

11: Best Practices for Managing Cisco Devices

Objectives

- Upon completion of this chapter, you should be able to
 - Describe and follow Best Practices for configuring Cisco routers to be managed
 - Configure Cisco devices for network management

Topics

- SNMP
- Syslog
- Other Amenities
- Time
- Best Practices

Configuring Cisco Devices for SNMP — 1

- Set community strings and enable SNMP

```
Rtr(config)# snmp-server community public RO  
Rtr(config)# snmp-server community private RW
```

- You can add an access list to control which stations SNMP is accepted from

```
Rtr(config)# snmp-server community private RW 60  
Rtr(config)# access-list 60 permit 148.33.1.1
```

Configuring Cisco Devices for SNMP — 2

- Enable SNMP traps
- Specify which management station(s) to send traps to

```
Rtr(config)# snmp-server host 148.33.2.3 public  
Rtr(config)# snmp-server enable trap
```

- Can control which traps go where, by listing specific traps for each host at the end of the **snmp-server host** line
- Can selectively enable only some traps with options at end of **snmp-server enable trap** line
 - One per line, repeat as needed

Configuring Cisco Devices for SNMP — 3

- It is generally a good idea to not enable a couple of the SNMP traps:

```
no snmp-server enable trap snmp authentication  
no snmp-server enable trap syslog
```

- The first of these disables traps when someone uses the wrong community string
 - If this ever happens, you tend to get **many** traps
- The second disables packaging up syslog messages and sending them as traps
 - It's generally adequate to just send them once as syslog messages

Configuring Cisco Devices for SNMP — 4

- Need to allow SNMP reboot of router for CiscoWorks IOS upgrades to succeed

```
Rtr(config)# snmp-server system-shutdown
```

Configuring Cisco Devices for SNMP — 5

- Set system location and contact

```
Rtr(config)# snmp-server location Rome, Italy NOC  
Rtr(config)# snmp-server contact John Doe, (800) 555-1212
```

- Set trap source address to that of loopback 0 for uniformity

```
Rtr(config)# snmp-server trap-source loopback 0
```

Configuring Cisco Devices for SNMP — 6

- Interface command to disable up/down

```
Rtr(config)# interface ...
```

```
Rtr(config-if)# no snmp-server trap link-status
```

- There are many other SNMP settings

```
Rtr(config)# snmp-server ?
```

- Monitoring SNMP

```
Rtr# show snmp
```

```
Rtr# debug snmp packet
```

Caution: debug output can be verbose and cause problems!

Topics

- SNMP
- Syslog
- Other Amenities
- Time
- Best Practices

Enabling Syslog Logging

- Send syslog messages to host(s)
 - Repeat as needed to send to multiple hosts

```
Rtr(config)# logging 148.33.2.3
```

- Set logging level (see also next slide)

```
Rtr(config)# logging trap informational
```

- Set logging source address

```
Rtr(config)# logging source-interface loop 0
```

Logging Levels

- When you configure logging levels, you may use the number or the keyword for the level
 - In the newer IOS releases
 - Older ones required the word
- This configures the router to send or show messages at that level or more severe levels (lower numbered levels)

Level	Keyword to Configure
7	Debug
6	Informational
5	Notifications
4	Warnings
3	Errors
2	Critical
1	Alerts
0	Emergency

Controlling Syslog Logging – 1

- Turn off console logging
 - This protects against having a 9600 baud bottleneck

```
Rtr(config)# no logging console
```

- Turn on logging to buffer (100K of memory)
 - This keeps a history of logging output in the router
 - View the buffer with the **show logging** command (later slide)

```
Rtr(config)# logging buffered 100000
```

Controlling Syslog Logging – 2

- Synchronized logging: no output of console messages or debug output when you're in the middle of typing a command

```
Rtr(config)# line con 0  
Rtr(config-line)# logging synch  
Rtr(config)# line vty 0 4  
Rtr(config-line)# logging synch
```

Checking Logging Status

```
top#show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-
limited, 0 flushes, 0 overruns)
  Console logging: level debugging, 22 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 1 messages logged
  Logging Exception size (0 bytes)
  Trap logging: level informational, 26 message lines logged
    Logging to 148.33.2.130, 26 message lines logged

Log Buffer (100000 bytes):

%SYS-5-CONFIG_I: Configured from console by vty0 (148.33.2.150)
```

Press Enter to get past the "--More--" and see buffered messages

The 4 ways to view syslog messages, and level of output for each



Copyright © 2003, Chesapeake Netcraftsmen

11-15

The 4 Ways to Syslog

- Console: settings for output on console
- Monitor: settings for what messages you get when you telnet into the router
 - Use the **terminal monitor** command to see the messages for the duration of the telnet session
 - Or can configure vty lines to permanently monitor, if desired
- Buffer: settings for buffered messages in memory
- Trap logging: messages sent via syslog to a management stations



Copyright © 2003, Chesapeake Netcraftsmen

11-16

Topics

- SNMP
- Syslog
- Other Amenities
- Time
- Best Practices

Setting Idle Timeout

- Idle timeout terminates console or telnet session if you don't type anything
 - Good security
 - Annoying in the middle of troubleshooting
- To control the idle timeout, can configure:

```
Rtr(config)# line con 0
Rtr(config-line)# exec-timeout 0 0
Rtr(config)# line vty 0 4
Rtr(config-line)# exec-timeout 10 0
```

Configuring to Allow RCP

- CiscoWorks can use RCP (reliable TCP-based protocol) to copy files to/from devices
- But you have to permit it on the device first
- Configure

```
Rtr(config)# ip rcmd rcp-enable  
Rtr(config)# ip rcmd remote-host cwuser 148.33.2.3  
cwuser enable
```

- where 148.33.2.3 is the CW management station
- cwuser is the CW default rcp user id, can be changed

Enabling Web Interface to Routers

- The Web router interface is enabled by configuring:

```
Rtr(config)# ip http server
```

- The Web interface is really the CLI help presented as links you can click on

Topics

- SNMP
- Syslog
- Other Amenities
- Time
- Best Practices

Configuring Timestamps

- You can turn on timestamps for syslog and debug messages as follows

```
Rtr(config)# service timestamps log datetime  
show-timezone  
Rtr(config)# service timestamps debug  
datetime show-timezone
```

- CW Best Practice: use GMT, timezones can lead to problems

Setting the Timezone

- Set the timezone with the command

```
Rtr(config)# clock timezone EST -5
```

Configuring NTP

- NTP provides consistent time
 - Need a time source
 - Can instead configure some router as ntp server, say at stratum 2

```
Rtr(config)# ntp master 2
```

- Build a hierarchy of routers, referring to higher-stratum routers / NTP servers:

```
Rtr(config)# ntp server 5.6.7.8
```

- Have computers refer to routers for time

Checking NTP

- Check on NTP with the **show ntp status** command
- Unsynchronized is bad...

```
top#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**16
reference time is 00000000.00000000 (19:00:00.000 EST Thu Dec 31 1899)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
```

Checking NTP

- Look for status to be synchronized

```
top#sho ntp st
Clock is synchronized, stratum 5, reference is 148.33.8.2
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**16
reference time is AF3BF74C.F0016C00 (21:45:32.937 EST Sun Feb 28 1993)
clock offset is 4.1810 msec, root delay is 3.22 msec
root dispersion is 1879.62 msec, peer dispersion is 1875.41 msec

top#sho ntp assoc

  address      ref clock    st when poll reach  delay  offset  disp
*~148.33.8.2  127.127.7.1  4   57   64  17    3.2   4.18  1875.4

* master (syncd), # master (unsyncd), + selected, - candidate, ~
  configured
```

Topics

- SNMP
- Syslog
- Other Amenities
- Time
- Best Practices

Best Practices — 1

- Consistent login passwords
- Consistent enable passwords
- Common SNMP community strings
 - Think twice about “public” RO
 - Do NOT do “private” as RW string
- Use interface description lines
- Consistent DNS / host table, or else use just addresses
 - HPOV netmon gets unhappy with inconsistent DNS information

Best Practices — 2

- CiscoWorks assumes the login prompt ends in “>”, enable prompt in “#”
 - Do not use the `prompt` command to change the prompt!
- Send syslog messages to CW workstation
- Send SNMP traps to HPOV workstation

Don't Forget

- After you make changes to the configuration, you need to:

```
Rtr# copy run start
```

Review Questions

- What is the bare minimum you need to configure to enable SNMP on a Cisco router?
- Explain the difference between the **snmp-server host** command and the **logging** command
- What's the best way to synchronize time between network devices? What commands are needed to do this?
- Why should you strongly consider not logging to console?
- Explain how logging levels work
- What's the difference between options at the end of the **snmp-server host** command and options at the end of the **snmp-server enable trap** command?

Summary

- Having completed this chapter, you should be able to
 - Describe and follow Best Practices for configuring Cisco routers to be managed
 - Configure Cisco devices for network management