## Lab 24: Compare CLI and SDN Controller Network Management

### Case Study

NetCore Solutions, a major telecommunications company in Ireland, delivers broadband and fiber-optic services to millions of customers. With over 1,000 skilled professionals, NetCore operates an extensive network infrastructure that requires consistent, reliable, and secure management. As the company expanded, its traditional network management practices centered around manual device configuration and isolated command-line interface (CLI) tasks proved inefficient and error-prone. To overcome these limitations, NetCore initiated a transition toward software-defined networking (SDN) and centralized automation using controller-based management tools.

### Business Challenge

NetCore’s day-to-day technical operations were hindered by several issues. Network administrators manually configured routers and switches, resulting in inconsistent changes, increased risk of human error, and long configuration times. Backup procedures for device configurations were also performed manually, which made disaster recovery and auditing more difficult. Additionally, the company lacked a centralized system to track device software versions, topology changes, or log system events. This decentralized approach made it hard to enforce uniform network policies or respond quickly to service-impacting issues. The absence of real-time visibility and centralized control posed a significant challenge to NetCore's goals for operational agility and service reliability.

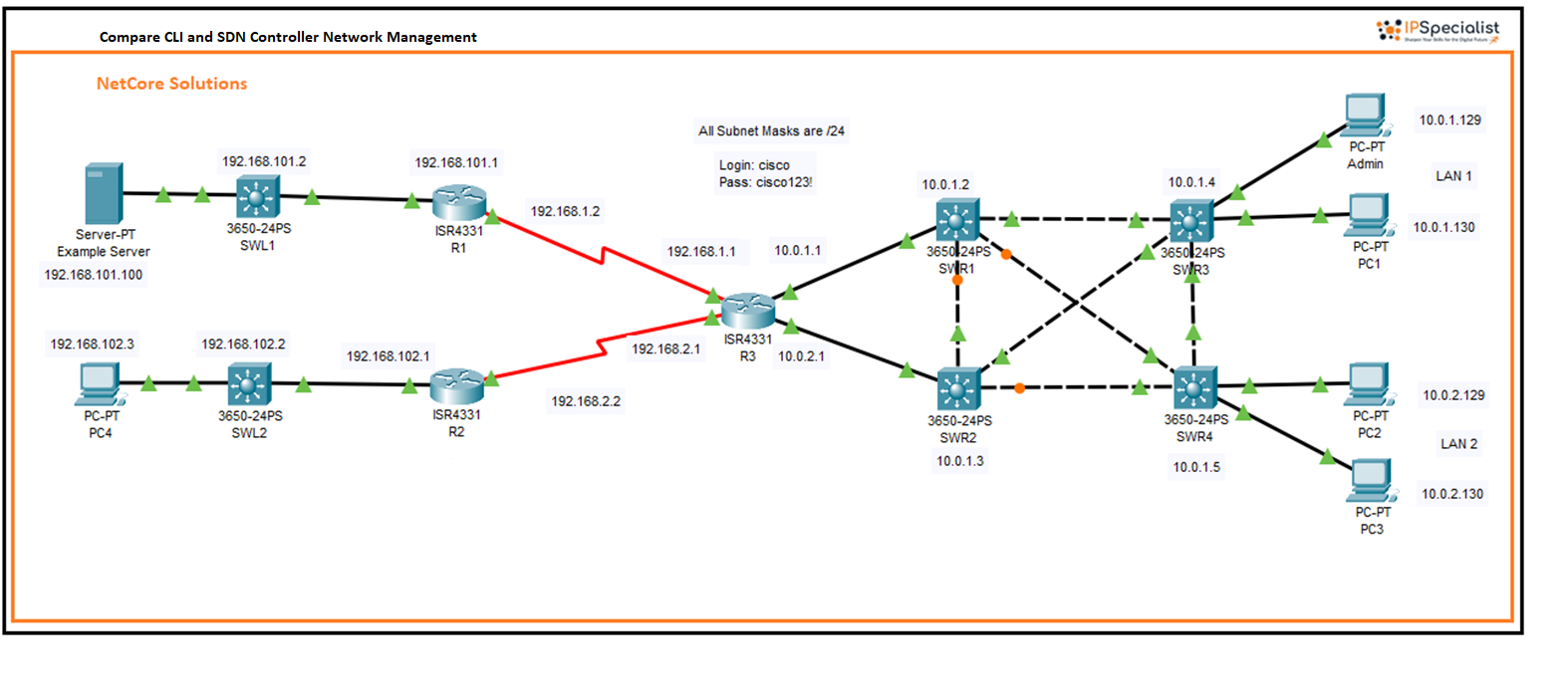
### Solution

To address these problems, NetCore Solutions adopted controller-based network management using Cisco’s Software-Defined Networking (SDN) model. The company implemented a centralized Network Controller to automate and manage device discovery, configuration, monitoring, and policy deployment.

The SDN controller allowed administrators to automatically discover network topology using Cisco Discovery Protocol (CDP) and securely access device information across the network. It provided a graphical interface to view network health, trace data paths, and analyze real-time connectivity between hosts and routers. Furthermore, the controller enabled the central deployment of Dns, NTP, and Syslog settings across supported devices, ensuring uniform configuration and simplifying troubleshooting.

Using controller-based automation, administrators could now push network settings to multiple routers with a single action. Key information such as software versions, device status, and system logs became readily available through the SDN dashboard, eliminating the need for individual CLI sessions on each device.

1. Explore the Network Topology
2. Use the CLI to Gather Information
3. Configure an SDN Controller
4. Use an SDN Controller to Discover a Topology
5. Use an SDN Controller to Gather Information
6. Use an SDN Controller to Configure Network Settings



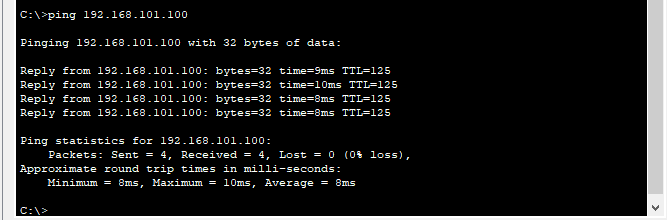
*Figure 24-01: Lab Topology*

**//Explore the Network Topology**

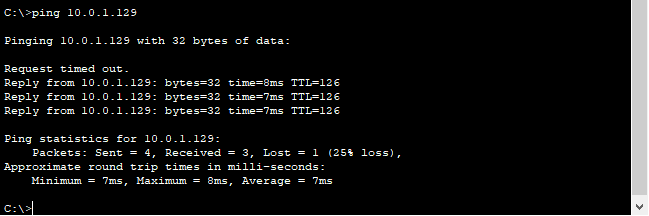
1. The network setup consists of routers configured with OSPFv2 to enable dynamic routing between devices. SSH access is enabled on all devices using the username **'cisco' and password 'cisco123!'** for secure remote management. **Router R1** has no connected hosts, while **R2** is configured with a static IPv4 address for its LAN segment. **Router R3** functions as the **DHCPv4 server**, dynamically assigning IP addresses to devices in **LAN1** and **LAN2**. The switches in the network operate at **Layer 2** and do not utilize VLANs. All switches labeled **SWR#** are part of **LAN1**, ensuring seamless local connectivity within that segment.

2. 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.

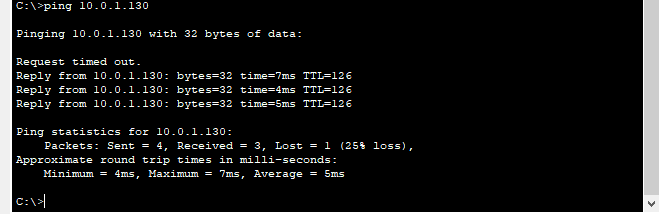
3. To verify example server use command **ping 192.168.101.100.**



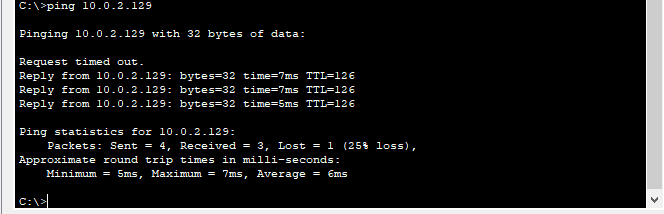
4. To verify PC-T Adminuse command **ping 10.0.1.129.**



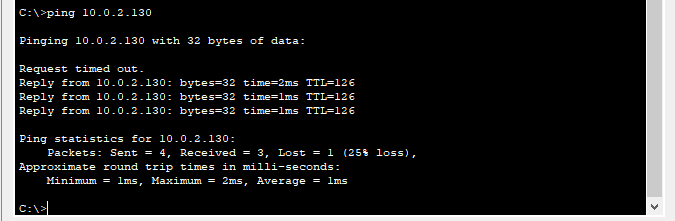
5. To verify PC1use command **ping 10.0.1.130.**



6. Verify PC2use command **ping 10.0.2.129**

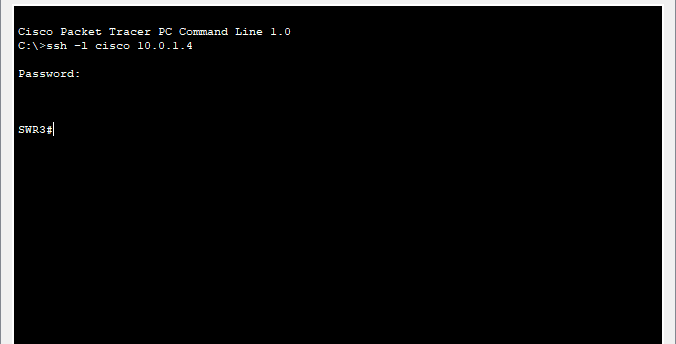


7. To verify PC3use command **ping 10.0.2.130**

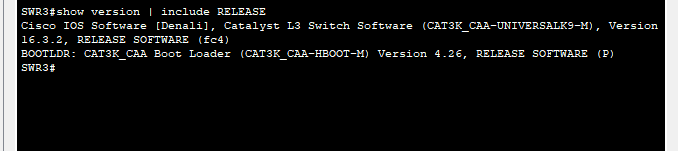


**//Use the CLI to Gather Information**

**1.** To gather information about the software version, begin by securely accessing the **SWR3** switch from the Admin PC using the Command-Line Interface (CLI). First, click on **Admin**, then navigate to the **Desktop** tab and open the **Command Prompt**. At the command prompt, type **ssh -l cisco 10.0.1.4.** Note that the **-l** option uses a lowercase "**L**", not the number one. When prompted for a password, enter **cisco123!.** Upon successful authentication, you will be logged into the **SWR3** switch, ready to retrieve system information.



2. To begin gathering software information, start by accessing the SWR3 switch from the Admin PC using the CLI. Click on the **Admin** PC, go to the **Desktop** tab, and open the **Command Prompt**. Use the command' **ssh -l cisco 10.0.1.4'** to initiate a secure connection to **SWR3**, ensuring that the lowercase "L" is used in the' -l' option. When prompted, enter the password **cisco123!** to log in. Once connected to SWR3, enter the command **show version | include RELEASE** to filter and view only the lines showing the installed IOS and Boot Loader software versions. You will see output indicating that SWR3 is running IOS Version 16.3.2 and Boot Loader Version 4.2.6.



3. After collecting the software version information from SWR3, proceed to gather the same details from the remaining network devices. From the **command prompt** on SWR3, initiate a **secure SSH** connection to another network device by using the appropriate **ssh-l cisco [device IP]** command and entering the password cisco123! When prompted. Once connected, use the show version | include RELEASE command to filter and view only the relevant lines that display the IOS and Boot Loader software versions. Continue this process for all nine network devices: SWL1, SWL2, SWR1, SWR2, SWR3, SWR4, R1, R2, and R3. Once the software version details for all devices have been collected and saved, make sure to exit each SSH session by typing exit to return to the previous device or close the command prompt.

SWR3#ssh -l cisco 10.0.1.5

Password:

SWR4#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)

SWR4#ssh -l cisco 10.0.1.2

Password:

SWR1#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)

SWR1#

SWR1#ssh -l cisco 10.0.1.3

Password:

SWR2#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)

SWR2#ssh -l cisco 10.0.1.1

Password:

R3#show version | include RELEASE

Cisco IOS Software, ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)

R3#ssh -l cisco 192.168.1.2

Password:

R1#show version | include RELEASE

Cisco IOS Software, ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)

R1#ssh -l cisco 192.168.2.2

Password:

R2#show version | include RELEASE

Cisco IOS Software, ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)

R2#ssh -l cisco 192.168.101.2

Password:

SWL1#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)

SWL1#ssh -l cisco 192.168.102.2

Password:

SWL2#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)

SWL2#exit

[Connection to 192.168.102.2 closed by foreign host]

SWL1#exit

[Connection to 192.168.101.2 closed by foreign host]

R2#exit

[Connection to 192.168.2.2 closed by foreign host]

R1#exit

[Connection to 192.168.1.2 closed by foreign host]

R3#exit

[Connection to 10.0.1.1 closed by foreign host]

SWR2#exit

[Connection to 10.0.1.3 closed by foreign host]

SWR1#exit

[Connection to 10.0.1.2 closed by foreign host]

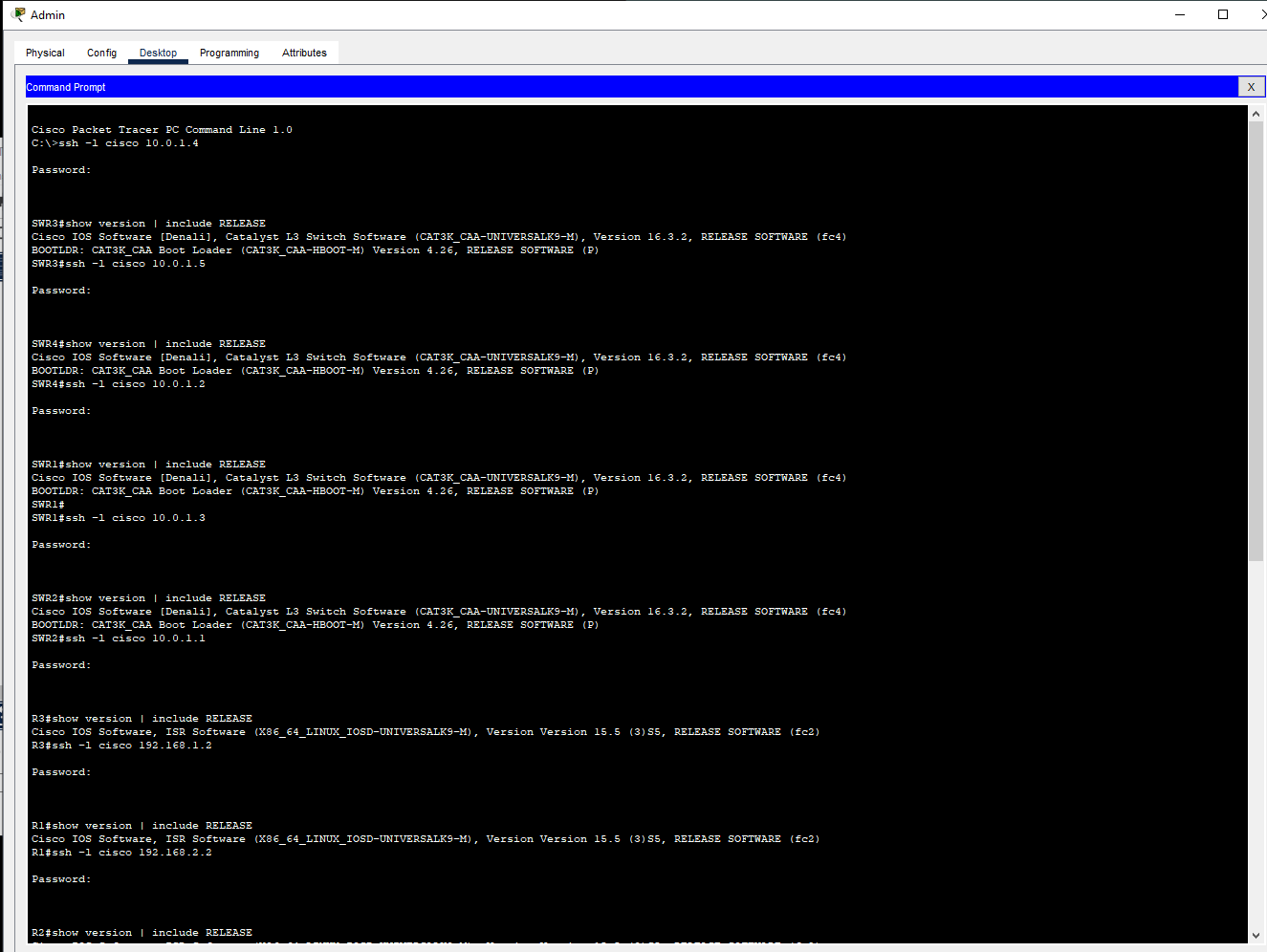
SWR4#exit

[Connection to 10.0.1.5 closed by foreign host]

SWR3#exit

[Connection to 10.0.1.4 closed by foreign host]

C:\>exit



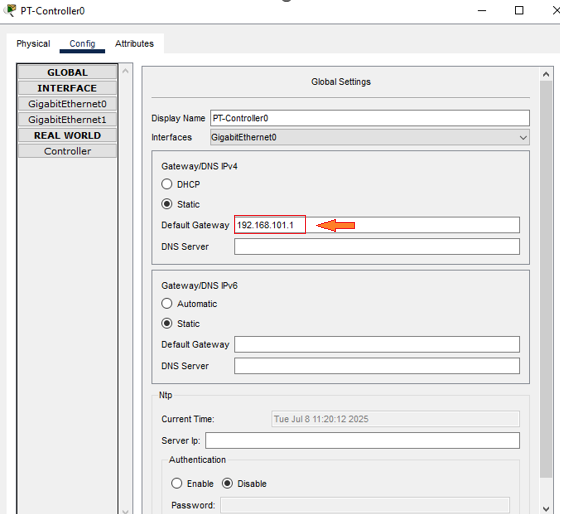
4. Exit out of all of your SSH sessions.

**// Configure the PT-Controller**

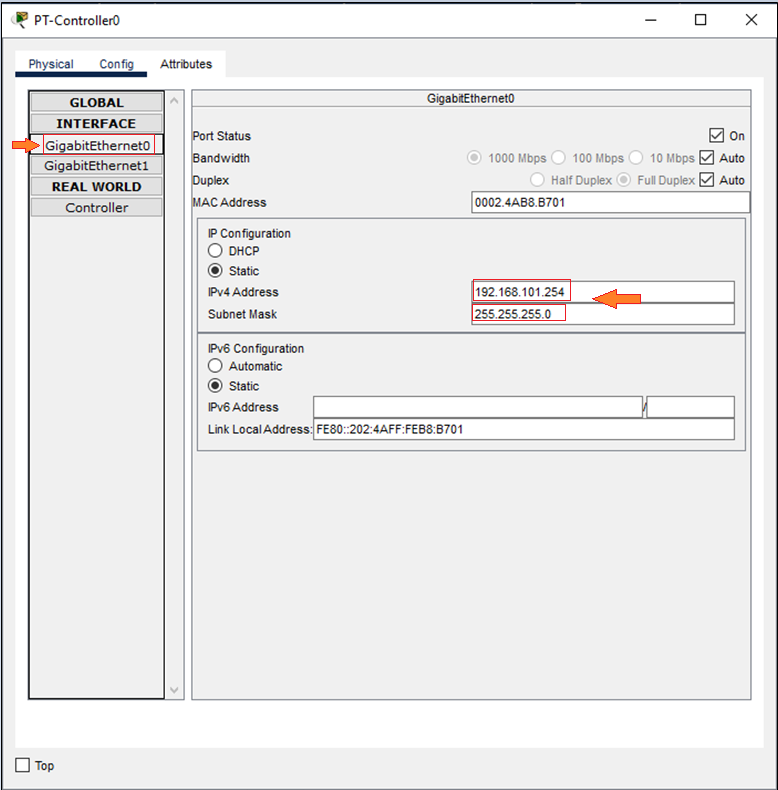
1. To begin configuring Software-Defined Networking (SDN) in Packet Tracer, you will first add a Network Controller to your topology. In the bottom-left corner of the Packet Tracer interface, click on **End Devices**, then select **Network Controller**. Drag and place the controller in the space to the left of the **SWL1** switch. The device should automatically be named **PT-Controller0**; if not, simply click on the name label and rename it accordingly.

2. Go back to the bottom toolbar and click the lightning bolt icon to open the **Connection**s menu. Select the solid black **Copper Straight-Through** cable. Click on **PT-Controller0**, select **GigabitEthernet0**, then click on **SWL1** and choose the first available Gigabit Ethernet interface to complete the physical connection.

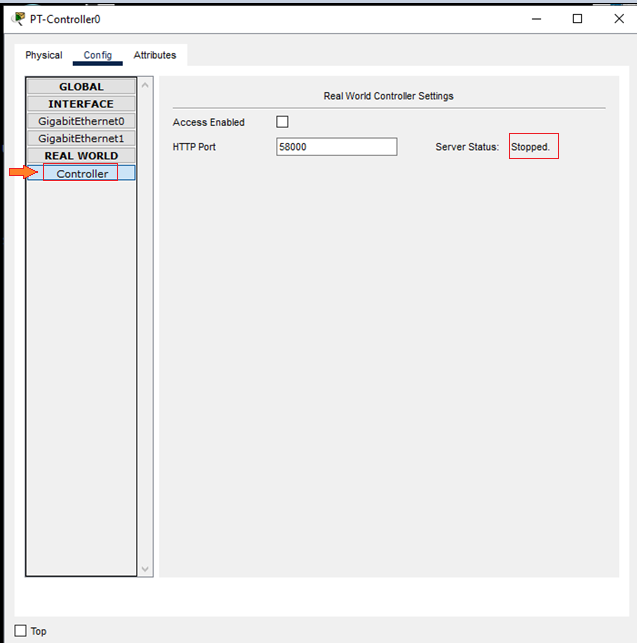
3. To configure connectivity for PT-Controller0, begin by clicking on **PT-Controller0** and selecting the **Config** tab. In the **Gateway/Dns IPv4** field, enter **192.168.101.1** as the **Gateway** address.



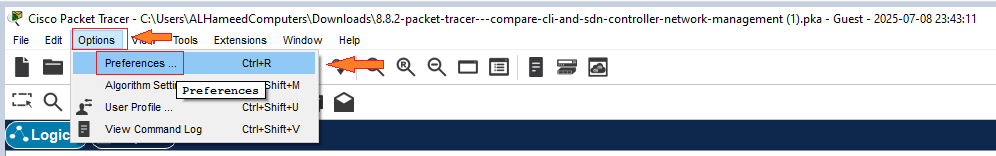
4. Then, on the left side under **INTERFACE,** click **GigabitEthernet0.** In **IP Configuration**, and set the IP Address to **192.168.101.254** with a Subnet Mask of **255.255.255.0.**



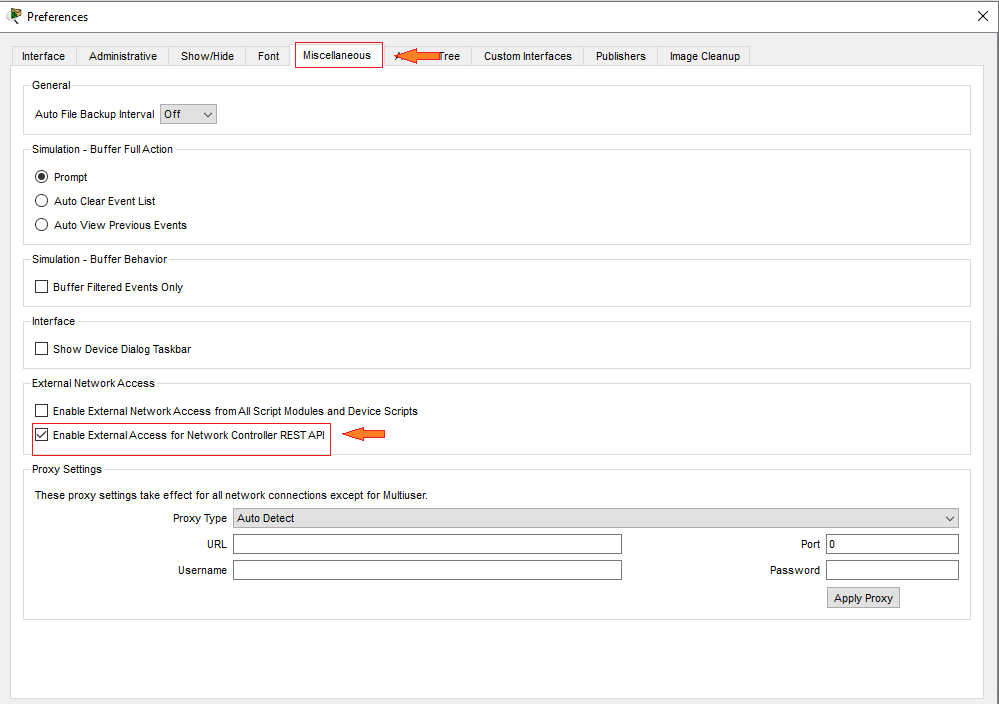
5. After assigning the IP configuration, scroll down the left panel and click on **Controller** under the **Real-World** section. If the Server Status is shown as Stopped, continue to the next step.



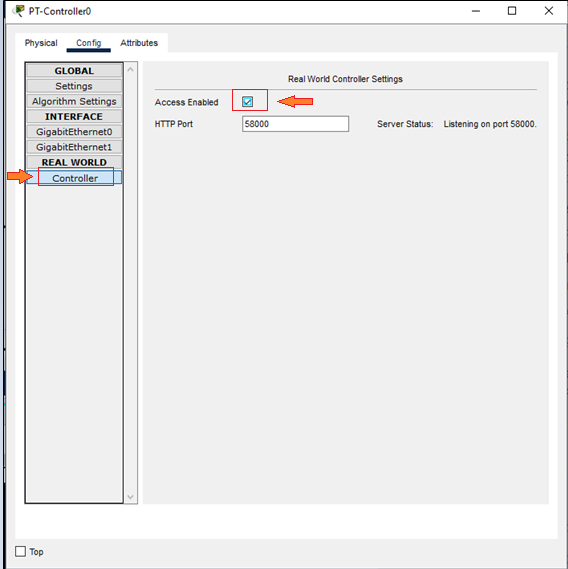
6. However, if the **Server Status** says **Disabled in Preferences**, you must enable it by navigating to the Packet Tracer menu and selecting **Options > Preferences**. Within the **Preferences** window.



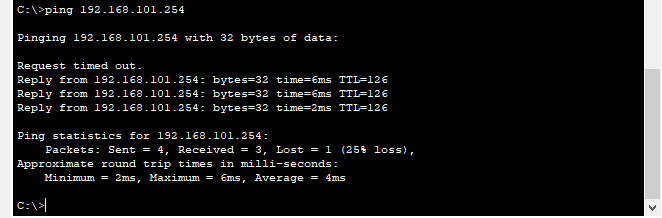
7. Click on the **Miscellaneous** tab and check the box to Enable **External Access for Network Controller REST API** under External Network Access.



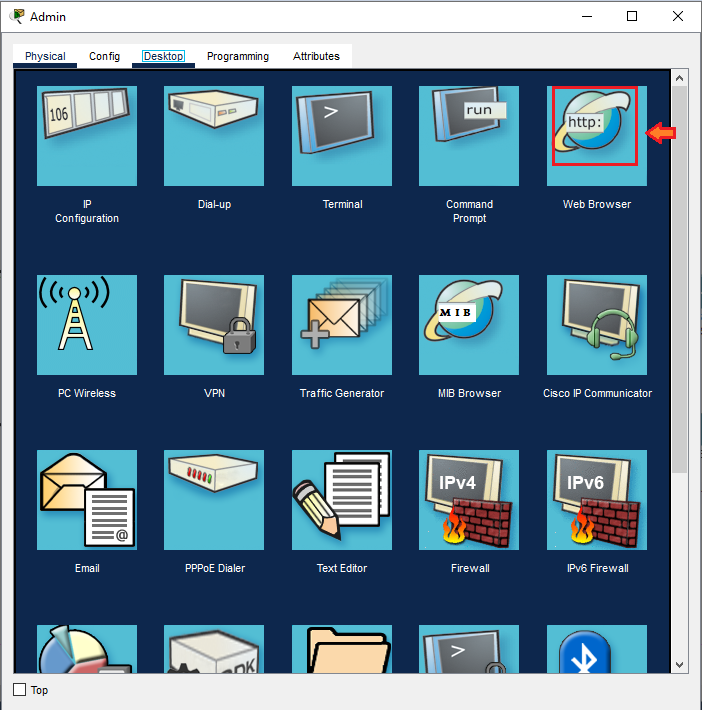
8. Close the **Preferences** window, return to **PT-Controller0 > Config**, and click **Controller** again. The **Server Status** should now be **Stopped**. Click **Access Enabled** to start it. The Server Status will update to Listening on **port 58000**. If a different port is displayed, manually change it to **58000**, as this port number is used by the Python scripts that interact with the controller.



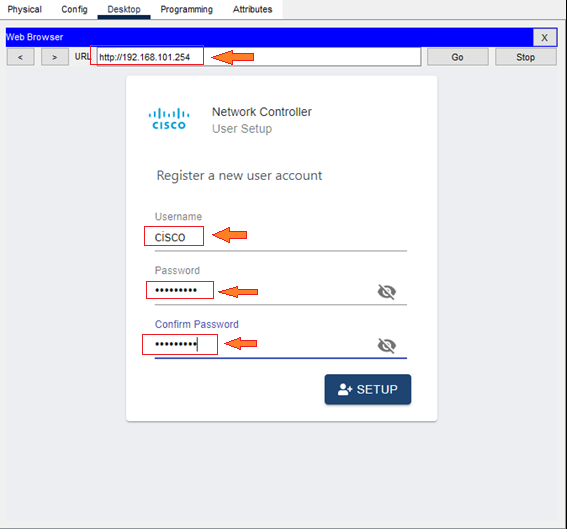
9.Verify that Admin can ping PT-Controller0 using **ping 192.168.101.254**. If you are not able to ping, make sure your configuration matches the specifications in the previous step.



10.To register a new user and log in to PT-Controller0, start by clicking on the **AdminPC**, then go to the **Desktop** tab and open the **Web Browser**.



11. In the address bar, enter the IP address **192.168.101.254** to access the **User Setup page** for **PT-Controller0**. When the setup page loads, type cisco in the **Username** field and enter **cisco123!** in both the **Password** and **Confirm Password** fields. Then, click the **Setup** button to create the user account. Although you may choose your credentials, it is recommended to use these standard ones for consistency.



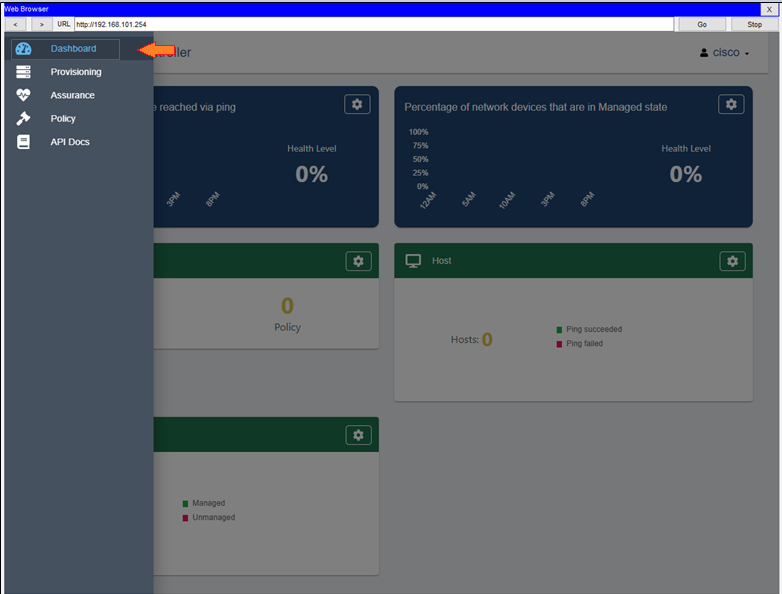
12.  On the **User Login** screen, enter your credentials and click **LOG IN**. You are now logged in to the dashboard for **PT-Controller0**. At this point, it may be helpful to expand the window so you can see the entire interface.



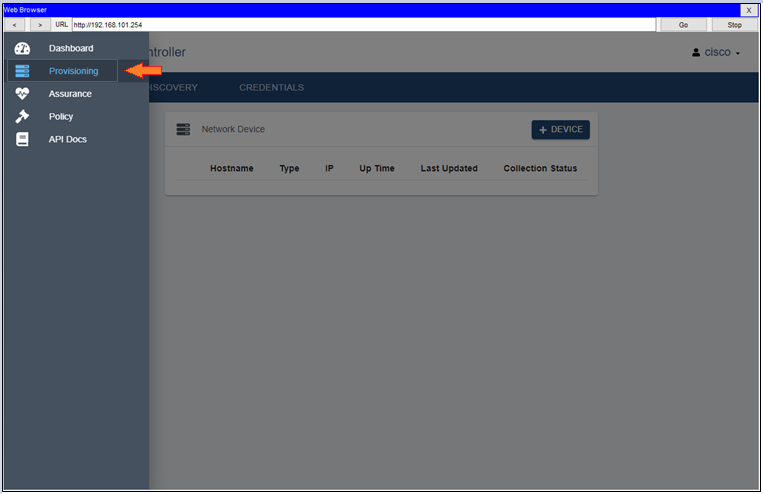
**//Use an SDN Controller to Discover a Topology**

1. In this part, you will configure PT-Controller0 to use Cisco Discovery Protocol (CDP) to automatically detect all nine network devices and five host devices within the network topology.

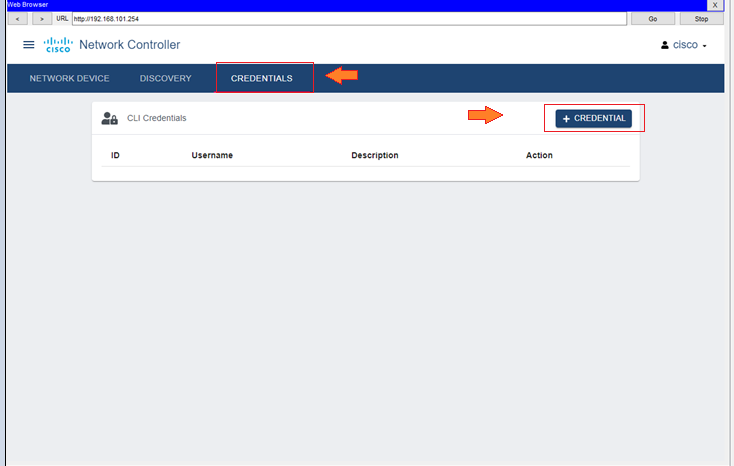
2. To begin, log in to the PT-Controller0 dashboard using the web browser on the Admin PC. Once on the **Dashboard**, click the **menu button** located to the left of the Cisco logo in the top-left corner of the screen. This opens the navigation panel, where you can begin adding credentials that the controller will use to access all network devices for discovery purposes.



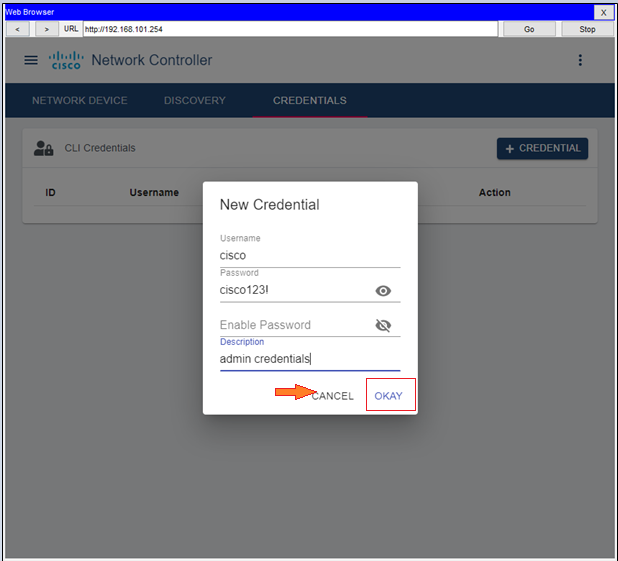
2. Select **Provisioning**. From here, you can manually add networking devices. However, you will use CDP to automatically discover devices for you.



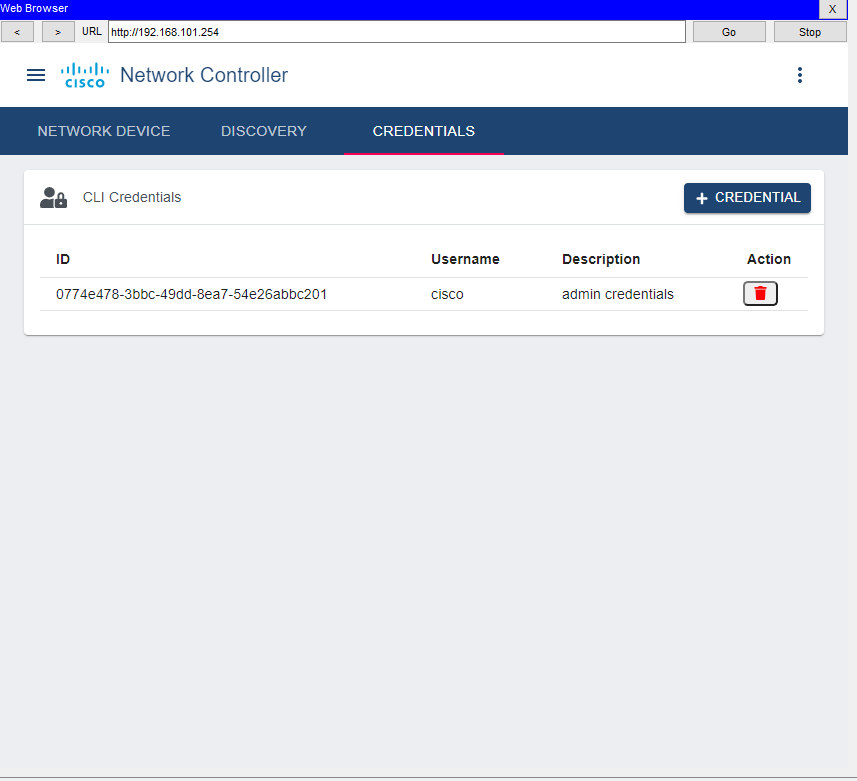
3. From the navigation panel in the PT-Controller0 dashboard, click on **Credentials**, then click the **+Credentials** button to add a new set of login credentials. This step allows the controller to authenticate with and manage all network devices in the topology during the discovery process.



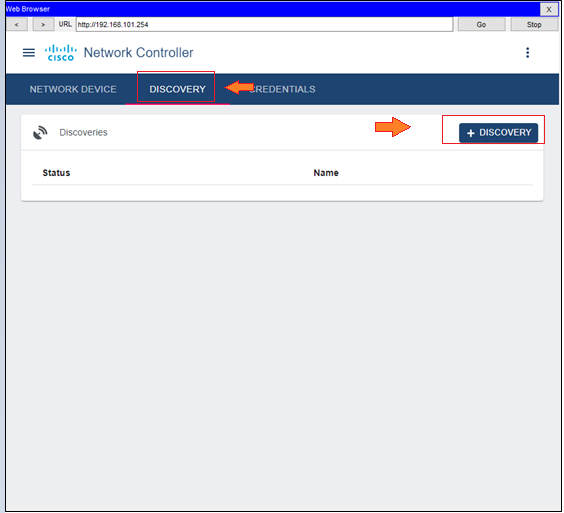
4. In the **New Credential** form, enter **cisco** in the **Username** field and **cisco123!** in the **Password** field. Leave the **Enable Password** field blank. In the **Description** field, type **admin credentials** to identify the purpose of this login. Once all fields are filled in correctly, click **OKAY** to save the credential. This allows the PT-Controller0 to use these credentials for accessing and managing the network devices.



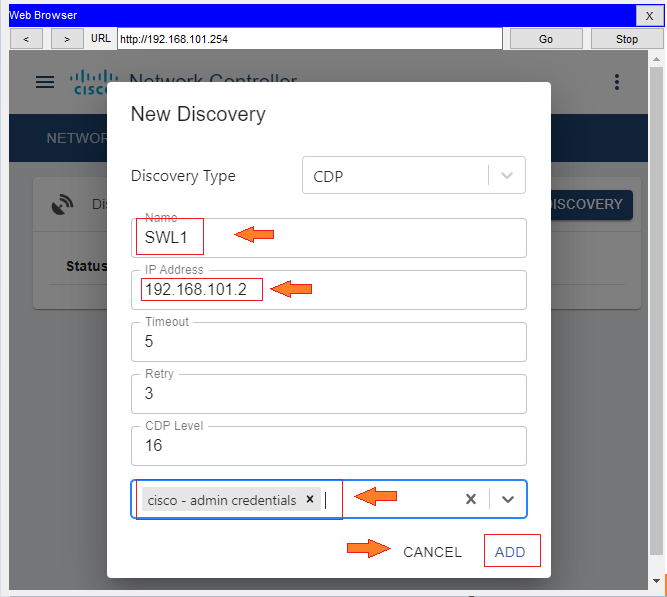
5. Once saved, the new CLI credentials are now securely stored on PT-Controller0 and are available for use in automation tasks, such as device discovery and configuration. These credentials will enable the controller to authenticate with the network devices and gather information or apply changes as needed.



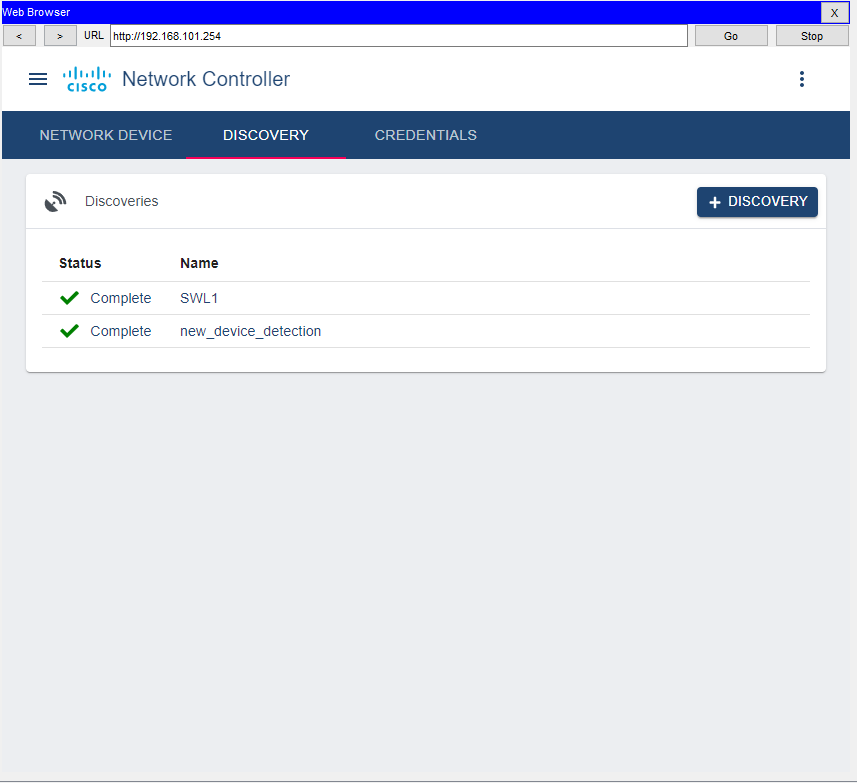
6. To begin discovering all devices on the network using Cisco Discovery Protocol (CDP), navigate back to the PT-Controller0 dashboard and click on **Discovery** from the side menu. Then, click the **+ Discovery** button to initiate the process of adding a new network discovery task. This will allow the controller to scan the network and identify connected devices automatically.



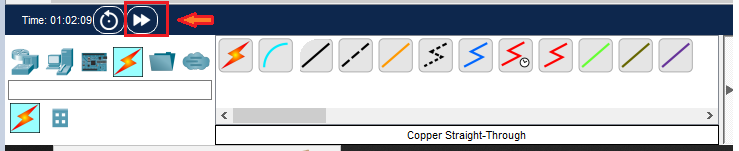
7. In the **New Discovery** setup window, enter **SWL1** in the **Name** field and **192.168.101.2** in the IP Address field. Then, under the **CLI Credential List**, click the dropdown menu and select **cisco – admin credentials** from the list. This tells the PT-Controller0 to use the stored credentials to access the SWL1 switch during the discovery process and click **Add.**



8. After starting the discovery process, you will see the **Status** listed as **In Progress** in the controller dashboard. At this point, you can either wait for Packet Tracer to simulate the discovery at normal speed.

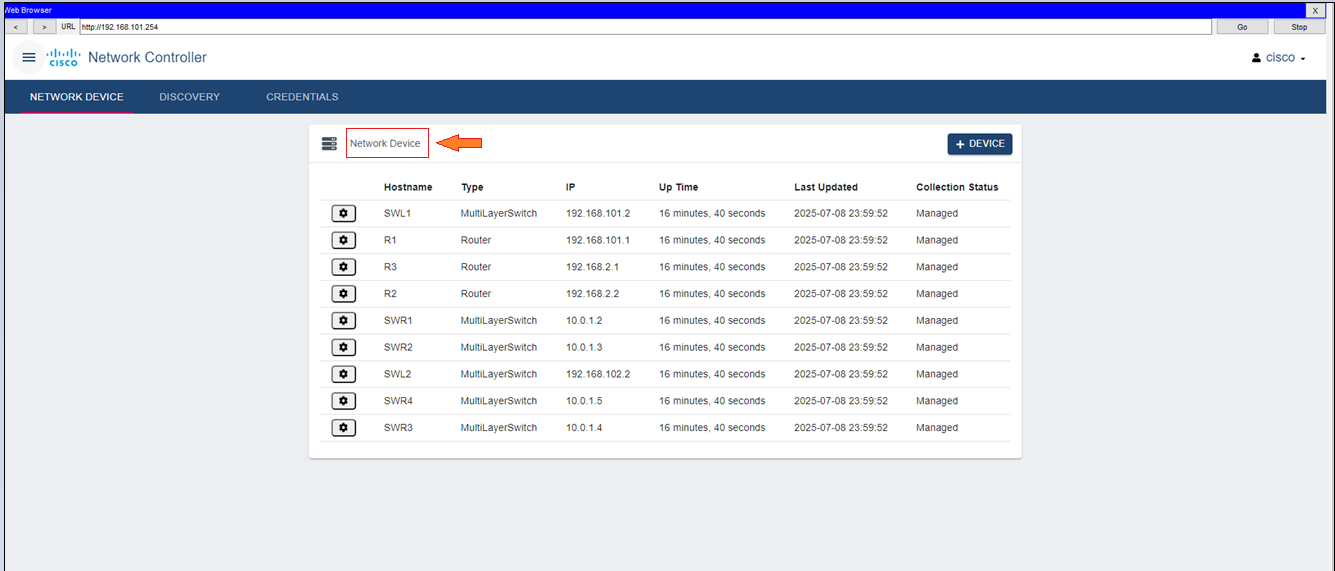


9. Click the **Fast Forward Time** button located in the main **Topology window** to accelerate the simulation. This speeds up the discovery process, allowing the PT-Controller0 to complete the identification of devices more quickly.

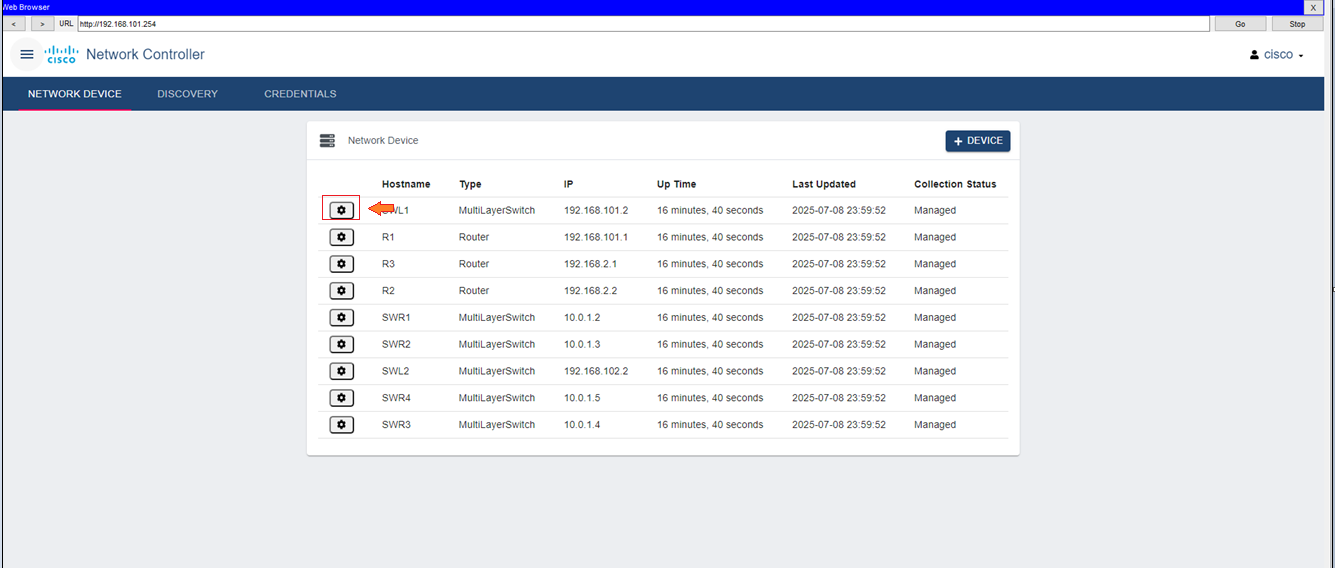


**//Use an SDN Controller to Gather Information**

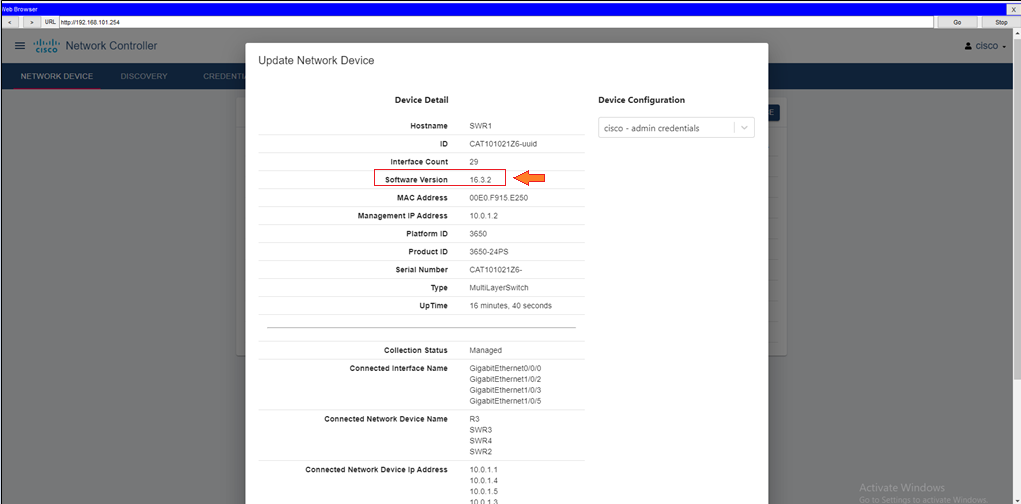
1. To begin gathering information using the SDN controller, access the PT-Controller0GUI and click on **Network Device** from the navigation menu. This will display a list of all the network devices that the controller has discovered. You should see all **nine devices,** including switches and routers, listed with their respective details, confirming that the discovery process was successful.



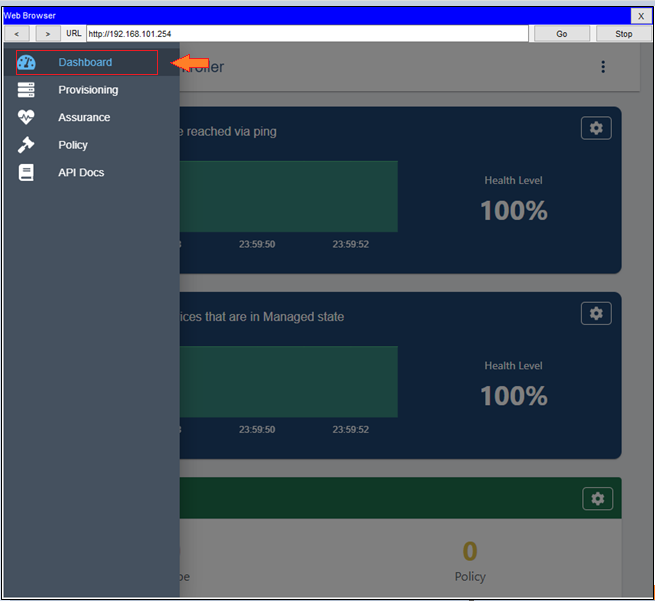
2. Click the **Gear** icon next to any device’s hostname to see the information collected by the discovery process.



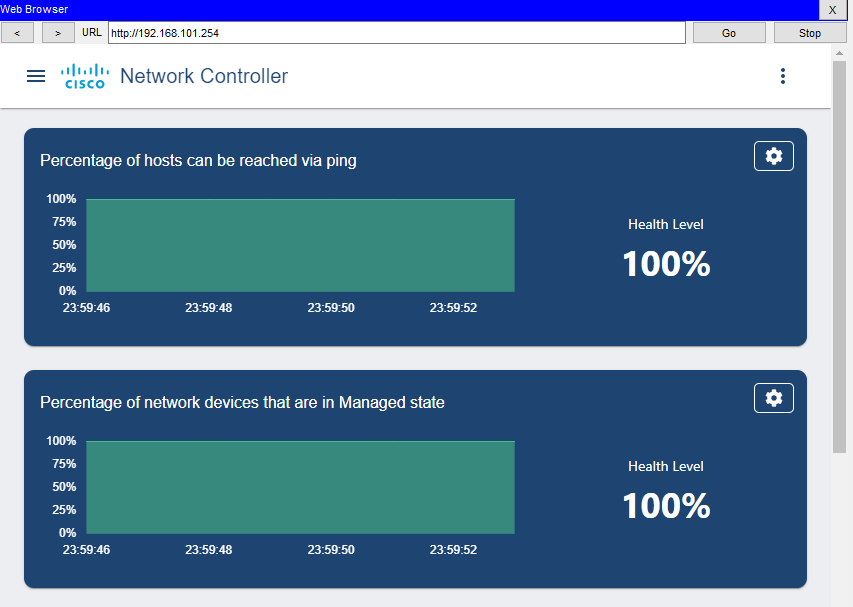
3. Notice that the S**oftware Version** is listed, as well as a variety of other detailed information about the device.



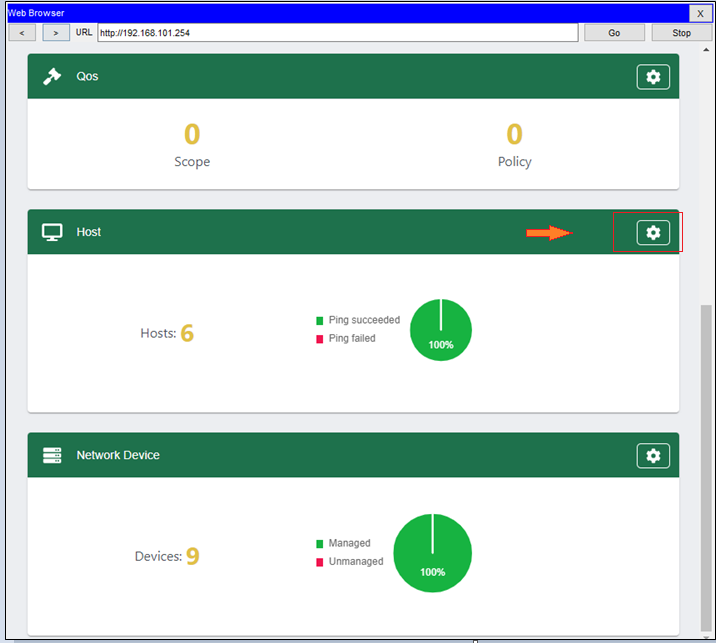
4. To view the list of **host devices** discovered by the PT-Controller0, return to the **Dashboard**. You can do this by clicking the **menu icon** next to the **Cisco logo** and then selecting **Dashboard**, or more simply, by clicking directly on the Network Controller banner at the top of the interface. This will bring you back to the main dashboard, where host device information can be accessed.



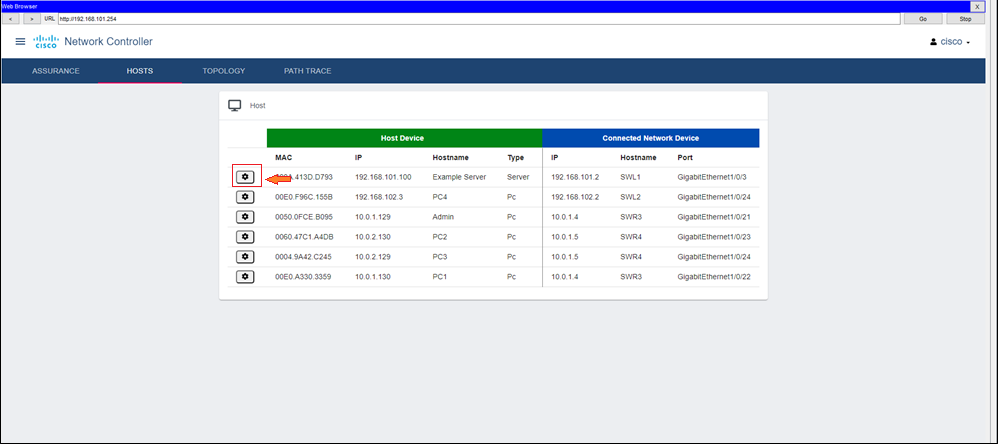
5. Once you are on the **Dashboard**, you will see visual charts displaying the **number of host devices** that can be reached via **ping**, as well as the **number of network devices** currently being managed by the controller. Both of these indicators should show **100%**, confirming that all host and network devices have been successfully discovered and are reachable by the PT-Controller0.



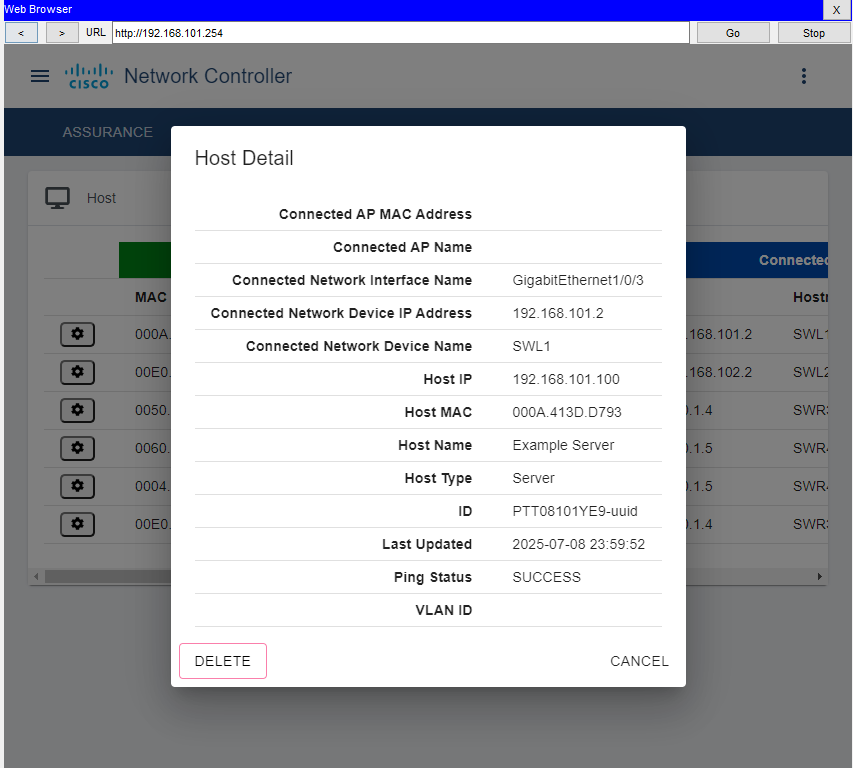
6. On the dashboard, you will also notice several tiles labeled **QoS, Network device**, and **Host**. To view more detailed information about the host devices, click the gear icon located on the host tile. This will take you to the hosts tab under the assurance section, where you can see performance and connectivity details for each discovered host in the network.



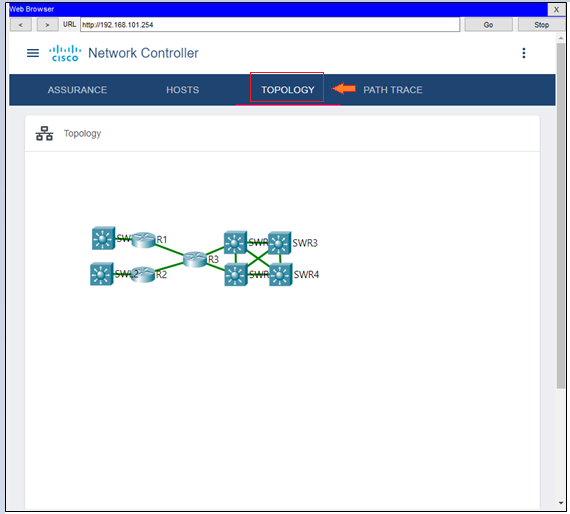
7. Click on the **Gear** button on the host. On the **host's** page under the **assurance** section, you can view detailed layer 2 and layer 3 connectivity information for each host device. this includes IP and MAC addresses, VLAN assignments, and routing details, along with the specific network device, such as a switch or router, to which each host is connected. this visibility helps verify proper network configuration and host connectivity across the topology.



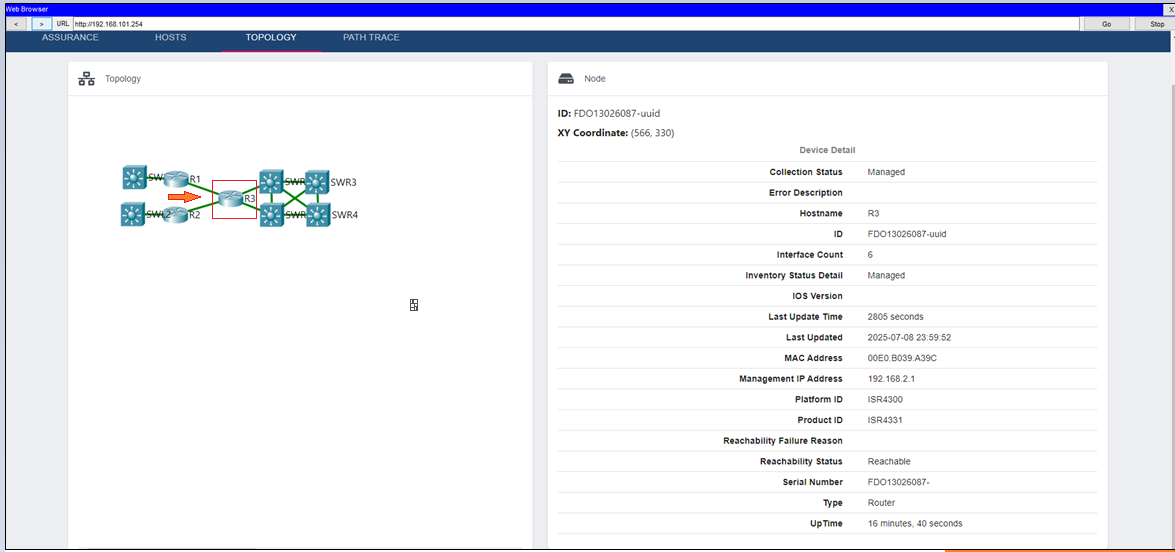
8. To view more detailed information about a specific host, click the **gear icon** next to any host listed on the host’s page. this will open a detailed view that displays additional data such as interface status, protocol information, and connection details with the associated network device.



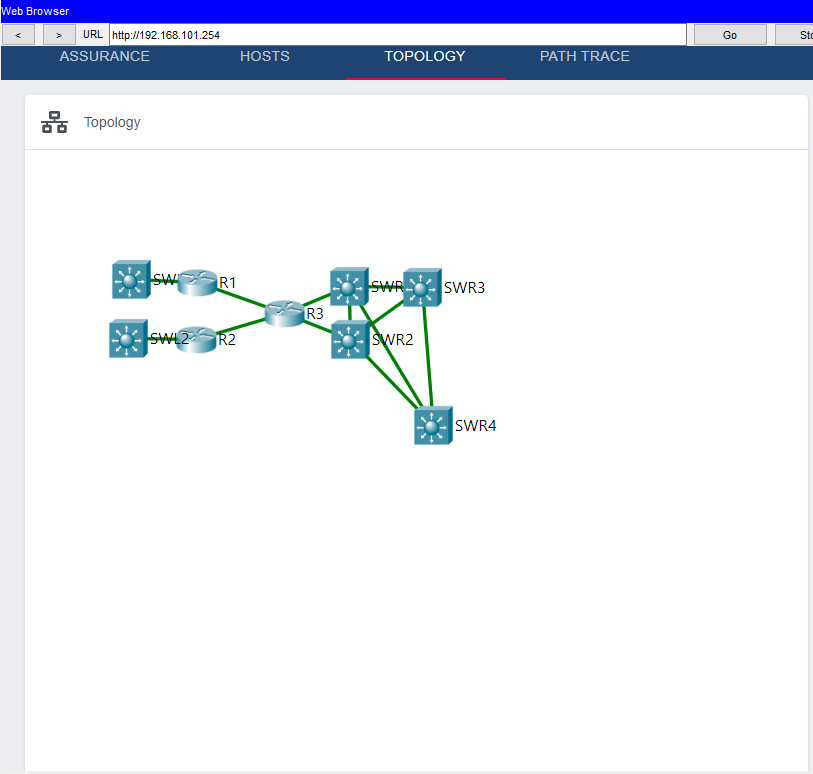
9. To view the topology created by pt-controller0, click the **TOPOLOGY** tab in the controller interface. you will notice that the PT-Controller has dynamically generated a network map that mirrors the same topology displayed in Packet Tracer’s main window, showing all discovered devices and their interconnections.



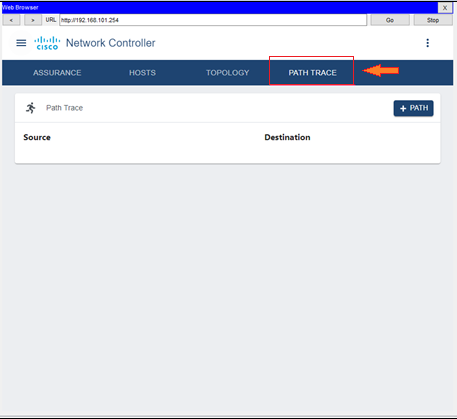
10. You can click on any **Network Device** within the topology map to see its details. this includes information such as device name, ip address, model, and connectivity status, allowing you to quickly assess the role and configuration of each device in the network.



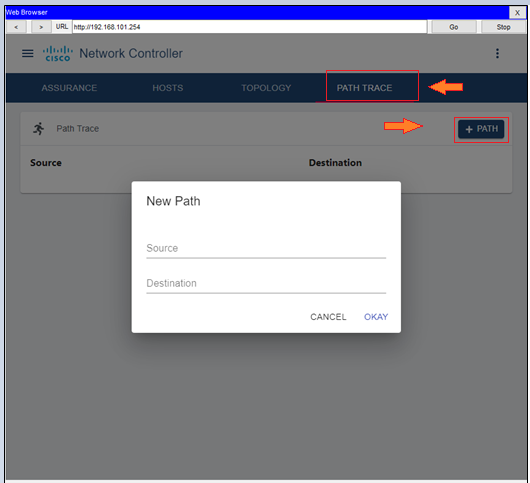
11. You can also click and drag the device icons within the topology view to rearrange the layout for better visibility. However, keep in mind that any changes you make to the arrangement will not be saved when you leave the topology workspace.



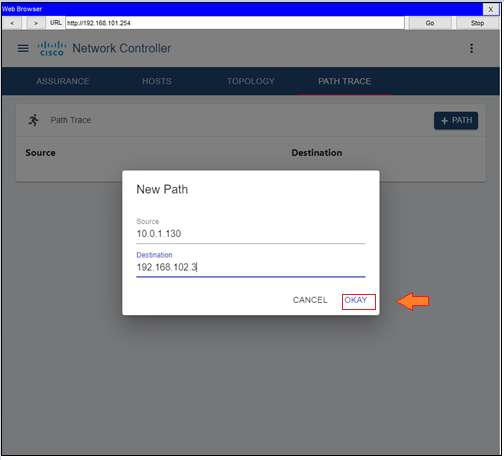
12. To begin tracing the path between two devices, click the **Path Trace** tab in the PT-Controller0 interface. This feature allows you to analyze the route taken by data as it travels across the network from a source device to a destination device.



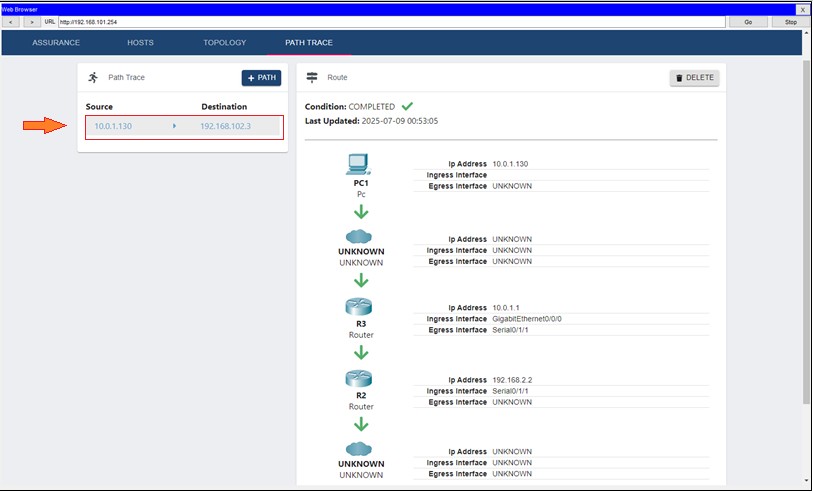
13. Click **+ Path** to add a **New Path** and to trace the path from one end of the network to the other.



14. Enter the ip address of the source device (for example, PC1) and the destination device (such as PC4) in the provided fields. once both addresses are entered, click **OKAY** to start the path trace. this will simulate and display the route taken by packets between the two devices across the network.



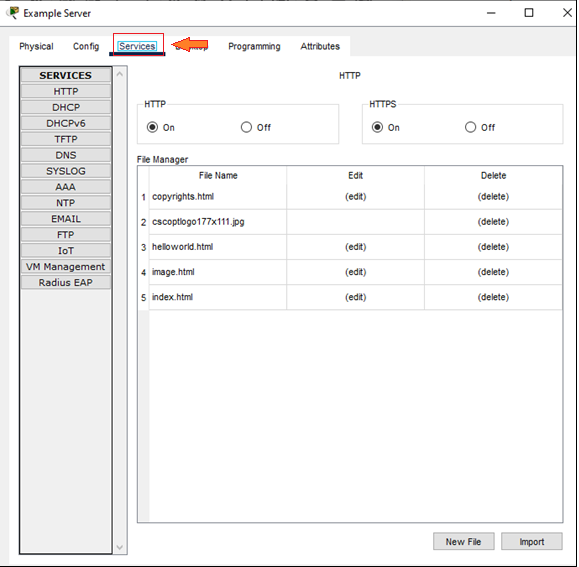
15. Click the newly added path to start the path trace. The **Route** Report will display all hops from the source to the destination, showing only Layer 3 devices like routers. Switches appear as **UNKNOWN** because they operate at Layer 2 and do not handle IP routing.



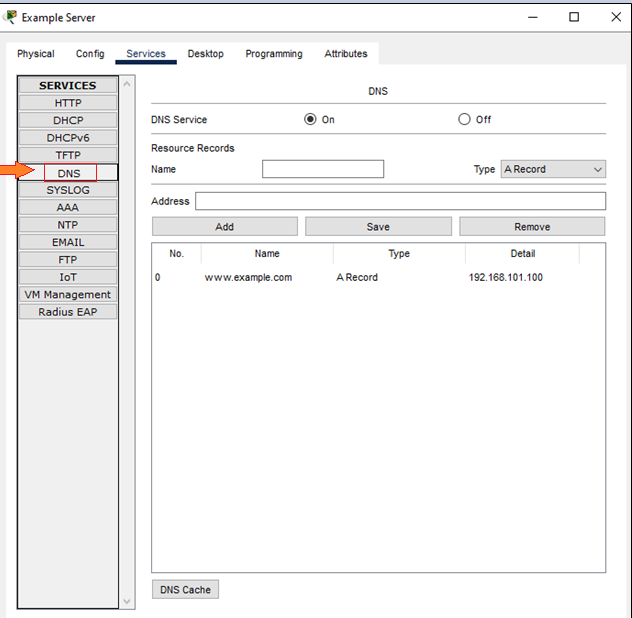
**//Use an SDN Controller to Configure Network Settings**

1. To begin configuring global network settings using pt-controller0, first investigate the configuration of the Example server, which will provide DNS, NTP, and syslog services. Click on example server.

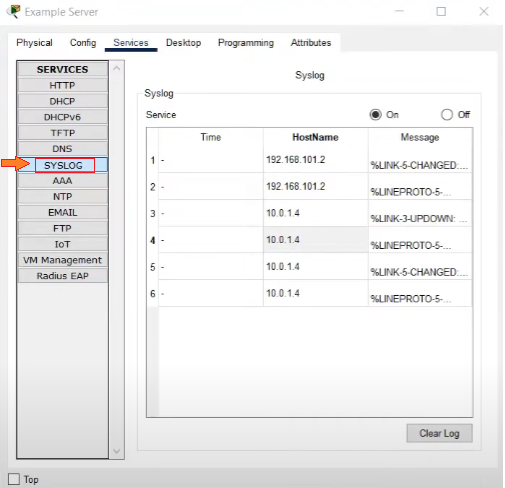
2. Then go to the **Services** tab to view the available services and ensure they are properly configured before applying them through the controller.



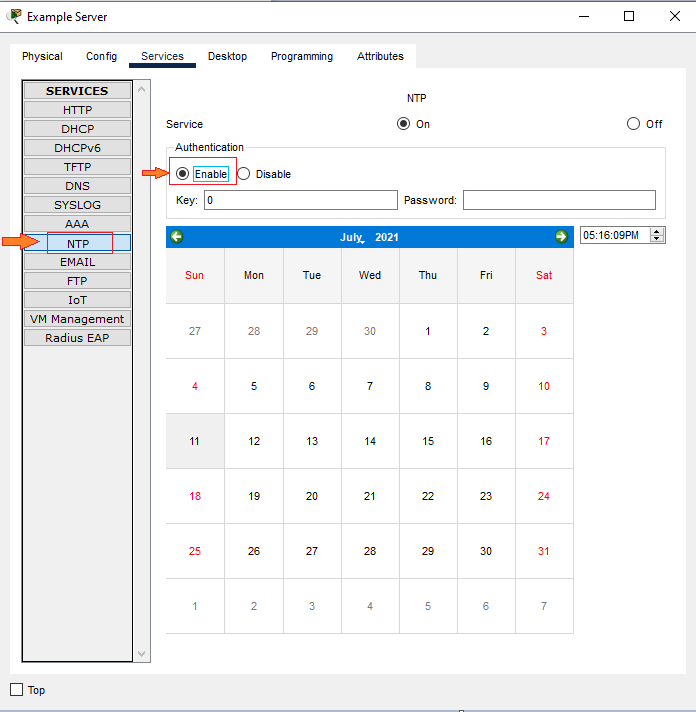
3. Under the **SERVICES** section, click on **DNS**. you will see that the **DNS Service** is **enabled**, and there is a single DNS record configured for [**www.example.com**](http://www.example.com). This confirms that the server is ready to provide DNS resolution to the network.



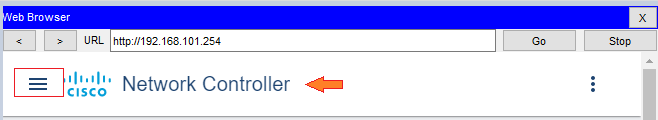
4. Under **SERVICES**, click on **SYSLOG**. You will see that the **Syslog service** is **enabled**, allowing the device to log system messages for monitoring and troubleshooting.



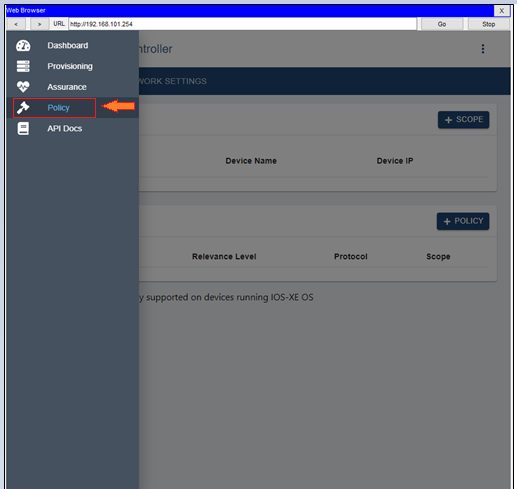
5. Under the **SERVICES** tab on the **example server**, click on **NTP**. You will see that the **NTP service is enabled**, indicating that the server is ready to provide time synchronization to other devices in the network. This is essential for accurate logging and coordinated network operations.



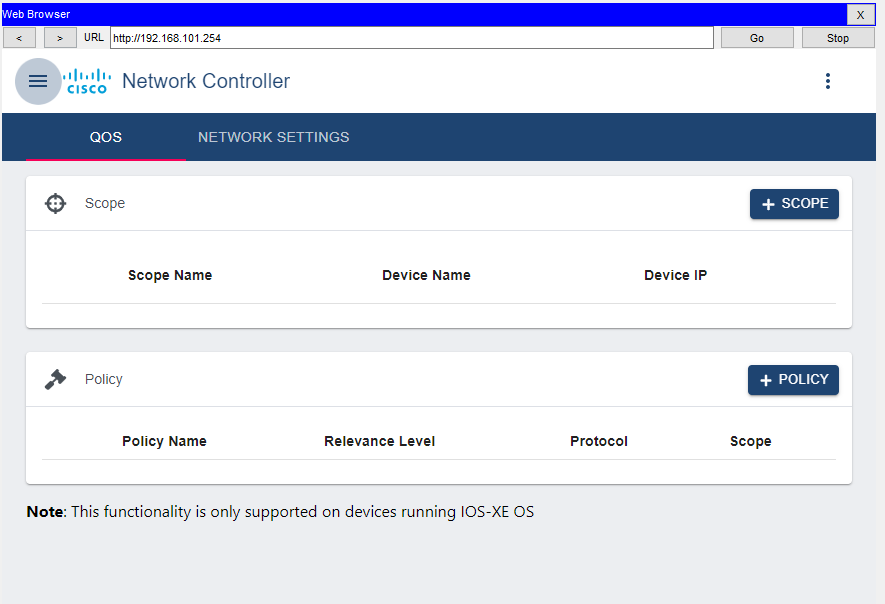
6. To configure a global policy for **DNS**, **syslog**, and **NTP**, click on **Admin**. If the **Admin pc** was closed earlier, reopen it, go to the **Desktop** tab, launch the web browser, and log back into pt-controller0 using your previously set credentials. This will bring you back to the controller dashboard, where you can begin configuring the global network settings. Click the menu to the left of the Cisco logo.



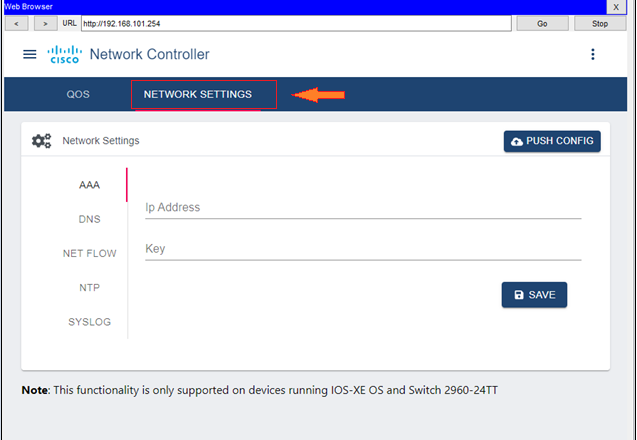
7. Click on **Policy.**



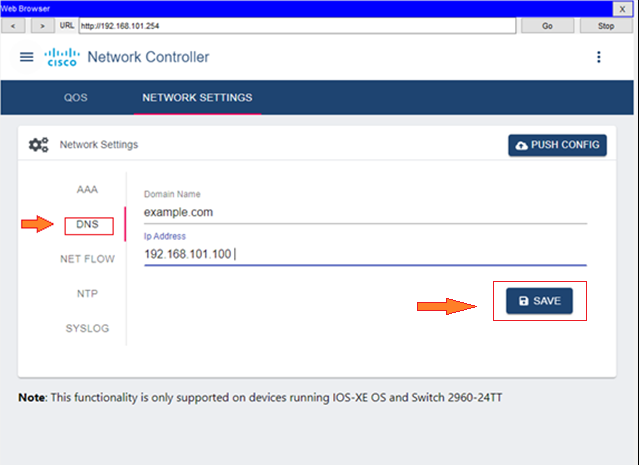
8. On the **QOS** tab in the **PT-Controller0** dashboard, you will notice there are options for configuring the **Scope** and **Policy**. However, for this activity, you will not be modifying QOS settings. Instead.



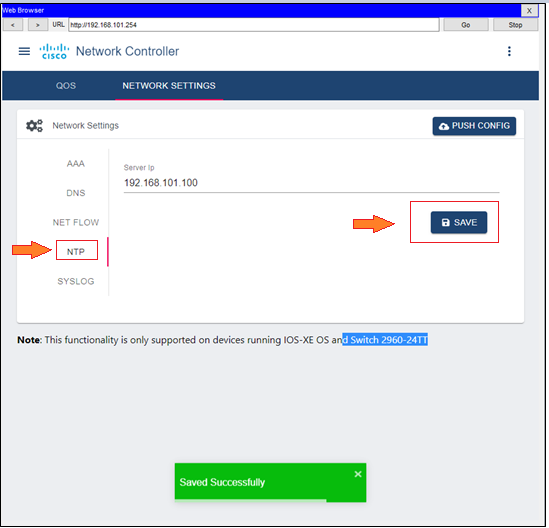
9. You will focus on configuring N**etwork Settings**, such as **DNS**, **SYSLOG**, and **NTP**, which will apply globally to the supported network devices in your topology. Click on **Network Settings** in the PT-Controller0 dashboard. This section allows you to configure global parameters such as **DNS server**, **syslog server**, and **NTP server**, which can then be pushed to all supported network devices in the topology.



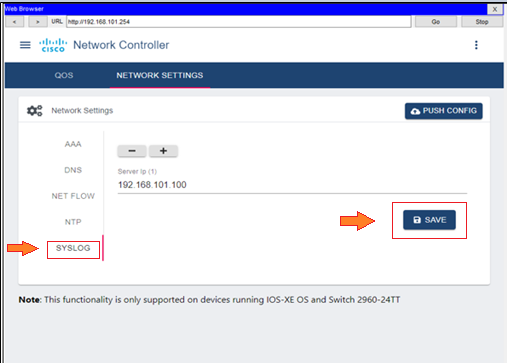
10. Click on **DNS** within the network settings section. In the **domain name** field, enter example.com, and in the ip address field, enter **192.168.101.100**. This sets up the global DNS configuration that will be applied to all network devices managed by the controller. Then click on **Save**.



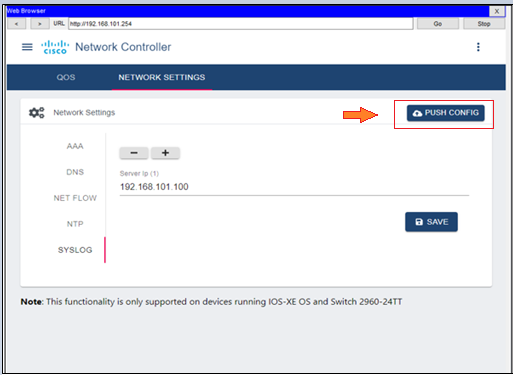
11. Click on **NTP** within the network settings section. In the ip address field, enter **192.168.101.100**, which points to the example server providing NTP service. Then click **Save** to store the configuration. This will allow all managed devices to synchronize their clocks with the NTP server.



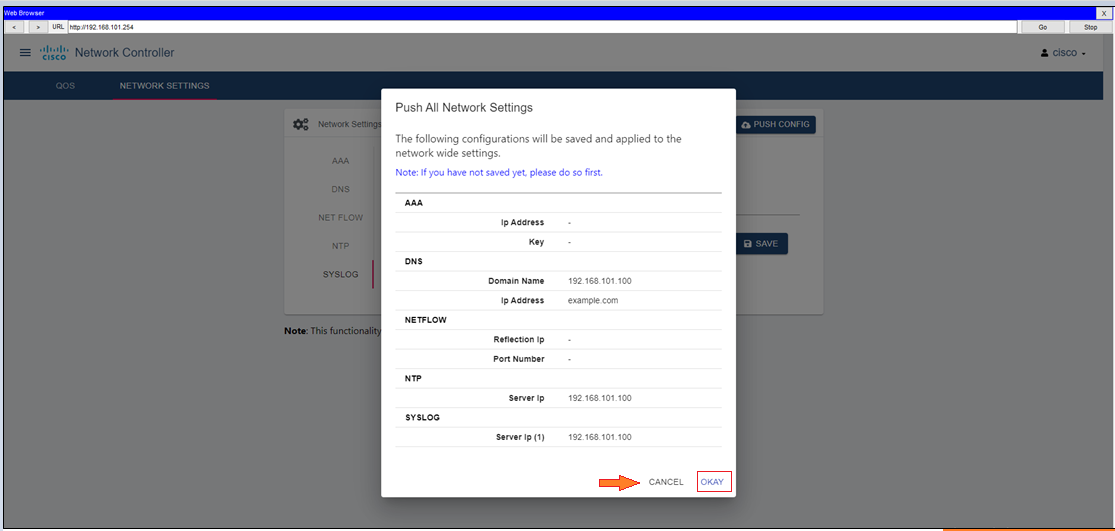
12. Click **SYSLOG,** enter **192.168.101.100** as the ip address to designate the example server as the syslog destination for all network logs. Then click **Save** to apply and store the configuration.



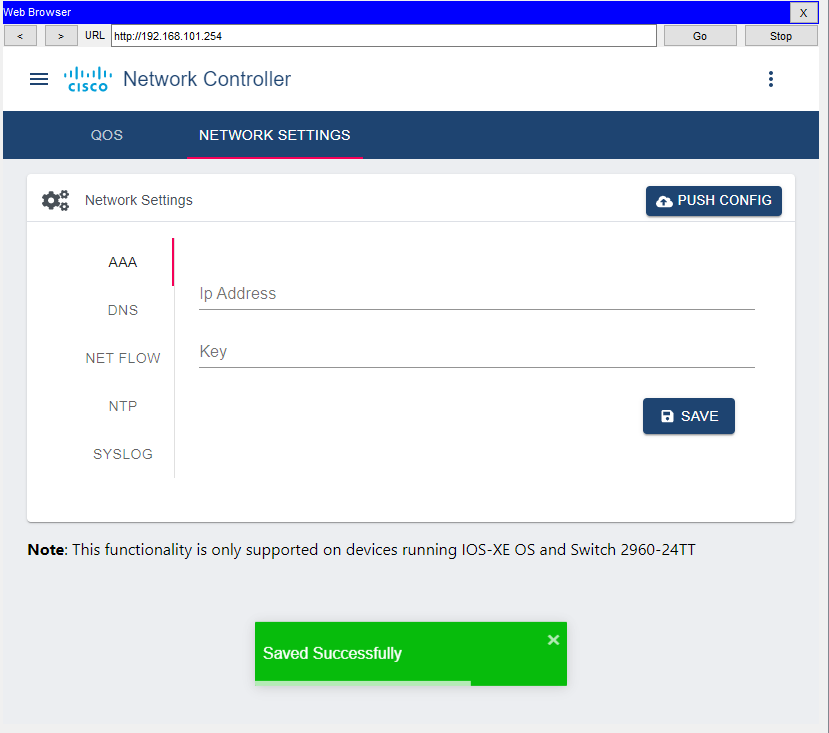
13. Click on **DNS**, **NTP**, and **SYSLOG** again to verify that the entered information is correct. If you notice any errors, update the fields accordingly and click S**ave** each time to ensure the changes are stored. Once all settings are confirmed, click **push CONFIG** to apply the global network configuration to all supported devices in the topology.



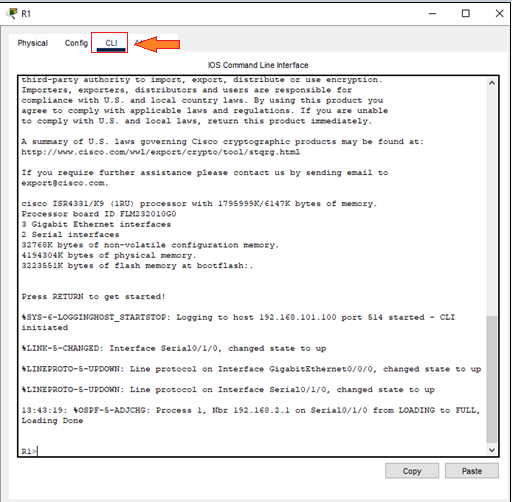
14. Click **OKAY** to proceed.



15. When the **PUSH** all network settings dialog box opens, review the displayed settings for **DNS**, **NTP**, and **SYSLOG** to ensure they are correct. Once verified, A brief message saying **“Saved Successfully”** will appear, confirming that the configuration has been pushed to all applicable network devices.



16. After pushing the network settings, it is important to understand that in this version of packet tracer, the configuration is only supported on ios-xe devices and the switch **2960-24tt**. As a result, the global settings were applied only to the **routers** in your topology. To verify this, click on any of the three router **R1** then go to the **CLI** tab to check the applied settings directly from the command-line interface.



17. Click inside the **CLI window** of the router and press **Enter** to activate the terminal and display the command prompt. This allows you to begin entering commands to verify the applied network settings.

R1> enable

R1# show run | begin ip domain

ip domain-name example.com

ip name-server 192.168.101.100



18. Enter the appropriate commands in the CLI to verify the **NTP settings** on the router. The system time on **R1** should synchronize with the **NTP server’s time**, reflecting your current time. Note that Packet Tracer may take a short while to propagate NTP messages across the network. To accelerate this process, you can click the **fast-forward time** button in the main topology window.

R1#show ntp associations

address ref clock st when poll reach delay offset disp

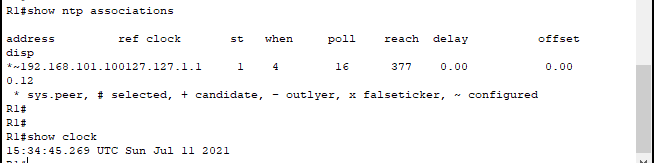
\*~192.168.101.100127.127.1.1 1 4 16 377 0.00 0.00 0.12

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#show clock

15:34:45.269 UTC Sun Jul 11 2021

R1#



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

R1#

R1#show run | include logging

logging 192.168.101.100

R1#



20. To test **SYSLOG logging**, shut down the **serial0/1/0 interface** on the router and then bring it back up. This action should trigger system log messages that will be sent to the configured syslog server, allowing you to verify that log reporting is functioning correctly.

R1#configure terminal.

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#interface s0/1/0

R1(config-if)#shutdown

R1(config-if)#

%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

15:38:17: %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 shut

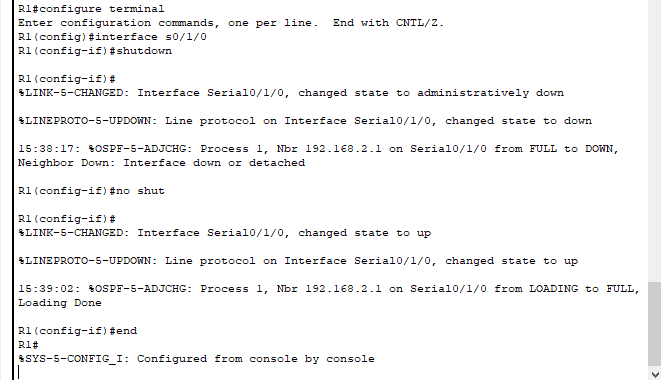
R1(config-if)#

%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

15:39:02: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0 from LOADING to FULL, Loading Done

R1(config-if)#end



21. Click on the **Example Server**, go to the **SERVICES** tab, and then select **SYSLOG**. You should see the same **Syslog messages** that appeared in the router's **CLI** now logged on the server. This confirms that the router is successfully sending log data to the syslog server. You can **double-click any of the entries** to view the full message details.

