Module Practice and Quiz

10.8.1

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

Configure CDP, LLDP, and NTP

Configure CDP, LLDP, and NTP

10.8.2

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

Configure CDP, LLDP, and NTP

10.8.3

What did I learn in this module?

Device Discovery with CDP

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. The device sends periodic CDP advertisements to connected devices. 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. CDP can assist in network design decisions, troubleshooting, and making changes to equipment. On Cisco devices, CDP is enabled by default. To verify the status of CDP and display information about CDP, enter the **show cdp** command. 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. The **show cdp neighbors** command provides helpful information about each CDP neighbor device, including device identifiers, port identifier, capabilities list, and platform. Use the **show cdp interface** command to display the interfaces that are CDP enabled on a device.

Device Discovery with LLDP

Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral neighbor discovery protocol similar to CDP. This protocol advertises its identity and capabilities to other devices and receives the information from a physically connected Layer 2 device. To enable LLDP globally on a Cisco network device, enter the **lldp run** command in the global configuration mode. To verify LLDP has been enabled on the device, enter the **show lldp** command in privileged EXEC mode. 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.

NTP

The software clock on a router or switch starts when the system boots and is the primary source of time for the system. 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. This protocol allows routers on the network to synchronize their time settings with an NTP server. When NTP is implemented in the network, it 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 networks use a hierarchical system of time sources and each level in this system is called a stratum. The synchronized time is distributed across the network by using NTP. 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. 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

SNMP allows administrators to manage servers, workstations, routers, switches, and security appliances, on an IP network. 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. To configure SNMP on a networking device, you must define the relationship between the manager and the agent. The SNMP manager is part of an 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 responds to SNMP manager GetRequest-PDUs (to get an MIB variable) and SetRequest-PDUs (to set an MIB variable). An NMS periodically uses the get request to poll the SNMP agents by querying the device for data. A network management application can collect information to monitor traffic loads and to verify device configurations of managed devices.

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. The community of managers that is able to access the agent's MIB is defined by a community string. SNMPv2c includes a bulk retrieval mechanism and more detailed error message reporting. SNMPv3 provides for both security models and security levels. SNMP community strings are read-only (ro) and read-write (rw). They are used to authenticate access to MIB objects. The MIB organizes variables hierarchically. MIB variables enable the management software to monitor and control the network device. OIDs uniquely identify managed objects in the MIB hierarchy. The snmpget utility gives some insight into the basic mechanics of how SNMP works. The Cisco SNMP Navigator on the http://www.cisco.com website allows a network administrator to research details about a particular OID.

Syslog

The most common method of accessing system messages is to use a protocol called syslog. The syslog protocol uses UDP port 514 to allow networking devices to send their system messages across the network to syslog servers. 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. This table shows syslog levels:

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 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.

Router and Switch File Maintenance

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 display lists all of the available file systems on a Cisco router. Use the directory command **dir** to display the directory of bootflash. Use the change directory command **cd** to view the contents of NVRAM. Use the present working directory command **pwd** to that you are viewing the current directory. Use the **show file systems** command to view the file systems on a Catalyst switch or a Cisco router. 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. Use the **dir** command to view the contents of the USB flash drive. Use the **copy run usbflash0:/** command to copy the configuration file to the USB flash drive. Use the **dir** command to see the file on the USB drive. Use the **more** command to see the contents of the drive. For encrypted passwords, such as the enable secret passwords, the passwords must be replaced after recovery.

IOS Image Management

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. Ping the TFTP server. Verify the amount of free flash. The amount of free flash can be verified by using the **show flash:** command. If there is enough free flash to hold the new IOS image, copy the new IOS image to flash. 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. Save the configuration. Reload the router to boot the router with new image. After the router has booted, to verify the new image has loaded, use the **show version** command.

10.8.4

Module Quiz - Network Management

1. What are two reasons for an administrator to issue the **copy running-config tftp** command on a switch or router? (Choose two.)
   - [x] to transfer the current configuration file to a server
   - [ ] to have a backup of the running configuration file in the router
   - [ ] to force an automatic reload of the device
   - [x] to save the running configuration file to a remote location
   - [ ] to overwrite the current configuration

2. What information can be gathered about a neighbor device from the **show cdp neighbors detail** command that cannot be found with the **show cdp neighbors** command?
   - ( ) the capabilities of the neighbor
   - ( ) the hostname of the neighbor
   - ( ) the platform that is used by the neighbor
   - (•) the IP address of the neighbor

3. When SNMPv1 or SNMPv2 is being used, which feature provides secure access to MIB objects?
   - ( ) message integrity
   - ( ) packet encryption
   - ( ) source validation
   - (•) community strings

4. What command must be issued on a Cisco router that will serve as an authoritative NTP server?
   - ( ) **ntp server 172.16.0.1**
   - (•) **ntp master 1**
   - ( ) **clock set 11:00:00 DEC 20 2010**
   - ( ) **ntp broadcast client**

5. Which protocol or service can be configured to send unsolicited messages to alert the network administrator about a network event such as an extremely high CPU utilization on a router?
   - (•) SNMP
   - ( ) NTP
   - ( ) syslog
   - ( ) NetFlow

6. Which statement describes a syslog message severity level?
   - ( ) A syslog alarm with a severity level of 7 indicates an emergency situation that can render the system unusable.
   - ( ) A syslog alarm at the severity level 4 and higher is sent to an external syslog server by default.
   - ( ) A severity level 7 message is only accessible through the terminal line.
   - (•) Severity level 0 is the most critical severity level.

7. What is an SNMP management agent?
   - ( ) a database that a device keeps about network performance
   - ( ) a computer loaded with management software and used by an administrator to monitor a network
   - (•) software that is installed on devices managed by SNMP
   - ( ) a communication protocol that is used by SNMP

8. What are two characteristics of SNMP community strings? (Choose two.)
   - [x] SNMP read-write community strings can be used to set information on an SNMP-enabled device.
   - [x] SNMP read-only community strings can be used to get information from an SNMP-enabled device.
   - [ ] Commonly known community strings should be used when configuring secure SNMP.
   - [ ] A vulnerability of SNMPv1, SNMPv2, and SNMPv3 is that they send the community strings in plaintext.
   - [ ] If the manager sends one of the correct read-only community strings, it can get information and set information in an agent.

9. A network administrator issues the **copy tftp running-config** command on a router. What is the administrator trying to achieve?
   - ( ) copy the configuration file from the RAM of the router to the TFTP server
   - (•) copy the configuration file from the TFTP server to the RAM of the router
   - ( ) copy the configuration file from the TFTP server to the NVRAM of the router
   - ( ) copy the configuration file from the NVRAM of the router to the TFTP server

10. What is a characteristic of the MIB?
    - (•) The OIDs are organized in a hierarchical structure.
    - ( ) Information in the MIB cannot be changed.
    - ( ) Information is organized in a flat manner so that SNMP can access it quickly.
    - ( ) A separate MIB tree exists for any given device in the network.

11. What data would be saved and where would the data be placed if a network administrator issued the following command? (Choose two.)

    R1# **copy startup-config tftp**

    - [x] The data to be saved is the configuration that is stored in NVRAM.
    - [x] The data will be saved to a TFTP server.
    - [ ] The data will be saved in NVRAM.
    - [ ] The data will be saved in RAM.
    - [ ] The data to be saved is the configuration that is stored on a TFTP server.
    - [ ] The data to be saved is the configuration that is being modified in RAM.

12. Which command would a network engineer use to restore the IOS image c1900-universalk9-mz.SPA.152-4.M3.bin to a router?
    - ( ) **copy c1900-universalk9-mz.SPA.152-4.M3.bin tftp:**
    - (•) **copy tftp: flash0:**
    - ( ) **copy flash0: tftp:**
    - ( ) **copy flash0: c1900-universalk9-mz.SPA.152-4.M3.bin**

13. Why would a network administrator issue the **show cdp neighbors** command on a router?
    - ( ) to display line status and other information about directly connected Cisco devices
    - (•) to display device ID and other information about directly connected Cisco devices
    - ( ) to display routing table and other information about directly connected Cisco devices
    - ( ) to display router ID and other information about OSPF neighbors

14. What are SNMP trap messages?
    - ( ) messages that are sent periodically by the NMS to the SNMP agents that reside on managed devices to query the device for data
    - ( ) messages that are used by the NMS to query the device for data
    - ( ) messages that are used by the NMS to change configuration variables in the agent device
    - (•) unsolicited messages that are sent by the SNMP agent and alert the NMS to a condition on the network

Check

Show Me

Reset