Network Monitoring and Management

Cisco Configuration

INNOG 6

March 22- 25, 2023

Topics

- CLI modes
- Accessing the configuration
- Basic configuration (hostname and DNS)
- Authentication and authorization (AAA)
- Log collection
- Time Synchronization (date/timezone)
- SNMP configuration
- Cisco Discovery Protocol (CDP)
- NetFlow flows (version 5 and 9)

CLI Modes

User EXEC

- Limited access to the router
- Can show some information but cannot view nor change configuration

```
rtr1-gY>
```

Privileged EXEC

- Full view of the router's status, troubleshooting, manipulate config, etc.

```
rtr1-gY> enable
rtr1-gY#
```

Accessing the router (first time)

Before setting up SSH

- telnet to a Cisco network device
- login “cisco” and “cisco” (user and password)
  (We use different <USER> and <PASS> in class)

Privileged user can go to privileged mode:

```
rtr1-gY> enable  (enter <PASS> default is “cisco”)
rtr1-gY# configure terminal
rtr1-gY(config)#
```

Accessing the router (first time) (Contd...)

Now that you are in “config” mode you can adjust router settings. When done:

Exit and save the new configuration

```
rtr1-gY(config)# end
rtr1-gY# write memory
```

- If you don’t “wr mem” (write memory) changes are lost if router reboots.
- We have added a space between “#” and commands for clarity. On the router there is no space.

Accessing the configuration

There are two configurations:

- **Running config** is the actual configuration that is active on the router and stored in RAM (will be gone if router is rebooted):

```
rtr1-gY# configure terminal
rtr1-gY(config)# end
rtr1-gY# show running-config
```

- **Startup config** Stored in NVRAM (Non-Volatile RAM):

```
rtr1-gY# copy running-config startup-config (or)
rtr1-gY# write memory
rtr1-gY# show startup-config
```

Basic configuration (hostname and DNS)

- Assign a name

  ```
  rtr(config)# hostname rtr1-gY
  ```

- Assign a domain

  ```
  rtr(config)# ip domainname lab.shakya.io
  ```

- Assign a DNS server

  ```
  rtr(config)# ip nameserver 183.91.133.2
  ```

- Or, disable DNS resolution

  ```
  rtr(config)# no ip domainlookup
  ```

  if no dns this is very useful to avoid long waits

Authentication & authorization

Configuring passwords:

- Passwords stored as a hash
  example:

```
rtr1-gY# enable secret 0 cisco
rtr1-gY# user admin secret 0 cisco
```

In class we use different user names and passwords.

Authentication & authorization (Contd…)

Configuring SSH with a 2048 bit key (at least 768 for OpenSSH clients)

```
rtr1-gY(config)# aaa newmodel
rtr1-gY(config)# crypto key generate rsa  (key size prompt)
```

Verify key creation:

```
rtr1-gY# show crypto key mypubkey rsa
```

Optionally register events. Restrict to only use SSH version 2 :

```
rtr1-gY(config)# ip ssh logging events
rtr1-gY(config)# ip ssh version 2
```

Use SSH, disable telnet (only use telnet if no other option):

```
rtr1-gY(config)# line vty 0 4
rtr1-gY(config)# transport input ssh
```

Log collection (syslog*)

Send logs to the syslog server:

```
rtr(config)# logging 100.68.1.130. (example)
```

Identify what channel will be used (local0 to local7):

```
rtr(config)# logging facility local5
```

Up to what priority level do you wish to record?

```
rtr(config)# 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)
```

[*] syslog, syslog-ng, rsyslog

Time synchronization

It is essential that all devices in our network are time-synchronized

In config mode:

```
rtr1-gY(config)# ntp server pool.ntp.org
rtr1-gY(config)# clock timezone <timezone>
```

To use UTC time:

```
rtr1-gY(config)# no clock timezone
```

If your site observes daylight savings time you can do:

```
rtr1-gY(config)# clock summertime recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Verify:

```
rtr1-gY# show clock
22:30:27.598 UTC Tue Feb 15 2011

rtr1-gY# show ntp status
Clock is synchronized, stratum 5, reference is 100.68.100.254
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**18
reference time is E174FB19.FE2DDF4A (09:34:17.992 UTC Tue Nov 12 2019)
clock offset is -20.5622 msec, root delay is 391.35 msec
```

SNMP configuration

Start with SNMP version 2

- It’s easier to configure and understand
- Example:

```
rtr1-gY(config)# snmpserver community NetManage ro 99
rtr1-gY(config)# accesslist 99 permit 36.0.4.0 0.0.0.255
rtr1-gY(config)# accesslist 99 permit 36.0.5.0 0.0.0.255
```

Note the Cisco subnet mask inversion:

```
0.0.0.255 == 255.255.255.0  == /24 (254 hosts)
0.0.0.15 == 255.255.255.240  == /28 (14 hosts)
```

SNMP configuration (contd...)

From a Linux machine (once snmp utils are installed), you might try:

```
snmpwalk –v2c –c NetManage rtr1-gY.lab.shakya.io sysDescr
```

Cisco Discovery Protocol (CDP)

Enabled by default in most modern routers

If it’s not enabled:

```
rtr(config)# cdp run
rtr(config-if)# cdp enable(per-interface)
```

To see existing neighbors:

```
rtr# show cdp neighbors
```

Tools to visualize/view CDP announcements:

```
tcpdump, cdpr, wireshark, tshark
```

Enabling NetFlow flows version 5

Configure version 5 NetFlow flows on FastEthernet interface 0/0 and export them to 100.68.1.130 on port 9996

```
rtr1-gY# configure terminal
rtr1-gY(config)# interface FastEthernet 0/0
rtr1-gY(config-if)# ip flow ingress
rtr1-gY(config-if)# ip flow egress
rtr1-gY(config-if)# exit
rtr1-gY(config-if)# ip flow-export destination 100.68.1.130 9996
rtr1-gY(config-if)# ip flow-export version 5
rtr1-gY(config-if)# ip flow-cache timeout active 5
```

This breaks up long-lived flows into 5-minute fragments. You can choose any number of minutes between 1 and 60. If you leave it at the default of 30 minutes your traffic reports will have spikes.

Enabling top-talkers NetFlow (Version 5)

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

Ensures that the ifIndex values are retained over router reboots or if you add/remove interface modules.

Now configure how you want the ip flow top-talkers to work:

```
rtr1-gY(config)# ip flow-top-talkers
rtr1-gY(config-flow-top-talkers)# top 20
rtr1-gY(config-flow-top-talkers)# sort-by bytes
rtr1-gY(config-flow-top-talkers)# end
```

Verify what we've done

```
rtr1-gY# show ip flow export
rtr1-gY# show ip cache flow
```

See your "top talkers" across your router interfaces:

```
rtr1-gY# show ip flow top-talkers
```

Enabling NetFlow IPv4 flows (version 9)

Configure version 9 NetFlow flows for IPv4 on FastEthernet interface 0/0 and export them to 100.68.1.130 on port 9996:

```
rtr1-gY# configure terminal
rtr1-gY(config)# flow exporter EXPORTER-1
rtr1-gY(config-flow-exporter)# description Export to srv1
rtr1-gY(config-flow-exporter)# destination 100.68.1.130
rtr1-gY(config-flow-exporter)# transport udp 9996
rtr1-gY(config-flow-exporter)# template data timeout 300
rtr1-gY(config-flow-exporter)# flow monitor FLOW-MONITOR-V4
rtr1-gY(config-flow-monitor)# exporter EXPORTER-1
rtr1-gY(config-flow-monitor)# record netflow ipv4 original-input
rtr1-gY(config-flow-monitor)# cache timeout active 300
rtr1-gY(config)# snmp-server ifindex persist
rtr1-gY(config)# interface FastEthernet 0/0
rtr1-gY(config-if)# ip flow monitor FLOW-MONITOR-V4 input
rtr1-gY(config-if)# ip flow monitor FLOW-MONITOR-V4 output
rtr1-gY(config-if)# exit
rtr1-gY# write memory
```

Enabling NetFlow IPv6 flows (version 9)

Configure version 9 NetFlow flows for IPv6:
To monitor IPv6 flows you would have to create a new flow monitor for IPv6 and attach it to the interface and the existing exporters.

```
rtr1-gY(config-flow-exporter)# flow monitor FLOW-MONITOR-V6
rtr1-gY(config-flow-monitor)# exporter EXPORTER-1
rtr1-gY(config-flow-monitor)# record netflow ipv6 original-input
rtr1-gY(config-flow-monitor)# cache timeout active 300
rtr1-gY(config)# interface FastEthernet 0/0
rtr1-gY(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 input
rtr1-gY(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 output
rtr1-gY(config-if)# exit
rtr1-gY# write memory
```

Viewing NetFlow flows (version 9)

These are no configuration directives, just a few samples of viewing flow information directly on your router.

To view your current configuration:

```
rtr1-gY# show flow exporter EXPORTER-1
rtr1-gY# show flow monitor FLOW-MONITOR-V4
```

It’s possible to see active individual flows on the device:

```
rtr1-gY# show flow monitor FLOW-MONITOR-V4 cache
```

Will display too many flows. Press ‘q’ to exit display. Group flows so you can see your “Top Talkers” by traffic destinations and sources. This is one long command:

```
rtr1-gY# show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source
         address ipv4 destination address sort counter bytes top 20
```