



Gestión de Redes

Configuración Cisco



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Temas

- Modos del CLI (línea de comandos)
- Acceder a la configuración
- Configuración básica (nombre y DNS)
- Autenticación y Autorización (AAA)
- Recopilación de Logs
- Sincronización de tiempo (fecha/zona horaria)
- Configuración de SNMP
- Cisco Discovery Protocol (CDP)
- Flujos de NetFlow (versión 5 y 9)

Modos del CLI

User EXEC

- Acceso limitado al enrutador
- Mostrar alguna información pero no se puede cambiar nada

```
rtr>
```

Privileged EXEC

- Vista completa del estado del enrutador, resolución de problemas, manipular configuración, etc.

```
rtr> enable
```

```
rtr#
```

Acceder al enrutador

Antes de tener SSH activado

- telnet 10.10.x.254
- login “cisco” y “cisco” (usuario y password)

Entrar en modo privilegiado:

- rtr> `enable` (password por defecto “cisco”)
- rtr# `configure terminal`
- rtr(config)#

1. Escribir comandos de configuración

2. Salir del modo privilegiado y guardar

- rtr(config)# `exit`
- rtr# `write memory`

Acceder a la configuración

- Hay dos configuraciones:
 - *Running config* es la configuración activa en el enrutador que está cargada en RAM (se borrará si el enrutador se reinicia):

```
rtr# configure terminal      (conf t)
rtr(config)# end
rtr# show running-config
```

- *Startup config*

Guardada en NVRAM (Non-Volatile RAM):

```
rtr# copy running-config startup-config  (o)
rtr# write memory                        (wr mem)
rtr# show startup-config                 (sh start)
```

Configuración Básica (nombre y DNS)

- Asignar un nombre

```
rtr(config)# hostname rtrX
```

- Asignar un dominio

```
rtr(config)# ip domain-name ws.nsrc.org
```

- Asignar un servidor DNS

```
rtr(config)# ip name-server 10.10.0.241
```

- O desactivar resolución de DNS

```
rtr(config)# no ip domain-lookup
```

Si no hay DNS, esto es muy útil para evitar largas esperas

Autenticación y Autorización

Configurar passwords de la manera más segura.

- Usar el método mejorado que utiliza la función hash

Example:

```
# enable secret 0 cisco
```

```
# user admin secret 0 cisco
```

Autenticación y Autorización

Configurar SSH con una clave de 2048 bits (al menos 768 para OpenSSH clients)

```
rtr(config)# aaa new-model  
rtr(config)# crypto key generate rsa (key size prompt)
```

Verificar que se ha creado:

```
rtr# show crypto key mypubkey rsa
```

Restringir a la versión 2 únicamente. Opcionalmente, registrar eventos:

```
rtr(config)# ip ssh logging events  
rtr(config)# ip ssh version 2
```

Usar SSH, desactivar *telnet* (sólo use telnet si no hay más opción)

```
rtr(config)# line vty 0 4  
rtr(config)# transport input ssh
```

Note: En CatOS, tiene que desactivar telnet explícitamente

Compilando Registros (syslog*)

Enviar logs (registros) al servidor de syslog

```
rtr# logging 10.10.x.x
```

Identificar el canal a usar (local0 to local7):

```
rtr# logging facility local5
```

Hasta qué nivel de prioridad desea registrar?

```
rtr# logging trap <logging_level>
```

<0-7>	Logging severity level	
emergencies	System is unusable	(severity=0)
alerts	Immediate action needed	(severity=1)
critical	Critical conditions	(severity=2)
errors	Error conditions	(severity=3)
warnings	Warning conditions	(severity=4)
notifications	Normal but significant conditions	(severity=5)
informational	Informational messages	(severity=6)
debugging	Debugging messages	(severity=7)

Sincronización temporal

Es esencial que todos los equipos de la red tengan sus relojes sincronizados

En modo config:

```
rtr(config)# ntp server pool.ntp.org          (solo funciona si tiene dns)
rtr(config)# clock timezone <timezone>
```

Para usar la zona horaria UTC

```
rtr(config)# no clock timezone
```

Si su localidad utiliza los horarios de verano:

```
rtr(config)# clock summer-time recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Comprobar

```
rtr# show clock
```

```
22:30:27.598 UTC Tue Feb 15 2011
```

```
rtr# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 4.79.132.217
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**18
reference time is D002CE85.D35E87B9 (11:21:09.825 CMT Tue Aug 3 2010)
clock offset is 2.5939 msec, root delay is 109.73 msec
root dispersion is 39.40 msec, peer dispersion is 2.20 msec
```

Configuración SNMP

Comience con SNMP versión 2

- Es más fácil de usar y configurar
- Ejemplo:

```
rtr(config)# snmp-server community NetManage ro 99  
rtr(config)# access-list 99 permit 10.10.0.0 0.0.255.255
```

Configuración SNMP

Desde una máquina Linux (con los utilitarios net-snmp),
pruebe:

```
snmpwalk -v2c -c NetManage 10.10.x.254 sysDescr
```

Cisco Discovery Protocol (CDP)

Activado por defecto en la mayoría de los enrutadores recientes

Si no está activado:

```
rtr# cdp enable
```

```
rtr# cdp run
```

 (En versiones IOS antiguas)

Para ver vecinos actuales:

```
rtr# show cdp neighbors
```

Herramientas para visualizar los anuncios CDP:

tcpdump

cdpr

wireshark

tshark

Activar NetFlow versión 5

(exportar registros de contabilidad de flujos de tráfico)

Configurar FastEthernet0/0 para generar flujos de NetFlow versión 5 y exportar flujos a 10.10.0.250 al puerto 9996:

```
rtr# configure terminal
rtr# interface FastEthernet 0/0
rtr(config-if)# ip flow ingress
rtr(config-if)# ip flow egress
rtr(config-if)# exit
rtr(config-if)# ip flow-export destination 10.10.0.250 9996
rtr(config-if)# ip flow-export version 5
rtr(config-if)# ip flow-cache timeout active 5
```

Esto secciona los flujos de larga vida en segmentos de 5 minutos. Puede usar cualquier número entre 1 y 60. Si lo deja en el valor por defecto de 30 minutos sus reportes de tráfico tendrán picos.

Nota! Versiones mas nuevas de Cisco IOS ha cambiado la sintaxis de configuración de NetFlow.

Habilitar *top-talkers* en NetFlow versión 5

```
rtr(config)# snmp-server ifindex persist
```

Esto activa la persistencia de los ifIndex. Esto asegura que los índices de interfaces no cambiarán con reinicios, y por lo tanto los registros de Netflow no estarán afectados.

Ahora configure cómo quiere que funcionen las listas top-ten de Netflow:

```
rtr(config)#ip flow-top-talkers
rtr(config-flow-top-talkers)#top 20
rtr(config-flow-top-talkers)#sort-by bytes
rtr(config-flow-top-talkers)#end
```

Ahora comprobaremos lo que hemos hecho

```
rtr# show ip flow export
rt# show ip cache flow
```

Compruebe sus "top talkers"

```
rtr# show ip flow top-talkers
```

Habilitar flujos de NetFlow IPv4 versión 9

Configurar versión 9 de flujos de NetFlow por IPv4 en el interfaz FastEthernet 0/0 y exportarlos a 10.10.0.250 al puerto 9001:

```
rtrX# configure terminal
rtrX(config)# flow exporter EXPORTER-1
rtrX(config-flow-exporter)# description Export to NOC
rtrX(config-flow-exporter)# destination 10.10.0.250
rtrX(config-flow-exporter)# transport udp 9001
rtrX(config-flow-exporter)# template data timeout 300
rtrX(config-flow-exporter)# flow monitor FLOW-MONITOR-V4
rtrX(config-flow-monitor)# exporter EXPORTER-1
rtrX(config-flow-monitor)# record netflow ipv4 original-input
rtrX(config-flow-monitor)# cache timeout active 300
rtr(config)# snmp-server ifindex persist
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 input
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 output
rtrX(config-if)# exit
rtrX# write memory
```

Habilitar flujos de NetFlow IPv4 versión 9

Configurar flujos de NetFlow versión 9 por IPv6:

Para hacer monitoreo de flujos de IPv6 tiene que crear un monitor de flujos nuevo por IPv6 y adjuntarlo a la interfaz y los exportadores existentes

```
rtrX(config-flow-exporter)# flow monitor FLOW-MONITOR-V6
rtrX(config-flow-monitor)# exporter EXPORTER-1
rtrX(config-flow-monitor)# record netflow ipv6 original-input
rtrX(config-flow-monitor)# cache timeout active 300
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 input
rtrX(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 output
rtrX(config-if)# exit
rtrX# write memory
```

Ver flujos de NetFlow versión 9

Estos no son comandos de configuración, solo algunos ejemplos de como ver información de flujos en su enrutador.

Para ver la configuración actual:

```
rtrX# show flow exporter EXPORTER-1
```

```
rtrX# show flow monitor FLOW-MONITOR-V4
```

Es posible ver los flujos individuos y activos en el dispositivo

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache
```

Esto mostrará demasiado flujos. Apreta 'q' y agrupar los flujos para que puedes ver sus "Top Talkers" por destinos de tráfico y fuentes. Esto es un solo comando largo:

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 \
      source address ipv4 destination address sort counter \
      bytes top 20
```

Preguntas?



Para más información

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html