CAPÍTULO 3

CONFIGURACIÓN INICIAL DEL ROUTER

PANORÁMICA DEL FUNCIONAMIENTO DEL ROUTER

Un router es un ordenador construido para desempeñar funciones específicas de capa tres, proporciona el hardware y software necesarios para encaminar paquetes entre redes. Se trata de dispositivos importantes de interconexión que permiten conectar subredes LAN y establecer conexiones de área amplia entre las subredes.

Las dos tareas principales son las de **conmutar** los paquetes desde una interfaz perteneciente a una red hacia otra interfaz de una red diferente y la de **enrutar**, es decir encontrar el mejor camino hacia la red destino. Además de estas funciones los router pueden llevar a cabo diferentes desempeños, tales como filtrados, traslación de direcciones, enlaces troncales, etc.

Además de los componentes de hardware los routers también necesitan un sistema operativo, los routers Cisco funcionan con un sistema operativo llamado **IOS** (Sistema operativo de internerworking). Un router puede ser exclusivamente un dispositivo LAN, o puede ser exclusivamente un dispositivo WAN, pero también puede estar en la frontera entre una LAN y una WAN y ser un dispositivo LAN y WAN al mismo tiempo.

Componentes principales del hardware de un router

Los componentes básicos de la arquitectura interna de un router comprenden:

CPU: La unidad central de procesamiento. (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

RAM: La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede ampliarse agregando más Módulos de memoria en línea doble (DIMM).

Memoria flash: La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede ampliar la cantidad de memoria flash.

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

Buses: La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces. La CPU usa el bus para tener acceso a los componentes desde el almacenamiento del router. Este bus transfiere las instrucciones y los datos hacia o desde las direcciones de memoria especificadas.

ROM: La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede

usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

Interfaces: Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring.
Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares.

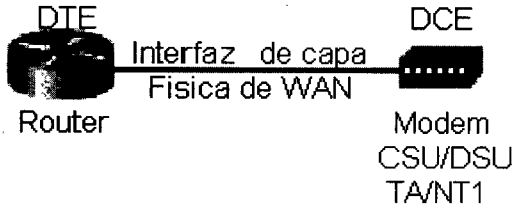
Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares.

Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.

Fuente de alimentación: La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externa al router.

WAN y Routers

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de transmisión de datos (DCE). Normalmente el **DCE** es el proveedor del servicio, mientras que el **DTE** es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o **CSU/DSU**.



Cuando un router usa los protocolos y los estándares de la capa de enlace de datos y física asociados con las WAN, opera como dispositivo WAN.
Los protocolos y estándares de la capa física WAN son:

- EIA/TIA -232
- EIA/TIA -449
- V.24
- V.35
- X.21
- G.703
- EIA-530
- RDSI
- T1, T3, E1 y E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

Los protocolos y estándares de la capa de enlace de datos WAN:

- Control de enlace de datos de alto nivel (HDLC)
- Frame-Relay
- Protocolo punto a punto (PPP)
- Control de enlace de datos síncrono (SDLC)
- Protocolo Internet de enlace serial (SLIP)
- X.25
- ATM
- LAPB
- LAPD
- LAPF

CONECTÁNDOSE POR PRIMERA VEZ AL ROUTER

Para la configuración inicial del router se utiliza el puerto de consola conectado a un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al puerto **COM1** del ordenador. Este debe tener instalado un software de emulación de terminal, como el HyperTerminal.

Los parámetros de configuración son los siguientes:

- ***El puerto COM adecuado***
- ***9600 baudios***
- ***8 bits de datos***
- ***Sin paridad***

- ***1 bit de parada***
- ***Sin control de flujo***

Cuando un switch Catalyst o un router Cisco se ponen en marcha, hay tres operaciones fundamentales que han de llevarse a cabo en el dispositivo de red:

Paso 1

El dispositivo localiza el hardware y lleva a cabo una serie de rutinas de detección del mismo. Un término que se suele utilizar para describir este conjunto inicial de rutinas es power-on self test (**POST**), o pruebas de inicio.

Paso 2

Una vez que le hardware se muestra en una disposición correcta de funcionamiento, el dispositivo lleva a cabo rutinas de inicio del sistema. Estas rutinas inician el switch o el router localizando y cargando el software del sistema operativo.

Paso 3

Tras cargar el sistema operativo, el dispositivo trata de localizar y aplicar las opciones de configuración que definen los detalles necesarios para operar en la red. Generalmente, hay una secuencia de rutinas de arranque que proporcionan alternativas al inicio del software cuando es necesario.

Un router o un switch pueden ser configurados desde distintas ubicaciones:

- En la instalación inicial, el administrador de la red configura generalmente los dispositivos de la red desde un terminal de consola, conectado por medio del puerto de consola.
- Si el administrador debe dar soporte a dispositivos remotos, una conexión local por módem con el puerto auxiliar del dispositivo permite a aquél configurar los dispositivos de red.
- Dispositivos con direcciones IP establecidas pueden permitir conexiones Telnet para la tarea de configuración.
- Descargar un archivo de configuración de un servidor Trivial File Transfer Protocol (TFTP).
- Configurar el dispositivo por medio de un navegador Hypertext Transfer Protocol (HTTP).

Al iniciar por primera vez un router Cisco, no existe configuración inicial alguna. El software del router le pedirá un conjunto mínimo de detalles a través de un diálogo opcional llamado setup.

Las rutinas de inicio del software Cisco IOS tienen por objetivo inicializar las operaciones del router. Para ello, las rutinas de puesta en marcha deben hacer lo siguiente:

- Asegurarse que el router cuenta con hardware verificado (POST).
- Localizar y cargar el software Cisco IOS que usa el router para su sistema operativo.
- Localizar y aplicar las instrucciones de configuración relativas a los atributos específicos del router, funciones del protocolo y direcciones de interfaz.

El router se asegura de que el hardware haya sido verificado. Cuando un router Cisco se enciende, realiza unas pruebas al inicio (POST). Durante este autotest, el router ejecuta una serie de diagnósticos para verificar la operatividad básica de la CPU, la memoria y la circuiteria de la interfaz. Tras verificar que el hardware ha sido probado, el router procede con la inicialización del software.

El modo Setup es el modo en el que inicia un router no configurado al arrancar. Se puede salir de este modo respondiendo que NO a la pregunta inicial.

```
Would you like to enter the initial configuration dialog?[yes]: No
Would you like to terminate autoinstall? [yes]: INTRO
```

Desde la línea de comandos el router se inicia en el modo EXEC **usuario**, las tareas que se pueden ejecutar en este modo son solo de verificación ya que NO se permiten cambios de configuración. En el modo EXEC **privilegiado** se realizan las tareas típicas de configuración.

Modo EXEC usuario:

```
Router>
```

Modo EXEC privilegiado:

```
Router#
```

Para pasar del modo usuario al privilegiado ejecute el comando **enable**, para regresar **disable.** Esto es posible porque no se ha configurado contraseña, de lo contrario seria requerida cada vez que se pasara al modo privilegiado.

```
Router>
Router>enable
Router#disable
Router>
```

Modo global y de interfaz:

```
Router>enable
Router#configure terminal
Router(config)#interface [tipo de interfaz][número]
Router(config)#interface ethernet 0
Router(config-if)#exit
Router(config)#exit
Router#
```

Para pasar del modo privilegiado al **global** debe introducir el comando **configure terminal,** para pasar del modo global al de interfaz ejecute **interface ethernet 0,** en este caso se ha elegido la ethernet 0. Para regresar un modo mas atrás utilice el **exit** o **Control+Z** que lo llevará directamente al modo privilegiado.

Comandos ayuda

El router nos da la posibilidad de ayudas pues resulta difícil memorizar todos los comandos disponibles, el signo de interrogación (**?**), y el tabulador del teclado nos brindan la ayuda necesaria a ese efecto. El tabulador completa los comandos que no recordamos completos o que no queremos escribir en su totalidad. El **?** colocado inmediatamente después de un comando nos muestra todos los que comienzan con esas letras, colocado después de un espacio (**barra espaciadora+?**) nos lista todos los comando que se pueden ejecutar en esa posición:

La ayuda se puede ejecutas desde cualquier modo:

```
Router#?
Exec commands:
  access-enable     Create a temporary Access-List entry
  access-template   Create a temporary Access-List entry
  bfe               For manual emergency modes setting
  clear             Reset functions
--More--
```

Inmediatamente o después de un espacio según la ayuda solicitada:

```
Router#sh?
Show

Router#show ?
  access-expression  List access expression
  access-lists       List access lists
  accounting         Accounting data for active sessions
  aliases            Display alias commands
 --More--
```

La indicación **—More**—significa que existe más información disponible. La barra espaciadora pasará de página en página, mientras que el INTRO lo hará línea por línea.

El acento circunflejo '^' indicará un fallo de escritura en un comando:

```
Router#configure terxinal
                  ^
% Invalid input detected at '^' marker.

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

El uso de **Control+P** (también flecha hacia arriba) permite ver los últimos comandos ejecutados, el **Control-N** (también flecha hacia abajo) la inversa del anterior. Estos comandos quedan registrados en un bufer llamado historial y pueden verse con el comando **show history**, por defecto la cantidad de comandos que se guardan en memoria es de 10, pero puede ser modificado por el administrador utilizando el **history size:**

```
Router#terminal history size ?
<0-256>  Size of history buffer
```

Asignación de nombre y contraseñas

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Router(config)#hostname MADRID
MADRID(config)#
```

Los comandos **enable password** y **enable secret** se utilizan para restringir el acceso al modo EXEC privilegiado. El comando **enable password** se utiliza sólo si no se ha configurado previamente enable secret.

Se recomienda habilitar siempre **enable secret**, ya que a diferencia de **enable password**, la contraseña estará siempre cifrada.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname MADRID
MADRID(config)#enable password cisco
MADRID(config)#enable secret cisco
```

Observe en el ejemplo que se copia parte de un **show runnig-config** que se ha configurado como hostname del router **MADRID** y como contraseña **cisco** en la enable secret y la enable password, abajo se ve como la contraseña secret aparece encriptada por default.

```
hostname MADRID
!
enable secret 5 $1$EBMD$0rTOiN4QQab7s8AFzsSof/
enable password cisco
```

Configuración de contraseñas de consola, auxiliar y telnet

Para configurar la contraseña para consola se debe acceder a la interfaz de consola con el comando **line console 0**:

```
Router#configure terminal
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password [contraseña]
```

El comando **exec-timeout** permite configurar un tiempo de desconexión determinado en la interfaz de consola.

Para configurar la contraseña para telnet se debe acceder a la interfaz de telnet con el comando **line vty 0 4**, donde **line vty** indica dicha interfaz, **0** el número de la interfaz y **4** la cantidad máxima de conexiones múltiples a partir de 0, en este caso se permiten 5 conexiones múltiples:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password [contraseña]
```

El comando **show sessions** muestra las conexiones de telnet efectuadas desde el router, el comando **show users** muestra las conexiones de usuarios remotos.

Para configurar la contraseña para auxiliar se debe acceder a la interfaz de auxiliar con el comando **line aux 0**:

```
Router(config)# line aux 0
Router(config-line)#login
Router(config-line)#password [contraseña]
```

En todos los casos el comando **login** permite que el router pregunte la contraseña al intentar conectarse, con el comando **login local** el router preguntará qué usuario intenta ingresar y su respectiva contraseña. Para que esto funcione se deben crear nombres de usuarios y contraseña con el siguiente comando:

```
Router(config)#username CORE_SUR password Ansur
Router(config)#username CORE_NOR password Anort
```

En el ejemplo se han creado dos usuarios **CORE_SUR** con una contraseña **Ansur** y **CORE_NOR** con una contraseña **Anort**. Se configura a continuación la línea de consola:

```
Router#configure terminal
Router(config)#line console 0
Router(config-line)#login local
```

Cuando el usuario **CORE_NOR** intente ingresar al router le será solicitado su usuario y contraseña, y luego la enable secret:

```
Press RETURN to get started.

 Usted intenta ingresar en un sistema protegido

User Access Verification

Username: CORE_NOR
Password:***** (contraseña de usuario, Anort)
Router>enable
Password:***** (enable secret, cisco)
Router#
```

El comando **service password-encryption** encriptara con un cifrado leve las contraseñas que no están cifradas por defecto como las de telnet, consola, auxiliar, etc.

Configuración por navegador

Los router pueden ser configurados por HTTP si el comando **ip http Server** está habilitado en el dispositivo. Por defecto la configuración por web viene

deshabilitada por defecto (**no ip http server**). Por razones de seguridad se recomienda dejarlo desactivado.

COMANDOS SHOW

Saber utilizar e interpretar los comandos show permite el rápido diagnóstico de fallos, el modo usuario se permite la ejecución de los comandos show de forma restringida, desde el modo privilegiado la cantidad es ampliamente mayor.

Lista de los comandos show más usados

show interfaces

Muestra las estadísticas completas de todas las interfaces del router. Para ver las de una interfaz específica, ejecute el comando seguido de la interfaz y el número de puerto.

```
Router#show interfaces serial 0/1
```

show controllers serial

Muestra información específica de la interfaz de hardware.

```
Router#show controllers serial 0/1
```

show clock

Muestra la hora fijada en el router.

show hosts

Muestra la lista en caché de los nombres de host y sus direcciones.

show users

Muestra todos los usuarios conectados al router.

show sessions

Muestra las conexiones de telnet efectuadas desde el router.

show history

Muestra un historial de los comandos ingresados.

show flash

Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.

show version

Despliega la información acerca del router y de la imagen de IOS que esté corriendo en al RAM. Este comando también muestra el valor del registro de configuración del router.

show arp
Muestra la tabla ARP del router.

show protocols
Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado.

show startup-config
Muestra el archivo de configuración almacenado en la NVRAM.

show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica.

CONFIGURACIÓN DE INTERFACES

Las interfaces de un router forman parte de las redes que están directamente conectadas al dispositivo. Estas interfaces activas deben llevar una dirección IP y su correspondiente máscara, como un host perteneciente a esa red. El administrador debe habilitar administrativamente la interfaz con el comando **no shutdown**, si fuera necesario la interfaz podrá deshabilitarse con el comando **shutdown**.

La captura muestra una configuración de una interfaz ethernet:

```
MADRID>enable
Password:*******
MADRID#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MADRID(config)#interface ethernet 0
MADRID(config-if)#ip address 192.168.1.1 255.255.255.0
MADRID(config-if)#no shutdown
MADRID(config-if)#description INTERFAZ_DE_LAN
```

El comando **show interfaces ethernet 0** muestra en la primer línea como la interfaz esta **UP** administrativamente y **UP** físicamente. Recuerde que si la interfaz no estuviera conectada o si existiesen problemas de conectividad, el segundo **UP** aparecería como **down.**

La tercera línea muestra la descripción configurada a modo de comentario puesto que solo tiene carácter informativo y NO afecta al funcionamiento del router. Puede tener cierta importancia para los administradores a la hora de

solucionar problemas. Mas abajo aparece la dirección IP, la encapsulación, paquetes enviados, recibidos, etc.

```
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0000.0cfb.6c19 (bia
0000.0cfb.6c19)
  Description: INTERFAZ_DE_LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 183/255,
load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10
sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
     0 input packets with dribble condition detected
     188 packets output, 30385 bytes, 0 underruns
     188 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     188 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Si el administrador deshabilita la interfaz se verá:

```
Ethernet0 is administratively down, line protocol is down
Hardware is Lance, address is 0000.0cfb.6c19 (bia
0000.0cfb.6c19)
Description: INTERFAZ_DE_LAN
Internet address is 192.168.1.1/24
. . . . . .
```

Las interfaces seriales se configuran siguiendo el mismo proceso que las ethernet, se debe tener especial cuidado para determinar quién es el **DCE** (equipo de comunicaciones) y quien el **DTE** (equipo Terminal del abonado) debido a que el DCE lleva el sincronismo de de la comunicación, este se configurará solo en la interfaz serial del DCE, el comando **clock rate** activara el sincronismo en ese enlace.

Clock rate Vs ancho de banda: recuerde que existe un comando **bandwidth** para la configuración del ancho de banda, el router solo lo utilizará para el calculo de costes y métricas para los protocolos de enrutamiento, mientras que el clock rate brinda la verdadera velocidad del enlace.

A continuación se observa la configuración de un enlace serial como DCE:

```
MADRID(config)#interface serial 0
MADRID(config-if)#ip address 170.16.2.1 255.255.0.0
MADRID(config-if)#clock rate 56000
MADRID(config-if)#bandwidth 100000
MADRID(config-if)#description RED_SERVIDORES
MADRID(config-if)#no shutdown
```

RECUERDE:

Algunos router llevan incorporados slots o ranuras para ampliar la cantidad de puertos, en ese caso las interfaces se identificaran con 0/0, esto hace referencia al slot 0, interfaz 0.

MENSAJES O BANNERS

Con el fin de brindar mensajes ante posibles averías o intrusos existen varios tipos de banners,

```
MADRID(config)#banner ?
LINE     c banner-text c, where 'c' is a delimiting character
exec       Set EXEC process creation banner
incoming   Set incoming terminal line banner
login      Set login banner
motd       Set Message of the Day banner
```

El banner motd ofrece la posibilidad de un mensaje diario, el banner login será visto al establecer una sesión de telnet, el banner exec al pasar la password al modo privilegiado.

Un mensaje de inicio de sesión debe advertir que sólo los usuarios autorizados deben intentar el acceso. Evite un mensaje del estilo "¡bienvenido!", por el contrario deje bien claro que cualquier intrusión sin autorización estará penalizada por la ley vigente, de esta manera advertirá que ir más allá está prohibido y es ilegal.

Configuración de un banner diario, el texto debe ir entre caracteres similares al comenzar y al terminar:

```
MADRID(config)#banner motd * Usted intenta ingresar en un sistema
protegido*
```

RESOLUCIÓN DE NOMBRES DE HOST

Seguramente resultará más familiar identificar un dispositivo, un host o un servidor con un nombre que lo asocie a sus funciones o a otros criterios de desempeño. Esto se hace creando una tabla de host, que asociara un nombre a una o varias direcciones IP.

A continuación se ha creado una tabla de host con el comando

```
ip host [nombre] dirección IP
```

```
MADRID(config)#ip host SERVIDOR 204.200.1.2
MADRID(config)#ip host ROUTER 220.220.10.32
MADRID(config)#ip host HOST 210.210.2.22
MADRID(config)#exit
```

```
MADRID#show host
Host                      Flags       Age Type    Address(es)
SERVIDOR                  (perm, OK)  0   IP      204.200.1.2
ROUTER                    (perm, OK)  0   IP      220.220.10.32
HOST                      (perm, OK)  0   IP      210.210.2.22
```

En el caso que se muestra arriba si se deseara enviar un ping a la dirección IP 204.200.1.2 bastaría con ejecutar **ping SERVIDOR**. Por defecto las tablas de host están asociadas al puerto **23** (telnet) si sólo se ejecutara **SERVIDOR** el router intentaría establecer una sesión de telnet con ese host, y sólo tienen carácter local.

GUARDAR Y COPIAR

Las configuraciones actuales del router son almacenadas en la memoria RAM, este tipo de memoria pierde el contenido al apagarse el router. Para que esto no ocurra es necesario poder hacer una copia a la NVRAM. El comando **copy** se utiliza con esta finalidad, identificando un origen con datos a guardar y un destino donde se almacenaran esos datos. Se puede guardar la configuración de la RAM a la NVRAM, de la RAM a un servidor TFTP, etc.

```
MADRID#copy running-config startup-config
```
Copia de la RAM a la NVRAM

```
MADRID#copy startup-config running-config
```
Copia de la NVRAM a la RAM

Copia de la RAM a un servidor TFTP, es este caso el router solicitará el nombre de archivo con el que se guardará la configuración y la dirección IP del servidor. Para ejecutar el proceso inverso el router debe tener como **mínimo una conexión de red activa hacia el servidor tftp**.

```
MADRID#copy running-config tftp
Remote host []? 204.200.10.56
Name of configuration file to write [madrid-confg]?
Write file madrid-confg on host 204.200.10.56? [confirm]
Building configuration...

Writing madrid-confg ..
!!!!!!!!!!!!!!!!!!!!
```

Los comandos

```
MADRID#show running-config

MADRID#show startup-config
```

muestran el contenido de la **RAM** y de la **NVRAM** respectivamente.

A continuación se copia parte de un **show startup-config**, se observa en la primera línea la cantidad de memoria y la que se esta utilizando, luego la versión del software IOS:

```
Using 886 out of 131066 bytes
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
```

```
!
hostname MADRID
!
enable secret 5 $1$EBMD$0rTOiN4QQab7s8AFzsSof/
enable password cisco
!
ip host SERVIDOR_WEB 204.200.1.2
ip host ROUTER_A 220.220.10.32
ip host HOST_ADMIN 210.210.2.22
!
interface Ethernet0
 description INTERFAZ_DE_LAN
 ip address 192.168.1.1 255.255.255.0
 shutdown
!
interface Ethernet1
 no ip address
```

Cómo borrar el contenido de las memorias

Los datos de configuración almacenados en la memoria no volátil no son afectados por la falta de alimentación, el contenido permanecerá en la NVRAM hasta tanto se ejecute el comando apropiado para su eliminación:

```
MADRID#erase startup-config
```

Por el contrario no existe comando para borrar el contenido de la RAM. Si el administrador pretende dejar sin ningún dato de configuración debe rebotar o apagar el router. La Runnig se borra únicamente ante la falta de alimentación eléctrica:

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

Para borrar completamente la configuración responda **NO** a la pregunta si quiere salvar.

RECUERDE:

Tenga especial cuidado al borrar las memorias, asegúrese de eliminar lo que desea antes de confirmar el borrado.

Copia de seguridad del IOS

Cuando sea necesario restaurar el IOS del router o actualizarlo se debe hacer desde un servidor **TFTP**. Es importante que se guarden copias de seguridad de todas las IOS en un servidor central.

El comando para esta tarea es el **copy flash tftp**, mediante el comando **show flash** se verificara el nombre del archivo a guardar:

```
Router#show flash

System flash directory:
File  Length    Name/status
  1   3709210   c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)

Router#copy flash tftp

System flash directory:
File  Length    Name/status
  1   3709210   c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
Address or name of remote host [255.255.255.255]?
200.200.10.1
Source file name? c4500-js-l_121-5.bin
Destination file name [c4500-js-l_121-5.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

En el proceso inverso al anterior o para actualizar el IOS se debe verificar el espacio en la memoria flash con el comando **show flash** y luego ejecutar el comando **copy tftp flash:**

```
Router#show flash

System flash directory:
File  Length    Name/status
  1   3709210   c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)

Router#copy tftp flash
Address or name of remote host?200.200.10.1
Source filename? c4500-js-l_121-5.bin
Destination filename [c4500-js-l_121-5.bin]?
Accessing tftp://200.200.10.1/ c4500-js-l_121-5.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
```

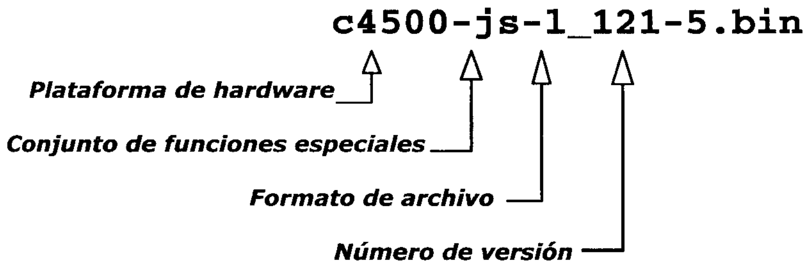
```
Continue?[confirm]
Erasing device eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeee erased
Loading c4500-js-l_121-5.bin from 200.200.10.1 (via Ethernet
0/2)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Verifying Check sum . . . . . . . . . . . . OK
[OK-9024523 bytes]
9024523 bytes copied in 310.12 secs
```

NOMBRES DEL CISCO IOS

Cisco desarrolla numerosas versiones del IOS y lanza nuevas versiones en forma continua.

El IOS ofrece diversas funciones y también corre sobre diversas plataformas de hardware.

Cisco ha establecido una convención para identificar por nombres a las distintas versiones, de los archivos del IOS. La convención de nombres del IOS utiliza varios campos. Entre ellos podemos mencionar el de identificación de la plataforma del hardware, el de identificación de la funcionalidad y el correspondiente a la secuencia numérica.



RECUERDE:

La información que aparece entre corchetes luego de una pregunta es la que el router sugiere como válida ***...dialog? [yes]:*** *bastará con aceptar con un intro.*

Las contraseñas sin encriptación aparecen en el ***show running*** *debiendo tener el debido cuidado ante la presencia de intrusos.*

Si una interfaz esta administrativamente down no significa que exista un problema pues el administrador ha decidido dejarla ***shutdown****. Por el contrario si el* ***line protocol is down*** *existe un problema, seguramente de capa física.*

La memoria ***RAM*** *es la running-config su contenido se pierde al apagar y no existe comando para borrado. La memoria* ***NVRAM*** *es la startup-config no pierde su contenido al apagar.*

PROTOCOLO CDP (Cisco Discovery Protocol)

El protocolo **CDP** se utiliza para obtener información de router y switches que están conectados localmente. El CDP es un protocolo propietario de Cisco, destinado al descubrimiento de vecinos y es independiente de los medios y del protocolo de enrutamiento. Aunque el CDP solamente mostrará información sobre los vecinos conectados de forma directa, este constituye una herramienta de gran utilidad.

El Protocolo de descubrimiento de Cisco (**CDP**) es un protocolo de Capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores.

La lectura del comando **show cdp neighbors** incluyen la siguiente información:

- Identificador del dispositivo
- Interfaz local
- Tiempo de espera
- Capacidad
- Plataforma
- Identificador del puerto

Los siguientes datos se agregan en el CDPv2:

- Administración de nombres de dominio VTP
- VLAN Nativas
- Full o half-duplex

Para obtener los nombres y tipos de plataforma de routers vecinos, nombres y versión de la imagen Cisco IOS:

```
Show cdp neighbors
```

Para obtener datos de routers vecinos en más detalle:

```
Show cdp neighbors detail
```

Para saber el tráfico de CDP que ocurre en el router.

```
Router#show cdp traffic
```

Hay dos formas de deshabilitar CDP, una es en un interfaz específico y la otra de forma general.

Desde una interfaz:

```
Router#configure terminal
Router(config)#[número de interfaz]
Router(config-if)#no cdp enable
```

De modo total:

Deshabilita CDP en el router:

```
Router(config)#no cdp run
```

Habilita CDP en el router:

```
Router(config)#cdp run
```

```
Show cdp interface
```

Muestra el estado de todos los interfaces que tienen activado CDP.

Restaura los contadores a cero:

```
Router#clear cdp counters
```

Borra la información contenida en la tabla de vecinos:

```
Router#clear cdp table
```

Los siguientes comandos pueden utilizarse para mostrar la versión, la información de actualización, las tablas y el tráfico:

- **show cdp traffic**
- **show debugging**
- **debug cdp adjacency**
- **debug cdp events**
- **debug cdp ip**
- **debug cdp packets**
- **cdp timer**
- **cdp holdtime**
- **show cdp**

Ejemplo de un **Show cdp neighbors**:

```
Router#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Sourse
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID  Local Interfce  Holdtme Capablyt Plataform Port ID
Router3   Ser0/1          150     R            2600    Ser0/1
Router4   Ser0/0          142     R            4500    Ser1/0
SWITCH     FASTET0/0      120     S            2950    FAST0/5
```