras comodín para aclarar el uso de las mismas:

	En decimal	**En binario**
Máscara comodín	0.0.0.0	00000000.00000000.0000000.00000000
Comentario	La dirección IP entera debe coincidir, es decir, deben examinarse los 32 bits en busca de una coincidencia	
Máscara comodín	0.0.0.255	00000000.00000000.00000000.11111111
Comentario	Solamente los primeros 24 bits de la dirección IP deben coincidir, es decir, solo deben examinarse los primeros 24 bits en busca de una coincidencia.	
Máscara comodín	0.0.15.255	00000000.00000000.00001111.11111111
Comentario	Solamente los primeros 20 bits de la dirección IP deben coincidir, es decir, solo deben examinarse los primeros 20 bits en busca de una coincidencia.	

Ejemplos de Aplicación

Volvamos ahora a nuestra interred del Capítulo 8 y establezcamos algunas Listas de Control de Acceso para limitar el tráfico en la misma. La interred del capítulo 8 se reproduce abajo en la figuna 13-1.

Vamos, en primer lugar, a filtrar todo el tráfico originado en la red local LAN 3 y destinado a la red local LAN 1. Puesto que para llegar a los hosts de la LAN 1, este tráfico debe pasar por el router A, debemos definir la lista en router A y luego aplicarla a alguna de sus interfaces.

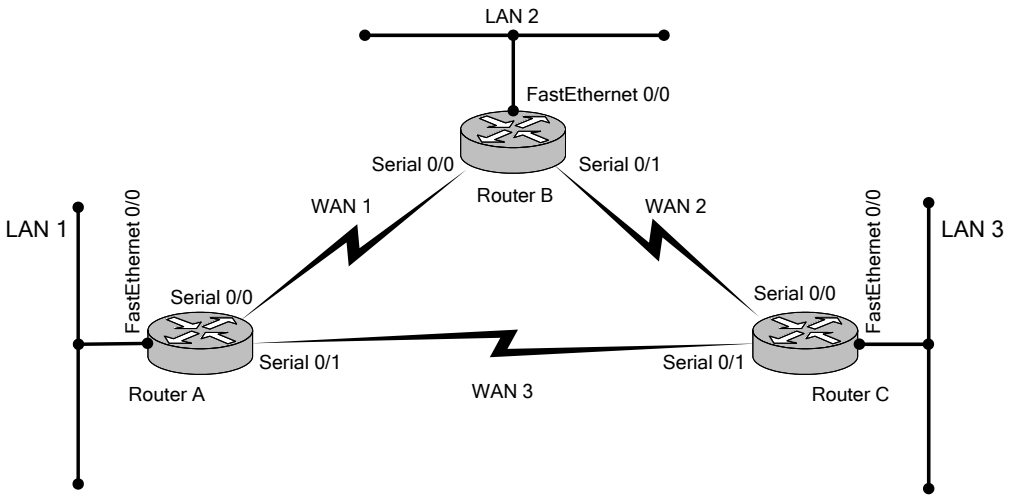


Fig. 13 - 1

Utilicemos la facilidad de ayuda de la Interfaz de Línea de Comandos para ir viendo como se define nuestra Lista de Control de Acceso:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z

RouterA(config)# access-list ?
  <1-99>      IP standard access list
  <100-199>   IP extended access list
  <1000-1099> IPX SAP access list
  <1100-1199> Extended 48-bit MAC address access list
  <1200-1299> IPX summary address access list
  <200-299>   Protocol type-code access list
  <300-399>   DECnet access list
  <400-499>   XNS standard access list
  <500-599>   XNS extended access list
  <600-699>   Appletalk access list
  <700-799>   48-bit MAC address access list
  <800-899>   IPX standard access list
  <900-999>   IPX extended access list
routerA(config)# access-list
```

Puesto que vamos a definir una lista estándar, su número de identificación debe estar entre 1 y 99; elijamos el 10 y continuemos solicitando ayuda:

```
RouterA(config)# access-list 10 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
routrA(config)# access-list 10
```

Puesto que lo que queremos es bloquear tráfico, indicamos la palabra clave `deny` y continuamos con la ayuda:

```
RouterA(config)# access-list 10 deny ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address
```

Aquí tenemos tres opciones: especificar una dirección IP para indicar o hacer coincidir una red o un host específico, utilizar la palabra clave `any` para permitir o denegar cualquier host o utilizar la palabra clave `host` para indicar un host en particular. Utilicemos la primera opción:

```
RouterA(config)# access-list 10 deny 197.168.100.0 0.0.0.255
RouterA(config)# <CNTL-Z>
RouterA#
```

En resumen, entonces, el número de identificación de la lista que hemos creado es `10` y en la lista hemos incluido solo una regla en la que la acción a realizar sobre los datagramas que cumplan con la condición es `deny`, es decir, denegar su pasaje. Por su parte, la condición a verificar es tal que los datagramas originados en cualquier host de la red 197.168.100.0 la cumplan y sean rechazados (deny); por eso la máscara comodín es 0.0.0.255 ya que de este modo IOS buscará una coincidencia en el valor de los tres primeros bytes de la dirección IP de origen.

Ahora que la lista ha sido definida, debemos aplicarla a una de las interfaces del router. Tenemos varias opciones para hacer esto, alguna mejor que las otras. En principio, lo más lógico parece ser aplicar la regla a la interfaz `serial 0/1` del router A puesto que los datagramas que se originen en la LAN 3 llegan a este router a través del enlace WAN 3. De este modo, serán rechazados antes de ingresar al router. Entonces:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# interface serial 0/1
RouterA(config-if)# ip access-group 10 in
RouterA(config-if)# end
RouterA(config)# <CNTL-Z>
RouterA#
```

De este modo, cuando un datagrama llegue al router por la interfaz serial 1, IOS aplicará la regla de la lista y si el criterio de comparación se cumple, se descartará el datagrama. Sin embargo, aquí podemos tener un problema. Si el enlace WAN 3 sale de funcionamiento, el router C tendrá un camino alternativo para hacer llegar los datagramas a la LAN 1. Este camino será a través del router B. Recordemos que sobre el final del Capítulo 9 dejamos funcionando un protocolo de encaminamiento dinámico en los tres routers de la interred y también vimos en ese capítulo que ocurre con las tablas de encaminamiento de los mismos cuando se quita este enlace.

En la situación potencial de que el enlace WAN 3 esté fuera de servicio, los datagramas se encaminarán a través del enlace WAN 2, pasarán por el router B, seguirán su camino por el enlace WAN 1 e ingresarán al router A por su interfaz `serial 0/0`. Sin embargo, nosotros aplicamos la Lista de Control de Acceso a la interfaz `serial 0/1`, de modo que a los datagramas que ingresen por aquella interface no se les aplicará la regla y en consecuencia no será filtrados.

Lo que queremos lograr es bloquear el tráfico desde LAN 3 a LAN 1, independientemente del camino que los datagramas hayan recorrido. Una alternativa es aplicar la misma Lista de Control de Acceso también a la interfaz `serial 0/0` del router A, de modo que los datagramas que lleguen a este router por esa interfaz sean filtrados también antes de ingresar al mismo. Ahora bein; sin importar por dónde ingresen los datagramas al router A, para que los mismos lleguen a la LAN 1 deben indefectiblemente salir por la interfaz `fastethernet 0/0` que es la que conecta el router a esa red local. Entonces, como segunda alternativa tenemos que, en lugar de aplicar el filtro a los datagramas que llegan al router por sus interfaces seriales, podemos aplicarlo a los datagramas que vayan a salir por la interfaz Ethernet. Si bien es preferible la primera alternativa (pues filtra los datagramas antes de que ingresen al router), vamos aplicar la segunda para ejercitar el comando que permite remover una lista de control de acceso de una interfaz.

Quitemos entonces la lista de la interfaz `serial 0/1` y apliquémosla a la interfaz `fastethernet 0/0`. Para quitar una Lista de Control de Acceso de una interfaz se utiliza la forma "no" del comando que permite aplicarla, es decir, `no ip access-group`:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# interface serial 0/1
RouterA(config-if)# no ip access-group 10 in
RouterA(config-if)# end
RouterA(config)#
RouterA(config)# interface fastethernet 0/0
RouterA(config-if)# ip access-group 10 out
RouterA(config-if)# end
RouterA(config)#
```

Bien; de este modo hemos resuelto el problema potencial de la caída del enlace WAN 3. Sin embargo, las cosas no están mejores que antes y el problema está en la forma en que hemos definido nuestra Lista de Control de Acceso y en su lógica de funcionamiento.

La pregunta es: ¿qué ocurrirá con los datagramas destinados a la LAN 1 pero originados en hosts de la LAN 2?

Mencionamos anteriormente que si un datagrama cumple con la condición de alguna de las reglas de la lista, se le aplicará la acción correspondiente que, en nuestro caso, es denegar el pasaje del mismo. Y también mencionamos que todas las listas tienen como última regla implícita denegar el pasaje de los paquetes que no cumplan con ninguna de las reglas anteriores. Los datagramas originados en la LAN 2 no cumplirán con la regla definida puesto que su dirección IP de origen no estará en la red 197.168.100.0 y, en consecuencia, serán bloqueados por esa última regla implícita.

A nuestra lista le está faltando, entonces, una segunda regla (usualmente ubicada en el último lugar) que permita el pasaje de todos los demás datagramas, es decir, de aquellos que no

cumplan con la condición de la primera regla. Agreguemos entonces a la lista una segunda regla que permita esto.

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# access-list 10 permit any
RouterA(config)# <CNTL-Z>
RouterA#
```

Veamos como ha quedado ahora nuestra Lista de Control de Acceso; para esto utilizamos el comando de modo Privilegiado `show access-list`:

```
RouterA# show access-list 10
  Standard IP access list 10
  deny 197.168.100.0 0.0.0.255 (50 matches)
  permit any (577 matches)
```

La nueva regla ha quedado en segundo lugar, que es precisamente donde queremos que esté. Recordemos que cuando se agrega una regla a una lista, la regla se ubica al final de la misma.

Nuestra lista va a funcionar, ahora, de la siguiente manera. Cuando llega al router un datagrama no destinado a él mismo, el proceso de encaminamiento de IOS determinará hacia dónde debe reencaminarlo. Si el caso es que el datagrama está destinado a la red LAN 1, entonces IOS sabe que debe retransmitirlo hacia fuera por su interfaz Ethernet 0. Como esta interfaz tiene aplicada una Lista de Control de Acceso, IOS aplicará al datagrama las reglas de la lista en el orden en que éstas están establecidas. Tomará entonces la primera regla (la que dice `deny`) y si se cumple su condición, descartará el datagrama y no lo reenviará por la interfaz. Esto ocurrirá con cada datagrama cuya dirección IP de origen comience con 197.168.100.

Si esta condición no se cumple, aplicará entonces la segunda regla cuya condición establece que se permita (`permit`) el pasaje de datagramas con cualquiera (`any`) dirección IP de origen. Esta condición será cumplida por todos los datagramas que no hayan sido bloqueados por la primera regla, es decir que se hayan originado en una red distinta a la 197.168.100.0.

Nuestra lista está ahora bien diseñada y aplicada a la interfaz más adecuada para su correcto funcionamiento. La interfaz más adecuada ha sido, en este caso, la que está "más cerca" del destino de los datagramas que se quieren bloquear. Este último comentario constituye, en realidad, una regla general a tener en cuenta al momento de implementar una Lista de Control de Acceso estándar, es decir, aplicar las listas estándares lo más cerca posible del destino.

Listas de Control de Acceso extendidas

Las Listas de Control de Acceso extendidas permiten hacer un control mas detallado de los paquetes de datos que se han de permitir o denegar en la red. Por ejemplo, es posible restringir el tráfico para permitir solo el acceso a un servidor de páginas web y bloquear el acceso a otros servicios. También es posible bloquear el tráfico de un determinado protocolo como, por ejemplo, ICMP, de modo que un usuario que haga ping a un host no reciba las respuestas "echo replay" del mismo.

La estructura de una lista extendida es más compleja que la de una lista estándar. El formato general de una lista extendida es:

```
Router(config)# access-list número acción protocolo origen destino puerto
```

Vamos a utilizar la facilidad de ayuda de la Interfaz de Línea de Comandos para ir analizando sus parámetros y palabras claves e ir construyendo una lista con una regla de ejemplo para bloquear el tráfico HTTP destinado a un servidor de páginas web en el host 10.1.10.20 y originado en cualquier host de la interred, excepto desde aquellos que están en la misma red local que el servidor.

Comencemos con el parámetro *número*:

```
Router(config)# access-list ?
  <1-99>  IP standard access list
  <100-199> IP extended access list
  ... [texto omitido]
```

Puesto que vamos a definir una Lista de Control de Acceso extendida, su número de identificación debe estar comprendido entre 100 y 199. Elijamos el 110 para identificarla y continuemos utilizando la ayuda para ver el parámetro *acción*:

```
Router(config)# access-list 110 ?
  deny        Specify packet
  dynamic     Specify a DYNAMIC list of PERMITs or DENYs
  permit      Specify packets to forward
```

La regla que vamos a crear es para denegar tráfico. Utilicemos entonces la palabra clave `deny` y pasemos al parámetro *protocolo*:

```
Router(config)# access-list 110 deny ?
  <0-255>     An IP protocol number
  eigrp       Cisco's EIGRP routing protocol
  gre         Cisco's GRE tunneling
  icmp        Internet Control Message Protocol
  igmp        Internet Gateway Message Protocol
  igrp        Cisco's IGRP routing protocol
  ip          Any Internet Protocol
  ipinip      IP in IP tunneling
  nos         KA9Q NOS compatible IP over IP tunneling
  ospf        OSPF routing protocol
  tcp         Transmission Control Protocol
  udp         User Datagram Protocol
```

Debemos indicar entonces el protocolo de capa de Transporte que la regla debe verificar. Puesto que el protocolo HTTP utilizado por el servidor de páginas web utiliza TCP como protocolo de Transporte, indiquemos la palabra clave `tcp` y pasemos al parámetro *origen*:

```
Router(config)# access-list 110 deny tcp ?
A.B.C.D  Source address
any      Any source host
host     A single source host
```

Puesto que vamos a bloquear el tráfico proveniente desde cualquier host, seleccionemos la palabra clave `any` y pasemos al parámetro *destino*:

```
Router(config)# access-list 110 deny tcp any ?
  A.B.C.D     Destination address
  any         Any destination host
  eq          Match only packets on a given port number
  gt          Match only packets with a greater port number
  host        A single destination host
  lt          Match only packets with a lower port number
  neq         Match only packets not on a given port number
  range       Match only packets in the range of port numbers
```

El destino de los paquetes a filtrar es el host 17.0.0.20. Agreguemos entonces la palabra clave `host` y la dirección IP del mismo:

```
Router(config)# access-list 110 deny tcp any host 17.0.0.20 ?
  eq          Match only packets on a given port number
  established Match established connections
  fragments   Check fragments
  gt          Match only packets with a greater port number
  log         Log matches against this entry
  log-input   Log matches against this entry,including inputinterface
  lt          Match only packets with a lower port number
  neq         Match only packets not on a given port number
  precedence  Match packets with given precedence value
  range       Match only packets in the range of port numbers
  tos         Match packets with given TOS value
  <cr>
```

Puesto que estamos interesados en filtrar solo el tráfico dirigido a un puerto TCP en particular, indicamos la palabra clave `eq` (equal, es decir, igual) para indicar el operador de comparación:

```
Router(config)# access-list 110 deny tcp any host 17.0.0.20 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         File Transfer Protocol (21)
  gopher      Gopher (70)
  hostname    NIC hostname server (101)
  ident       Ident Protocol (113)
  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       Nicname (43)
  www         World Wide Web (HTTP, 80)
```

Para indicar el puerto TCP de destino de los paquetes a filtrar podemos indicar su número o la palabra clave que lo representa. En nuestro caso, el número de puerto es `80` o la palabra clave es `www`:

```
Router(config)# access-list 110 deny tcp any host 17.0.0.20 eq 80 log
```

La última palabra clave en el comando anterior, `log`, es para indicarle a IOS que registre información sobre los paquetes que verificaron la regla y que, por lo tanto, fueron bloqueados.

Listas de Control de Acceso con Nombre

Las listas de control de acceso con nombre son aquellas que se identifican por un nombre en lugar de ser identificadas por un número. La sintaxis para definir y aplicar una lista con nombre es muy similar a la de las listas numeradas y su lógica de funcionamiento es la misma.

Una diferencia importante entre ambos tipos de listas es que en las listas con nombre es posible modificar o eliminar una de sus reglas sin que las otras reglas se vean afectadas.

La creación de una lista con nombre se hace ingresando a un nuevo submodo de configuración, el submodo de Configuración de Listas de Acceso. Para acceder a este submodo se utiliza el comando de Configuración Global `ip access-list` en el cual debemos

especificar las palabras claves `standard` o `extended` según quiera crearse una lista estándar o una extendida.

Tomemos como ejemplo la lista de control de acceso extendida que creamos anteriormente y veamos cómo es el procedimiento para crear y aplicar una lista con nombre:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# ip access-list extended trafico-web
RouterA(config-ext-nacl)# deny any host 17.0.0.20 eq 80
RouterA(config-ext-nacl)# end
RouterA#
```

Para aplicar la lista anterior a una interface del router se utiliza el comando de submodo de Configuración de Interfaz `ip access-group` que hemos utilizado anteriormente pero, en lugar de especificar un número de lista, se debe especificar su nombre.

14. Configuración de los protocolos WAN

En este capítulo vamos a abordar los aspectos esenciales relativos a la configuración de dos de las principales tecnologías de conectividad WAN soportadas por los routers de Cisco: Frame Relay e ISDN.

Frame Relay

Frame Relay es un protocolo de capa de Enlace orientado a conexión. Previo a que dos dispositivos puedan intercambiar datos, debe establecerse una conexión lógica entre ellos, la cual recibe el nombre de "circuito virtual". Estos circuitos virtuales pueden ser de dos tipos:

- Circuitos Virtuales Conmutados o SVC, Switched Virtual Circuit
- Circuitos Virtuales Permanentes o PVC, Permanent Virtual Circuit

Los circuitos virtuales de tipo conmutado (SVC) se activan cuando hay datos para ser transmitidos y se desactivan cuando la transmisión ha finalizado. Cuando un dispositivo conectado a la red Frame Relay tiene datos para enviar a otro dispositivo, iniciará el proceso de establecimiento del circuito mediante una llamada, de manera similar al inicio de una llamada telefónica. Luego de establecida la comunicación, los dispositivos en ambos extremos del enlace, en nuestro caso los routers, intercambian paquetes de datos de manera habitual. Cuando cesa el intercambio de datos el circuito permanece activo por un período de tiempo luego del cual, si se mantiene la inactividad, se desactiva. Estas acciones son tomadas por el prestador de servicios (por ejemplo, ANTEL Data)

Los circuitos virtuales de tipo permanente, en cambio, se mantienen siempre activos aún cuando no haya intercambio de datos y no requieren de la realización de la llamada inicial.

La forma de identificar un circuito virtual es mediante la asignación de un Identificador de Conexión de Enlace de Datos o DLCI, Data-Link Connection Identifier. Los DLCI solo tienen significado local y se usan para identificar un circuito particular entre el router y el switch Frame Relay al cual está conectado. Para ver esto con más detalle, hagamos algunos cambios a la interred que presentamos en el Capítulo 8. En la figura siguiente la red Frame Relay está representada por la "nube" central y los tres routers están conectados a la misma.

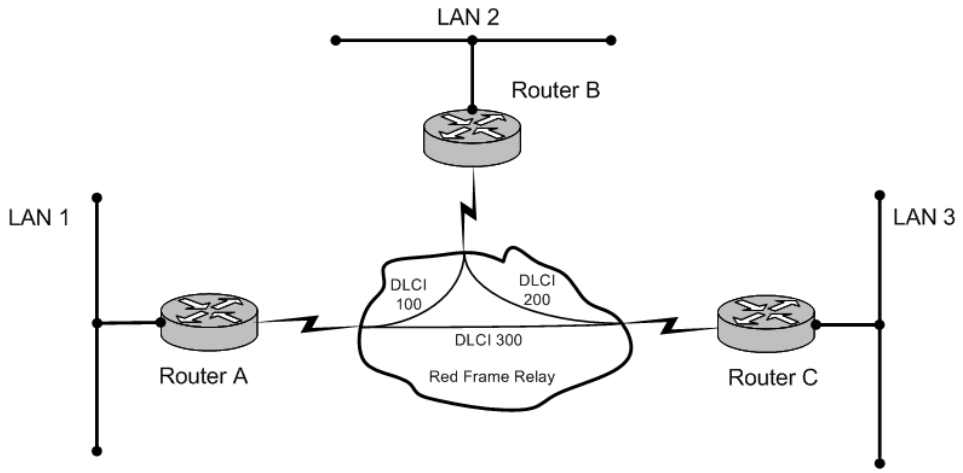


Fig. 14 - 1

Si bien nuestros routers tienen dos interfaces del tipo Serial, alcanza con utilizar solo una para conectar cada router a la red Frame Relay y, aún así, disponer de la conectividad entre las redes LAN. En otras palabras, es posible tener varios circuitos virtuales, todos usando una sola conexión física. Cuando un router deba enviar datos a otro, identificará el destino de los mismos mediante el DLCI del otro extremo del circuito virtual en el encabezado de la trama Frame Relay. Para configurar el DLCI local de un circuito virtual en una interfaz serial se utiliza el comando de submodo de Configuración de Interface `frame-relay interface-dlci`.

Una vez identificado cada circuito virtual con su DLCI es necesario establecer la correspondencia entre estos identificadores de capa de Enlace con las direcciones de red a nivel de la capa de Red. En el ejemplo de la figura debemos indicar que el DLCI 100 conecta con la dirección IP remota 200.10.10.6 y que el DLCI 300 con la dirección IP remota 200.10.30.6. Para establecer esta correspondencia se utiliza el comando de submodo de Configuración de Interfaz `frame-relay map`.

En 1990, Cisco junto con otras empresas del sector desarrollaron una serie de extensiones al estándar de Frame Relay para facilitar la configuración y la administración. Una de las extensiones es la denominada Interfaz Local de Gestión o LMI, Local Management Interface. LMI provee, entre otras funcionalidades, mensajes de estado de los circuitos virtuales y ARP inverso para descubrir en forma automática la dirección IP del otro extremo del enlace.

Los routers de Cisco soportan las versiones Cisco, ANSI y q933a del estándar LMI y, a partir de la versión 11.2 de IOS, la detección del tipo de LMI es automática, aunque también es posible configurar este parámetro en forma manual. Para configurar manualmente el tipo de LMI se utiliza el comando `frame-relay lmi-type`. Una vez establecido el tipo de LMI entre el router y el switch Frame Relay, IOS puede determinar tanto el DLCI del circuito como la dirección IP de router del otro extremo.

En nuestra interred modificada de la figura 14-1, en el router A utilizamos una interfaz física para establecer dos circuitos virtuales. Este tipo de configuración se denomina multipunto. Hay situaciones en las que es conveniente que una conexión multipunto se comporte como si cada conexión fuera punto a punto. Para esto, IOS permite crear interfaces lógicas o subinterfaces para cada circuito y hacer corresponder un DLCI con cada una de ellas. Una vez definidas, cada subinterfaz puede configurarse en forma independiente.

Para crear una subinterface se debe indicar el número de la misma, separado por un punto del número de interfaz física, de acuerdo al formato general #RANURA/#INTERFACE.#SUBINTERFACE

Configuración de Frame Relay

Con los elementos anteriores, comencemos por configurar la interfaz `serial 0/0` del router A:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)# interface serial 0/0
RouterA(config-if)# encapsulation frame-relay
RouterA(config-if)# interface serial 0.100 point-to-point
RouterA(config-subint)# frame-relay interface-dlci 100
RouterA(config-subint)# frame-relay lmi-type cisco
```

```
RouterA(config-subint)# no shutdown
RouterA(config-subint)# end
RouterA(config-if)# interface serial 0.300 point-to-point
RouterA(config-subint)# frame-relay interface-dlci 300
RouterA(config-subint)# frame-relay lmi-type cisco
RouterA(config-subint)# no shutdown
RouterA(config-subint)# exit
RouterA(config-if)# end
RouterA#
```

Con la secuencia de comandos anteriores establecimos la configuración básica de Frame Relay a nivel de la capa de Enlace. Lo que corresponde hacer ahora es establecer la configuración a nivel de la capa de Red. Puesto que hemos definido dos subinterfaces en la interface serial 0/0, debemos configurar cada una de ellas con la dirección IP que corresponda, una para el enlace WAN 1 y la otra para el enlace WAN 3, es decir, son las subinterfaces las que deben tener una dirección IP asignada en lugar de la interface física. El comando para configurar la dirección IP de una subinterfaz es el mismo que hemos utilizado anteriormente para configurar las interfaces FastEthernet y Serial.

Por su parte, la propia interface física serial 0/0 no debe tener una dirección IP; solo las subinterfaces deben tenerla. En consecuencia, a la subinterfaz 0.100 debemos asignarle la dirección IP 200.10.10.5 puesto que es la que conecta con el router B y a la subinterfaz 0.300, que conecta con el router C, la dirección IP 200.10.30.5.

Rescribamos entonces la secuencia de comandos anterior para establecer las configuraciones Frame Relay e IP:

```
RouterA# configure terminal
Enter configuration commands,
RouterA(config)# interface serial 0/0
RouterA(config-if)# encapsulation frame-relay
RouterA(config-if)# no ip address
RouterA(config-if)# interface serial 0.100 point-to-point
RouterA(config-subint)# frame-relay interface-dlci 100
RouterA(config-subint)# frame-relay lmi-type cisco
RouterA(config-subint)# description Conexion Frame Relay al router B
RouterA(config-subint)# ip address 200.10.10.5 255.255.255.252
RouterA(config-subint)# no shutdown
RouterA(config-subint)# end
RouterA(config-if)# interface serial 0.300 point-to-point
RouterA(config-subint)# frame-relay interface-dlci 300
RouterA(config-subint)# frame-relay lmi-type cisco
RouterA(config-subint)# description Conexion Frame Relay al router C
RouterA(config-subint)# ip address 200.10.30.5 255.255.255.252
RouterA(config-subint)# no shutdown
RouterA(config-subint)# exit
RouterA(config-if)# end
RouterA#
```

Verificación de Frame Relay

IOS dispone de varios comandos show que permiten verificar el estado y el funcionamiento de un enlace Frame Relay:

```
RouterA# show frame ?
  ip      show frame relay ip statistics
 lmi      show frame relay lmi statistics
 map      Frame-Relay map table
  pvc          show frame relay pvc statistics
  route        show frame relay route
  traffic      Frame-Relay protocol statistics
```

ISDN

La Red Digital de Servicios Integrados o ISDN, Integrated Service Digital network constituye una red digital para la transmisión de datos, voz y video entre sitios remotos y es un servicio habitualmente provisto por las compañías telefónicas.

ISDN ofrece dos tipos de servicios, denominados Interfaz de Tasa Básica o BRI, Basic Rate Interface e Interface de Tasa Principal o PRI, Primary Rate Interface.

Un servicio BRI proporciona dos canales denominados B para la transmisión de datos de usuario y un canal denominado D para la transmisión de información de control del enlace. Los canales B pueden transmitir datos a una tasa máxima de 64 Kbps cada uno, mientras que el canal D lo hace a una tasa de 16 Kbps.

Por su parte, un servicio PRI se presenta en dos modalidades, denominadas T1 y E1. Un servicio PRI del tipo T1 tiene 23 canales B y un canal D de 64 Kbps, mientras que un servicio PRI del tipo E1 tiene 30 canales B y un canal D también de 64 Kbps.

Configuración del servicio BRI

Para ver los aspectos básicos de configuración de ISDN en un router de Cisco, vamos a modificar nuevamente la arquitectura de nuestra interred, asumiendo que nuestros routers utilizan servicios BRI para conectarse a la red ISDN.

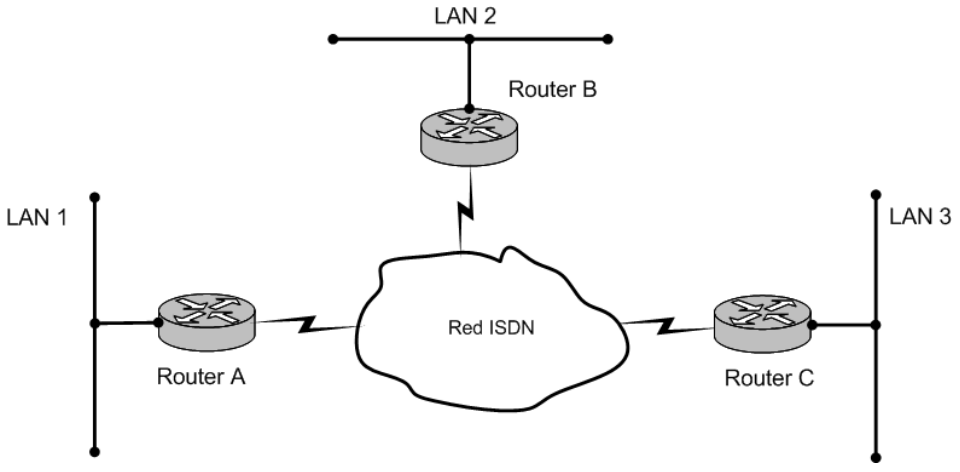


Fig. 14 - 2

Para comenzar la configuración de este servicio es necesario conocer dos parámetros cuyos valores deben ser proporcionados por el proveedor del servicio. Estos dos parámetros son:

- El tipo de switch ISDN del proveedor del servicio al cual se va a conectar el router para acceder a la red.
- El Identificador de Perfil de Servicio o SPID, Service Profile Identifier, para cada uno de los canales B del servicio BRI. Un SPID es un número cuyo formato es similar al de un número de teléfono.

Las interfaces del router a través de las cuales se accede a un servicio BRI de ISDN se denominan, precisamente, BRI y se identifican por un número de interfaz, de manera similar a como se identifican las interfaces FastEthernet o Serial.

Para nuestra configuración de ejemplo vamos a establecer la configuración del router A para conectar a la red ISDN usando un servicio BRI y establecer un enlace a través de la misma con el router B, de modo de habilitar el tráfico de datos IP entre las redes LAN 1 y LAN 2. El router B también utiliza un servicio BRI para acceder a la red ISDN.

En la tabla siguiente se muestran los valores de los parámetros mencionados anteriormente, tanto para el router A como para el router B, y las correspondientes direcciones IP que deben tener asignadas las interfaces BRI:

Router A	Router B
Interface BRI 0	Interface BRI 0
Tipo de switch: basic-5ees	Tipo de switch: basic-5ees
SPID 1: 24441111	SPID 1: 24442221
SPID 2: 24441112	SPID 2: 24442222
Dirección IP: 200.10.10.5	Dirección IP: 200.10.10.6

Comencemos entonces por configurar, en el router A, el tipo de switch ISDN y los SPIDs de los canales B del servicio BRI. Para configurar el tipo de switch se utiliza el comando de Configuración Global `isdn switch-type`:

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# isdn switch-type basic-5ees
RouterA(config)#
```

Para configurar los SPIDs de la interface BRI se utilizan los commandos de submodo de Configuración de Interface `isdn spid1` e `isdn spid2`:

```
RouterA(config)# interface bri 0
RouterA(config-if)# isdn spid1 24441111
RouterA(config-if)# isdn spid2 24441112
```

A continuación corresponde configurar las direcciones IP de esta interface BRI, así como indicar el método de encapsulamiento de datos:

```
RouterA(config-if)# ip address 200.10.10.5 255.255.255.252
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# no shutdown
RouterA(config-if)# end
RouterA#
```

Detengámonos por un momento aquí y veamos dos aspectos que son particularmente importantes cuando se utiliza un servicio BRI: el concepto de "tráfico interesante" y el de "encaminamiento por discado a demanda" o DDR, Dial-on-Demand Routing.

En términos generales, tráfico interesante es aquél que debe ser transmitido hacia un destino a través del enlace ISDN. Para el router A de nuestra interred, el tráfico interesante estará constituido por aquellos paquetes de datos destinados a las redes LAN 2 y LAN 3.

Por su parte, el encaminamiento por discado a demanda funciona de la siguiente manera. Cuando el router A tenga datagramas destinados a la red LAN 2 deberá encaminarlo al router B para que éste, a su vez, lo reenvíe al host de destino en la LAN 2. En tal caso, el router A procederá a realizar la llamada ISDN para activar el enlace al router B y, una vez establecida la comunicación, transmitirá los datagramas. Una vez que el tráfico interesante hacia la LAN 2 haya sido transmitido y haya transcurrido un tiempo de espera adicional, la llamada ISDN se corta. Este ciclo de realización de la llamada, transferencia del tráfico y corte de la llamada se repite cada vez que el router A reciba tráfico interesante destinado a la LAN 2.

Continuemos ahora con la configuración del router A y veamos los pasos a seguir para configurar DDR y especificar el tráfico que debe considerarse interesante para activar la conexión a través de la interfaz BRI.

Para configurar DDR se deben seguir los siguientes tres pasos:

1. definir las rutas estáticas para especificar cómo llegar hasta la red LAN 2
2. definir el tráfico que debe considerarse interesante
3. configurar la información de discado ISDN para realizar la llamada y activar la conexión con el router B

Para definir la ruta estática a la red LAN 2 se utiliza el comando de Configuración Global `ip route` que vimos y utilizamos en el Capítulo 9.

```
RouterA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
RouterA(config)# ip route 177.16.0.0 255.255.0.0 200.10.10.6
RouterA(config)#
```

Para especificar el tráfico IP que debe considerarse interesante y que provocará la realización de la llamada y la activación del enlace se utiliza una Lista de Control de Acceso del tipo que hemos utilizado en el Capítulo 13. Definamos entonces una Lista de Control de Acceso extendida que permita el tráfico destinado a la red 177.16.0.0, es decir, a la red LAN 2:

```
RouterA(config)# access-list 110 permit ip any 177.16.0.0 0.0.255.255
```

Una vez definida la Lista de Control de Acceso debemos indicar a IOS que utilice las reglas de esa lista para determinar el tráfico que debe considerarse interesante. Para esto se utiliza el comando de Configuración Global `dialer-list`:

```
RouterA(config)# dialer-list 1 list 110
```

Por último, debemos establecer la correspondencia entre el tráfico interesante definido recién con la interfaz BRI que debe utilizarse para transmitir ese tráfico. Para esto se utiliza el comando de submodo de Configuración de Interface `dialer-group`, el cual requiere como parámetro el número de lista de discado definido con el comando `dialer-list` anterior:

```
RouterA(config)# interface bri 0
RouterA(config-if)# dialer-group 1
RouterA(config-if)#
```

Hasta aquí, entonces, hemos completado los pasos 1 y 2 para la configuración de DDR. El tercer y último paso es configurar en la interfaz BRI la información necesaria para realizar la llamada ISDN al router B. Para esto se utiliza el comando de submodo de Configuración de Interface `dialer map`. Este comando requiere como parámetros la dirección IP del router con el cual va a establecer la conexión, el nombre de host de ese router en caso que se utilice autenticación y el número de teléfono ISDN al cual llamar para acceder a él:

```
RouterA(config-if)# dialer map 200.10.10.6 name routerB 24442221
RouterA(config-if)# dialer map 200.10.10.6 name routerB 24442222
```

Dos comandos adicionales que son de interés cuando se configura una interface BRI son los comandos de submodo de Configuración de Interface `dialer idle-timeout` y `dialer load-threshold`. El comando `dialer idle-timeout` permite especificar la cantidad de segundos que se mantendrá activa la conexión luego de que todo el tráfico interesante haya sido enviado. El valor predeterminado para este parámetro es 120 segundos; el siguiente comando modifica este valor y lo establece en 180 segundos:

```
RouterA(config-if)# dialer idle-timeout 180
```

Por su parte, el comando `dialer load-threshold` le indica a la interface BRI cuando debe activar el segundo canal B. Este comando requiere que se especifique un valor entre 1 y 255, donde 255 corresponde a una carga de tráfico de 100 % en el canal B activo. Esta carga de tráfico puede ser de tráfico entrante, tráfico saliente y la combinación de ambos tipos de tráfico. Para especificar el sentido de transferencia del tráfico, el comando admite, respectivamente, las palabras claves `in`, `out` o `either`. La siguiente línea establece que el segundo canal B se active cuando la carga de tráfico saliente en el primer canal B sea del 50 %:

```
RouterA(config-if)# dialer load-threshold 127 out
```

Hasta aquí hemos configurado el router A con la información necesaria para comunicarse con el router B y poder encaminar tráfico interesante destinado a la red LAN 2.

El router A también debe poder comunicarse con el router C para poder encaminar tráfico destinado a la red LAN 3. Modifiquemos entonces la configuración de DDR del router A,

incorporando la información necesaria para que pueda activar el enlace ISDN al router C utilizando la misma interface BRI. Para esto es necesario:

1. establecer una ruta estática a la red LAN 3
2. modificar la definición de tráfico interesante para que incluya el tráfico destinado a esa red
3. disponer de la dirección IP de la interface BRI que el router C utiliza para conectarse a la red ISDN
4. disponer de los números de teléfono ISDN de los canales B que utiliza el router C

Comencemos, entonces, por incorporar la ruta estática a la red LAN 3:

```
RouterA# configure terminal
Enter configuration commands, one per line.
RouterA(config)# ip route 197.168.100.0 255.255.255.0 200.10.30.6
```

Modifiquemos ahora la Lista de Control de Acceso para incorporare una regla que permita el tráfico IP hacia la red 197.168.100.0:

```
RouterA(config)# access-list 110 permit ip any 197.168.100.0 0.0.0.255
```

Finalmente, modifiquemos la configuración de la interfaz BRI e incorporemos los comandos `dialer map` que permitan saber al router A a cuales números de teléfono ISDN debe llamar para activar el enlace ISDN con el router C:

```
RouterA(config)# interface bri 0
RouterA(config-if)# dialer map 200.10.30.6 name routerB 24443331
RouterA(config-if)# dialer map 200.10.30.6 name routerB 24443332
RouterA(config-if)# end
RouterA#
```

Por ultimo, no olvidemos salvar la configuración en ejecución en la configuración de arranque:

```
RouterA# copy running-config startup-config
Building configuration...

[OK]
```

Verificación de ISDN

Para verificar el estado y el funcionamiento del enlace ISDN, IOS proporciona varios comandos del tipo `show`:

Comando	Descripción
show interface bri *id*	Despliega información sobre la interface BRI identificada como *id*
show isdn status	Despliega el estado de todas las interfaces ISDN.
show isdn active	Despliega información de la llamada actual, incluyendo el número llamado, y el tiempo que falta hasat que se desconecte la llamada.
show dialer	Despliega información general de diagnóstico para la sinterfaces configuradas para DDR.

Apéndice: Resumen de comandos

En este apéndice se presenta la lista de los principales comandos utilizados a lo largo del libro junto con la indicación del modo de la Interface de Línea de Comandos en que se utiliza y el capítulo en el cual fue utilizado por primera vez.

Comando	Modo o Sub-modo	Capítulo
`access-list`	Configuración Global	
`banner`	Configuración Global	5
`bandwidth`	Configuración de Interface	8
`boot`	Monitor ROM	10
`boot system`	Configuración Global	10
`clock`	Usuario	2
`clock rate`	Configuración de Interface	8
`configure terminal`	Privilegiado	2
`config-register`	Configuración Global	10
`conf-reg`	Monitor ROM	10
`copy`	Privilegiado	4
`description`	Configuración de Interface	8
`dialer`	Configuración de Interface	14
`dialer-list`	Configuración Global	14
`dir`	Monitor ROM	10
`disable`	Privilegiado	2
`enable`	Usuario	2
`enable password`	Configuración Global	7
`enable secret`	Configuración Global	7
`encapsulation`	Configuración de Interface	8
`end`	Configuración Global	2
`erase`	Privilegiado	4
`frame-relay`	Configuración de Subinterface	14
`hostname`	Configuración Global	5
`interface`	Configuración Global	2
`ip access-group`	Configuración de Interface	13
`ip address`	Configuración de Interface	8
`ip domain-lookup`	Configuración Global	5
`ip host`	Configuración Global	5
`ip name-server`	Configuración Global	5
`ip rip send`	Configuración de Interface	9
`ip rip receive`	Configuración de Interface	9
`ip route`	Configuración Global	9
`line`	Configuración Global	7
`login`	Configuración de Línea	7
`logging`	Configuración Global	12

`logout`	Usuario	2
`network`	Configuración de Router	8
`no shutdown`	Configuración de Interface	8
`passive-interface`	Configuración de Router	9
`password`	Configuración de Línea	7
`ping`	Usuario / Privilegiado	8
`reload`	Privilegiado	4
`reset`	Monitor ROM	10
`router`	Configuración Global	9
`router rip`	Configuración Global	9
`router igrp`	Configuración Global	9
`router eigrp`	Configuración Global	9
`router ospf`	Configuración Global	9
`service password-encryption`	Configuración Global	7
`show access-list`	Privilegiado	13
`show clock`	Usuario	4
`show dialer`	Privilegiado	14
`show flash`	Usuario	4
`show history`	Usuario / Privilegiado	2
`show hosts`	Usuario	4
`show interfaces`	Privilegiado	4
`show ip eigrp`	Privilegiado	9
`show ip ospf`	Privilegiado	9
`show ip protocols`	Privilegiado	8
`Show ip route`	Privilegiado	8
`show isdn active`	Prvilegiado	14
`show isdn status`	Privilegiado	14
`show protocols`	Usuario / Privilegiado	4
`show running-config`	Privilegiado	6
`show startup-config`	Privilegiado	6
`show users`	Usuario	4
`show version`	Usuario	4
`terminal full-help`	Usuario / Privilegiado	4
`tftpdnld`	Monitor ROM	10
`xmodem`	Monitor ROM	10

Bibliografía

Cisco Systems	Cisco IOS Configuration Fundamentals Configuration Guide, San José, CA, Cisco Systems
___	Cisco IOS Configuration Fundamentals Command Reference, San José, CA, Cisco Systems
___	Cisco IOS IP Configuration Guide, San José, CA, Cisco Systems
___	Cisco IOS IP Command Reference Vol. 1: Addressing and Services, San José, CA, Cisco Systems
___	Cisco IOS IP Command Reference Vol. 2: Routing Protocols, San José, CA, Cisco Systems
___	Cisco IOS Interface Configuration Guide, San José, CA, Cisco Systems
___	Cisco IOS Interface Command Reference, San José, CA, Cisco Systems
___	Cisco IOS Wide-Area Networking Configuration Guide, San José, CA, Cisco Systems
___	Cisco IOS Wide-Area Networking Command Reference, San José, CA, Cisco Systems
GOUGH, C.,	Cisco CCNP Routing Exam Certification Guide, Indianapolis, IN, Cisco Press, 2001
HILL, B.	Manual de Referencia Cisco, Madrid, McGraw-Hill, 2002
LAMMLE, T.	CCNA: Cisco Certified Network Associate Study Guide, Alameda, CA, Sybex, 2da. ed., 2002
LEINWAND, A., PINSKY, B.	Configuración de routers Cisco, Madrid, Pearson Educación, 2da. ed., 2001
MALHOTRA, R	IP Routing, Sebastopol, CA, O'Reilly, 2002
ODOM, W	CCNA Exam 640-607 Certification Guide, Indianapolis, IN, Cisco Press, 2002
PADJEN, R., LAMMLE, T., EDWARDS, W.	CCNP: Remote Access Study Guide, Alameda, CA, Sybex, 2da. ed., 2002
SACKETT, G	Manual de routers Cisco, Madrid, McGraw-Hill Interamericana de España, 2002

Educando para la vida

Cuareim 1451 Tel. 902 15 05 Fax 908 13 70
info@ort.edu.uy - www.ort.edu.uy

Diciembre 2007