Packet Tracer - Compare CLI and SDN Controller Network Management (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Answers: 8.8.2 Packet Tracer - Compare CLI and SDN Controller Network Management

Addressing Table

Note: All subnet masks are /24 (255.255.255.0).

Device	Interface	IP Address
R1	G0/0/0	192.168.101.1
	S0/1/0	192.168.1.2
R2	G0/0/0	192.168.102.1
	S0/1/1	192.168.2.2
R3	G0/0/0	10.0.1.1
	G0/0/1	10.0.2.1
	S0/1/0	192.168.1.1
	S0/1/1	192.168.2.1
SWL1	VLAN 1	192.168.101.2
SWL2	VLAN 1	192.168.102.2
SWR1	VLAN 1	10.0.1.2
SWR2	VLAN 1	10.0.1.3
SWR3	VLAN 1	10.0.1.4
SWR4	VLAN 1	10.0.1.5
Admin	NIC	10.0.1.129
PC1	NIC	10.0.1.130
PC2	NIC	10.0.2.129
PC3	NIC	10.0.2.130
PC4	NIC	192.168.102.3
Example Server	NIC	192.168.101.100
PT-Controller*	NIC	192.168.101.254

* In Part 3, you will add and configure PT-Controller0.

Objectives

Part 1: Explore the Network Topology

Part 2: Use the CLI to Gather Information

Part 3: Configure an SDN Controller

Part 4: Use an SDN Controller to Discover a Topology

Part 5: Use an SDN Controller to Gather Information

Part 6: Use an SDN Controller to Configure Network Settings

Background / Scenario

In this Packet Tracer activity, you will compare the differences between managing a network from the command line interface (CLI) and using a software-defined networking (SDN) controller to manage the network.

Instructions

Part 1: Explore the Network Topology

In this Part, you will become familiar with the topology you will use for network programmability activities.

Step 1: Review the network configuration documentation

The network is configured as follows:

- Routers are running OSPFv2.
- SSH is enabled on all devices with user **cisco** and password **cisco123!**
- R1 has no hosts.
- R2 LAN IPv4 is statically configured.
- R3 is the DHCPv4 server for LAN1 and LAN2.
- Switches are Layer 2 (no VLANs).
- All **SWR#** switches belong to LAN1.

Step 2: Verify that all devices can ping each other.

Either use the command line on each device or use the **Add Simple PDU (P)** tool to verify that all devices can ping each other.

Part 2: Use the CLI to Gather Information

In this part, you manually access each device to gather information about the software version.

Step 1: From the Admin PC, securely access the SWR3 switch.

a. Click **Admin > Desktop > Command Prompt**.

b. Enter the command **ssh -l cisco 10.0.1.4**. The -l option is the letter “L”, not the number one.

c. When prompted, enter **cisco123!** as the password. You are now logged in to SWR3.

Step 2: Gather information about the software on SWR3.

a. Enter the following command to filter the output of the **show version** command to view just the RELEASE SOFTWARE installed on the device. Notice that SWR3 is running IOS 16.3.2 and Boot Loader 4.2.6.

```
SWR3# show version | include RELEASE
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.3.2, RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26, RELEASE SOFTWARE (P)
SWR3#
```

b. Copy the information to your clipboard

c. Open a text file editor and paste the information into a text file.

d. Save the file as **software-versions.txt**.

Step 3: Gather the software information for the rest of the network devices.

a. From the **Command Prompt** on SWR3, securely access another network device and repeat Step 2 above.

b. Continue documenting the software versions until you have completed all nine network devices: SWL1, SWL2, SWR1, SWR2, SWR3, SWR4, R1, R2, and R3.

c. Exit out of all of your SSH sessions.

Part 3: Configure the PT-Controller

For many years, network administrators have used early automation tools such as bash scripts or SNMP-enabled software to complete a process similar to what you did in the previous step. However, with the introduction of SDN, this process has been greatly enhanced. Packet Tracer provides a simple PT-Controller to simulate an SDN controller. In this Part, you will connect and configure the PT-Controller.

Note: To learn more about Packet Tracer's implementation of the Network Controller, click the **Help** menu, then **Contents**. In the Index on the left, about midway down, you will find the heading **Configuring Devices**. Underneath this heading, find **Network Controllers**. Here you will find a wealth of information, much of which you will explore in the activities in this course.

Step 1: Add a Network Controller to the topology.

a. At the bottom left corner of the Packet Tracer interface, click **End Devices > Network Controller**.

b. Add the Network Controller in the blank spot left of the **SWL1** switch. The name should already by **PT-Controller0**. If not, click the name and change it.

c. At the bottom again, click the lightening bolt for **Connections**. Click the solid black **Copper Straight-Through** cable.

d. Click **PT-Controller0** and choose **GigabitEthernet0**. Then click **SWL1** and choose the first available Gigabit Ethernet interface.

Step 2: Configure connectivity for the PT-Controller0.

a. Click **PT-Controller0 > Config**.

b. For **Gateway/DNS IPv4**, enter 192.168.101.1 as the **Gateway** address.

c. On the left under **INTERFACE**, click **GigabitEthernet0**.

d. For **IP Configuration**, enter the **IP Address** 192.168.101.254 and **Subnet Mask** 255.255.255.0.

e. On the left, under **REAL WORLD**, click **Controller**. If the **Server** Status is **Stopped**, move on to the next substep. If the **Server Status** is **Disabled in Preferences**, then you will need to enable external access by following these instructions:

1) Select **Options > Preferences** from the Packet Tracer menus.

2) Click **Miscellaneous**.

3) Under **External Network Access**, click **Enable External Access for Network Controller REST API**.

4) Close **Preferences** and click **PT-Controller0 > Config**, if necessary.

5) On the left under **REAL WORLD**, click **Controller**.

f. The **Server Status** should now be **Stopped**. Click **Access Enabled** to enable it. **Server Status** changes to **Listening on port 58000**. If the port is some other value, change it to **58000**. This is the port number in the Python scripts.

Step 3: From Admin, verify connectivity to the PT-Controller0.

Verify that Admin can ping PT-Controller0. If you are not able to ping, make sure your configuration matches the specifications in the previous step.

Step 4: Register a new user and log into the PT-Controller0.

a. Click **Admin > Desktop > Web Browser**.

b. Enter the IPv4 address 192.168.101.254 to access the **User Setup** for **PT-Controller0**.

c. Enter **cisco** in the **Username** field and **cisco123!** in the **Password** and **Confirm Password** fields, and then click **SETUP**.

Note: You can use whatever username and password you want here. For simplicity, we recommend using common credentials used in the rest of the activity.

d. On **User Login** screen, enter your credentials and click **LOG IN**.

e. You are now logged in to the dashboard for **PT-Controller0**. At this point, it may be helpful to expand the window so you can see the entire interface.

Part 4: Use an SDN Controller to Discover a Topology

In this Part, you will configure PT-Controller0 to use Cisco Discover Protocol (CDP) to automatically discover the nine network devices in your topology. The PT-Controller0 will also discover all five host devices attached to the network.

Step 1: Add credentials to access all the network devices in the topology.

a. From the **Network Controller** GUI, click the menu button to the left of the Cisco logo.

b. Select **Provisioning**. From here, you can manually add networking devices. However, you will use CDP to automatically discover devices for you.

c. Click **CREDENTIALS** and then click **+ CREDENTIAL** to add a **New Credential**.

d. For **Username**, enter **cisco**, and for **Password**, enter **cisco123!**. Leave **Enable Password** blank. For **Description**, enter **admin credentials**, and then click **OKAY**.

e. The new CLI Credentials are now stored on PT-Controller0 for use in automation tasks.

Step 2: Use CDP to discover all the devices on the network.

a. Click **DISCOVERY** and the click **+ DISCOVERY** to add a **New Discovery**.

b. For **Name**, enter **SWL1**. For **IP Address**, enter **192.168.101.2**. For **CLI Credential List**, drop down the list and choose **cisco - admin credentials**.

c. Click **ADD**.

d. You should now see the **Status** as **In Progress**. You can wait for Packet Tracer to finish simulating this process. Or you can **Fast Forward Time** button on the main Topology window to speed up the process.

Part 5: Use an SDN Controller to Gather Information

In this Part, you will use the PT-Controller0 GUI to view information about the network devices and host devices in the topology. You will view the topology created by the controller and then conduct a path trace across the network.

Step 1: View the list of network devices discovered.

a. Click **NETWORK DEVICE**. You should now see all nine network devices listed.

b. Click the Gear icon next to any device's hostname to see the information collected by the discover process. Notice that the **Software Version** is listed as well as a variety of other detailed information about the device.

Step 2: View a list of all the host devices discovered.

a. Return to the Dashboard. Click the menu next to the Cisco logo, then click **Dashboard**. (You can also simply click the **Network Controller** banner to return to the **Dashboard** from anywhere.)

b. On the Dashboard, you will see charts with the number of hosts that can be reached via ping and the number of network devices that are managed. Both should be 100%.

c. You should also see tiles for **QoS**, **Network Device**, and **Host**. Click the Gear icon for **Host**. This will take you to the **HOSTS** tab for **ASSURANCE**.

d. On this page, you can view all the Layer 2 and Layer 3 connectivity information for each host as well as the network device to which each is attached.

e. Click the Gear icon next to any host to view more detailed information.

Step 3: View the topology created by PT-Controller0.

a. Click the **TOPOLOGY** tab. Notice that the PT-Controller dynamically created the same topology you see in Packet Tracer's main window.

b. From this view, you can click any network device to see its details.

c. You can also click and drag the device icons to rearrange the topology. However, your changes will not be saved when you leave the **TOPOLOGY** workspace.

Step 4: Trace the path from one device to another device.

a. Click the **PATH TRACE** tab.

b. Click **+ PATH** to add a **New Path**.

c. Trace the path from one end of the network to the other. For example, you could enter the IP addresses for PC1 to PC4. Then click **OKAY**.

d. Click the new path that was added to initiate the path trace.

You will get a **Route** report that shows all the hops from source to destination. Notice that only Layer 3 device information is listed. The switches are shown as an **UNKNOWN** device. This is because they are all operating at Layer 2 only.

Part 6: Use an SDN Controller to Configure Network Settings

A major benefit of network automation using a controller is the ability to configure global network settings and policies for all devices and then push that configuration with the click of a button. In this Part, you will configure **PT-Controller0** with network settings for DNS, NTP, and Syslog. You will then push this configuration to supported network devices. Finally, you will verify and test the policy.

Step 1: Investigate the configuration of the Example server.

a. Click **Example Server > Services**.

b. Under **SERVICES**, click **DNS**. Notice that the DNS service is enabled and that there is one record for www.example.com.

c. Under **SERVICES**, click **SYSLOG**. Notice that the Syslog service is enabled.

d. Under **SERVICES**, click **NTP**. Notice that the NTP service is enabled.

Step 2: Configure a global policy for DNS, SYSLOG, and NTP.

a. Click **Admin**. If you closed **Admin**, you will need to open the **Web Browser** app and reauthenticate with **PT-Controller0**.

b. Click the menu to the left of the Cisco logo.

c. Click **Policy**.

d. On the **QOS** tab, notice there are options for configuring the **Scope** and **Policy**. In this activity, you will configure **NETWORK SETTINGS**.

e. Click **NETWORK SETTINGS**.

f. Click **DNS**. Enter **example.com** as the **Domain Nam**e and **192.168.101.100** as the **IP Address**.

g. Click **Save**.

h. Click **NTP**.

i. Enter **192.168.101.100** as the **IP Address**.

j. Click **Save**.

k. Click **SYSLOG**.

l. Enter **192.168.101.100** as the **IP Address**.

m. Click **Save**.

n. Click **DNS**, **NTP**, and **SYSLOG** again to verify the information is correct. If not, correct the information saving each time.

o. Click **PUSH CONFIG**.

p. The **Push All Network Settings** dialog box opens. Verify your settings and click **OKAY**. A “Saved Successfully” message appears briefly.

Step 3: Verify and test the network settings that were pushed to devices.

At the bottom of the **NETWORK SETTINGS** window, there is the following:

Note: This functionality is only supported on devices running IOS-XE OS and Switch 2960-24TT

This means that, for this version of Packet Tracer, your global settings were only applied to the routers.

a. Click any of the three routers. **R1** is shown in the following output.

b. Click **CLI**.

c. Click inside the window and press **Enter** to get a command prompt.

d. Enter the privileged EXEC mode and verify the DNS settings.

```
R1> enable
R1# show run | begin ip domain
ip domain-name example.com
ip name-server 192.168.101.100
!
<output omitted>
R1#
```

e. Enter the following commands to verify the NTP settings. The time on R1 should match your current time. Packet Tracer may take a little time to propagate NTP messages. You can click the **Fast Forward Time** button to speed up the process.

```
R1# show ntp associations

address         ref clock       st   when     poll    reach   delay           offset
disp
*~192.168.101.100127.127.1.1     1    12       16      377     0.00            0.00
0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1# show clock
15:30:54.268 UTC Thu Jun 11 2020
R1#
```

f. Enter the following command to verify logging is configured.

```
R1# show run | include logging
logging 192.168.101.100
R1#
```

g. To test logging, shut down the Serial0/1/0 interface and then reactivate it.

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface s0/1/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
15:36:37: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
15:36:53: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0 from LOADING to
FULL, Loading Done
R1(config-if)# end
R1#
```

h. Click **Example Server > Services > SYSLOG**. You should see the same syslog messages you saw on in the CLI are also logged to the server. Double-click any of the entries to review the messages.