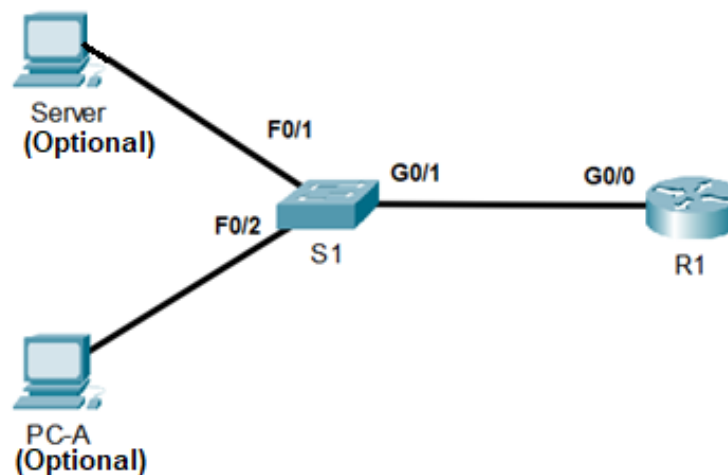![Cisco Networking Academy logo]

Dave Aldwin Bolima

Aldrich Matthew Go

Bernard Dimero

Shaun Tristan Lim

Lab 6.1 Using Network Management Tools (CDP, LLDP) – F2F

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
PC-A (optional)	NIC	192.168.10.4	255.255.255.0	192.168.10.1
Server (optional)	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Explore CDP and LLDP

Background / Scenario

Network management is an essential task of a network administrator once a network is deployed and operational. It involves regularly monitoring device operations and making the necessary configuration changes in response to various network scenarios. To reduce the administrative overhead of performing network management, several tools are available. These include device discovery tools, logging, and

centralized management. In this lab, you will configure and explore the capabilities of widely used network management tools and protocols: CDP and LLDP

Required Resources

- 1 Router
- 1 Switch
- 1 PC with terminal emulation program
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the router and switches.

Step 1:   Cable the network as shown in the topology.

Note: Server and PC1 are optional devices in this activity. These may be preconnected and configured to skip initial device setup and configuration for lab activity 6.2 if it will be performed immediately after this activity. If not using, these may be used solely for configuring devices through console connection.

Step 2:   Initialize and reload the network devices as necessary.

Step 3:   Configure basic device settings for the switches.

a. Console into the device and enable privileged EXEC mode.

b. Enter configuration mode.

c. Configure the hostname and IP address according to the topology.

d. Verify that the switchports with connected Ethernet cables are enabled.

Step 4:   Configure basic device settings for the routers.

a. Console into the device and enable privileged EXEC mode.

b. Enter configuration mode.

c. Configure the hostname and interface IP addresses according to the topology.

Step 5:   Test Connectivity

Perform a ping test between S1 and R1. If this is not successful, perform the necessary troubleshooting to resolve the issue.

Part 2: Explore CDP and LLDP

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions, with other physically connected Cisco devices. Link Layer Discovery Protocol (LLDP) is vendor-neutral protocol using on the data link layer for network discovery. It is mainly used with network devices in the local area network (LAN). The network devices advertise information, such as their identities and capabilities to their neighbors.

In Part 2, you will use these protocols to gather information about devices in the topology. You will also enable or disable these discovery protocols as necessary.

Step 1: Discover Device Information with CDP

On Cisco devices, CDP is commonly enabled by default. You will use CDP to discover details about the devices in the topology.

a. On R1, enter the **show cdp** command in the privileged EXEC mode to verify that status of CDP.

    R1# **show cdp**

Is CDP currently running?	Yes
How often are advertisements sent?	Every 60 seconds

b. Issue the **show cdp interface** to list the interfaces that are participating in CDP advertisements.

    R1# **show cdp interface**

Which interfaces are active and sending CDP advertisements?	FastEthernet0/1

c. Issue the **show cdp neighbors** command to determine the CDP neighbors.

    R1# **show cdp neighbors**

Notice that CDP shows the device 'S1' that is connected to R1.

On which R1 interface is S1 connected?	FastEthernet0/1
Which interface of S1 is connected to R1?	FastEthernet0/9

d. Issue the **show cdp neighbors detail** command on R1. This shows additional information on CDP neighbors. Further details about S1 can be found in the output.

From the command output, gather the following details about this device.

What type of device is S1?	Layer 2 Switch
What is the device model / platform of S1?	Cisco WS-C2960-24TT-L
What is the OS version of S1?	Version 15.0(2) SE-4
What is the IP address of S1?	192.168.10.2

e. For security reasons, it is good practice to turn off CDP on an interface facing an external network. Issue the **no cdp enable** in the interface configuration mode on the G0/1 interface on R1.

    R1(config)# **interface g0/0**
    R1(config-if)# **no cdp enable**
    R1(config-if)# **end**

f. Verify that CDP is no longer running on R1 G0/0

    1) Issue the **show cdp interface** on R1.

Is G0/1 still listed among the CDP interfaces?	No

    2) Issue the **show cdp neighbors** on R1.

What difference do you notice in the command output?

> The difference in the command output is that MyDevice, connected to the GigabitEthernet0/1 interface on R1, is no longer listed in the second output. This suggests that the Cisco Discovery Protocol (CDP) has been successfully disabled on the GigabitEthernet0/1 interface of R1. As a result, MyDevice is no longer sending CDP advertisements to R1, and hence it's not listed in the CDP neighbor details of R1.

g. To disable CDP globally, issue the **no cdp run** command in the global configuration mode.

```
R1# conf t
R1(config)# no cdp run
R1(config)# end
```

Which command(s) would you use to verify that CDP has been disabled for the entire device?

> To verify that Cisco Discovery Protocol (CDP) has been disabled globally on the device, the show cdp command can be used to display the global CDP information for the device. If CDP is disabled, the output will indicate that CDP is not enabled. If CDP is still running, it will show the details of the CDP advertisements. Another command that can be used is the show cdp interface command. This command will display the CDP information for each interface. If CDP is disabled globally, no interfaces should be listed. If some interfaces are still running CDP, they will be listed in the output.

Step 2: Discover Device Information using LLDP

On Cisco devices, LLDP maybe enabled by default. You will use LLDP to discover the ports that are currently connected.

a. Enable LLDP On R1.

```
R1(config)# lldp run
```

b. Use the **show lldp** command to verify that LLDP is enabled on Gateway.

```
R1# show lldp
```

c. Issue the show lldp neighbors command.

Are there any LLDP neighbors to R1?	No

d. Enable LLDP on S1 then verify that LLDP is running.

```
S1(config)# lldp run
S1(config)# end
S1# show lldp
```

e. Issue the show lldp neighbors on R1.

Are there any LLDP neighbors to R1 this time?	Yes

What are the similarities between the information gathered by LLDP and CDP?

The Link Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP) are network discovery protocols that operate at the Data Link layer. They are used by network devices to discover information about neighboring devices connected to a local network. Both protocols gather similar types of information. This includes device identification, which comprises the name of the device, its IP address, and sometimes a unique identifier like a MAC address. They also identify the type of device, whether it's a router, switch, wireless access point, computer, printer, etc. Information about the network ports on the device, including port numbers and types, is also collected. Additionally, they gather data about the software and firmware versions running on the device. The protocols also exchange information about the features and capabilities of the device, such as supported network protocols, speeds, and other functionalities.

f.   Disable LLDP On R1 and S1.

```
R1(config)# no lldp run

S1(config)# no lldp run
```

Reflection Question

Why is it important to disable CDP and LLDP when you are not using these protocols to perform management tasks on devices?

It is important to disable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) when not in use. This is to help prevent a security breach. This is because the protocols can reveal sensitive information about network devices, such as the operating system version, port details, and hardware type. This information can be a goldmine for potential attackers, giving them an edge in identifying system vulnerabilities. Moreover, disabling these protocols can reduce the risk of bugs and attacks, as it's a good practice to shut down anything that is not needed in the system.