Configuración Básica de Ruteadores Cisco

Carlos Vicente
Servicios de Redes
Universidad de Oregón

* Adaptado del original de Mark Tinka (Uganda) presentado en AFNOG 2004

Componentes de un enrutador Cisco
Tipos de Memoria

- RAM: Aloja los búfers de paquetes, la caché de ARP, la tabla de rutas, el software y las estructuras de datos que permiten al enrutador funcionar; la configuración actual se guarda en RAM, así como la IOS descomprimida en los modelos más nuevos.
- ROM: Contiene software básico que hace pruebas de hardware e inicia el enrutador
- Flash: Aloja la IOS. No se borra cuando se inicia el equipo. También se puede guardar en ella copias del archivo de configuración
- NVRAM (RAM No-Volátil): Guarda la configuración del enrutador. No se borra cuando se reinicia el equipo.

Componentes de un enrutador Cisco Software

- POST: Power On Self Test – Alojado en ROM. Revisa las funcionalidades básicas del enrutador y determina cuáles interfaces están hábiles.
- Bootstrap: Alojado en ROM – Inicia el enrutador y carga el sistema operativo (IOS).
- ROM Monitor: Alojado en ROM – Utilizado para pruebas y resolución de problemas. Un interfaz básico para cuando no hay IOS
- IOS: Internetwork Operating System – El sistema operativo principal del enrutador. Contiene todas las funcionalidades de éste.

Componentes del enrutador

- Config-Register (Registro de Configuración):
  - Controla cómo se inicia el enrutador.
  - Su valor actual se muestra con el comando "`show version`"
  - Generalmente es 0x2102, lo cual indica al enrutador que cargue la IOS desde memoria Flash y la configuración de inicio desde NVRAM

Cuándo modificar el Config-Register

- Razones posibles:
  - Forzar al enrutador a entrar en modo ROM-monitor
  - Indicar dónde buscar la configuración de inicio
  - Activar/Desactivar la función de “Break”
  - Configurar la tasa de bits de la consola
  - Cargar el sistema operativo desde ROM
  - Activar el inicio desde un servidor TFTP

Configuración

- **La configuración del enrutador afecta:**
  - Las direcciones IP y las máscaras de cada interfaz
  - Información de ruteo (estático, dinámico o por defecto)
  - Información de inicio
  - Seguridad (contraseñas)

¿Dónde está la configuración?

- El enrutador siempre tiene dos configuraciones:
  - "Running" (actual)
    - En RAM, indica con qué parámetros el enrutador está operando actualmente
    - Se modifica con el comando `configure`
    - Para verla: `show running-config`
  - "Startup" (de inicio)
    - En NVRAM, determina cómo va a operar el enrutador cuando sea reiniciado
    - Se modifica usando el comando `copy`
    - Para verla: `show startup-config`

¿Dónde está la configuración?

- También se puede guardar en sitios más permanentes:
  - Otras máquinas, usando TFTP (Trivial File Transfer Protocol)
  - En la memoria Flash del enrutador
- Se mueve de un lugar a otro con el comando `copy`
  - `copy run start`
  - `copy run tftp`
  - `copy start tftp`
  - `copy tftp start`
  - `copy flash start`
  - `copy start flash`

Modos de Acceso

- Modo de ejecución de usuario (**User EXEC):** Examinar el enrutador de forma limitada
  - `Router>`
- Modo de ejecución privilegiado **(Privileged EXEC):** Examen detallado, resolución de problemas, pruebas, manipulación de ficheros
  - `Router#`
- **ROM Monitor:** Útil para recuperación de contraseñas y para instalar IOS
- Modo **Setup –** Disponible cuando no existe el fichero `startup-config`

Fuentes de Configuración Externas

- **Consola**: Acceso directo vía puerto serie
- **Puerto Auxiliar**: Acceso vía modem
- **Terminales Virtuales**: Acceso Telnet/SSH
- **Servidor TFTP**: Copiar la configuración en la NVRAM
- **Software de Gestión**: CiscoWorks

Cambiar la Configuración

- Los comandos de configuración se pueden ejecutar de forma interactiva. Los cambios se activan (casi) inmediatamente en la configuración corriente.
- Puede usar una conexión directa vía puerto serie, o
- Hacer Telnet/SSH a las vty's ("virtual terminals"), o
- Una conexión vía módem al puerto auxiliar, o
- Escribir los comandos en un fichero de texto y cargarlo luego en el enrutador vía TFTP
  - `copy tftp start` o `config net`

Entrar al enrutador (Login)

- Conectarse al puerto consola o hacer Telnet

```
router>
router>enable
password
router#
router#?
```

- Configurar el enrutador
  - Terminal (Entrar los comandos directamente)

```
router# configure terminal
router(config)#
```

Conectar su máquina (Linux) al enrutador vía puerto serie

- Conecte su máquina al enrutador con el cable serie provisto
- Utilice el programa 'minicom' para emular un terminal vía puerto serie
  - En Windows puede usar:
    - HyperTerminal (incluído en Windows)
    - TeraTerm, CRT, etc. (freeware)

Configuración de un enrutador nuevo

- Cargar los parámetros de configuración en la RAM
  - `Router#configure terminal`
- Dar al enrutador una identificación
  - `Router#(config)hostname RouterA`
- Asignar contraseñas de acceso
  - `RouterA#(config)line console 0`
  - `RouterA#(config-line)password cisco`
  - `RouterA#(config-line)login`

Configuración de un enrutador nuevo

- Configurar interfaces
  - `RouterA#(config)interface ethernet 0/0`
  - `RouterA#(config-if)ip address n.n.n.n m.m.m.m`
  - `RouterA#(config-if)no shutdown`
- Configurar protocolos ruteados y de ruteo
- Guardar la configuración en NVRAM
  - `RouterA#copy running-config startup-config o write memory`

Indicadores – Cómo saber dónde está usted en el enrutador

- Puede saber en qué área de la configuración se encuentra sólo mirando los indicadores

  - `Router>` - modo USER
  - `Router#` – modo PRVILEDGED EXEC
  - `Router(config)` – modo configuración global
  - `Router(config-if)` – modo configuración interfaz
  - `Router(config-subif)` – modo configuración sub-interfaz
  - `Router(config-route-map)` – modo configuración route-map
  - `Router(config-router)` – modo configuración enrutamiento
  - `Router(config-line)` – modo configuración de línea
  - `rommon 1>` - modo configuración ROM Monitor

Configuración Global

- Los comandos de configuración globales son independientes de interfaces o protocolos específicos
  - `hostname` *`router1`*
  - `enable-password` *`cisco`*
  - `service password-encryption`
  - `logging facility` *`local0`*
  - `logging` *`n.n.n.n`*

Configuración Global

- Configure la contraseña "enable secret":
  - `router(config)# enable secret <clave>`
    - La clave aparecerá en texto en claro. Ejecute el comando siguiente para hacer más segura:
  - `router(config)# service password-encryption`
    - Otro método es usar el comando 'enable password'. Este no es seguro (débil y texto en claro) y NO ES RECOMENDADO.
- Comandos globales relacionados con IP:
  - `ip classless`
  - `ip name-server` *`n.n.n.n`*
- Creación de rutas estáticas
  - `ip route <n.n.n.n> <m.m.m.m> <g.g.g.g>`
  - **`n.n.n.n`** = bloque IP
  - **`m.m.m.m`** = máscara de red (tamaño del bloque)
  - **`g.g.g.g`** = enrutador del próximo salto por omisión

El comando ‘no’

- Utilizado para desactivar o invertir un comando
  - `ip domain-lookup`
  - `no ip domain-lookup`
  - `router ospf 1`
  - `no router ospf 1`
  - `ip address 1.1.1.1 255.255.255.0`
  - `no ip address`

Configuración de Interfaces

- Su nombre tiene el formato *Tipo/Ranura/[Número]*. *ej.*:
  - ethernet0, ethernet1,... Ethernet5/1
  - Serial0/0, serial1 ... Serial3
- Y se pueden abreviar:
  - ethernet0 o eth0 or e0
  - Serial0/0 o ser0/0 or s0/0

Configuración de Interfaces

- Configuración de la dirección IP y máscara

```
router#configure terminal
router(config)#interface e0/0
router(config-if)#ip address n.n.n.n m.m.m.m
router(config-if)#no shutdown
router(config-if)#^Z
router#
```

Configuración de Interfaces

- **Activar/Desactivar la interfaz con carácter administrativo**
  - `router(config-if)#no shutdown`
  - `router(config-if)#shutdown`
- **Descripción**
  - `router(config-if)#description enlace ethernet al edificio de administración`

Mostrar la configuración

- Use `"show running-configuration"` para ver la configuración corriente
- Use `"show startup-configuration"` para ver la configuración guardada en NVRAM

Guardar la configuración en un servidor

- Requiere *tftpd* en una máquina unix. El fichero destino debe existir en el directorio antes de ser copiado y debe tener permiso de escritura

```
Router#copy run tftp
Address or name of remote host []? 192.168.1.5
Destination filename [Router-confg]? y
!!!!!
15693 bytes copied in 0.792 secs (19814 bytes/sec)
```

Recuperar la Configuración desde el servidor

- Use 'tftp' para cargar la configuración desde el servidor TFTP, copiandola en running-config o startup-config

```
Router#copy tftp start
Address of remote host [255.255.255.255]? 192.168.1.5
Name of configuration file [Router-confg]?
Configure using Router-confg from 192.168.1.5? [confirm]
Loading Router-confg from 192.168.1.5(via Ethernet0/0): !
[OK - 1005/128975 bytes]
[OK]
Router# reload
```

Obtener Ayuda en línea

- La IOS tiene una utilidad integrada para ayuda
  - use "?" para obtener una lista de posibles comandos
  - `router#?`
- "<comando incompleto> ?" Lista todos los posibles sub-comandos, ej:
  - `router#show ?`
  - `router#show ip ?`

Obtener Ayuda en línea

- "<cadena incompleta>?" También muestra los posibles comandos que empiezan con la cadena

```
router#con?
configure  connect
```

- Esto es diferente que

```
router#conf ?
 memory              Configure from NVRAM
 network             Configure from a TFTP network host
 overwrite-network   Overwrite NV memory from TFTP network host
 terminal            Configure from the terminal
 <cr>
```

Obtener Ayuda en línea

- También funciona en modo de configuración:

```
router(config)#ip a?
accounting-list  accounting-threshold  accounting-transits
  address-pool  alias as-path

router(config)#int e0/0
router(config-if)#ip a?
access-group  accounting  address
```

Obtener Ayuda en línea

- "Explorar" un comando para determinar su sintaxis:

```
router(config-if)#ip addr ?
  A.B.C.D  IP address

router(config-if)#ip addr n.n.n.n ?
  A.B.C.D  IP subnet mask

router(config-if)#ip addr n.n.n.n m.m.m.m ?
  secondary  Make this IP address a secondary address
  <cr>

router(config-if)#ip addr n.n.n.n m.m.m.m
router(config-if)#
```

Ayuda para perezosos

- La tecla TAB puede completar una cadena icompleta

```
router(config)#int<TAB>
router(config)#interface et<TAB>
router(config)#interface ethernet 0
router(config-if)#ip add<TAB>
router(config-if)#ip address n.n.n.n m.m.m.m
```

- Aunque no es necesario. También se aceptan comandos incompletos:

```
router#conf t
router(config)#int e0/0
router(config-if)#ip addr n.n.n.n
```

Más trucos para perezosos

- Registro de comandos
  - IOS mantiene una lista de los comandos introducidos recientemente
    - ↑ trae el comando anterior
    - ↓ trae el comando siguiente
- Edición de la línea
    - ← y → mueven el cursor dentro del comando
    - Ctrl-a le lleva al comienzo de la línea
    - Ctrl-e le lleva al final de la línea
    - Ctrl-k borra desde el cursor hasta el final de la línea

Borrar la configuración

- Para borrar la configuración completamente

```
Router#erase startup-config
```

O

```
Router#write erase
```

Y luego

```
Router#reload
```

El enrutador se reiniciará en modo “setup”, porque no encontrará el archivo de configuración

Listas de Control de Acceso

- Las “access lists” se utilizan para implementar seguridad en los enrutadores
  - Permiten alto grado de control en la red
  - Filtran el flujo de paquetes entrando o saliendo de las interfaces del enrutador
  - Restringen el uso de la red a ciertos usuarios o equipos
  - Prohiben o permiten tipos de tráfico

Reglas de Aplicación de las Listas de Acceso

- Se analizan en orden secuencial: línea 1, línea 2, etc.
- La información de un paquete se compara con la lista hasta que una coincidencia ocurre. Luego de esto NO se sigue comparando.
- Existe una línea de prohibición tácita al final de cada lista. Si un paquete no coincide con ninguna regla, al final se descarta.

Utilización de las listas de acceso

- Listas de Acceso Estándar (1 - 99)
  - Especificaciones de direcciones más simples
  - Generalmente permiten o prohíben el datagrama IP completo
- Listas de Acceso Extendidas (100 - 199)
  - Forma más compleja de especificar direcciones
  - Generalmente permiten o prohíben protocolos (puertos) específicos

Sintaxis de las Listas de Acceso

- Sintaxis de las listas estándar

```
access-list access-list-number {permit | deny} source
  {source-mask}

ip access-group access-list-number {in | out}
```

- Sintaxis de las listas extendidas

```
access-list access-list-number {permit | deny} protocol
  source {source-mask} destination {destination-mask}

ip access-group access-list-number {in | out}
```

Dónde Aplicar las Listas de Acceso

- Aplique las listas de acceso lo más cerca posible de donde se origina el tráfico

Meta-Máscaras

- (Wildcard Masks)
- Se incluyen en las listas de acceso para especificar un nodo, una subred o parte de ella.
- Ejemplos:
  - Para especificar un nodo:
    - 192.168.1.5 0.0.0.0
  - Especificar una red pequeña:
    - 192.168.1.0 – 192.168.1.7 (sería una /29)
      - El tamaño del bloque es 8 y la metamáscara es siempre un número menos que el tamaño del bloque
      - El bloque será entonces: 192.168.1.0 **0.0.0.7**

Meta-Máscaras

- Más ejemplos:
  - Todos los nodos en una /24 (equivalente a clase C)
    - 192.168.1.0 0.0.0.255

Truco para calcular una meta-máscara

- Restar cada octeto (en decimal) de 255
- Para determinar la meta-máscara de 192.168.1.0 255.255.255.240
  - 192.168.1.0 0.0.0.15 {255 – 240}
- Para 192.168.1.0 255.255.252.0
  - 192.168.1.0 0.0.3.255

Ejemplo de Lista de Acceso

- Hacer coincidir las subredes 192.168.0.0 a 192.168.64.0

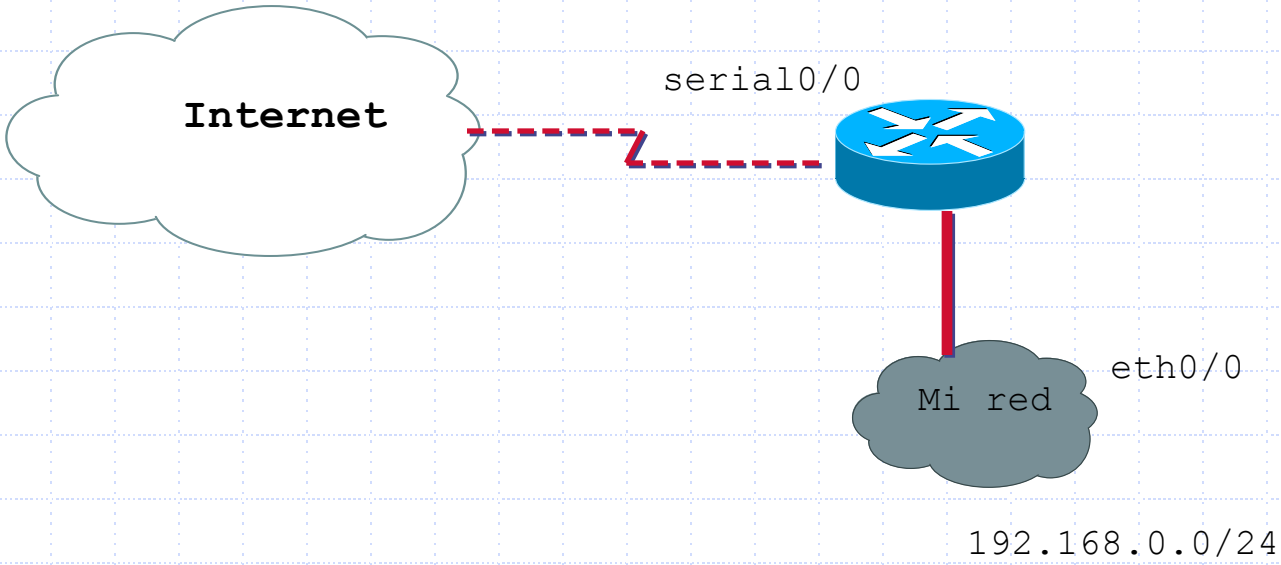
```
ip access-list 99 192.168.0.0 0.0.63.255
```

- Los bits de la meta-máscara indican cómo interpretar los bits de la dirección
  - 0=coincide
  - 1=ignora
- Coincidir con cualquier dirección IP
  - 0.0.0.0 255.255.255.255
  - O abrevie la expresión utilizando la palabra `any`
- Concidir con un nodo en específico
  - 192.168.1.5 0.0.0.0
  - O abrevie la expresión utilizando la palabra `host`

Permitir acceso Telnet a mi red solamente

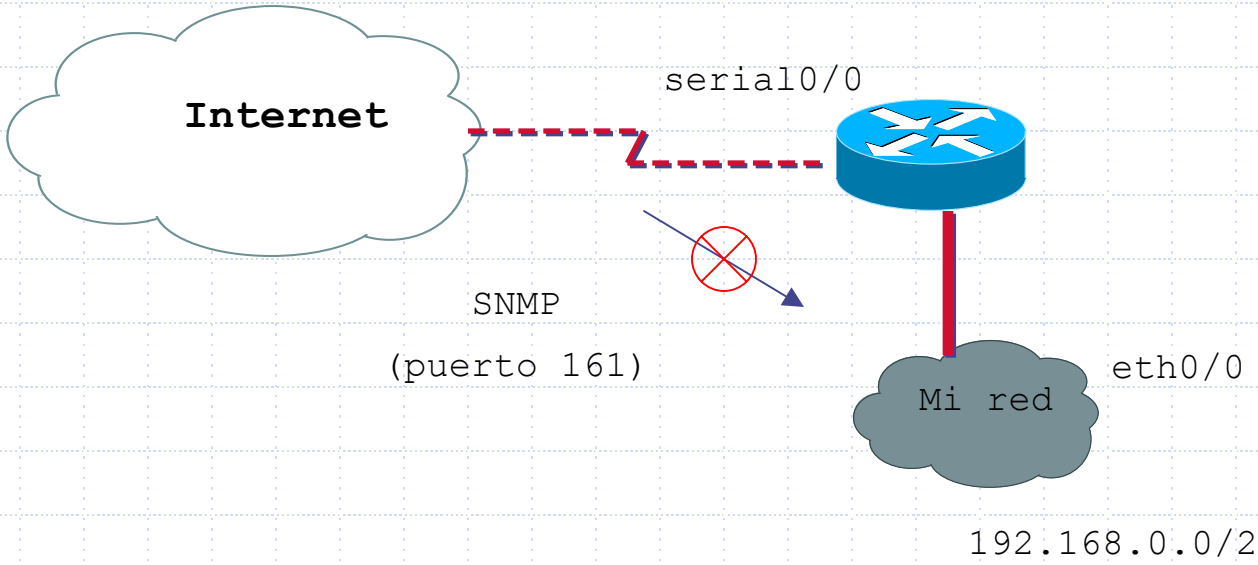
```
access-list 1 permit 192.168.32.192 0.0.0.15
access-list 1 deny any
line vty 0 4
  access-class 1 in
```

Ejemplo de lista de acceso estándar




```
ip access-list 99 permit 192.168.0.0 0.0.0.255
interface eth0/0
   access-group 99 in
```

Ejemplo de lista de acceso extendida
Prohibir la entrada de tráfico SNMP




```
access-list 101 deny udp any 192.168.0.0 0.0.0.255 eq 161 log
access-list 101 permit ip any any

interface serial 0/0
   ip access-group 101 in
```

Recuperación de Desastres – ROM Monitor

- El ROM monitor es muy útil para resolver problemas tales como:
  - Recuperación de contraseñas
  - Instalar una nueva IOS cuando el enrutador no tiene ninguna
  - Seleccionando el lugar dónde buscar el fichero de configuración y su nombre
  - Cambiar la tasa de de bits de la consola para cargar la IOS más rápidamente
  - Cargar un sistema operativo desde el ROM
  - Activar la opción de cargar la configuración desde un servidor TFTP al iniciar

Recuperación de Desastres – ROM Monitor

- Cómo entrar en ROM Monitor
  - Revisar en su emulador de terminal cómo se envía la secuencia de abortar (CTRL-Break)
    - Cuál es en Minicom?

Recuperación de Desastres – Cómo recuperar la contraseña

- Su *config-register* normalmente es 0x2102; use "`show version`" para verificar
- Reinicie el enrutador y envíe la secuencia de "break" durante los primeros 60 segundos para entrar en ROM Monitor
- Una vez allí:

```
rommon 1>confreg 0x2142
rommon 2>reset
```

  - El enrutador se reinicia, ignorando el fichero de configuración

Recuperación de Desastres – Cómo recuperar la contraseña

- **Le preguntará si quiere iniciar "Setup". Diga que no.**

```
Router>enable
Router#copy start run (¡¡no al revés!!)
Router#show run
Router#conf t
Router(config)enable secret <clave nueva>
Router(config)int e0/0…
Router(config-if)no shut
Router(config)config-register 0x2102
Router(config)end
Router#copy run start
Router#reload
```

Gracias