Module 10: Network Management

Instructor Materials

Enterprise Networking, Security, and Automationv7.0 (ENSA)

Module 10: Network Management

Enterprise Networking, Security, and Automation v7.0 (ENSA)

Module Objectives

Module Title: Network Management

Module Objective: Implement protocols to manage the network.

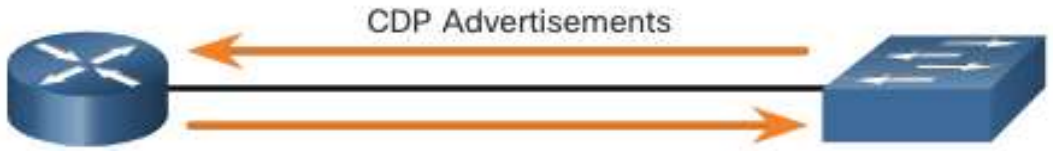
Topic Title	Topic Objective
Device Discovery with CDP	Use CDP to map a network topology.
Device Discovery with LLDP	Use LLDP to map a network topology.
NTP	Implement NTP between an NTP client and NTP server.
SNMP	Explain how SNMP operates.
Syslog	Explain syslog operation.
Router and Switch File Maintenance	Use commands to back up and restore an IOS configuration file.
IOS Image Management	Implement protocols to manage the network.

10.1 Device Discovery with CDP

CDP Overview

CDP is a Cisco proprietary Layer 2 protocol that is used to gather information about Cisco devices which share the same data link. CDP is media and protocol independent and runs on all Cisco devices, such as routers, switches, and access servers.

The device sends periodic CDP advertisements to connected devices. These advertisements share information about the type of device that is discovered, the name of the devices, and the number and type of the interfaces.



Configure and Verify CDP

- For Cisco devices, CDP is enabled by default. To verify the status of CDP and display information about CDP, enter the **show cdp** command.
- To disable CDP on a specific interface, enter **no cdp enable** in the interface configuration mode. CDP is still enabled on the device; however, no more CDP advertisements will be sent out that interface. To enable CDP on the specific interface again, enter **cdp enable.**
- To enable CDP globally for all the supported interfaces on the device, enter **cdp run** in the global configuration mode. CDP can be disabled for all the interfaces on the device with the **no cdp run** command in the global configuration mode.
- Use the **show cdp interface** command to display the interfaces that are CDP-enabled on a device. The status of each interface is also displayed.

Discover Devices by Using CDP

- With CDP enabled on the network, the **show cdp neighbors** command can be used to determine the network layout, as shown in the output.
- The output shows that there is another Cisco device, S1, connected to the G0/0/1 interface on R1. Furthermore, S1 is connected through its F0/5

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme  Capability   Platform     Port ID
S1               Gig 0/0/1           179       S I       WS-C3560-    Fas 0/5
```

Discover Devices by Using CDP (Cont.)

The network administrator uses **show cdp neighbors detail** to discover the IP address for S1. As displayed in the output, the address for S1 is 192.168.1.2.

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

(output omitted)
```

Packet Tracer - Use CDP to Map a Network

A senior network administrator requires you to map the Remote Branch Office network and discover the name of a recently installed switch that still needs an IPv4 address to be configured. Your task is to create a map of the branch office network. To map the network, you will use SSH for remote access and the Cisco Discovery Protocol (CDP) to discover information about neighboring network devices, like routers and switches.

10.2 Device Discovery with LLDP

LLDP Overview

Link Layer Discovery Protocol (LLDP) is a vendor-neutral neighbor discovery protocol similar to CDP. LLDP works with network devices, such as routers, switches, and wireless LAN access points. This protocol advertises its identity and capabilities to other devices and receives the information from a physically-connected Layer 2 device.

Configure and Verify LLDP

- LLDP may be enabled by default. To enable LLDP globally on a Cisco network device, enter the **lldp run** command in the global config mode. To disable LLDP, enter the **no lldp run** command in the global config mode.
- LLDP can be configured on specific interfaces. However, LLDP must be configured separately to transmit and receive LLDP packets.
- To verify LLDP is enabled, enter the **show lldp** command in privileged EXEC mode.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

Discover Devices by Using LLDP

With LLDP enabled, device neighbors can be discovered by using the **show lldp neighbors** command.

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf     Hold-time      Capability     Port ID
R1             Fa0/5          117            R              Gi0/0/1
S2             Fa0/1          112            B              Fa0/1
Total entries displayed: 2
```

Discover Devices by Using LLDP (Cont.)

When more details about the neighbors are needed, the **show lldp neighbors detail** command can provide information, such as the neighbor IOS version, IP address, and device capability.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1
System Description: Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_.....,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
(output omitted)
```

Packet Tracer - Use LLDP to Map a Network

In this Packet Tracer activity, you will complete the following objectives:

- Build the Network and Configure Basic Device Settings
- Network Discovery with CDP
- Network Discovery with LLDP

10.3 NTP

Time and Calendar Services

- The software clock on a router or switch starts when the system boots. It is the primary source of time for the system. It is important to synchronize the time across all devices on the network. When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event.
- Typically, the date and time settings on a router or switch can be set by using one of two methods You can manually configure the date and time, as shown in the example, or configure the Network Time Protocol (NTP).

```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been
updated from 21:32:31 UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15
2019, configured from console by console.
```

Time and Calendar Services (Cont.)

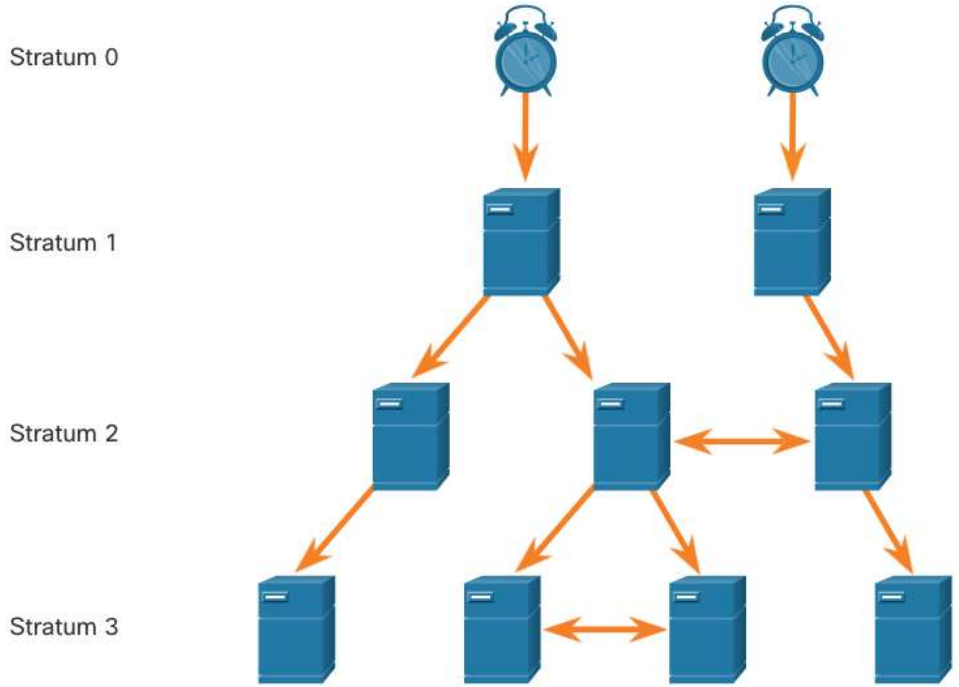
As a network grows, it becomes difficult to ensure that all infrastructure devices are operating with synchronized time using the manual method.

A better solution is to configure the NTP on the network. This protocol allows routers on the network to synchronize their time settings with an NTP server, which provides more consistent time settings. NTP can be set up to synchronize to a private master clock, or it can synchronize to a publicly available NTP server on the internet. NTP uses UDP port 123 and is documented in RFC 1305.

NTP Operation

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum level is defined as the number of hop counts from the authoritative source. The synchronized time is distributed across the network by using NTP.

The max hop count is 15. Stratum 16, the lowest stratum level, indicates that a device is unsynchronized.



NTP Operation (Cont.)

- **Stratum 0:** These authoritative time sources are high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them.
- **Stratum 1:** Devices that are directly connected to the authoritative time sources. They act as the primary network time standard.
- **Stratum 2 and Lower:** Stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time by using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

Time servers on the same stratum level can be configured to act as a peer with other time servers on the same stratum level for backup or verification of time.

Configure and Verify NTP

- Before NTP is configured on the network, the **show clock** command displays the current time on the software clock. With the **detail** option, notice that the time source is user configuration. That means the time was manually configured with the **clock** command.
- The **ntp server** *ip-address* command is issued in global configuration mode to configure 209.165.200.225 as the NTP server for R1. To verify the time source is set to NTP, use the **show clock detail** command. Notice that now the time source is NTP.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

Configure and Verify NTP (Cont.)

The **show ntp associations** and **show ntp status** commands are used to verify that R1 is synchronized with the NTP server at 209.165.200.225. Notice that R1 is synchronized with a stratum 1 NTP server at 209.165.200.225, which is synchronized with a GPS clock. The **show ntp status** command displays that R1 is now a stratum 2 device that is synchronized with the NTP server at 209.165.220.225.

```
R1# show ntp associations

address             ref clock      st   when poll each delay offset disp
*~209.165.200.225   .GPS.          1    61   64   377  0.481 7.480  4.261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
(output omitted)
```

Configure and Verify NTP (Cont.)

- The clock on S1 is configured to synchronize to R1 with the **ntp server** command and the configuration is verified with the **show ntp associations** command.
- Output from the **show ntp associations** command verifies that the clock on S1 is now synchronized with R1 at 192.168.1.1 via NTP. R1 is a stratum 2 device, making S1 is a stratum 3 device that can provide NTP service to other devices in the network.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
address         ref clock       st when poll reach  delay  offset  disp
*~192.168.1.1   209.165.200.225  2   12   64   377    1.066  13.616  3.840
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
(output omitted)

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
(output omitted
```

Packet Tracer - Configure and Verify NTP

In this Packet Tracer, you will configure NTP on R1 and R2 to allow time synchronization.

10.4 SNMP

Introduction to SNMP

SNMP was developed to allow administrators to manage nodes on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

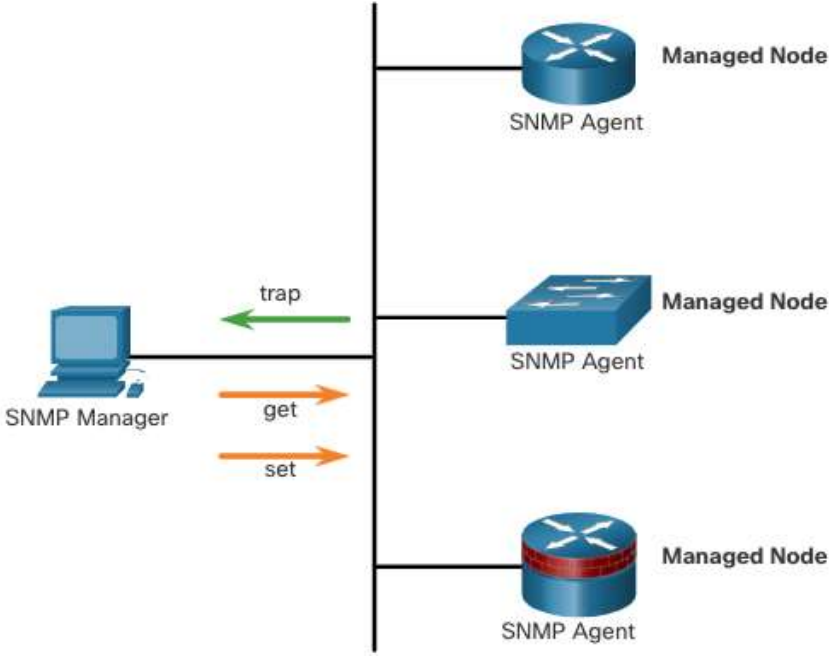
SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements:

- SNMP manager
- SNMP agents (managed node)
- Management Information Base (MIB)

SNMP defines how management information is exchanged between network management applications and management agents. The SNMP manager polls the agents and queries the MIB for SNMP agents on UDP port 161. SNMP agents send any SNMP traps to the SNMP manager on UDP port 162.

Introduction to SNMP (Cont.)

- The SNMP manager is part of a network management system (NMS). The SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action. SNMP agents can forward information directly to a network manager by using “traps”.
- The SNMP agent and MIB reside on SNMP client devices. MIBs store data about the device and operational statistics and are meant to be available to authenticated remote users. The SNMP agent is responsible for providing access to the local MIB.



SNMP Operation

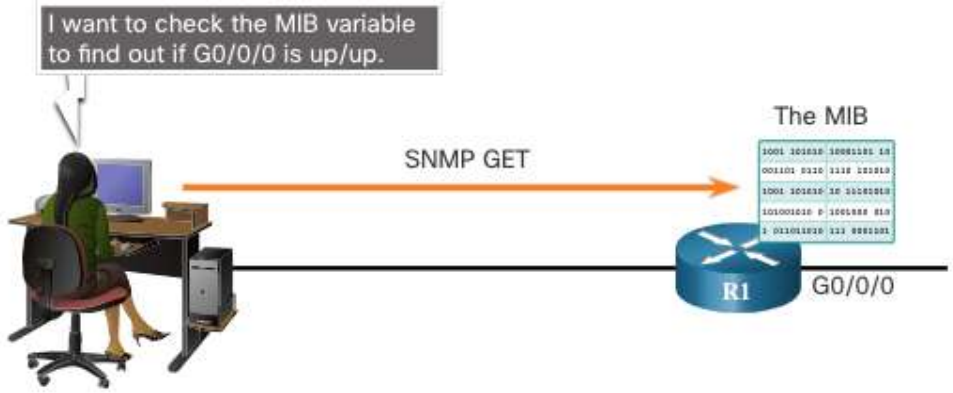
- SNMP agents that reside on managed devices collect and store information about the device and its operation locally in the MIB. The SNMP manager then uses the SNMP agent to access information within the MIB.
- There are two primary SNMP manager requests, get and set. In addition to configuration, a set can cause an action to occur, like restarting a router.

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
get-bulk-request	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
get-response	Replies to a **get-request, get-next-request,** and **set-request** sent by an NMS.
set-request	Stores a value in a specific variable.

SNMP Operation (Cont.)

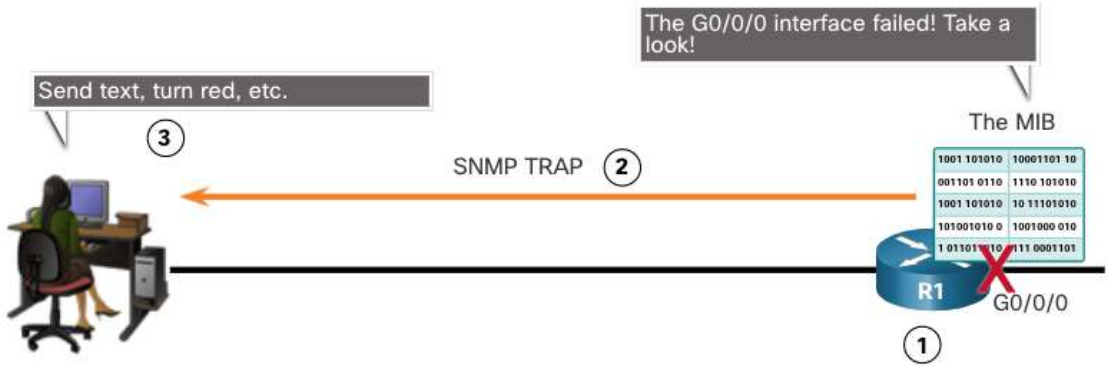
The SNMP agent responds to SNMP manager requests as follows:

- **Get an MIB variable** - The SNMP agent performs this function in response to a GetRequest-PDU from the network manager. The agent retrieves the value of the requested MIB variable and responds to the network manager with that value.
- **Set an MIB variable** - The SNMP agent performs this function in response to a SetRequest-PDU from the network manager. The SNMP agent changes the value of the MIB variable to the value specified by the network manager. An SNMP agent reply to a set request includes the new settings in the device.



SNMP Agent Traps

- Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network. Trap-directed notifications reduce network and agent resources by eliminating the need for some of SNMP polling requests.
- The figure illustrates the use of an SNMP trap to alert the network administrator that interface G0/0/0 has failed. The NMS software can send the network administrator a text message, pop up a window on the NMS software, or turn the router icon red in the NMS GUI.



SNMP Versions

- SNMPv1 - Legacy standard defined in RFC 1157. Uses a simple community-string based authentication method. Should not be used due to security risks.
- SNMPv2c - Defined in RFCs 1901-1908. Uses a simple community-string based authentication method. Provides for bulk retrieval options, as well as more detailed error messages.
- SNMPv3 - Defined in RFCs 3410-3415. Uses username authentication, provides data protection using HMAC-MD5 or HMAC-SHA and encryption using DES, 3DES, or AES encryption.

Community Strings

SNMPv1 and SNMPv2c use community strings that control access to the MIB. Community strings are plaintext passwords. SNMP community strings authenticate access to MIB objects.

There are two types of community strings:

- **Read-only (ro)** - This type provides access to the MIB variables, but does not allow these variables to be changed, only read. Because security is minimal in version 2c, many organizations use SNMPv2c in read-only mode.
- **Read-write (rw)** - This type provides read and write access to all objects in the MIB.

To view or set MIB variables, the user must specify the appropriate community string for read or write access.

MIB Object ID

The MIB organizes variables hierarchically. Formally, the MIB defines each variable as an object ID (OID). OIDs uniquely identify managed objects. The MIB organizes the OIDs based on RFC standards into a hierarchy of OIDs, usually shown as a tree.

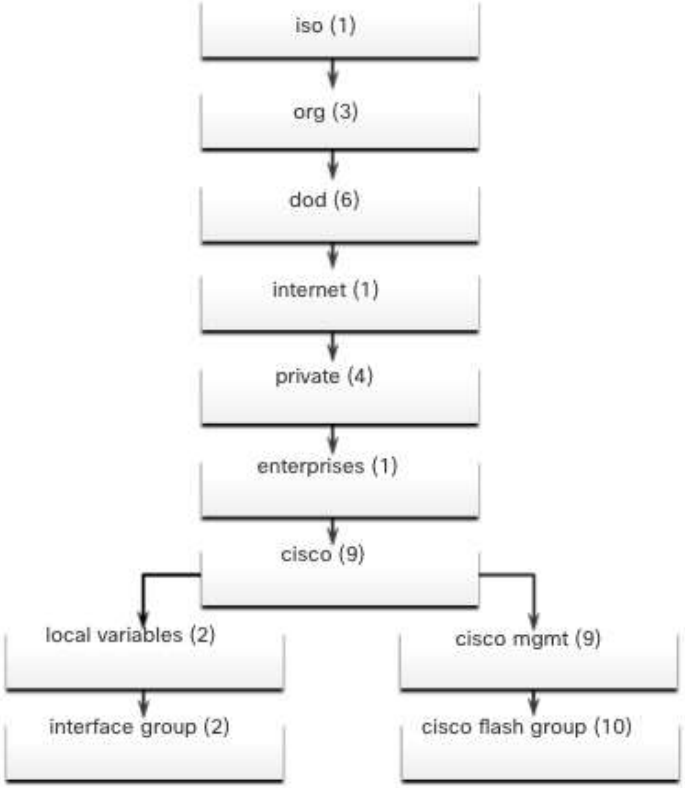
- The MIB tree for any given device includes some branches with variables common to many networking devices and some branches with variables specific to that device or vendor.
- RFCs define some common public variables. Most devices implement these MIB variables. In addition, networking equipment vendors, like Cisco, can define their own private branches of the tree to accommodate new variables specific to their devices.

MIB Object ID (Cont.)

The figure shows portions of the MIB structure defined by Cisco. Note how the OID can be described in words or numbers to help locate a particular variable in the tree.

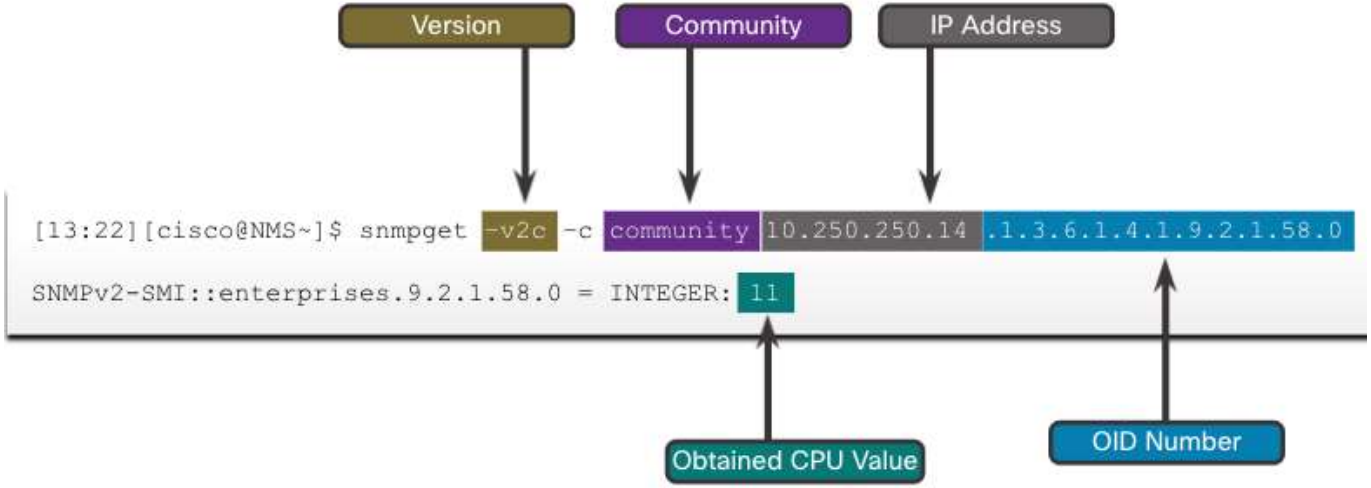
OIDs belonging to Cisco, are numbered as follows: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9).

Therefore, the OID is 1.3.6.1.4.1.9.



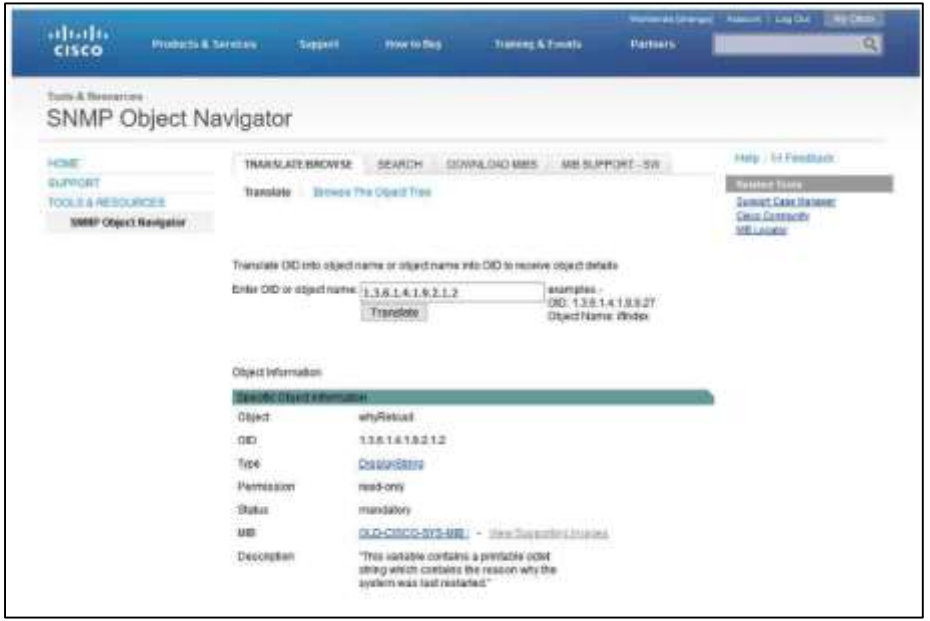
SNMP Polling Scenario

- SNMP can be used is to observe CPU utilization over a period of time by polling devices. CPU statistics can then be compiled on the NMS and graphed. This creates a baseline for the network administrator.
- The data is retrieved via the snmpget utility, issued on the NMS. Using the snmpget utility, you can manually retrieve real-time data, or have the NMS run a report. This report would give you a period of time that you could use the data to get the average.



SNMP Object Navigator

The snmpget utility gives some insight into the basic mechanics of how SNMP works. However, working with long MIB variable names like 1.3.6.1.4.1.9.2.1.58.0 can be problematic for the average user. More commonly, the network operations staff uses a network management product with an easy-to-use GUI, which makes the entire MIB data variable naming transparent to the user.



The Cisco SNMP Navigator on the http://www.cisco.com website allows a network administrator to research details about a particular OID.

Lab - Research Network Monitoring Software

In this lab, you will complete the following objectives:

- Part 1: Survey Your Understanding of Network Monitoring
- Part 2: Research Network Monitoring Tools
- Part 3: Select a Network Monitoring Tool

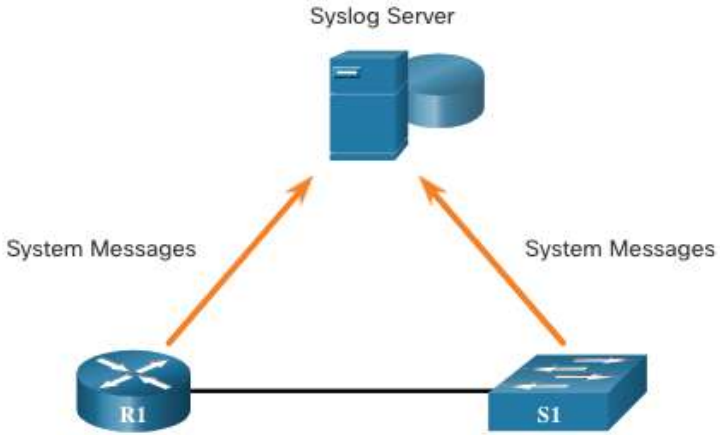
10.5 Syslog

Introduction to Syslog

Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors, as shown in the figure.

The syslog logging service provides three primary functions, as follows:

- The ability to gather logging information for monitoring and troubleshooting
- The ability to select the type of logging information that is captured
- The ability to specify the destinations of captured syslog messages



Syslog Operation

The syslog protocol starts by sending system messages and **debug** output to a local logging process. Syslog configuration may send these messages across the network to an external syslog server, where they can be retrieved without needing to access the actual device.

Alternatively, syslog messages may be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device.

The network administrator may specify that only certain types of system messages be sent to various destinations. Popular destinations for syslog messages include the following:

- Logging buffer (RAM inside a router or switch)
- Console line
- Terminal line
- Syslog server

Syslog Message Format

Cisco devices produce syslog messages as a result of network events. Every syslog message contains a severity level and a facility.

The smaller numerical levels are the more critical syslog alarms. The severity level of the messages can be set to control where each type of message is displayed (i.e. on the console or the other destinations). The complete list of syslog levels is shown in the table.

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Syslog Facilities

In addition to specifying the severity, syslog messages also contain information on the facility. Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting. The logging facility options that are available are specific to the networking device.

Some common syslog message facilities reported on Cisco IOS routers include:

- IP
- OSPF protocol
- SYS operating system
- IP security (IPsec)
- Interface IP (IF)

Syslog Facilities (Cont.)

By default, the format of syslog messages on the Cisco IOS Software is as follows:

%facility-severity-MNEMONIC: description

For example, sample output on a Cisco switch for an EtherChannel link changing state to up is:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN.

Configure Syslog Timestamp

By default, log messages are not timestamped. Log messages should be timestamped so that when they are sent to another destination, such as a Syslog server, there is record of when the message was generated. Use the command **service timestamps log datetime** to force logged events to display the date and time.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

10.6 Router and Switch File Maintenance

Router File Systems

The Cisco IOS File System (IFS) allows the administrator to navigate to different directories and list the files in a directory. The administrator can also create subdirectories in flash memory or on a disk. The directories available depend on the device.

The example displays the output of the **show file systems** command, which lists all of the available file systems on a Cisco 4221 router.

```
Router# show file systems
File Systems:
      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
*  7194652672    6294822912      disk     rw   bootflash: flash:
   256589824     256573440      disk     rw   usb0:
  1804468224    1723789312      disk     ro   webui:
            -             -    opaque     rw   null:
            -             -    opaque     ro   tar:
            -             -   network     rw   tftp:
            -             -    opaque     wo   syslog:
     33554432      33539983     nvram     rw   nvram:
            -             -   network     rw   rcp:
            -             -   network     rw   ftp:
            -             -   network     rw   http:
            -             -   network     rw   scp:
            -             -   network     rw   sftp:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
Router#
```

The asterisk indicates the current default file system. The pound sign (#) indicates a bootable disk. Both of these are assigned to the flash file system by default

Router File Systems (Cont.)

Because flash is the default file system, the **dir** command lists the contents of flash. Of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.

```
Router# dir
Directory of bootflash:/
   11  drwx            16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx             4096    Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx             4096    Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx             4096    Aug 2 2019 04:17:59 +00:00  core
379009  drwx             4096   Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx              4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx             4096    Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx           102400    Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx             4096   Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx             4096    Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30    Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx             4096    Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34    Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx             4096   Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037    Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908   Sep 19 2019 14:16:23 +00:00
isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193   Sep 21 2019 04:24:04 +00:00  isr4200-
universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

Router File Systems (Cont.)

To view the contents of NVRAM, you must change the current default file system by using the **cd** (change directory) command, as shown in the example.

The present working directory command is **pwd**. This command verifies that we are viewing the NVRAM directory. Finally, the **dir** command lists the contents of NVRAM. Although there are several configuration files listed, of specific interest is the startup-configuration file.

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-             1024                    startup-config
32770  ----               61                    private-config
32771  -rw-             1024                    underlying-config
    1  ----                4                    private-KS1
    2  -rw-             2945                    cwmp_inventory
    5  ----              447                    persistent-data
    6  -rw-             1237                    ISR4221-2x1GE_0_0_0
    8  -rw-               17                    ecfm_ieee_mib
    9  -rw-                0                    ifIndex-table
   10  -rw-             1431                    NIM-2T_0_1_0
   12  -rw-              820                    IOS-Self-Sig#1.cer
   13  -rw-              820                    IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

Switch File Systems

With the Cisco 2960 switch flash file system, you can copy configuration files, and archive (upload and download) software images.

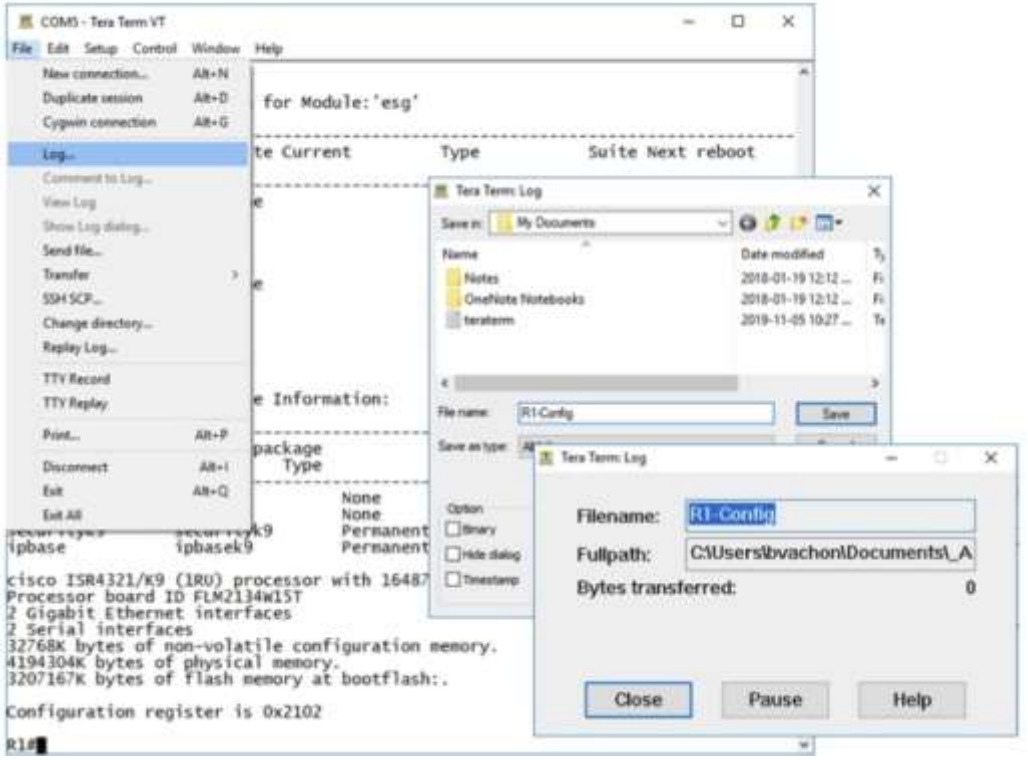
The command to view the file systems on a Catalyst switch is the same as on a Cisco router: **show file systems.**

```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*     32514048    20887552     flash     rw   flash:
          -           -       opaque    rw      vb:
          -           -       opaque    ro      bs:
          -           -       opaque    rw  system:
          -           -       opaque    rw  tmpsys:
         65536       48897     nvram     rw   nvram:
          -           -       opaque    ro  xmodem:
          -           -       opaque    ro  ymodem:
          -           -       opaque    rw    null:
          -           -       opaque    ro     tar:
          -           -      network    rw    tftp:
          -           -      network    rw     rcp:
          -           -      network    rw    http:
          -           -      network    rw     ftp:
          -           -      network    rw     scp:
          -           -      network    rw   https:
          -           -      opaque     ro     cns:
Switch#
```

Use a Text File to Back Up a Configuration

Configuration files can be saved to a text file by using Tera Term:

Step 1. On the File menu, click **Log**.
Step 2. Choose the location to save the file. Tera Term will begin capturing text.
Step 3. After capture has been started, execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be directed to the chosen file.
Step 4. When the capture is complete, select **Close** in the Tera Term: Log window.
Step 5. View the file to verify that it was not corrupted.



Use a Text File to Restore a Configuration

A configuration can be copied from a file and then directly pasted to a device. The file will require editing to ensure that encrypted passwords are in plaintext, and that non-command text such as **--More--** and IOS messages are removed.

In addition, you may want to add **enable** and **configure terminal** to the beginning of the file or enter global configuration mode before pasting the configuration. Instead of copying and pasting, a configuration can be restored from a text file by using Tera Term. When using Tera Term, the steps are as follows:

Step 1. On the File menu, click **Send** file.
Step 2. Locate the file to be copied into the device and click **Open**.
Step 3. Tera Term will paste the file into the device.

The text in the file will be applied as commands in the CLI and become the running configuration on the device.

Using TFTP to Back Up and Restore a Configuration

Follow these steps to back up the running configuration to a TFTP server:

Step 1. Enter the **copy running-config tftp** command.
Step 2. Enter the IP address of the host where the configuration file will be stored.
Step 3. Enter the name to assign to the configuration file.
Step 4. Press Enter to confirm each choice.

Use the following steps to restore the running configuration from a TFTP server:

Step 1. Enter the **copy tftp running-config** command.
Step 2. Enter the IP address of the host where the configuration file is stored.
Step 3. Enter the name to assign to the configuration file.
Step 4. Press **Enter** to confirm each choice.

```
R1# copy running-config tftp
Remote host []?192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!!! [OK]
```

USB Ports on a Cisco Router

The Universal Serial Bus (USB) storage feature enables certain models of Cisco routers to support USB flash drives. The USB flash feature provides an optional secondary storage capability and an additional boot device. The USB ports of a Cisco 4321 Router are shown in the figure.

Use the **dir** command to view the contents of the USB flash drive.

Using USB to Back Up and Restore a Configuration

- Issue the **show file systems** command to verify that the USB drive is there and confirm its name. For this example, the USB file system is named **usbflash0:**.
- Use the **copy run usbflash0:/** command to copy the configuration file to the USB flash drive. Be sure to use the name of the flash drive, as indicated in the file system. The slash is optional but indicates the root directory of the USB flash drive.
- The IOS will prompt for the filename. If the file already exists on the USB flash drive, the router will prompt to overwrite.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

Using USB to Back Up and Restore a Configuration (Cont.)

Use the **dir** command to see the file on the USB drive and use the **more** command to see the contents.

To Restore Configurations with a USB Flash Drive, it will be necessary to edit the USB R1-Config file with a text editor. Assuming the file name is **R1-Config**, use the command **copy usbflash0:/R1-Config** *running-config* to restore a running configuration.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
R1#
```

Password Recovery Procedures

Passwords on devices are used to prevent unauthorized access. For encrypted passwords, such as the enable secret passwords, the passwords must be replaced after recovery. Depending on the device, the detailed procedure for password recovery varies.

However, all the password recovery procedures follow the same principle:

Step 1. Enter the ROMMON mode.
Step 2. Change the configuration register.
Step 3. Copy the startup-config to the running-config.
Step 4. Change the password.
Step 5. Save the running-config as the new startup-config.
Step 6. Reload the device.

Password Recovery Example

Step 1. Enter the ROMMON mode. With console access, a user can access the ROMMON mode by using a break sequence during the boot up process or removing the external flash memory when the device is powered off.

When successful, the **rommon 1 >** prompt displays, as shown in the example.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Password Recovery Example (Cont.)

Step 2. Change the configuration register. The **confreg 0x2142** command allows the user to set the configuration register to 0x2142, which causes the device to ignore the startup config file during startup.

After setting the configuration register to 0x2142, type **reset** at the prompt to restart the device. Enter the break sequence while the device is rebooting and decompressing the IOS. The example displays the terminal output of a 1941 router in the ROMMON mode after using a break sequence during the boot up process.

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

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Password Recovery Example (Cont.)

Step 3. Copy the startup-config to the running-config. After the device has finished reloading, issue the **copy startup-config running-config** command.

CAUTION: Do not enter **copy running-config startup-config**. This command erases your original startup configuration.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Password Recovery Example (Cont.)

Step 4. Change the password. Because you are in privileged EXEC mode, you can now configure all the necessary passwords.

Note: The password **cisco** is not a strong password and is used here only as an example

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable secret cisco
```

Password Recovery Example (Cont.)

Step 5. Save the running-config as the new startup-config. After the new passwords are configured, change the configuration register back to 0x2102 by using the **config-register 0x2102** command in the global configuration mode. Save the running-config to startup-config.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

Packet Tracer - Backup Configuration Files

In this activity, you will complete the following objectives:

- Part 1: Establish Connectivity to TFTP Server
- Part 2: Transfer the Configuration File from TFTP Server
- Part 3: Backup Configuration and IOS to TFTP Server

Lab - Use Tera Term to Manage Router Configuration Files

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Use Terminal Emulation Software to Create a Backup Configuration File
- Part 3: Use a Backup Configuration File to Restore a Router

Packet Tracer - Use TFTP, Flash, and USB to Manage Configuration Files – Physical Mode
Lab - Use TFTP, Flash, and USB to Manage Configuration Files

In this Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Part 1: Cable the Network and Configure Basic Device Settings
- Part 2: Use TFTP to Back Up and Restore the Switch Running Configuration
- Part 3: Use TFTP to Back Up and Restore the Router Running Configuration
- Part 4: Back Up and Restore Running Configurations Using Router Flash Memory
- Part 5: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration (Lab only)

Packet Tracer – Research Password Recovery Procedures – Physical Mode
Lab - Research Password Recovery Procedures

In this Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Part 1: Research the Configuration Register
- Part 2: Document the Password Recovery Procedure for a Specific Cisco Router

10.7 IOS Image Management

Video - Managing Cisco IOS Images

This video will demonstrate the process of upgrading the IOS on a Cisco router.

TFTP Servers as a Backup Location

As a network grows, Cisco IOS Software images and configuration files can be stored on a central TFTP server. This helps to control the number of IOS images and the revisions to those IOS images, as well as the configuration files that must be maintained.

Production internetworks usually span wide areas and contain multiple routers. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image on the router becomes corrupted or accidentally erased.

Widely distributed routers need a source or backup location for Cisco IOS Software images. Using a network TFTP server allows image and configuration uploads and downloads over the network. The network TFTP server can be another router, a workstation, or a host system.

Backup IOS Image to TFTP Server Example

To maintain network operations with minimum down time, it is necessary to have procedures in place for backing up Cisco IOS images. This allows the network administrator to quickly copy an image back to a router in case of a corrupted or erased image. Use the following steps:

Step 1. Ping the TFTP server. Ping the TFTP server to test connectivity.

Step 2. Verify image size in flash. Verify that the TFTP server has sufficient disk space to accommodate the Cisco IOS Software image. Use the **show flash0:** command on the router to determine the size of the Cisco IOS image file.

Step 3. Copy the image to the TFTP server. Copy the image to the TFTP server by using the **copy** *source-url destination-url* command. After issuing the command by using the specified source and destination URLs, the user is prompted for the source file name, IP address of the remote host, and destination file name. The transfer will then begin.

Copy an IOS Image to a Device Example

Step 1. Ping the TFTP server. Ping the TFTP server to test connectivity.

Step 2. Verify the amount of free flash. Ensure that there is sufficient flash space on the device being upgraded by using the **show flash:** command. Compare the free flash space with the new image file size.

Step 3. Copy the IOS image file from the TFTP server to the router by using the **copy tftp: flash:** command. After issuing this command, the user will be prompted for the IP address of the remote host, source file name, and destination file name.

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin...
Loading isr4200-universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0/0): !!!!!!!!!!!!!!!!!!!

[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

The boot system Command

During startup, the bootstrap code parses the startup configuration file in NVRAM for the **boot system** commands that specify the name and location of the Cisco IOS Software image to load. Several **boot system** commands can be entered in sequence to provide a fault-tolerant boot plan.

If there are no **boot system** commands in the configuration, the router defaults to loading the first valid Cisco IOS image in flash memory and runs it.

To upgrade to the copied IOS image after that image is saved on the flash memory of the router, configure the router to load the new image by using the **boot system** command. Save the configuration. Reload the router to boot the router with new image.

```
R1# configure terminal
R1(config)# boot system flash0:isr4200-universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

Packet Tracer - Use a TFTP Server to Upgrade a Cisco IOS Image

In this Packet Tracer, you will complete the following objectives:

- Part 1: Upgrade an IOS Image on a Cisco Device
- Part 2: Backup an IOS Image on a TFTP Server

10.8 Module Practice and Quiz

Packet Tracer - Configure CDP, LLDP, and NTP

In this Packet Tracer activity, you will complete the following objectives:

- Build the Network and Configure Basic Device Settings
- Network Discovery with CDP
- Network Discovery with LLDP
- Configure and Verify NTP

Lab- Configure CDP, LLDP, and NTP

In this lab, you will complete the following objectives:

- Build the Network and Configure Basic Device Settings
- Network Discovery with CDP
- Network Discovery with LLDP
- Configure and Verify NTP

What Did I Learn In This Module?

- Cisco Discovery Protocol (CDP) is a Cisco proprietary Layer 2 protocol that is used to gather information about Cisco devices which share the same data link.
- CDP can be used as a network discovery tool to determine the information about the neighboring devices. This information gathered from CDP can help build a logical topology of a network when documentation is missing or lacking in detail.
- On Cisco devices, CDP is enabled by default. To enable CDP globally for all the supported interfaces on the device, enter cdp run in the global configuration mode. To enable CDP on the specific interface, enter the cdp enable command.
- To verify the status of CDP and display a list of neighbors, use the show cdp neighbors command in the privileged EXEC mode.
- Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral neighbor discovery protocol similar to CDP.
- To enable LLDP globally on a Cisco network device, enter the lldp run command in the global configuration mode.

What Did I Learn In This Module? (Cont.)

- With LLDP enabled, device neighbors can be discovered by using the show lldp neighbors command. When more details about the neighbors are needed, the show lldp neighbors detail command can provide information, such as the neighbor IOS version, IP address, and device capability.
- When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event.
- You can manually configure the date and time, or you can configure the NTP, which allows devices on the network to synchronize their time settings with an NTP server.
- NTP networks use a hierarchical system of time sources and each level in this system is called a stratum. Authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices. Stratum 1 devices are directly connected to the authoritative time sources. Stratum 2 devices, such as NTP clients, synchronize their time by using the NTP packets from stratum 1 servers.
- The ntp server ip-address command is issued in global configuration mode to configure a device as the NTP server.

What Did I Learn In This Module? (Cont.)

- To verify the time source is set to NTP, use the show clock detail command. The show ntp associations and show ntp status commands are used to verify that a device is synchronized with the NTP server.
- SNMP is an application layer protocol that provides a message format for communication between managers and agents.
- The SNMP system consists of three elements: SNMP manager, SNMP agents, and the MIB.
- The SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action. SNMP agents can forward information directly to a network manager by using “traps”.
- SNMPv1, SNMPv2c, and SNMPv3 are all versions of SNMP. SNMPv1 is a legacy solution. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMPv3 provides for both security models and security levels.
- The MIB organizes variables hierarchically. OIDs uniquely identify managed objects in the MIB hierarchy. The Cisco SNMP Navigator on the http://www.cisco.com website allows a network administrator to research details about a particular OID.
- The syslog protocol uses UDP port 514 to allow networking devices to send their system messages across the network to syslog servers.

What Did I Learn In This Module? (Cont.)

- The syslog logging service provides three primary functions: gather logging information for monitoring and troubleshooting, select the type of logging information that is captured, and specify the destinations of captured syslog messages.
- Destinations for syslog messages include the logging buffer (RAM inside a router or switch), console line, terminal line, and syslog server.
- Syslog facilities identify and categorize system state data for error and event message reporting. Common syslog message facilities reported on Cisco IOS routers include: IP, OSPF protocol, SYS operating system, IPsec, and IF.
- The default format of syslog messages on Cisco IOS software is: %facility-severity-MNEMONIC: description.
- Use the command service timestamps log datetime to force logged events to display the date and time.
- The Cisco IFS lets the administrator navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk.
- Use the show file systems command to view the file systems on a Catalyst switch or a Cisco router.

What Did I Learn In This Module? (Cont.)

- Configuration files can be saved to a text file by using Tera Term. A configuration can be copied from a file and then directly pasted to a device.
- Configuration files can be stored on a TFTP server, or a USB drive.
- To save the running configuration or the startup configuration to a TFTP server, use either the copy running-config tftp or copy startup-config tftp command.
- Cisco IOS Software images and configuration files can be stored on a central TFTP server to control the number of IOS images and the revisions to those IOS images, as well as the configuration files that must be maintained.
- Select a Cisco IOS image file that meets the requirements in terms of platform, features, and software. Download the file from cisco.com and transfer it to the TFTP server.
- To upgrade to the copied IOS image after that image is saved on the router's flash memory, configure the router to load the new image during bootup by using the boot system command.


CISCO