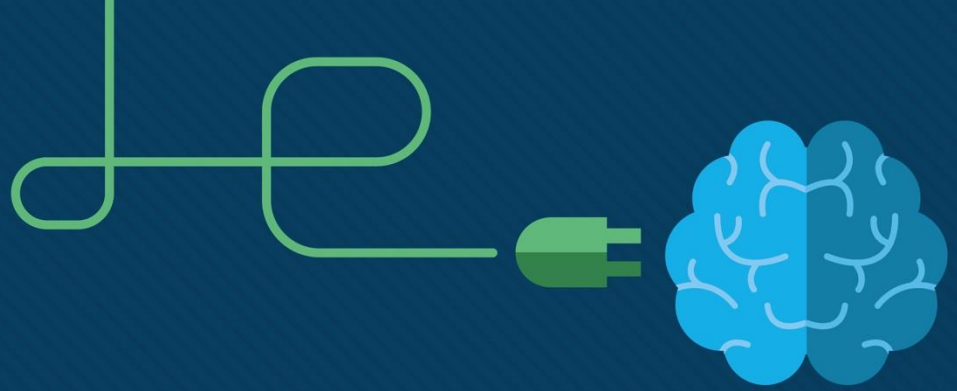


Network Management (Part-3)

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.
Syslog	Explain syslog operation.
DHCP	Explain and Configure of DHCP

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.

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. **If connect with Switch it should be enable also.**
- LLDP can be configured on specific interfaces. However, LLDP must be configured separately to transmit and receive LLDP packets.
- To

```
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

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.)

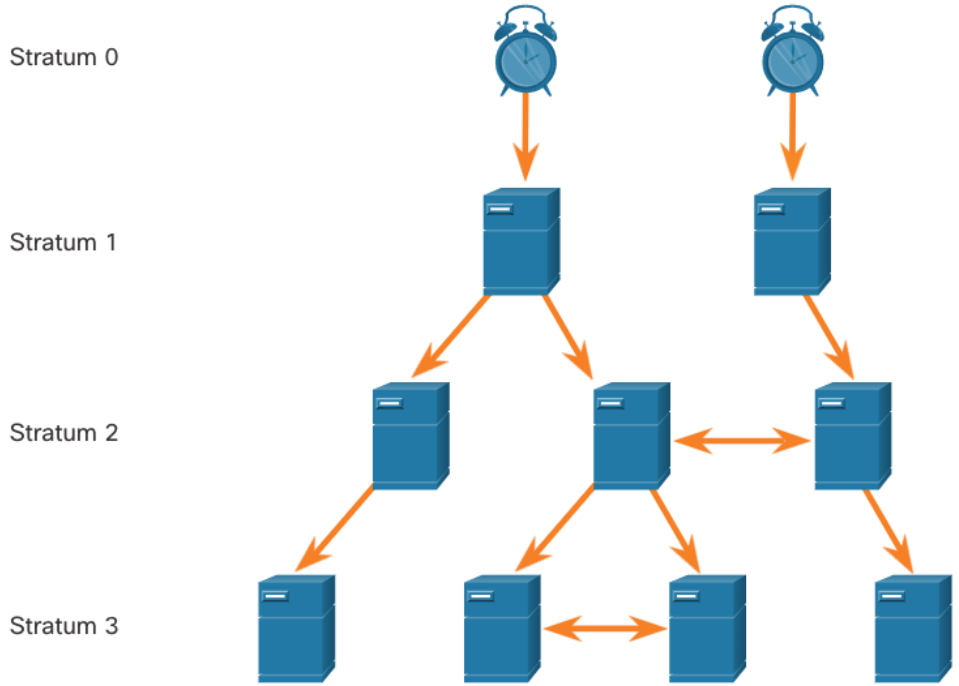
As a network grows, it becomes difficult to ensure that all infrastructure devices are operating with synchronized time using the manual method.

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
```

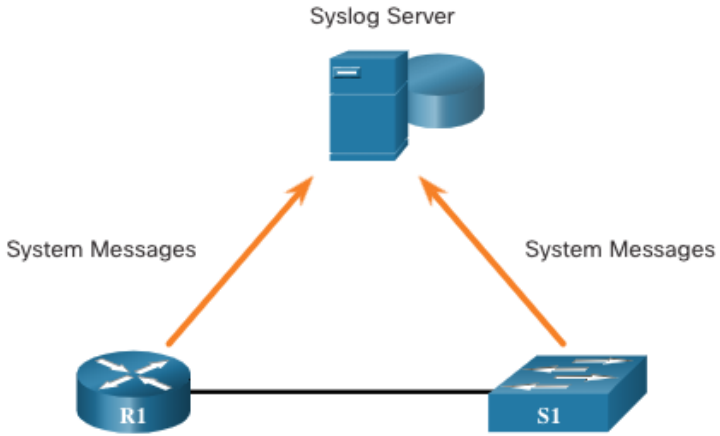
Syslog

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)

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)#
```

Syslog Configuration

NTP Server:
R1 (Config)# ntp server 192.168.0.2

Sys-Log Server:
R1 (Config)# service timestamps log datetime msec
R1 (Config)# logging host 192.168.0.2 (Server IP)

DHCP

Configuration

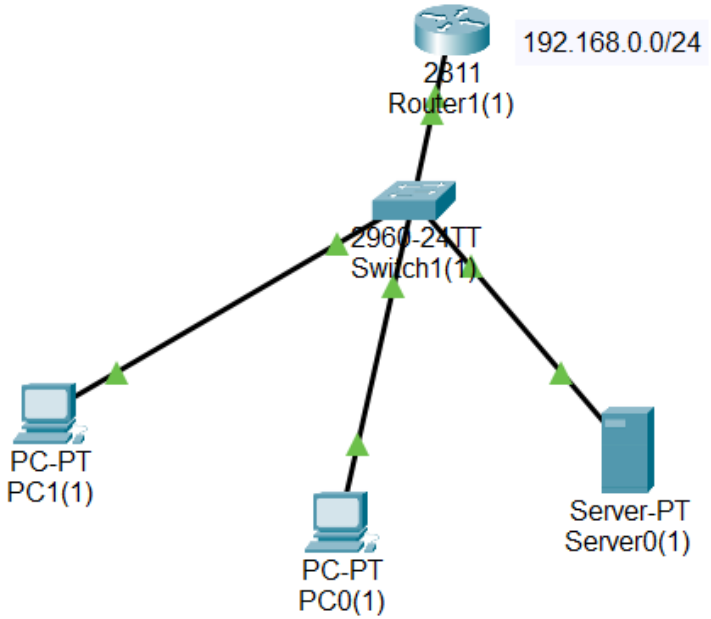
Here is an example configuration:

```
Floor1(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.50
Floor1(config)#ip dhcp pool Floor1DHCP
Floor1(dhcp-config)#network 192.168.0.0 255.255.255.0
Floor1(dhcp-config)#default-router 192.168.0.1
Floor1(dhcp-config)#dns-server 192.168.0.1
```

In the example above you can see that the DHCP server with the following parameters:

- the IP addresses from the **192.168.0.1 – 192.168.0.50** range will not be assigned to hosts
- the DHCP pool was created and named **Floor1DHCP**
- the IP addresses assigned to the hosts will be from the **192.168.0.0/24** range
- the default gateway's IP address is **192.168.0.1**
- the DNS server's IP address is **192.168.0.1**

Lab on DHCP



Thank You