Cambium Networks™

Manual
CLI Configuration

Table of Contents

Contents

1 Getting Started

1.1 Interfaces

1.1.1 cnMaestro

cnMaestro is a cloud-based or on-premises platform specialized for secure, end-to-end network lifecycle management: inventory management, device onboarding, daily operations, and maintenance and is recommended for managing **cnMatrix** switches based networks.

The **cnMaestro** network manager simplifies device management by offering full network visbility. Network operators can have a real-time view of their complete end-to-end network and perform a full suite of network management functions to optimize system availability, maximize throughput and meet emerging needs of business and residential customers.

Starting with 2.0.3, cnMaestro Cloud supports cnMatrix devices with minimum 2.0.3-r4 build. You should manually upgrade your cnMatrix switch to version 2.0.3–r4.

For more information about cnMaestro, please visit cnMaestro Online Help.

The cnMatrix switches with 2.0.1 version will be automatically upgraded during the onboarding process.

1.1.2 CLI

CLI

This section describes the configuration of **cnMatrix** using the Command Line Interface.

The **Command Line Interface** (CLI) can be used to configure, show the configuration, monitor statistics and troubleshoot the switch.

Authentication

The CLI interface can be accessed after you passed the authentication process, based on a user and a password.

The default user name is **admin** and the default password is **admin.** After you logged in as an admin user, you can create a new user or delete an existing user and modify your own password or the ones created for the new users.

CLI Command Modes

Depending on the CLI mode, your prompt will be specific:

Command Mode	Access Method	Prompt	Exit Command
Privileged EXEC	The User EXEC mode command **enable** is used to enter the Privi-	`cnMatrix#`	To logout from Privileged EXEC mode the

	leged EXEC mode. **Starting with version 2.1**, you can perform any command from the Privileged mode in the Global or Interface Configuration, by using the following command: `do <any command>`		**exit** command is used.
Global Configuration	In the Privileged EXEC mode, type the **configure terminal** command to enter the Global Configuration mode.	`cnMatrix(config)#`	To exit to the Privileged EXEC mode the **end** command is used.
Interface Configuration	In the Global Configuration mode, type the **<interface-type><interface-id>** command to enter the Interface configuration mode.	`cnMatrix(config-if)#vlan1`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
Interface Range Mode	In the Global Configuration mode, type the **range ({ <interface-type> <slot/port-port>} {vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>})** command to enter the Interface range mode.	`cnMatrix(config-if-range)#`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
Config-VLAN	In the Global Configuration mode type the **vlan vlan-id** command to enter the Config-VLAN mode.	`cnMatrix(config-vlan)#`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
Out of Band Interface Mode	In the Global Configuration mode, type the **interface mgmt0** command to enter the Out of Band mode.	`cnMatrix(config-if)#`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
DHCP Pool Configuration Mode	In the Global Configura-		To exit to the Global

	tion mode, type the **ip dhcp pool <id>** command to enter the DHCP Pool Configuration Mode.	`cnMatrix(dhcp-config)#`	Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
SNTP Configuration Mode	In the Global Configuration Mode, type the **sntp** command to enter the SNTP Configuration mode.	`cnMatrix(config-sntp)#`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
MSTP Configuration Mode	In the Global Configuration mode, type the **spanning-tree mst configuration** command to enter the MSTP Configuration mode.	`cnMatrix(config-mst)#`	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

1.2 Basic Switch Configuration in CLI Interface

1.3 Configuring CLI and cnMaestro

1.3.1 Accessing CLI Interface (examples)

1.3.1.1 Accessing CLI Interface Using SSH

1. Open **PuTTY** application.
2. In the **PuTTY Configuration** window, select **SSH** in the **Connection type** section.
3. On the **PuTTY Configuration** window, in the **Host Name** field, enter 192.168.0.1 as IP address and in the Port field, enter 22 port as value.
4. Click **Open**. The login prompt is displayed.
5. In the cnMatrix login prompt enter the default username: **admin**
6. In the Password prompt enter the default login password: **admin**

1.3.1.2 Accessing CLI Interface Using Serial Port

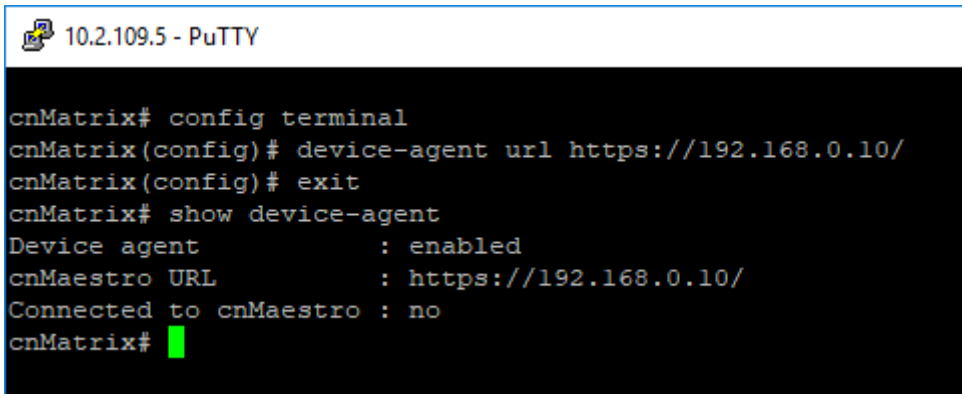
1. Connect console cable to PC and to console port on the switch.
2. Open **PuTTY** application.
3. In the **PuTTY Configuration** window, select **Serial** in the **Connection type** section.
4. In the **Serial line** section, enter the name of the serial connection.
5. In the **Speed** section, enter 115200 as speed value.
6. Click **Open**. The login prompt is displayed.
7. Log in with the following credentials:

username: admin

password: admin

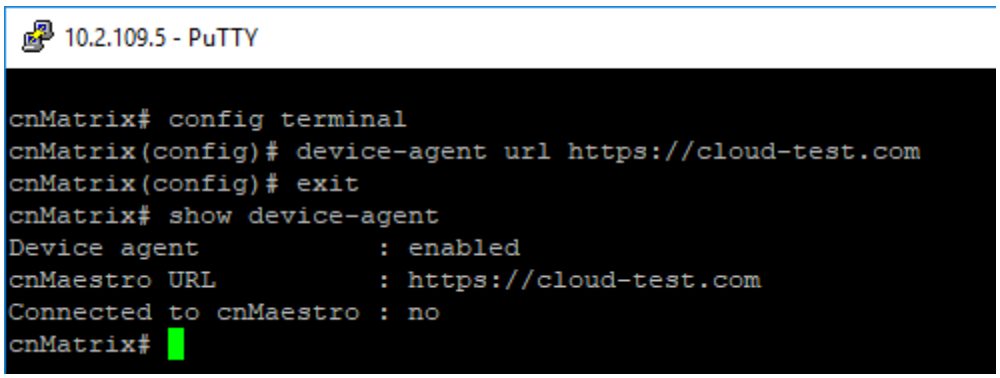
1.3.2 Configuring cnMaestro CLI

1.3.2.1 cnMaestro URL Configuration as IP



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **device-agent url https://192.168.0.10/** command into the terminal. Press the Enter key.
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show device-agent** command into the terminal. Press the Enter key.

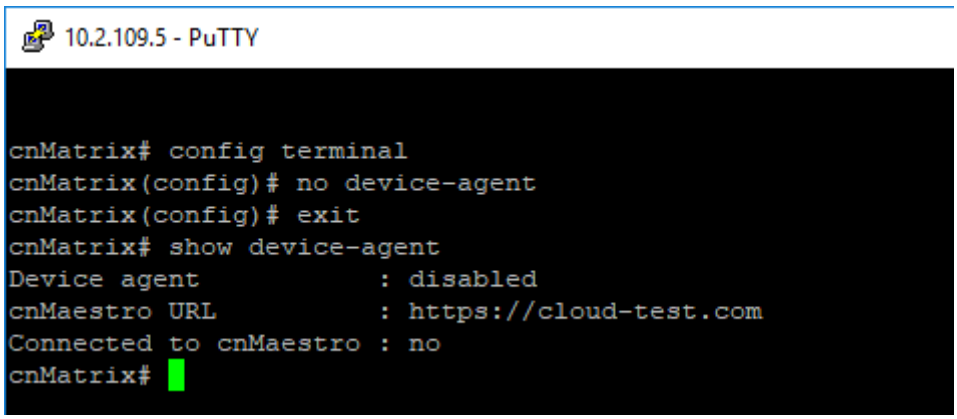
1.3.2.2 cnMaestro URL Configuration as String



5. Type the **config terminal** command into the terminal. Press the Enter key.
6. Type the **device-agent url https://cloud-test.com** command into the terminal. Press the Enter key.
7. Type the **exit** command into the terminal. Press the Enter key.
8. Type the **show device-agent** command into the terminal. Press the Enter key.

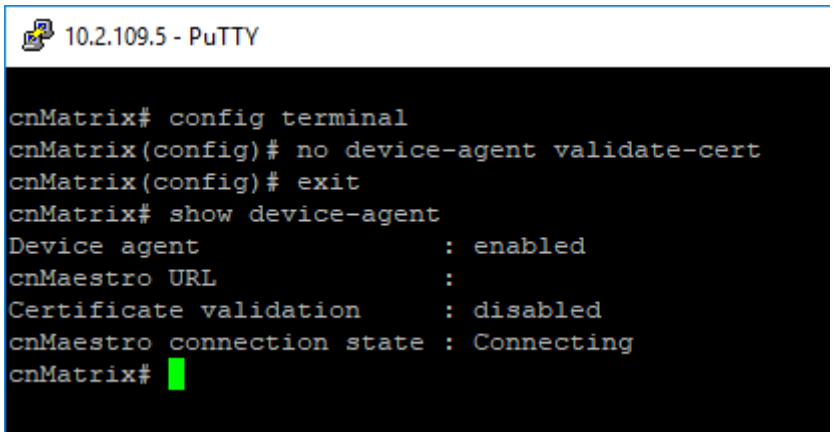
The default device-agent url: https://cloud.cambiumnetworks.com.

1.3.2.3 Disable cnMaestro



9. Type the **config terminal** command into the terminal. Press the Enter key.
10. Type the **no device-agent** command into the terminal. Press the Enter key.
11. Type the **exit** command into the terminal. Press the Enter key.
12. Type the **show device-agent** command into the terminal. Press the Enter key.

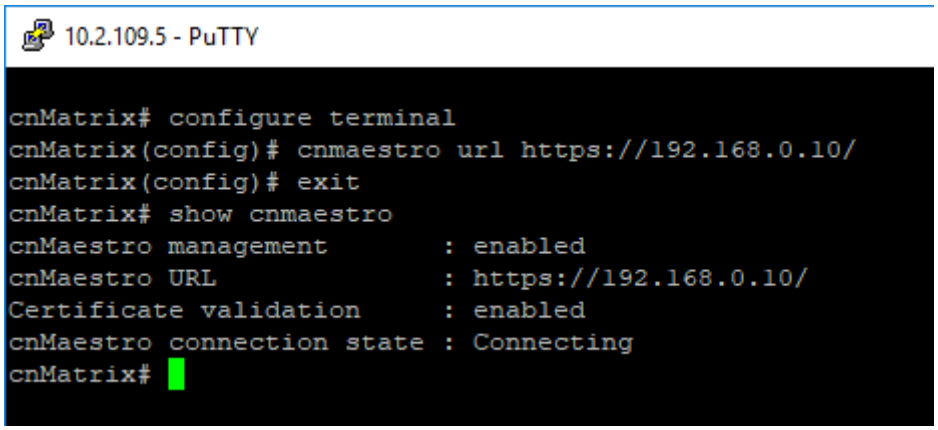
1.3.2.4 How to Disable cnMaestro Server Certificate Validation



13. Type the **config terminal** command into the terminal. Press the Enter key.
14. Type the **no device-agent validate-cert** command into the terminal. Press the Enter key.
15. Type the **exit** command into the terminal. Press the Enter key.
16. Type the **show device-agent** command into the terminal. Press the Enter key.

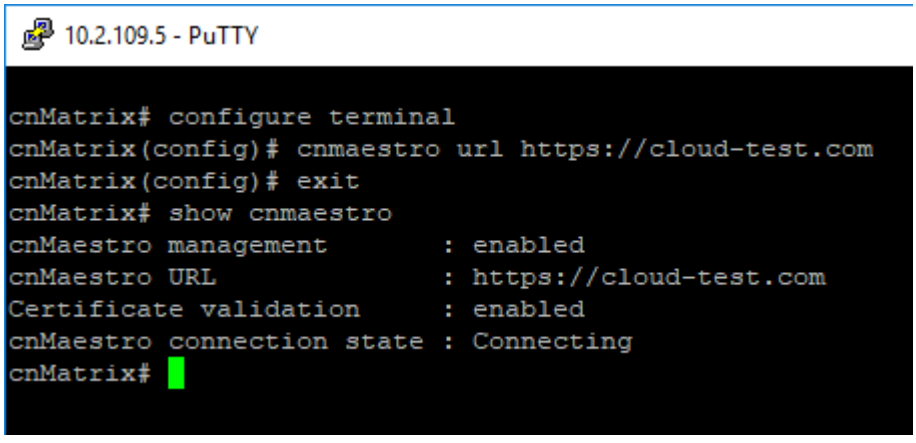
1.3.3 Configuring cnMaestro CLI (Starting with version 2.0.5)

1.3.3.1 cnMaestro URL Configuration as IP



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **cnmaestro url https://192.168.0.10/** command into the terminal to configure cnMaestro URL as IP. Press the Enter key.
3. Type the **exit** command into the terminal. Press the Enter key.
4. Type the **show cnmaestro** command into the terminal to display cnMaestro information. Press the Enter key.

1.3.3.2 cnMaestro URL Configuration as String

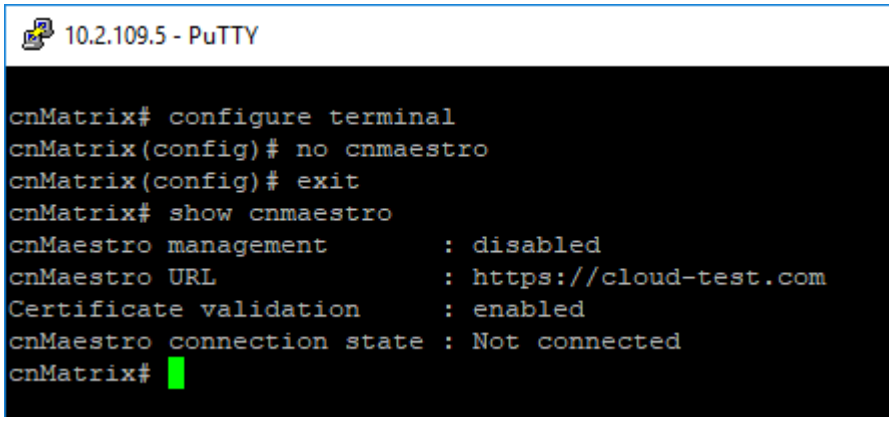


1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **cnmaestro url https://cloud-test.com** command into the terminal to configure cnMaestro URL as String. Press the Enter key.

> The default cnMaestro url: https://cloud.cambiumnetworks.com.

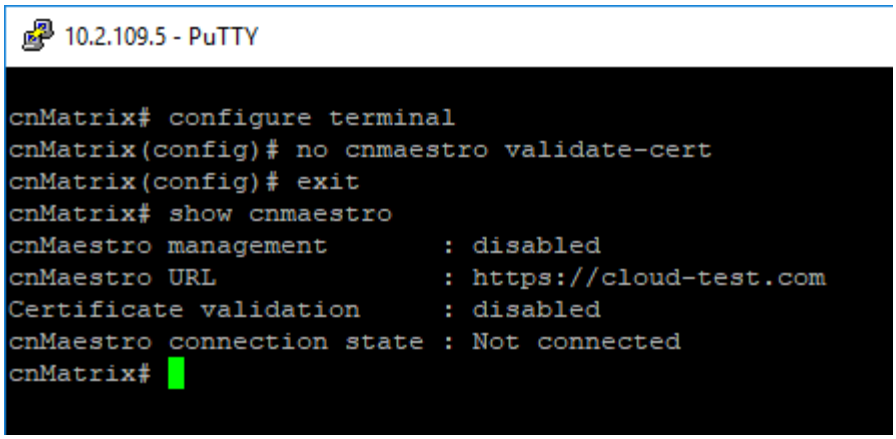
3. Type the **exit** command into the terminal. Press the Enter key.
4. Type the **show cnmaestro** command into the terminal to display cnMaestro information. Press the Enter key.

1.3.3.3 Disable cnMaestro



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **no cnmaestro** command into the terminal to disable cnMaestro. Press the Enter key.
3. Type the **exit** command into the terminal. Press the Enter key.
4. Type the **show cnmaestro** command into the terminal to display cnMaestro information. Press the Enter key.

1.3.3.4 How to Disable cnMaestro Server Certificate Validation



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **no cnmaestro validate-cert** command into the terminal to disable certificate validation. Press the Enter key.
3. Type the **exit** command into the terminal. Press the Enter key.
4. Type the **show cnmaestro** command into the terminal to display cnMaestro information.

1.4 Save/Restore/Erase Configurations in CLI Interface

1.4.1 Save/Restore/Erase/Download Configurations in CLI

Feature Overview

In order for you to save the configurations performed on the cnMatrix switch after a system reset, the settings have to be saved in a configuration file on the Flash.

- The **Configuration Save** feature saves the configurations performed on the switch by writing them either locally on the Flash or on a remote host (TFTP server or SFTP server).

- The **Configuration Restore** feature handles the restoration of settings found within the configuration file at system start-up. To enable this feature, make sure that a local configuration file exists or a configuration download is issued.
- The **Configuration Download** feature retrieves a configuration file from an external source (TFTP server or SFTP server), and these are effective after a system restart.
- The **Configuration Erase** feature offers the capability to use the switch with its factory defaults settings.

The **configuration restore** feature can be used only if a configuration file is present when restarting the switch.

The save / restore / download / erase features are available in CLI,SNMP and WEB interfaces.

- The **Configuration Save** feature has the **Autosave** option, so that the local configuration can be saved auttomaticaly everytime a change in the settings is performed. The **Autosave** option needs incremental save because of its triggering mechanism which determines when a configuration change occurred.

Default Values

- Autosave is disabled by default
- The incremental-save option is disabled by default.
- The auto-save trigger option is disabled by default.
- The startup configuration restore option is set to norestore by default.

Scaling Numbers

- The configurations features either work locally on the box or interact with a third party server. In the second scenario, the scaling capability is dependent on the server.

For more information, see Save/Restore/Erase/Download Configurations - Parameters and Commands in CLI .

1.5 Boot Partial Default

1.5.1 Boot Partial Default

The **boot partial default** feature enables you to delete all configuration, except for:

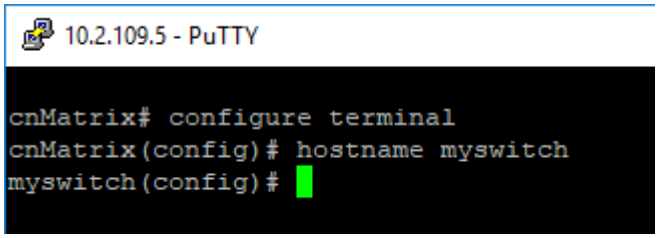
- User configuration for IP address on VLAN 1.
- Default and Static routes.
- Device agent status.
- cnMaestro URL.
- User configuration for username and password to login cnMatrix switch.
- User configuration for DNS servers.

To reset the switch to partial configuration, run the following command:

```
boot partial default
```

1.6 How to Change the Host Name

1.6.1 How to Change the Host Name



1 Enter **configure terminal** into the field. Press the Enter key.

2 Enter **hostname myswitch** into the field to change the host name . Press the Enter key.

Starting with version 2.1, the default host name is generated using the last 6 digits of the base MAC address (e.g: EX2010P-FEB436) .

Make sure to perform one of the following commands to save the configured host name:

- **write startup-config**.
- **copy running-config startup-config**.

2 L2 Features

2.1 VLAN

2.1.1 Managing VLAN

2.1.1.1 Feature Description

Feature Overview

The **VLAN** feature represents a group of devices on one or more LANs that are configured to communicate with each other as a whole, even if they are located on different LAN segments. The VLAN feature segments a broadcast domain in multiple broadcast domains and allows network administrators to group hosts together even if those hosts are not connected to the same switch.

Available **switchport modes** (define the way of handling the traffic for VLANs):

- **access** - Configures the port as access port that accepts and sends only untagged frames. This kind of port is added as a member to a single VLAN, and carries traffic only for the VLAN to which the port is assigned.

The port can be set as access port, only if the following 3 conditions are met:

1. The port is an UNTAGGED member in a single VLAN.
2. The PVID of the port is equal to the VLAN ID of the corresponding VLAN.
3. Acceptable frame type is automatically set as **untaggedAndPriorityTagged** if the first two conditions are met.

- **trunk** - Configures the port as trunk port that accepts and sends only tagged frames, if the **Acceptable Frame Type** is set as **tagged**.

The port can be set as trunk port only if the port is NOT a member of untagged port list for any VLAN in the switch.

If the **Acceptable Frame Type** is set to **All**, the trunk port will accept untagged frames as

well.

- **hybrid** - Configures the port as a hybrid port that accepts and sends both tagged and untagged frames.

  The hybrid port works in conjuction with the Acceptable Frame Type:

  - If the **Acceptable Frame Type** is set to **All**, the hybid port will accept and send both tagged and untagged frames.
  - If the **Acceptable Frame Type** is set to **Tagged**, the hybrid port will accept and send only the tagged frames.
  - If the **Acceptable Frame Type** is set to **untaggedAndPriorityTagged**, the hybrid port will accept and send the untagged and priority tagged traffic.

Please be aware of the fact that when the **Acceptable Frame Type** is set to **All** or **Tagged**, you have to configure the PVID value in conjuction with the Acceptable Frame Type in order for the selected port to carry traffic only for a specific VLAN.

Standards

- IEEE 802.1Q – defines a system of VLAN tagging for Ethernet frames.
- 802.1Q is the IEEE standard for tagging frames and supports up to 4096 VLANs. In 802.1Q, the trunking device inserts a 4-byte tag into the original frame and recomputes the frame check sequence (FCS) before the device sends the frame over the trunk link. At the receiving end, the tag is removed and the frame is forwarded to the assigned VLAN.

Scaling Numbers

- A maximum of 4066 series can be created.

Limitations

- A maximum of 32 VLANs can be configured in PVRST mode.

Default Values

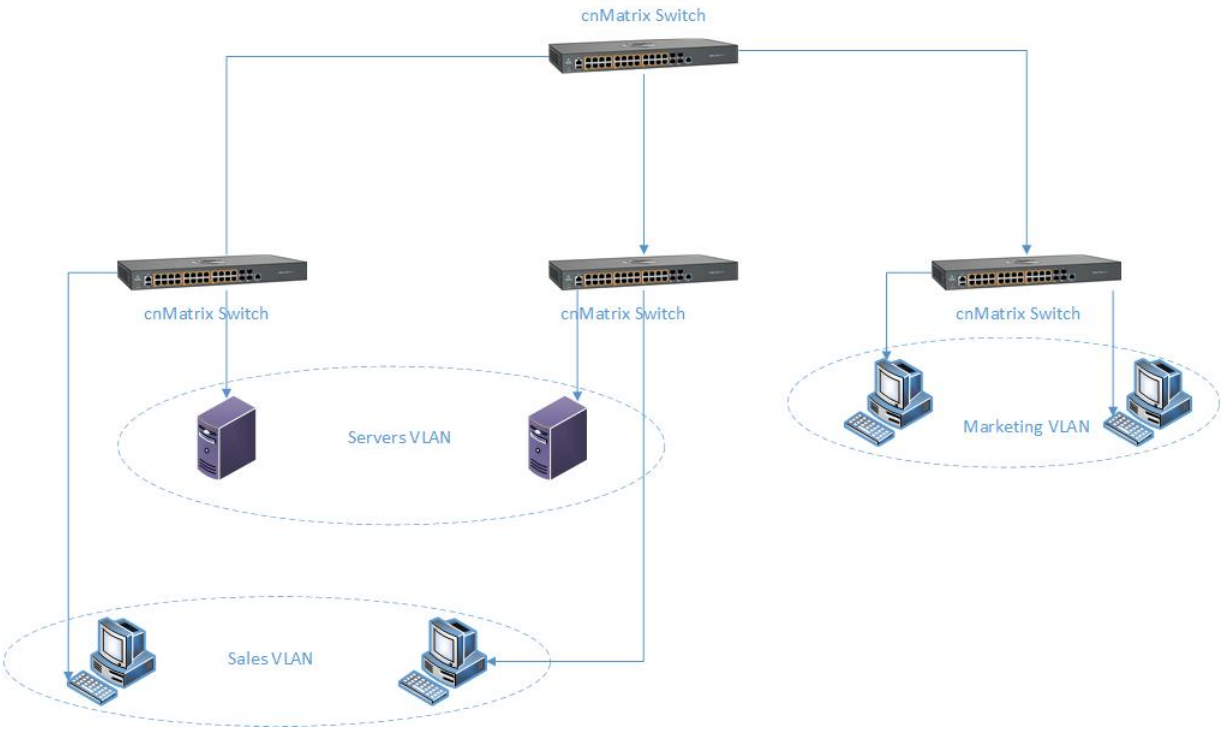
- VLAN is enabled by default.
- VLAN 1 is created by default.
- All available ports are configured as member ports and untagged ports of the default VLAN (VLAN 1).
- The default operation mode for all ports: hybrid.

The static MAC address of a specific VLAN will be removed after deleting the VLAN.

The static ARP will be removed after deleting the VLAN interface.

VLAN 1 cannot be deleted using the no form of the command: no vlan <vlan-id>.

2.1.1.2 Network Diagram



2.1.2 How to Create a VLAN in CLI Interface

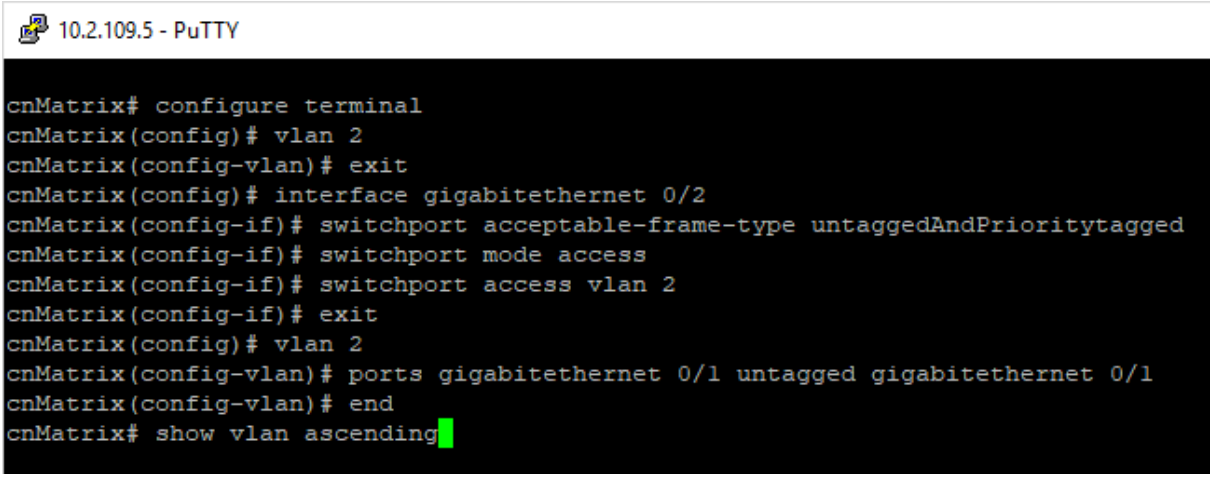
10.2.109.5 - PuTTY

```
cnMatrix# config terminal
cnMatrix(config)# vlan 50
cnMatrix(config-vlan)# ports add gigabitethernet 0/3 untagged gigabitethernet 0/3
cnMatrix(config-vlan)# end
cnMatrix# show vlan id 50

Vlan database
-------------
Vlan ID             : 50
Member Ports        : Gi0/3
Untagged Ports      : Gi0/3
Name                :
Status              : Static
Egress Ethertype    : 0x8100
-----------------------------------------------------

cnMatrix# show vlan port gigabitethernet 0/3

Vlan Port configuration table
-----------------------------
Port Gi0/3
 Port Vlan ID                       : 1
 Port Acceptable Frame Type         : Admit All
 Port Mac Learning Status           : Enabled
 Port Ingress Filtering             : Enabled
 Port Mode                          : Hybrid
 Port-and-Protocol Based Support    : Enabled
 Default Priority                   : 0
 Port Protected Status              : Disabled
 Ingress EtherType                  : 0x8100
 Egress EtherType                   : 0x8100
 -----------------------------------------------------
```

1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **vlan 50** command into the terminal to configure a VLAN.Press the Enter key.
3. Type the **ports add gigabitethernet 0/3 untagged gigabitethernet 0/3** command into the terminal to configure port list for a VLAN. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
5. Type the **show vlan id 50** command into the field to display the VLAN global status for the specified VLAN. Press the Enter key.
6. Type the **show vlan port gigabitethernet 0/3** command into the field to display the interface information.Press the Enterkey.

For more information, see VLAN Parameters and Commands.

2.1.3 Configuring Port Based VLAN (Example)



1. Type the **configure terminal** command into the terminal. Press the Enterkey.
2. Type the **vlan 2** command into the terminal to configure a VLAN. Press the Enter key.
3. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key.
4. Type the **interface gigabitethernet 0/2** command into the terminal to select the interface to be configured. Press the Enter key.
5. Type the **switchport acceptable-frame-type untaggedAndPrioritytagged** command into the terminal to set the acceptable frame type for the port. Press the Enter key.
6. Type the **switchport mode access** command into the terminal to configure the VLAN port mode. Press the Enter key.
7. Type the **switchport access vlan 2** command into the terminal to set port as an untagged member port of a VLAN. Press the Enter key.
8. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key.
9. Type the **vlan 2** into the terminal to enter the configuration vlan mode. Press the Enter key.
10. Type the **ports gigabitethernet 0/1 untagged gigabitethernet 0/1** command into the terminal to configure port list for VLAN 2.

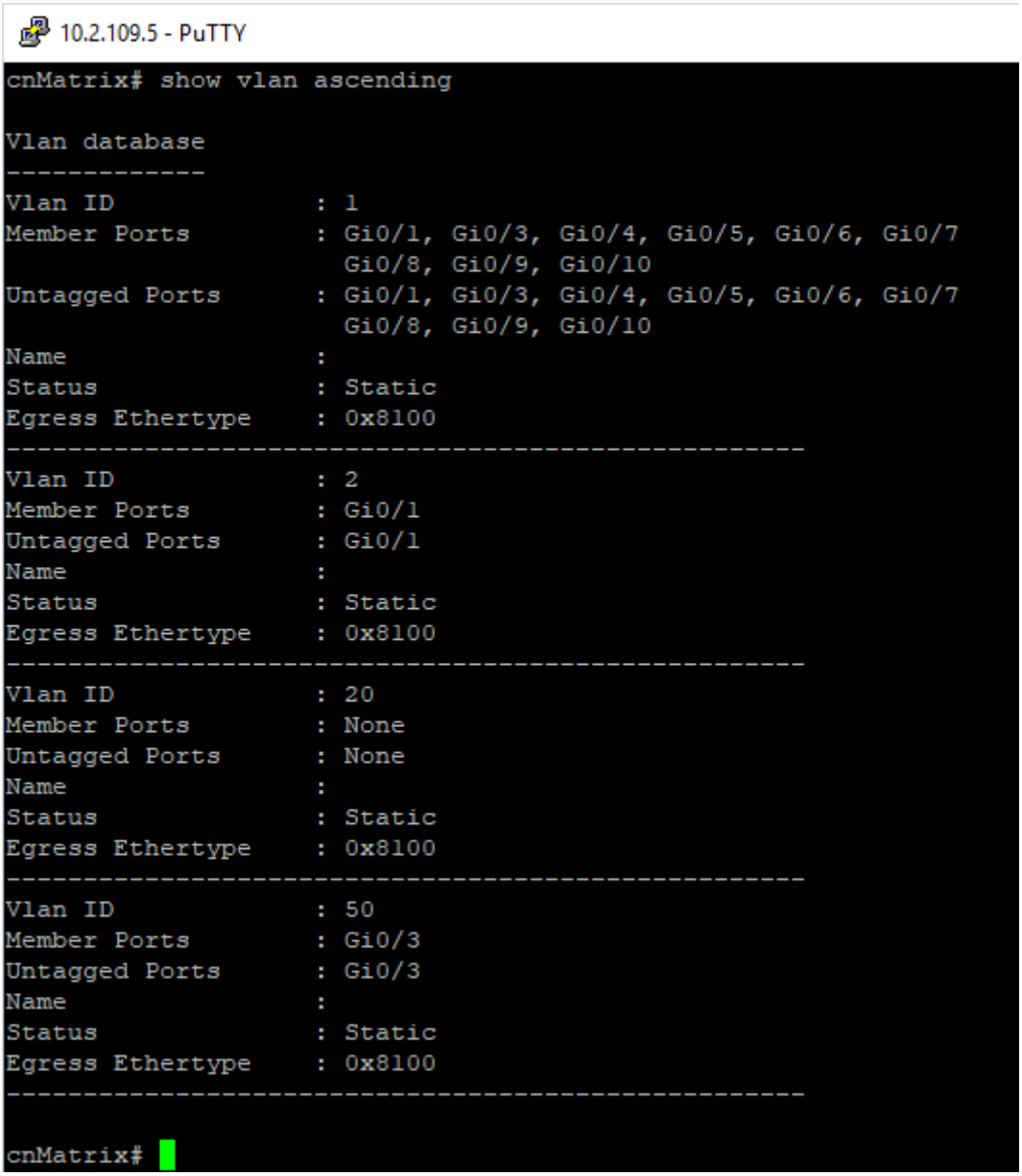
11 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

12 Type the **show vlan ascending** command into the terminal to display the VLAN global status. Press the Enter key.

10.2.109.5 - PuTTY

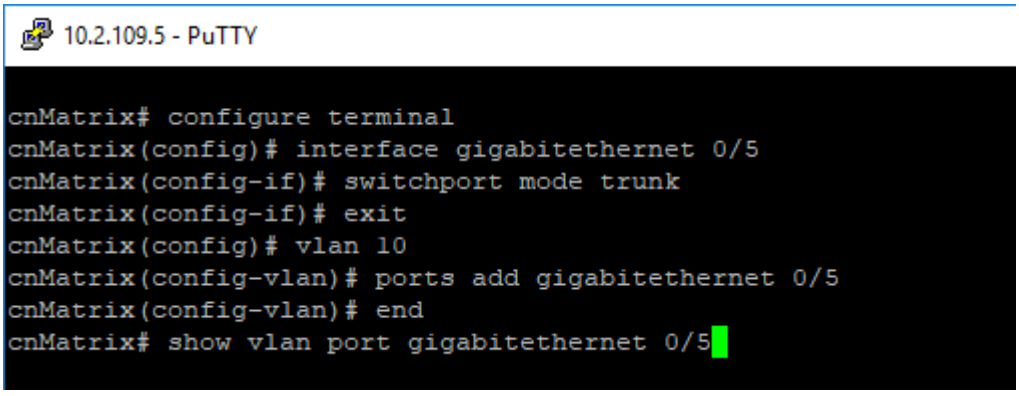
```
cnMatrix# configure terminal
cnMatrix(config)# vlan 2
cnMatrix(config-vlan)# exit
cnMatrix(config)# interface gigabitethernet 0/2
cnMatrix(config-if)# switchport acceptable-frame-type untaggedAndPrioritytagged
cnMatrix(config-if)# switchport mode access
cnMatrix(config-if)# switchport access vlan 2
cnMatrix(config-if)# exit
cnMatrix(config)# vlan 2
cnMatrix(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
cnMatrix(config-vlan)# end
cnMatrix# show vlan ascending

Vlan database
-------------
Vlan ID             : 1
Member Ports        : Gi0/1, Gi0/3, Gi0/4, Gi0/5, Gi0/6, Gi0/7
                      Gi0/8, Gi0/9, Gi0/10
Untagged Ports      : Gi0/1, Gi0/3, Gi0/4, Gi0/5, Gi0/6, Gi0/7
                      Gi0/8, Gi0/9, Gi0/10
Name                :
Status              : Static
Egress Ethertype    : 0x8100
----------------------------------------------------
Vlan ID             : 2
Member Ports        : Gi0/1
Untagged Ports      : Gi0/1
Name                :
Status              : Static
Egress Ethertype    : 0x8100
----------------------------------------------------
Vlan ID             : 20
Member Ports        : None
Untagged Ports      : None
Name                :
--More--
```

13 Press the Space key.



For more information, see VLAN Parameters and Commands.

2.1.4 Configuring 802.1Q Tagging VLAN



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/5** command into the terminal to select the interface to be configured. Press the Enter key.

3. Type the **switchport mode trunk** command into the terminal to select the trunk port mode. Press the Enter key.

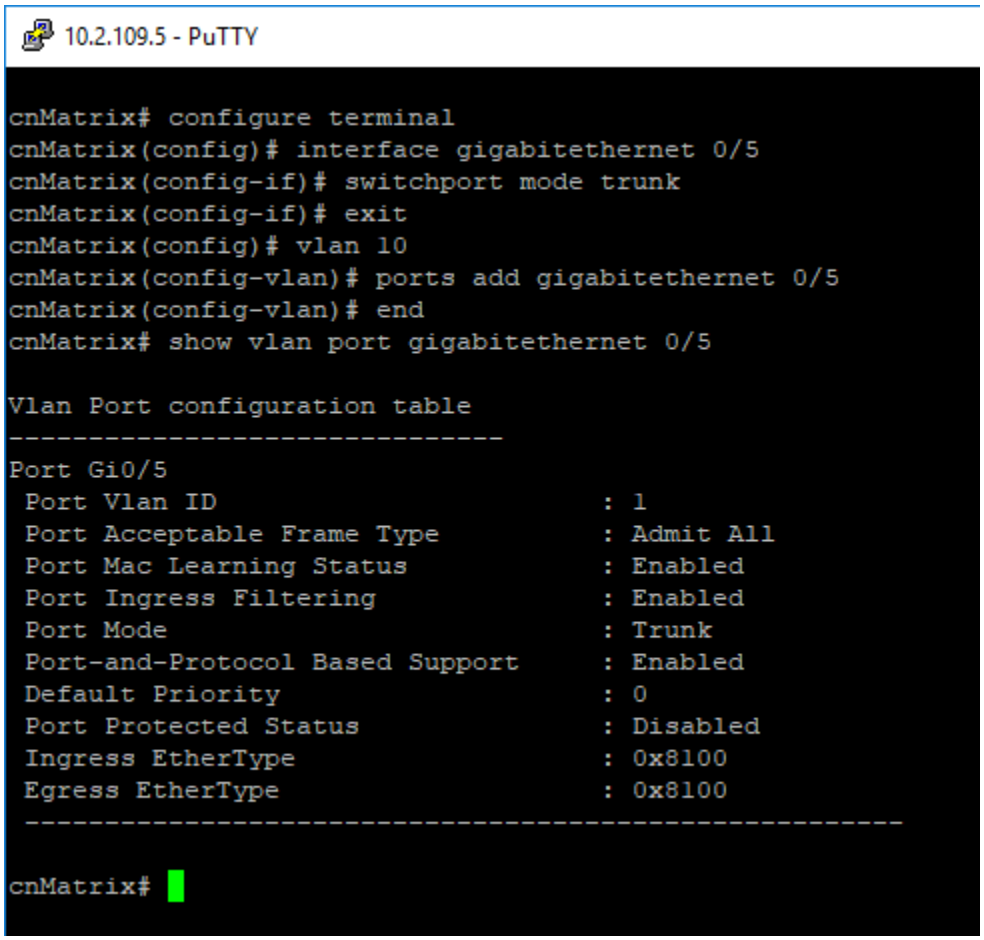
4. Type the **exit** commandinto the terminal to go back to the global configuration mode. Press the Enter key.

5. Type the **vlan 10** command into the terminal to enter the configuation vlan mode, and to select the VLAN to be configured. Press the Enter key.

6. Type the **ports add gigabitethernet 0/5** command into the terminal to configure the port list for VLAN 10.

7. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

8. Type the **show vlan port gigabitethernet 0/5** command into the terminal to display information about the configured interface. Press the Enter key.



For more information, see VLAN Parameters and Commands.

2.1.5 Troubleshooting VLAN

Useful commands for troubleshooting:

- To check the VLAN created in ports' membership:

```
cnMatrix# show vlan brief
```

- To check the operation mode of each interface:

```
cnMatrix# show vlan port Gigabitethernet 0/2
```

- To check the interface status:

```
cnMatrix# show interface status
```

- To check the ingress/egress counters on each interface:

```
cnMatrix# show interface counters
```

- To check the global status for the specified VLAN range:

```
cnMatrix#  show vlan ascending
```

```
cnMatrix#  show mac-address-table [vlan <vlan-range>]
```

2.2 STP

2.2.1 STP

Feature Overview

The **STP** feature is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations.The STP feature enables you to form a loop free network topology. Depending upon the path cost and the priority of the ports and bridges, the STP selects a bridge as a root bridge and forms a loop-free logical topology, which ensures a single path between any two-end stations.

STP in cnMatrix

Standards

The STP functionality is realized in the network using one of the three following STPs:

- RSTP (802.1w)
- MSTP (802.1s)
- PVRST

Scaling Numbers

- A maximum of 32PVRST instances can be configured in PVRST mode.
- A maximum of 8 MSTP instances can be configured in MSTP mode.

Limitations

- 802.1d standard is supported only in compatibility mode which allows cnMatrix to interact with legacy bridges who supports legacy STP feature.

Default Values

- The STP feature is enabled by default in RSTP mode.

Prerequisites

N/A

2.2.2 Managing RSTP

Feature Overview

Rapid Spanning-Tree, specified by standard 802.1w, is an evolution of the original Spanning-Tree

protocol, specified by standard 802.1d.

RSTP provides quicker convergence time compared to 802.1d STP, by not relying on timers to move an interface to Forwarding state.

All RSTP ports send BPDUs at each hello time (2 sec) intervals, which also helps with reducing up the convergence time.

RSTP has three port states:

- Discarding
- Learning
- Forwarding

RSTP ports can have the following roles: Alternate, Backup, Root, Designated.

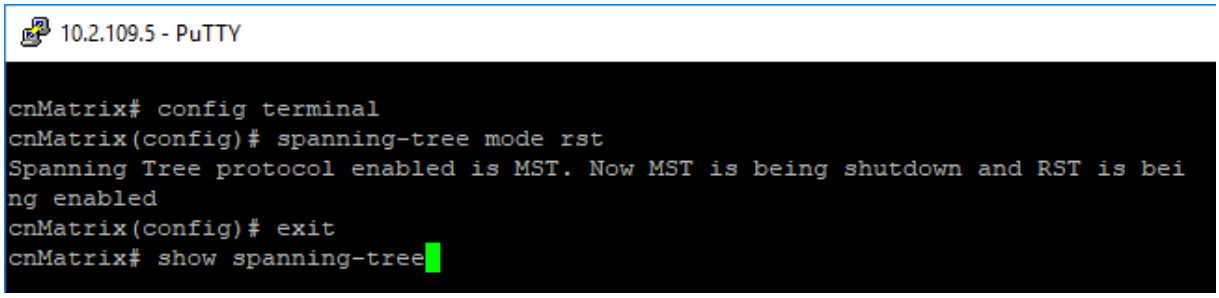
Standards

- 802.1w

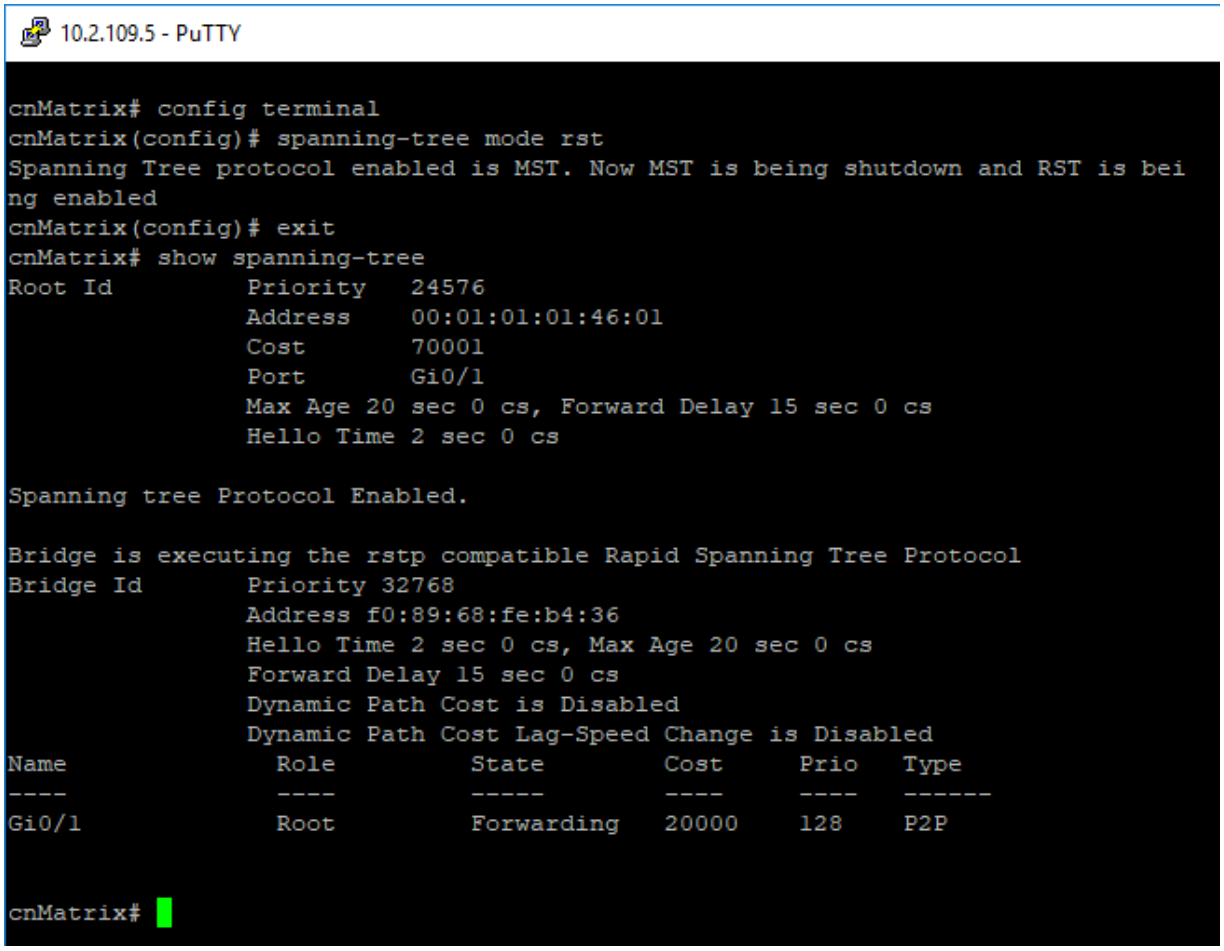
Default Values

- Hello time - 2 seconds.

2.2.3 How to Enable RSTP in CLI Interface

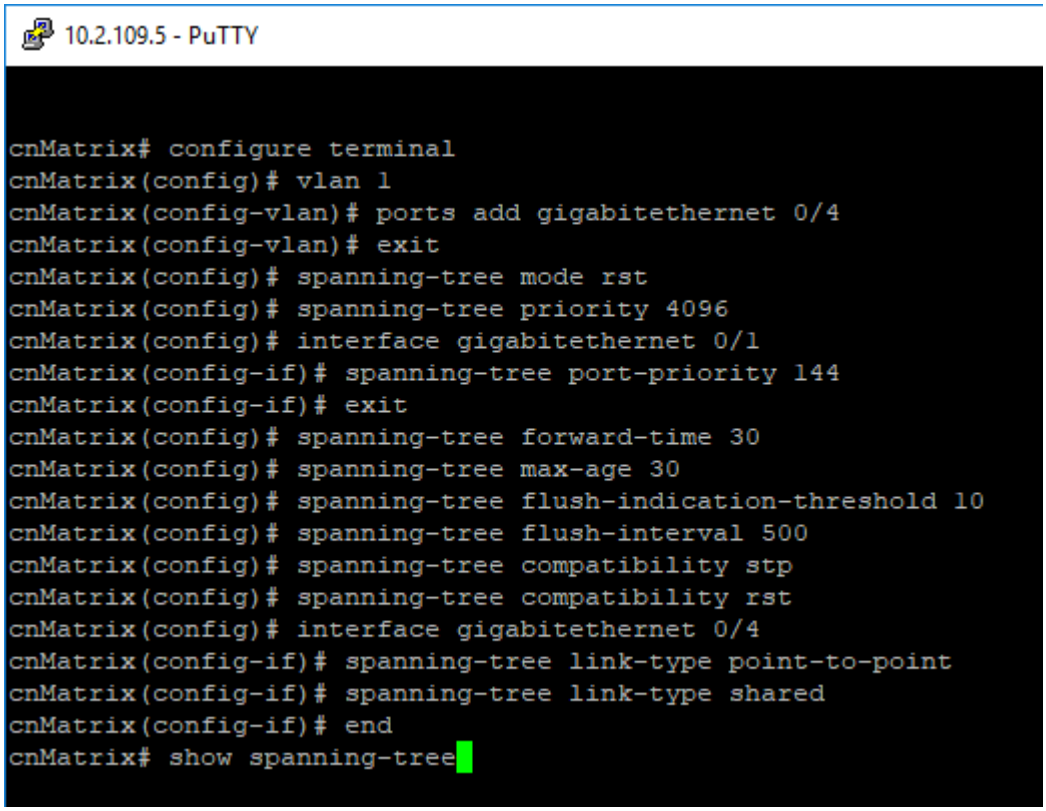


1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **spanning-tree mode rst** command into the terminal to set the spanning tree operating mode. Press the Enter key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
4. Type the **show spanning-tree** command into the terminal to display the spanning tree information. Press the Enter key.



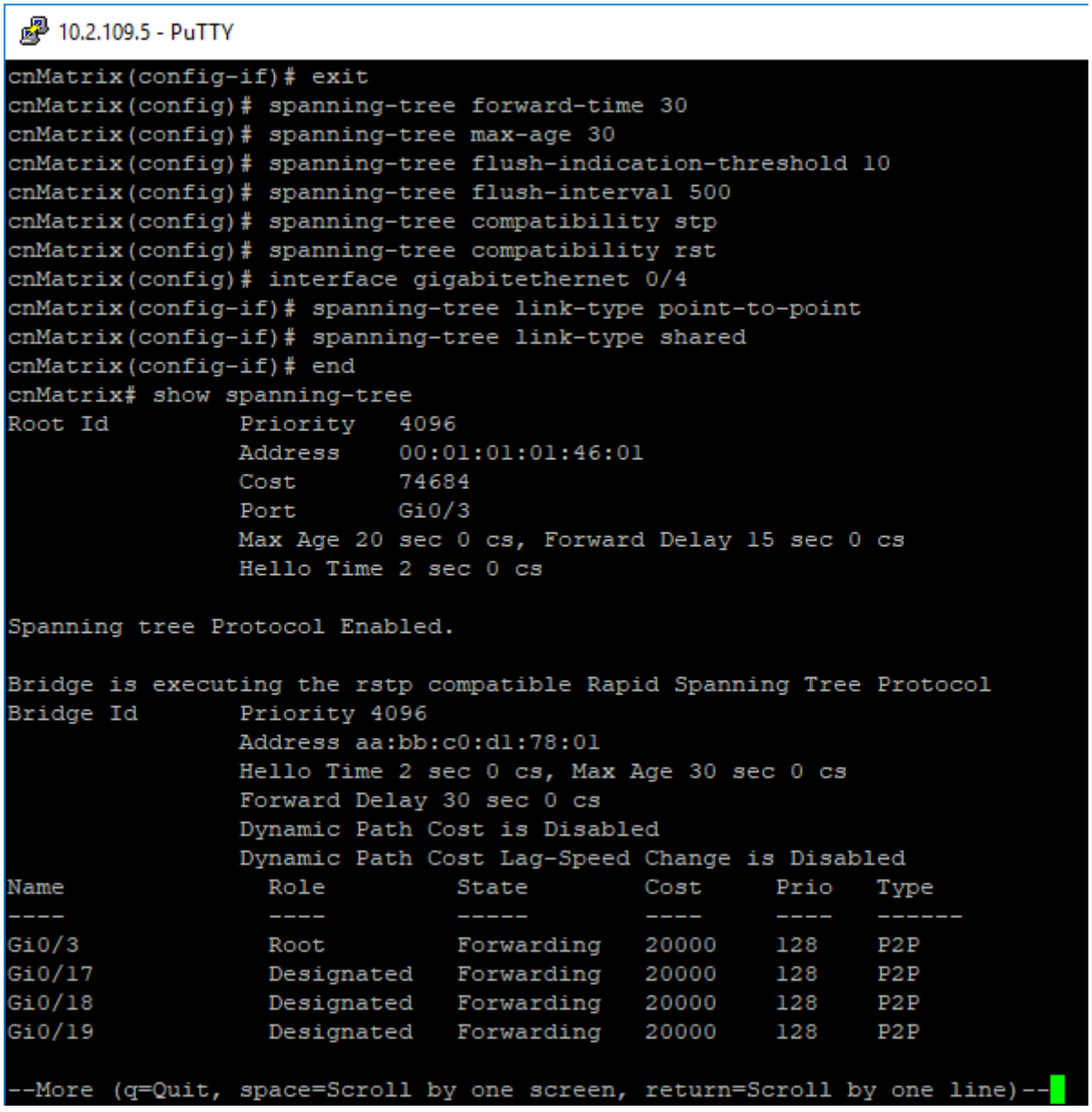
For more information, see RSTP Parameters and Commands.

2.2.4 Configuring RSTP in CLI Interface(Example)

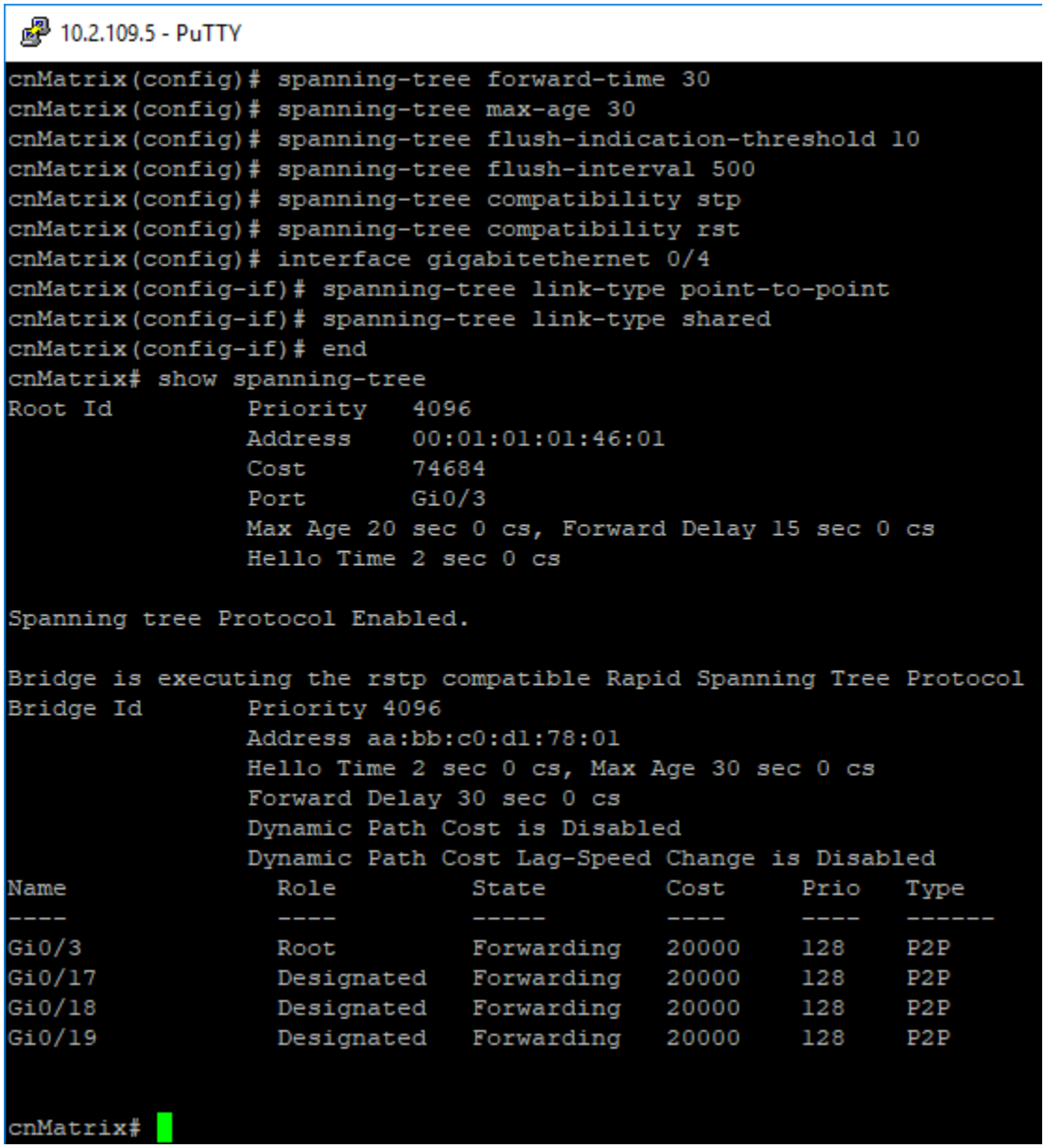


1 Type the **configure terminal** command into the terminal. Press the Enter key.

2. Type the **vlan 1** command into the terminal to configure a VLAN. Press the Enter key.
3. Type the **ports add gigabitethernet 0/4** command into the terminal to configure port list for the selected VLAN. Press the Enter key.
4. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key.
5. Type the **spanning-tree mode rst** command into the terminal to enable the rstp mode. Press the Enter key.
6. Type the **spanning-tree priority 4096** command into the terminal to configure the bridge priority value . Press the Enter key.
7. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
8. Type the **spanning-tree port-priority 144** command into the terminal to configure the port priority value. Press the Enter key.
9. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key
10. Type the **spanning-tree forward-time 30** command into the terminal to configure the forwarding-delay time. Press the Enter key.
11. Type the **spanning-tree max-age 30** command into the terminal to configure the spanning tree timers. Press the Enter key.
12. Type the **spanning-tree flush-indication-threshold 10** command into the terminal to configure the flush indications that go before the flush trigger timer method. Press the Enter key.
13. Type the **spanning-tree flush-interval 500** command into the terminal to configure the time in which the flush indications will be optimized. Press the Enter key.
14. Type the **spanning-tree compatibility stp** command into the terminal to configure the compatibility version for the spanning tree protocol. Press the Enter key.
15. Type the **spanning-tree compatibility rst** command into the terminal to configure the compatibility version for the spanning tree protocol. Press the Enter key.
16. Type the **interface gigabitethernet 0/4** command into the terminal to select an interface to be configured. Press the Enter key.
17. Type the **spanning-tree link-type point-to-point** command into the terminal to specify the link type for a rapid transition. Press the Enter key.
18. Type the **spanning-tree link-type shared** command into the terminal. Press the Enter key.
19. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
20. Type the **show spanning-tree** into the terminal to display the spanning tree information. Press the Enter key.



21 Press the Space key.



For more information, see RSTP Parameters and Commands.

2.2.5 Troubleshooting RSTP

1. Make sure that the same STP mode is running on all switches.
2. Make sure that the selected root is elected correctly using the lowest bridge priority.
3. Verify the redundant paths and the STP ports has the corresponsive states.

Useful commands for troubleshooting:

```
cnMatrix#show spanning-tree

cnMatrix#show spanning-tree root

cnMatrix#show spanning-tree interface

cnMatrix#show spanning-tree vlan

cnMatrix#show spanning-tree detail
```

2.2.6 Managing MSTP

2.2.6.1 Feature Description

To enable the MSTP functionality, RSTP and PVRST should be disabled.

Feature Overview

The **MSTP** feature enables VLANs to be grouped into spanning-tree instances, with each instance having a spanning-tree topology independent of other spanning-tree instances.

The **MSTP** feature enables the VLAN bridges to use multiple spanning trees, providing traffic belonging to different VLANs to flow over potentially different paths within the virtual bridged LAN.

Standards

- 802.1s

Scaling Numbers

- Up to 8 MSTP instances.

Limitations

N/A

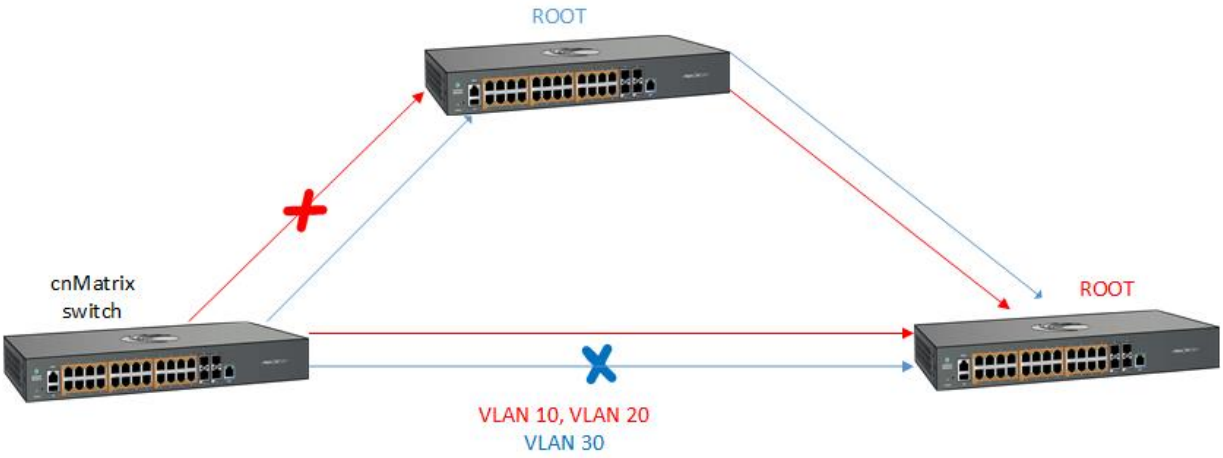
Default Values

- The default value for the forward time of the spanning tree: 15 seconds.
- The default value for the max-age timer of the spanning tree: 20 seconds.
- The default value for the revision number for the MST region: 0.
- The MST instance 0 is created and mapped with all VLANs.
- The default spanning tree hello time: 2 seconds.

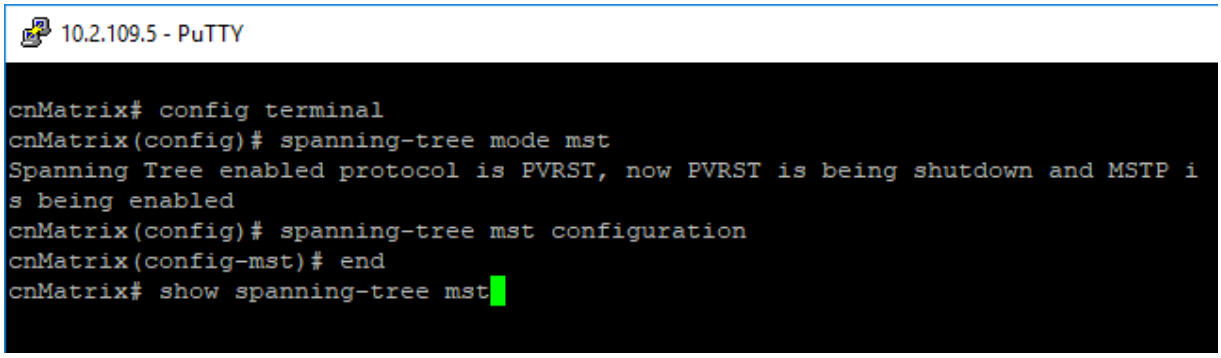
Prerequisites

- N/A

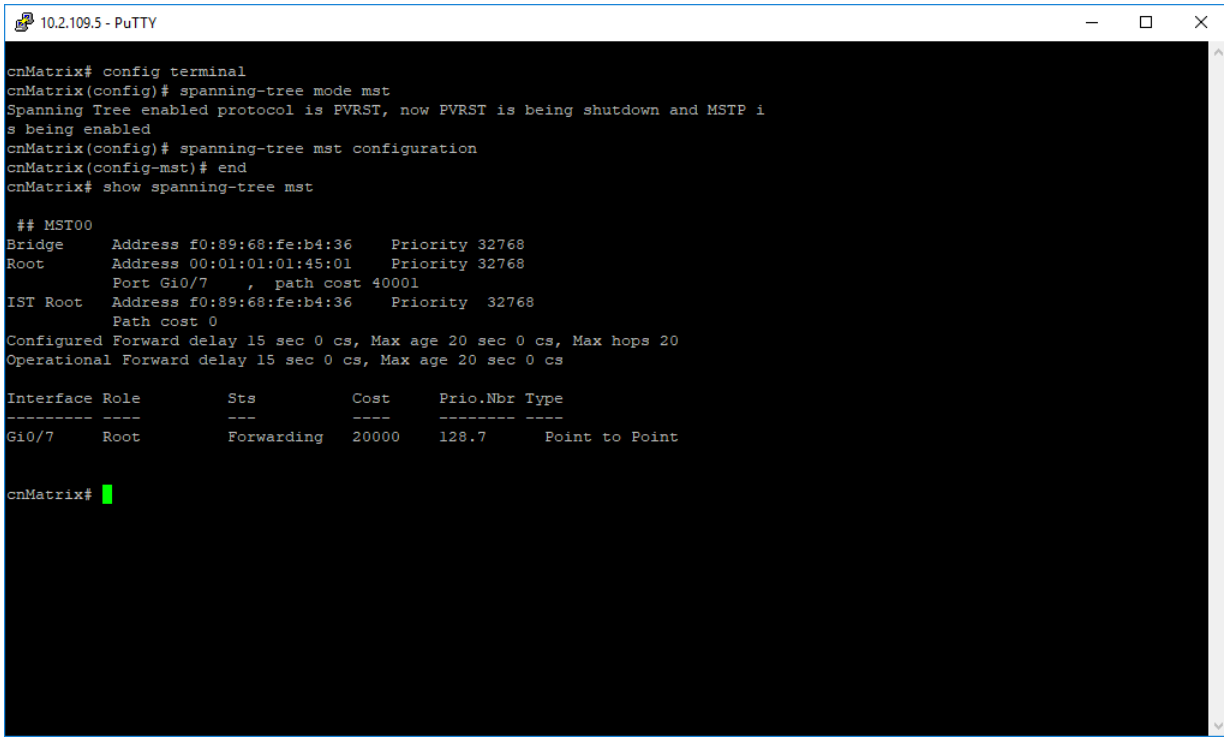
2.2.6.2 Network Diagram



2.2.7 How to Enable MSTP in CLI Interface

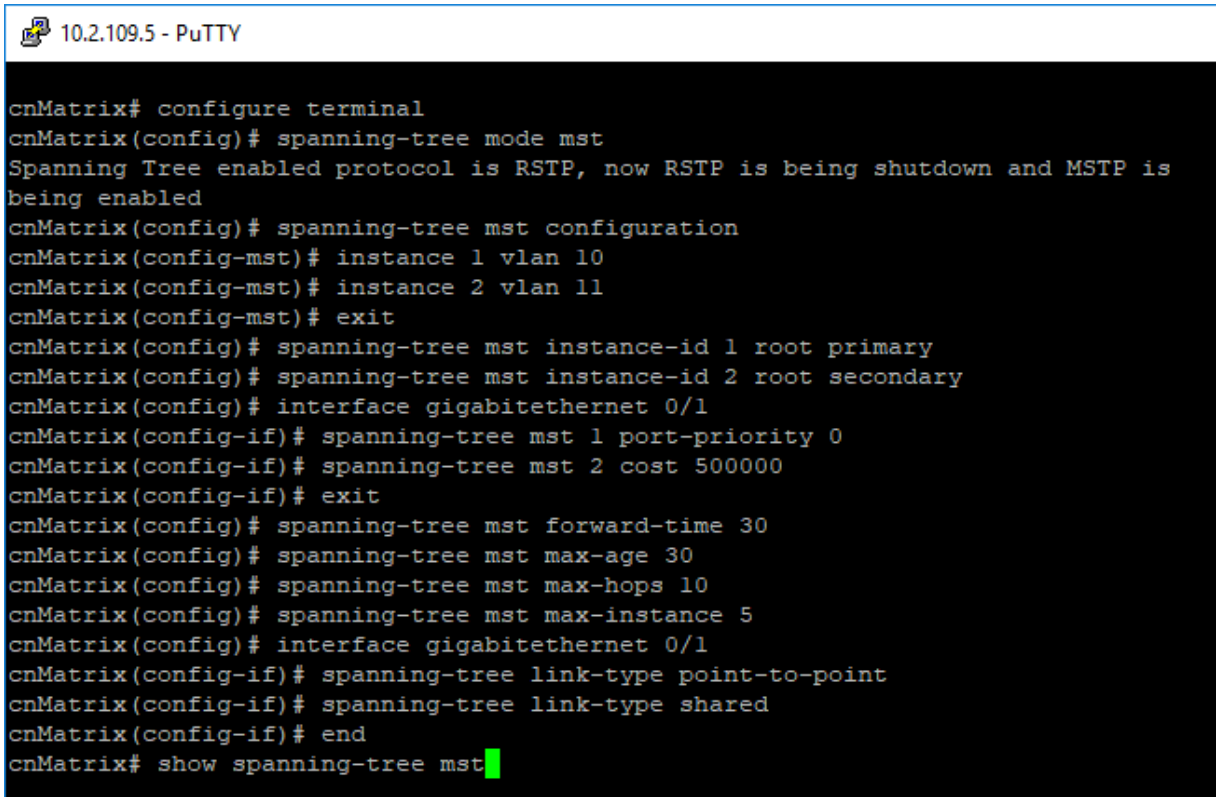


1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **spanning-tree mode mst** command into the terminal to set the spanning tree operating mode. Press the Enter key.
3. Type the **spanning-tree mst configuration** command into the terminal to enter MST configuration submode. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
5. Type the **show spanning-tree mst** command into the terminal to display the multiple spanning tree information. Press the Enter key.



For more information, see MSTP Parameters and Commands.

2.2.8 Configuring MSTP in CLI Interface(Example)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **spanning-tree mode mst** command into the terminal to enable the MSTP feature. Press the Enter key.
3. Type the **spanning-tree mst configuration** command into the terminal to enter the MSTP mode. Press the Enter key.

4. Type the **instance 1 vlan 10** command into the terminal to assign VLAN 10 in instance 1. Press the Enter key.

5. Type the **instance 2 vlan 11** command into the terminal to assign VLAN 11 in instance 2. Press the Enter key.

6. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key

7. Type the **spanning-tree mst instance-id 1 root primary** command into the terminal to configure the root switch for instance 1. Press the Enter key.

8. Type the **spanning-tree mst instance-id 2 root secondary** command into the terminal to configure a secondary root switch for instance 2. Press the Enter key.

9. Type the **interface gigabitethernet 0/1** command into the terminal. Press the Enter key.

10. Enter **spanning-tree mst 1 port-priority 0** into the field to configure port priority for instance 1. Press the Enter key.

11. Type the **spanning-tree mst 2 cost 500000** command into the field to configure the cost value associated with the port . Press the Enter key.

12. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key

13. Type the **spanning-tree mst forward-time 30** command into the terminal to configure the forwarding-delay time. Press the Enter key.

14. Type the **spanning-tree mst max-age 30** command into the terminal to configure the max age time. Press the Enter key.

15. Type the **spanning-tree mst max-hops 10** command into the terminal to configure the maximum-hop count. Press the Enter key.

16. Type the **spanning-tree mst max-instance 5** command into the terminal to configure the maximum instance. Press the Enter key.

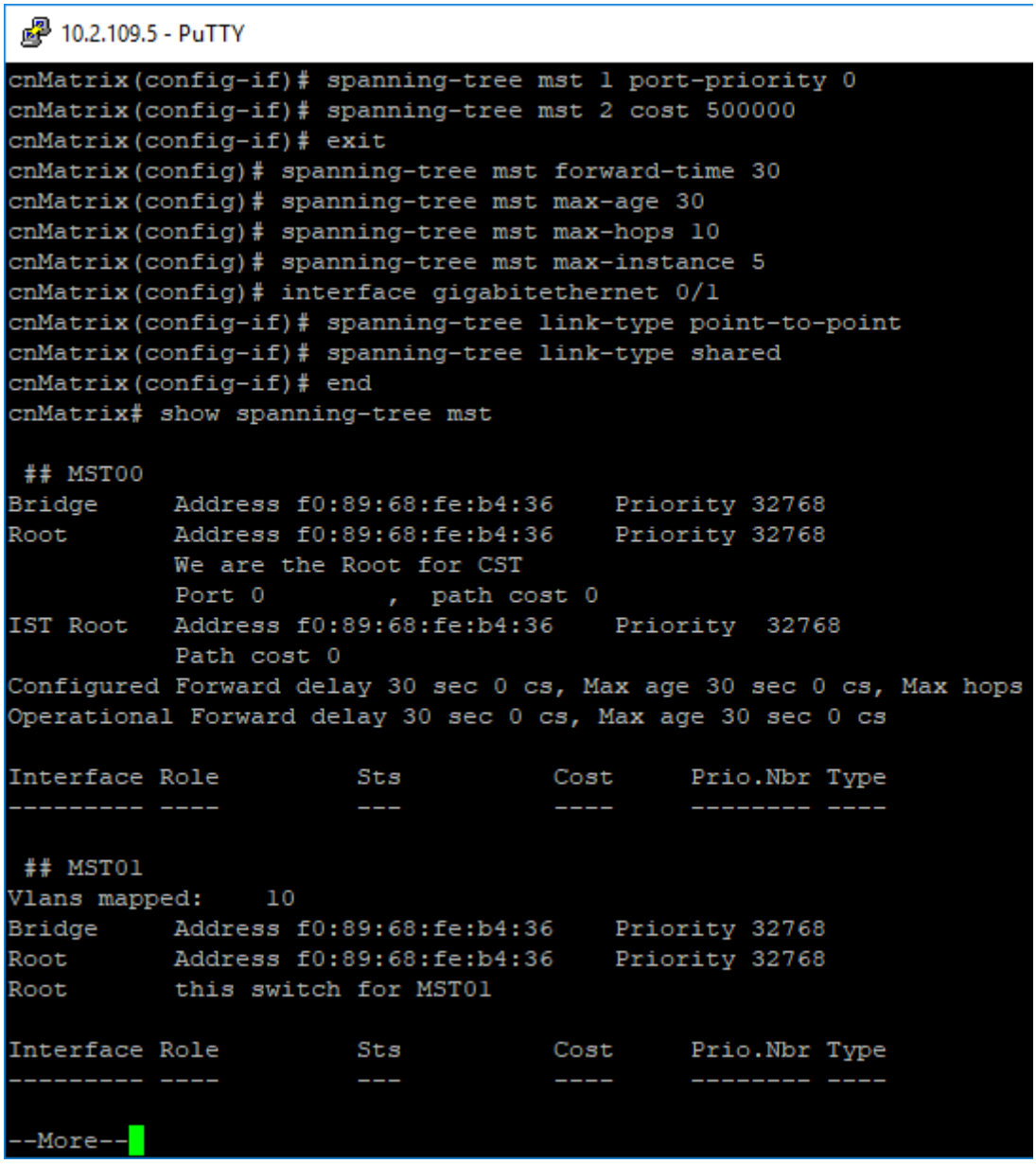
17. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.

18. Type the **spanning-tree link-type point-to-point** command into the terminal to specify the link type to ensure rapid transitions. Press the Enter key.

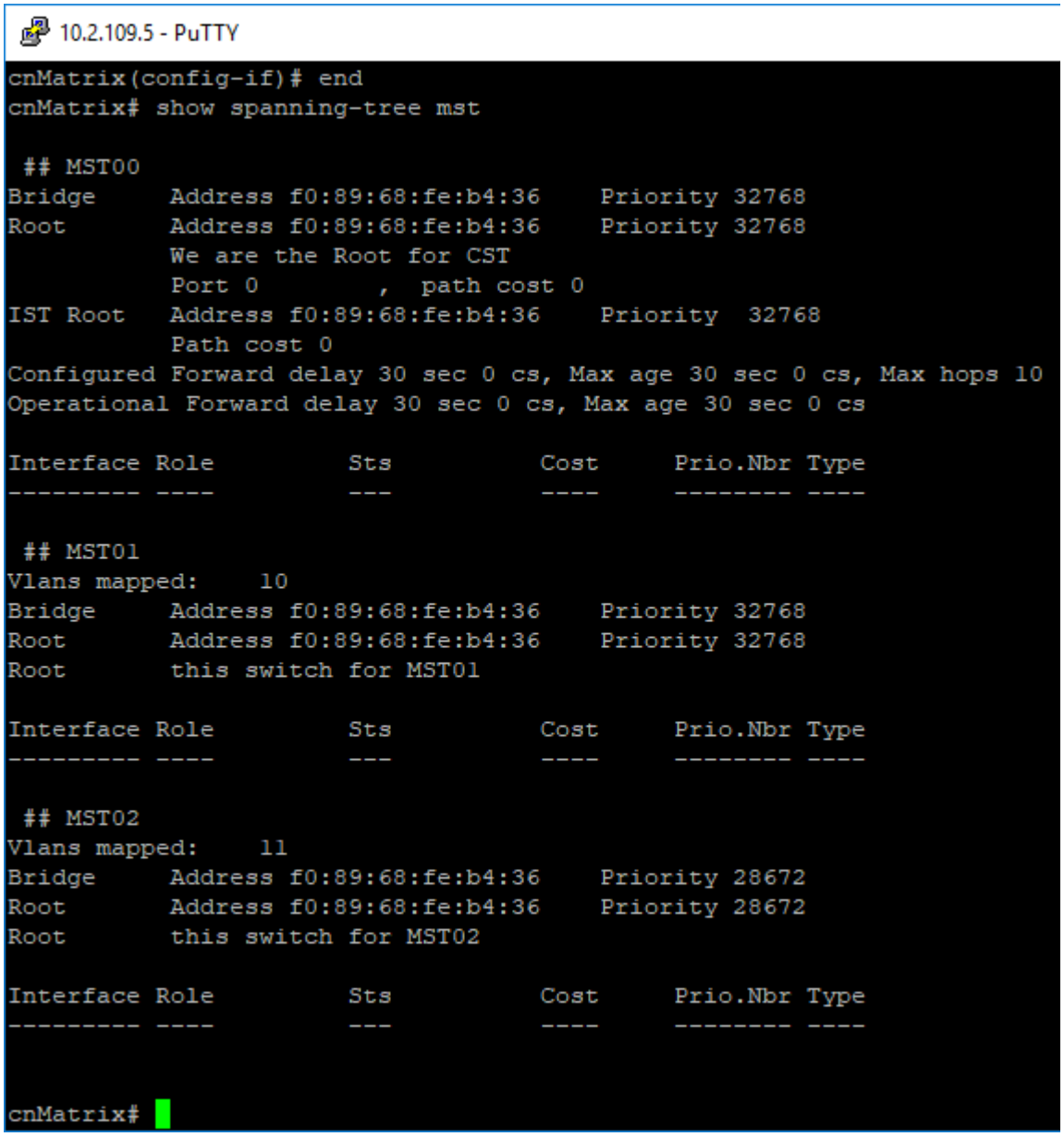
19. Type the **spanning-tree link-type shared** command into the terminal to specify the link type (does not ensure rapid transitions). Press the Enter key.

20. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

21. Type the **show spanning-tree mst** command into the terminal. Press the Enter key.



22 Press the Space key.



For more information, see MSTP Parameters and Commands.

2.2.9 Troubleshooting MSTP

Useful commands for troubleshooting:

```
cnMatrix#show spanning-tree mst

cnMatrix#show spanning-tree mst configuration

cnMatrix#show spanning-tree mst interface

cnMatrix#show spanning-tree mst detail
```

2.2.10 Managing PVRST

2.2.10.1 Feature Description

Feature Overview

The **PVRST** feature provides better control traffic in the network and enables the RSTP feature to work in conjunction with VLAN in order to provide better control traffic in the network.

Standards

- 802.1w

Scaling Numbers

- Up to 32 PVRST instances.

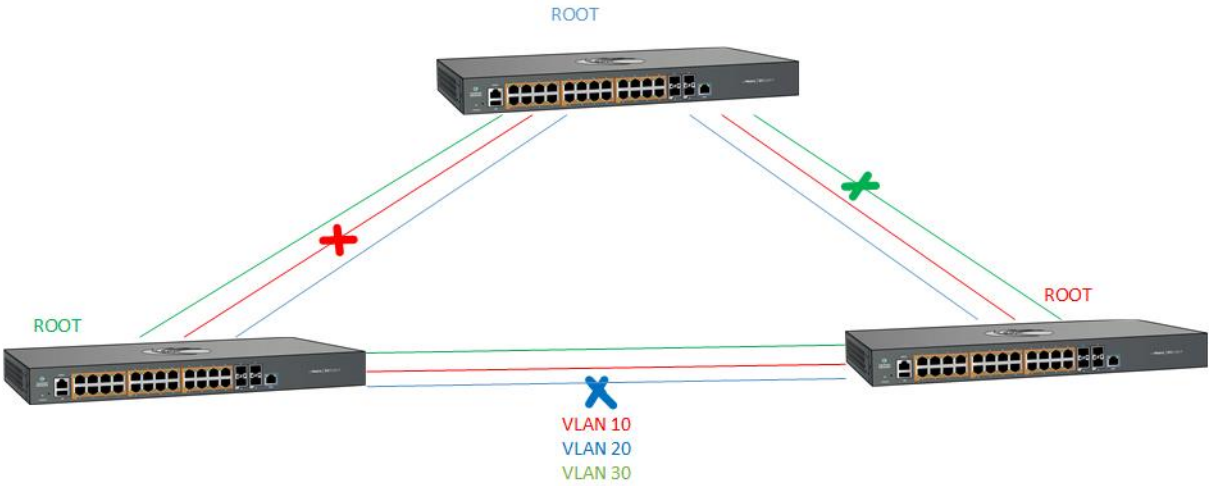
Default Values

- The default value for the forward time of the spanning tree: 15 seconds.
- The default value for the max-age timer of the spanning tree: 20 seconds.
- The default value for the revision number for the PVRST region: 0.
- The PVRST instance 0 is created and mapped with all VLANs.
- The default spanning tree hello time: 2 seconds.

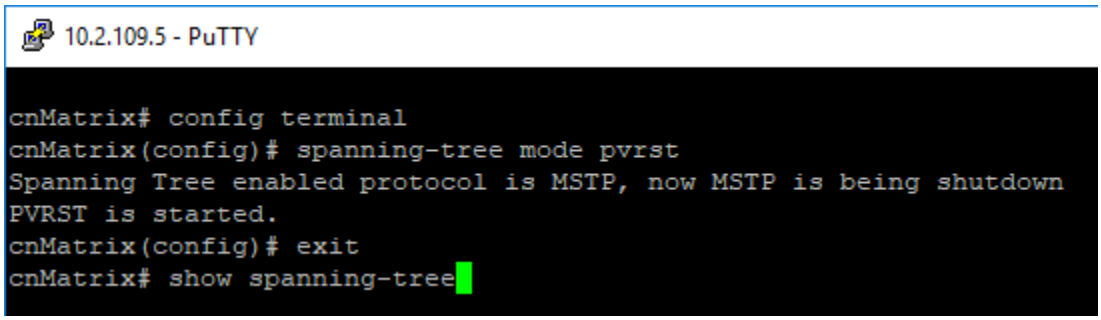
Prerequisites

- To enable the PVRST Functionality, MSTP and RSTP should be disabled.

2.2.10.2 Network Diagram



2.2.11 How to Enable PVRST in CLI Interface

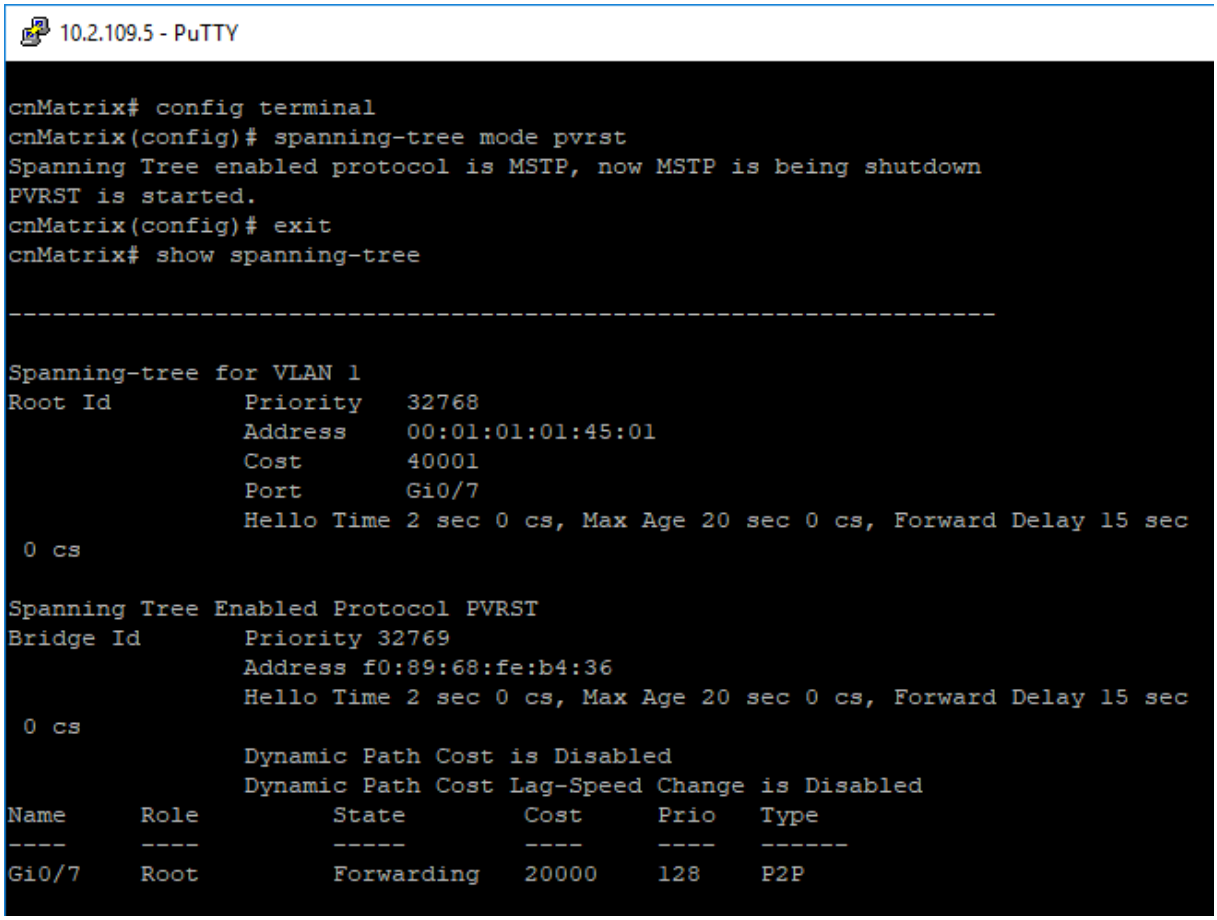


1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **spanning-tree mode pvrst** command into the terminal to set the spanning tree operating mode. Press the Enter key.

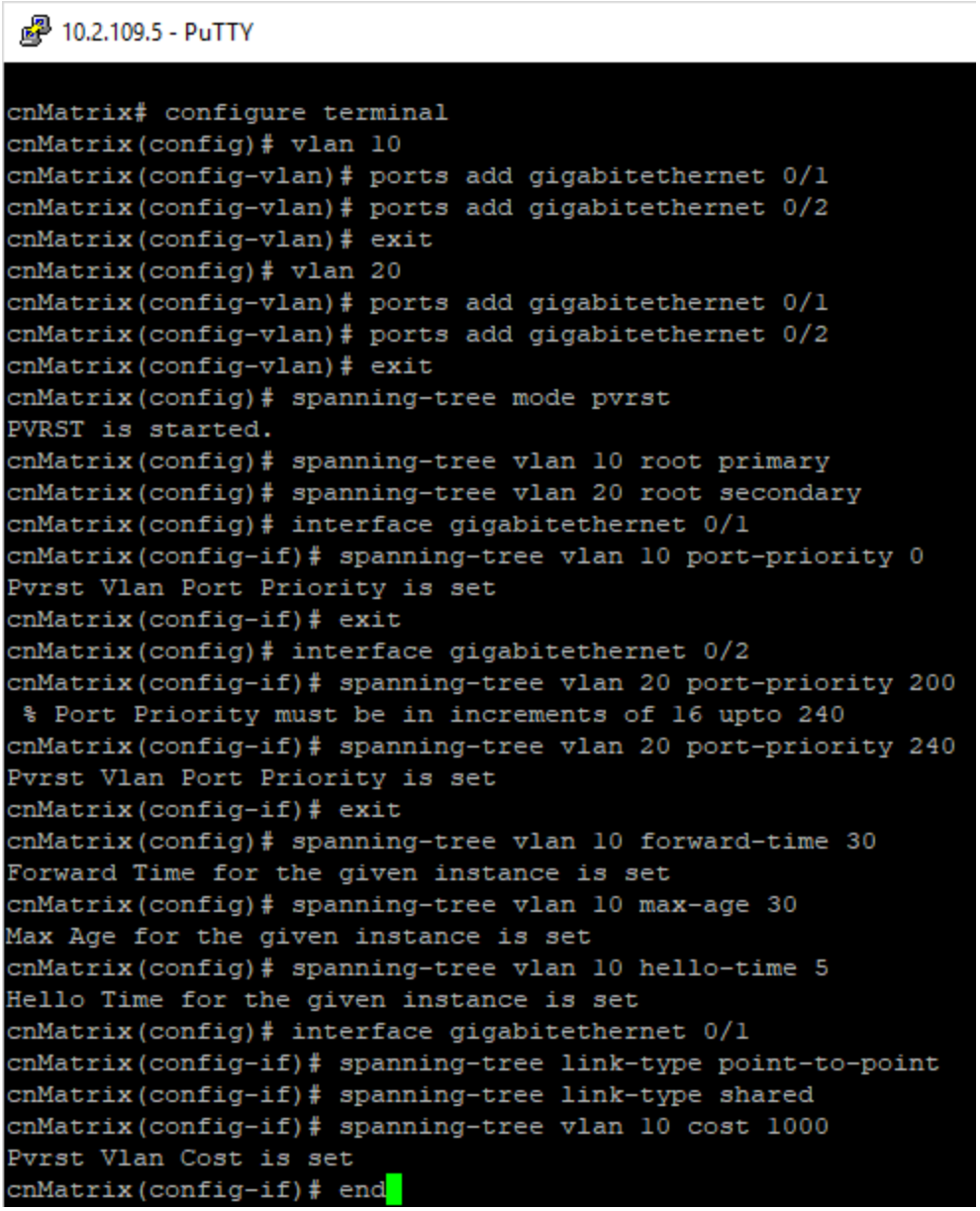
3 Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the key

4 Type the **show spanning-tree** command into the terminal to display the spanning tree information. Press the Enter key.



For more information, see PVRST Parameters and Commands.

2.2.12 Configuring PVRST in CLI Interface(Example)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **vlan 10** command into the terminal to configure VLAN 10. Press the Enter key.
3. Type the **ports add gigabitethernet 0/1** command into the terminal. Press the Enter key.
4. Type the **ports add gigabitethernet 0/2** command into the terminal. Press the Enter key.
5. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key
6. Type the **vlan 20** command into the terminal to create VLAN 20. Press the Enter key.
7. Type the **ports add gigabitethernet 0/1** command into the terminal. Press the Enter key.
8. Type the **ports add gigabitethernet 0/2** command into the terminal. Press the Enter key.
9. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key

10 Type the **spanning-tree mode pvrst** command into the terminal to enable PVRST. Press the Enter key.

11 Type the **spanning-tree vlan 10 root primary** command into the terminal to configure the root switch for VLAN 10. Press the Enter key.

12 Type the **spanning-tree vlan 20 root secondary** command into the terminal to configure a secondary root switch for VLAN 20. Press the Enter key.

13 Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured . Press the Enter key.

14 Type the **spanning-tree vlan 10 port-priority 0** command into the terminal to configure port priority for VLAN 10. Press the Enter key.

15 Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key

16 Type the **interface gigabitethernet 0/2** command into the terminal to select an interface to be configured. Press the Enter key.

17 Type the **spanning-tree vlan 20 port-priority 200** command into the terminal to configure port priority for VLAN 20. Press the Enter key.

⚡ An error message is displayed. Port priority value should be increments of 16 up to 240.

18 Type the **spanning-tree vlan 20 port-priority 240** command into the terminal. Press the Enter key.

19 Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key

20 Type the **spanning-tree vlan 10 forward-time 30** command into the terminal to configure the forwarding-delay time . Press the Enter key.

21 Type the **spanning-tree vlan 10 max-age 30** into the terminal to configure the maximum age. Press the Enter key.

22 Type the **spanning-tree vlan 10 hello-time 5** command into the terminal to configure the hello time. Press the Enter key.

23 Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.

24 Type the **spanning-tree link-type point-to-point** command into the terminal to specify the link type, for a rapid transition. Press the Enter key.

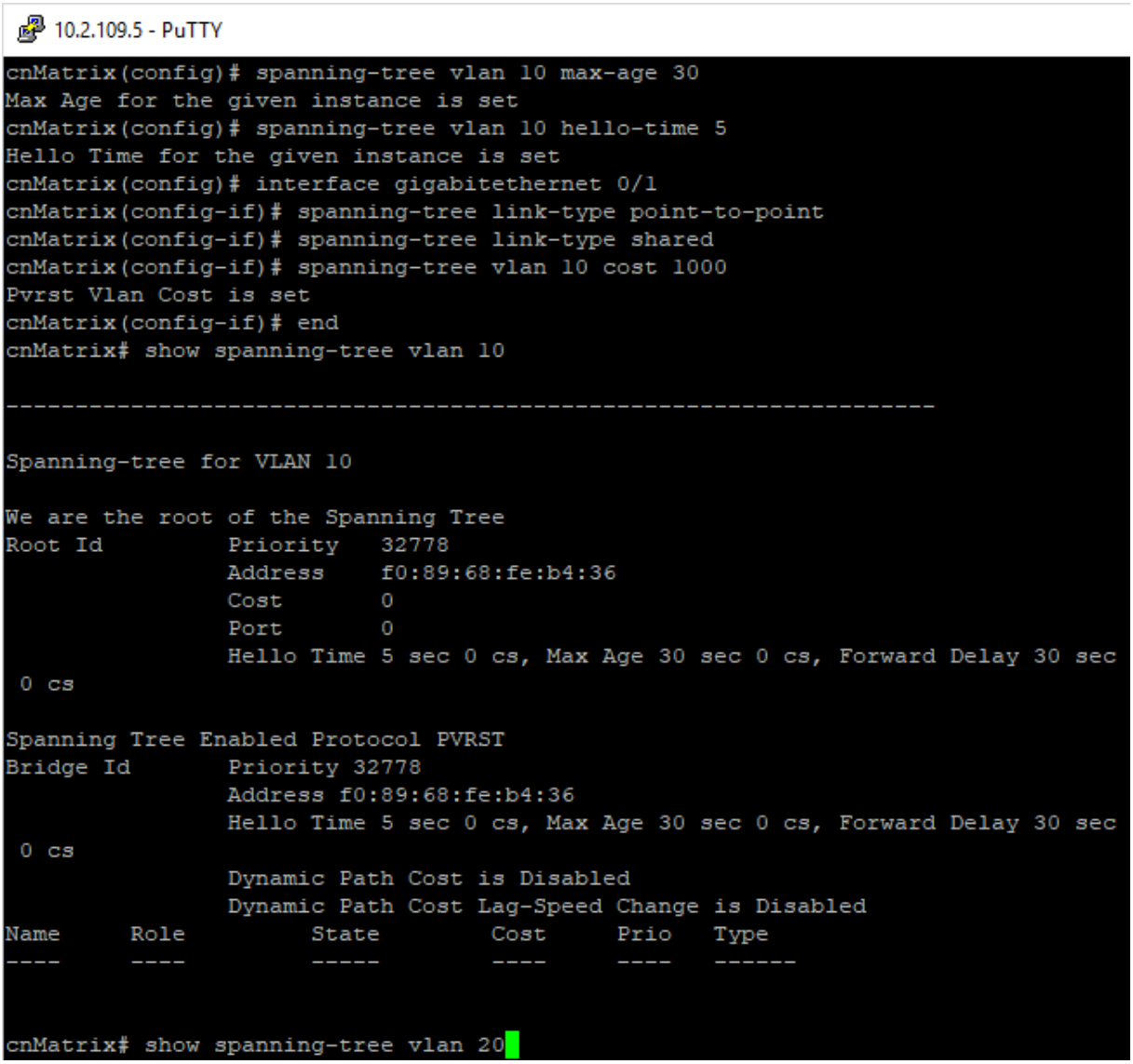
25 Type the **spanning-tree link-type shared** command into the terminal. Press the Enter key.

26 Type the **spanning-tree vlan 10 cost 1000** command into the terminal to specify the interface cost. Press the Enter key.

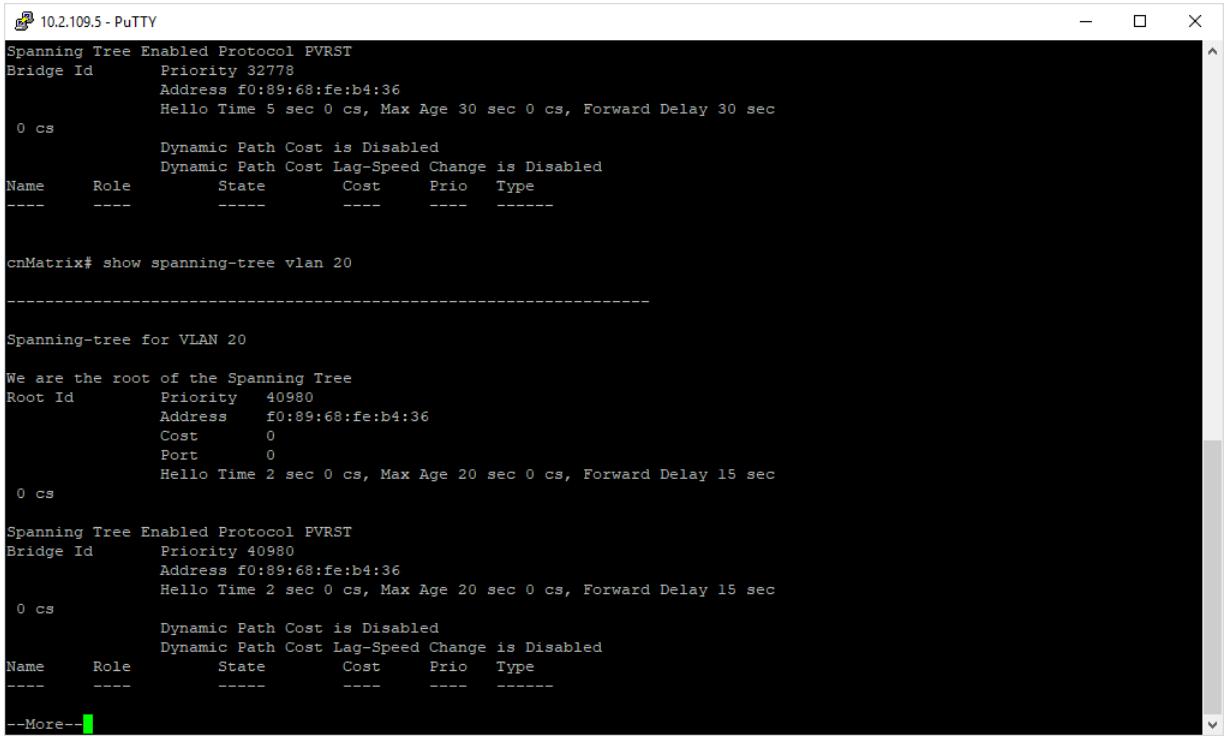
27 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

28 Type the **show spanning-tree vlan 10** command into the terminal to display the PVRST configurations and status. Press the Enter key.

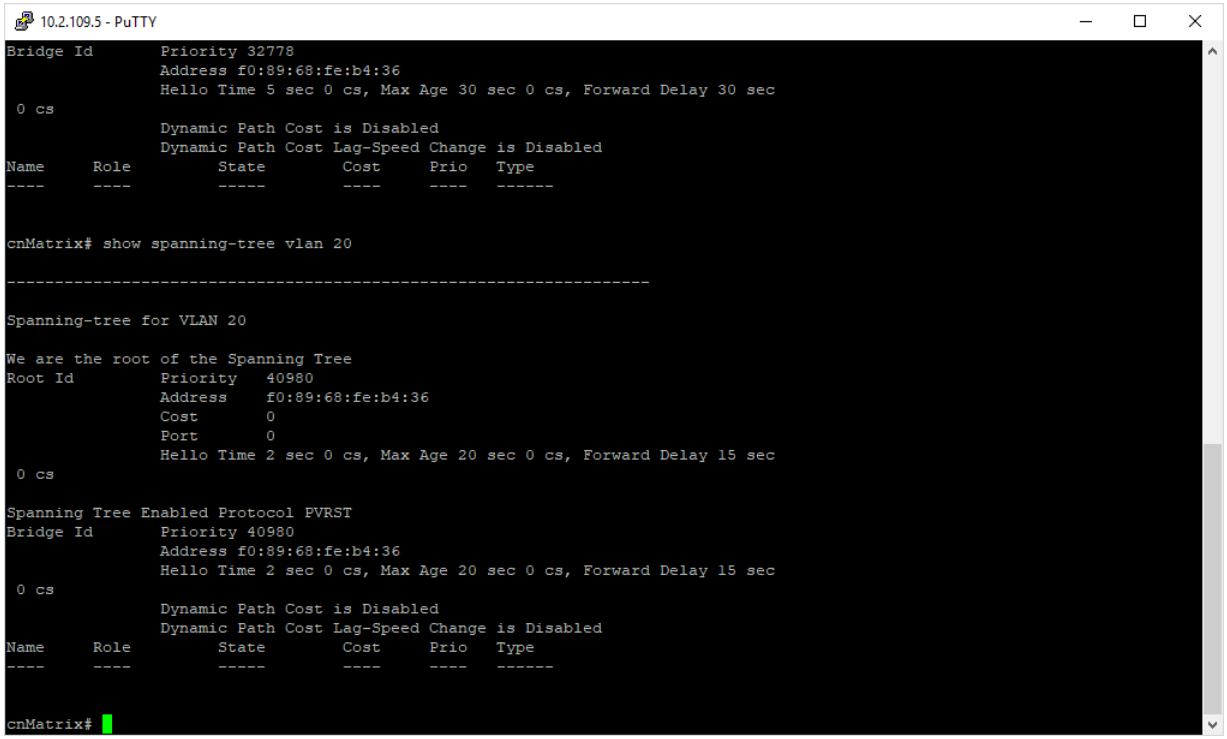
29 Press the Space key.



30 Type the **show spanning-tree vlan 20** command into the terminal to display the PVRST configurations and status. Press the Enter key.



31 Press the Space key.



For more information, see PVRST Parameters and Commands.

2.2.13 Troubleshooting PVRST

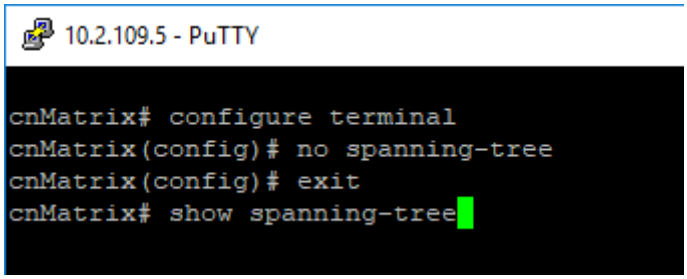
Useful commands for troubleshooting:

```
cnMatrix#show spanning-tree vlan
```

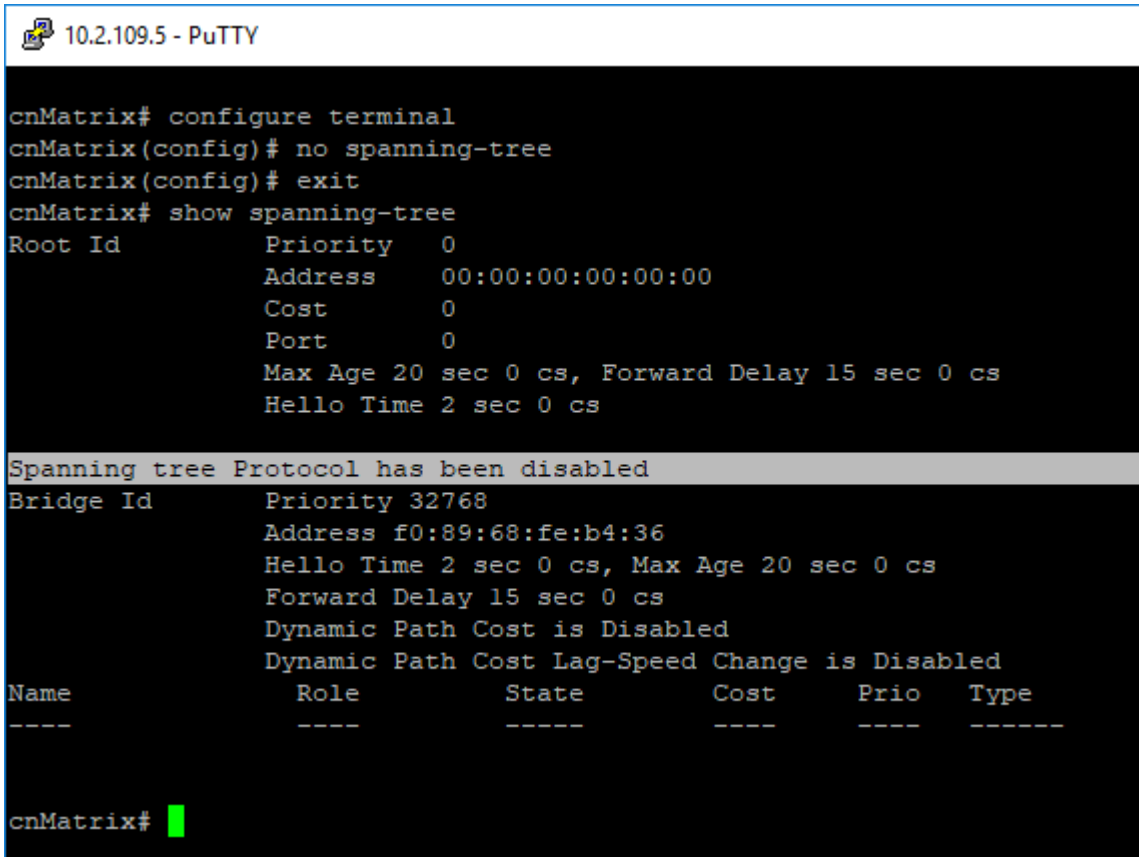
2.2.14 How to Enable/Disable Spanning Tree

2.2.14.1 How to Disable Spanning Tree Globally

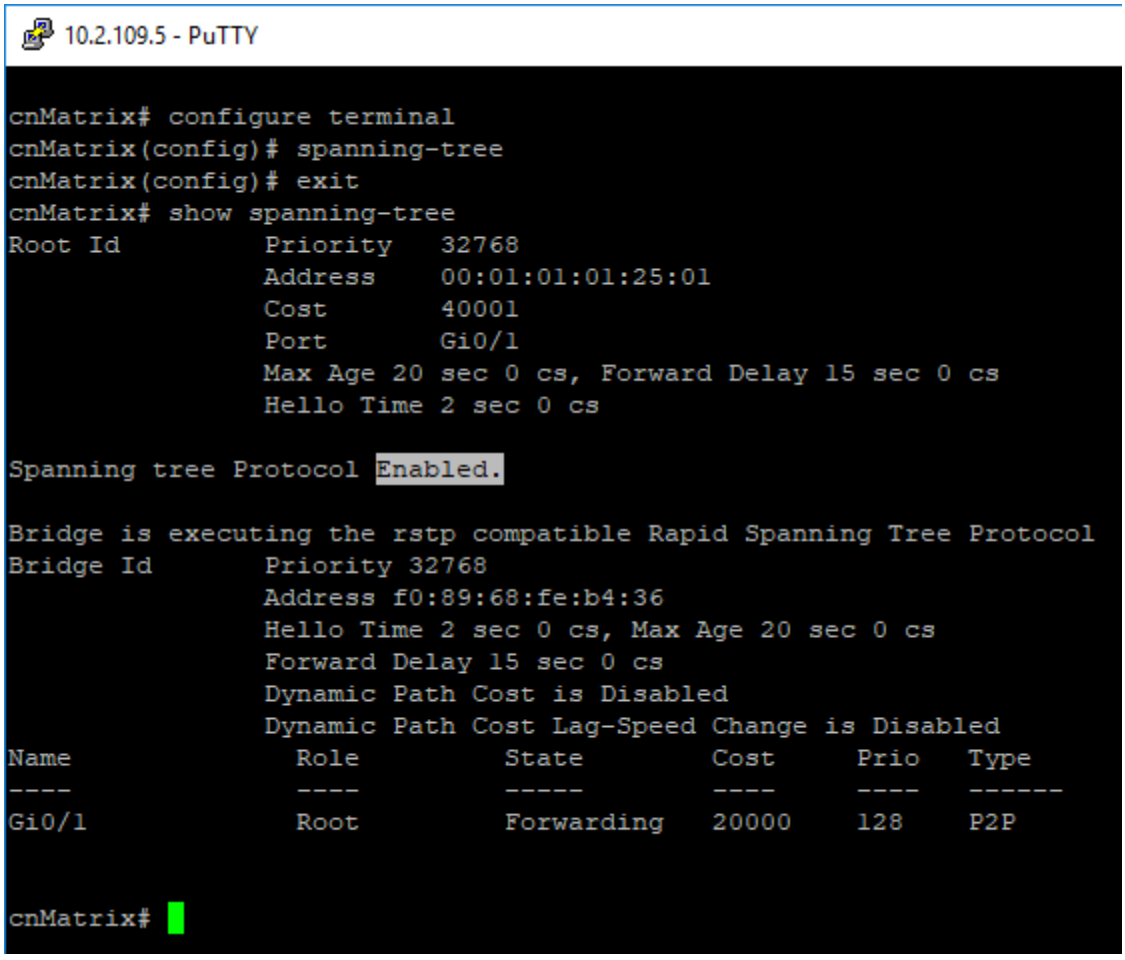
Note: Spanning Tree is enabled by default.



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **no spanning-tree** command into the terminal to disable Spanning Tree globally. Press the Enter key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
4. Type the **show spanning-tree** command into the terminal to display spanning-tree information . Press the Enter key.



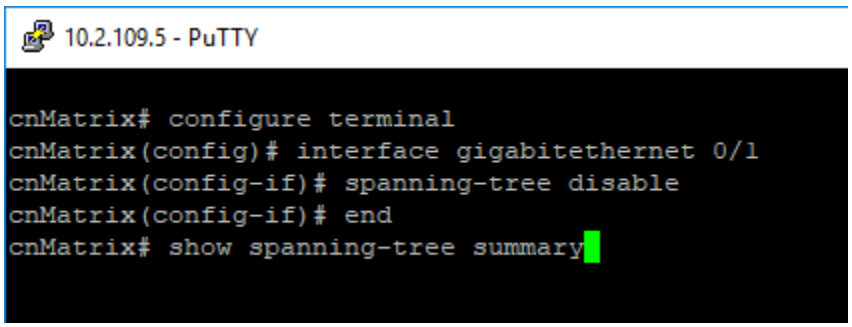
2.2.14.2 How to Enable Spanning Tree Globally



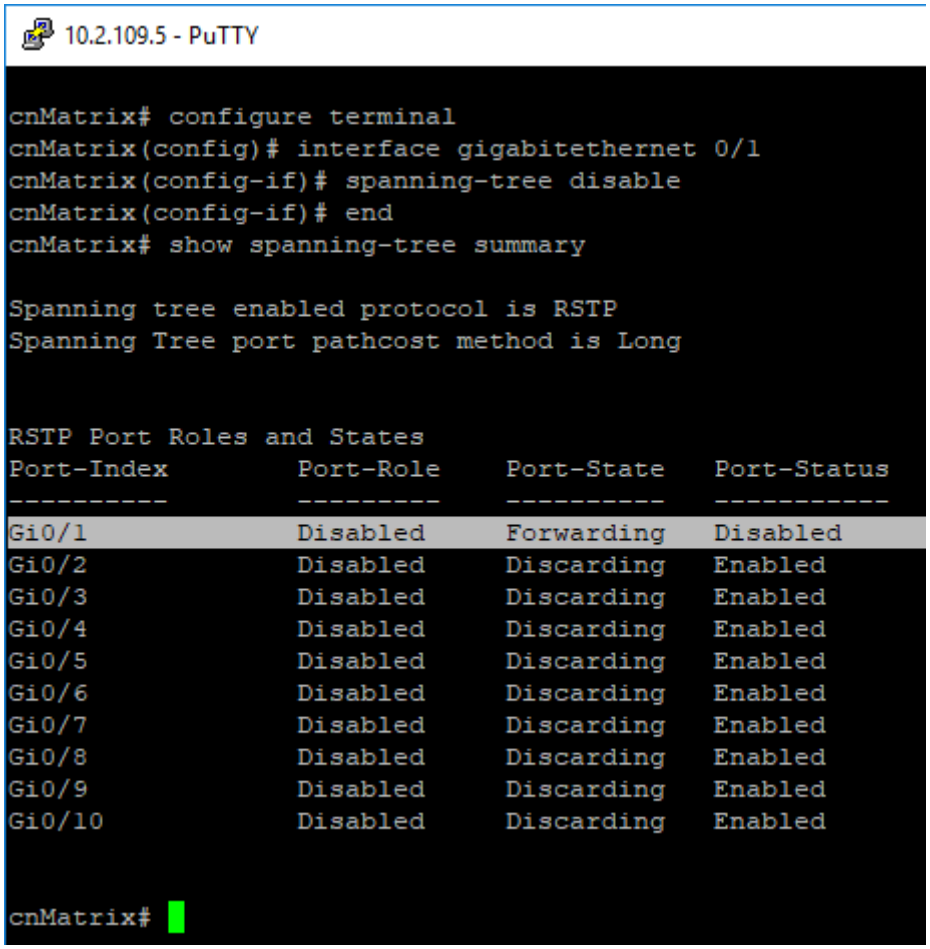
1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **spanning-tree** command into the terminal to enable Spanning Tree globally . Press the Enter key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
4. Type the **show spanning-tree** command into the terminal to display the spanning tree interface information. Press the Enter key.

2.2.14.3 How to Disable Spanning Tree per Interface

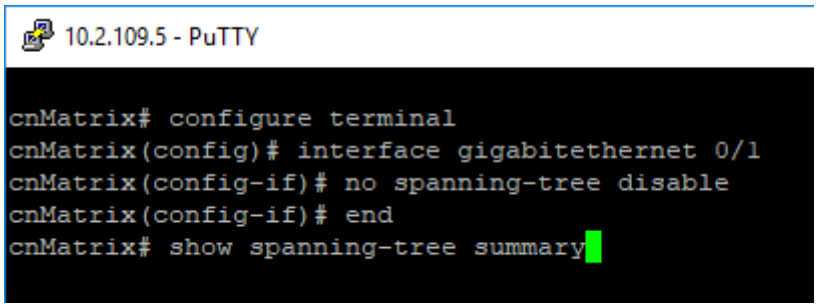
> Note: Spanning Tree is enabled by default per interface.



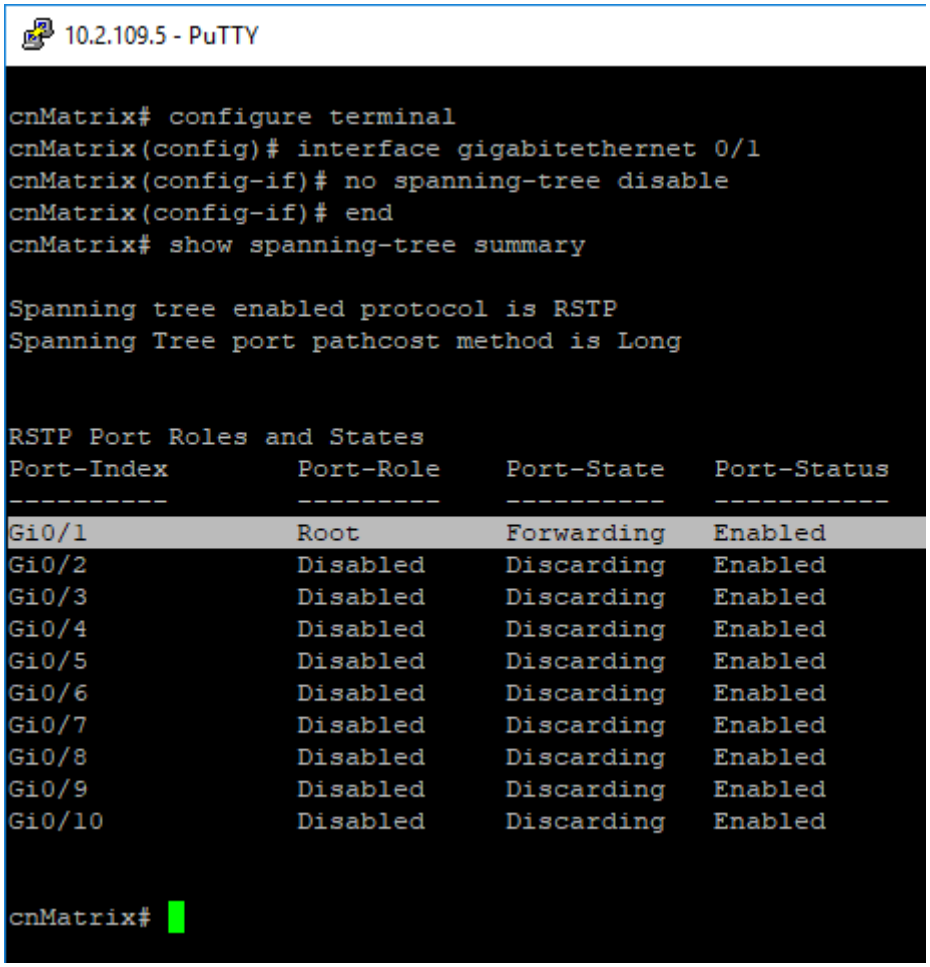
1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal. Press the Enter key.
3. Type the **spanning-tree disable** command into the terminal. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
5. Type the **show spanning-tree summary** command into the terminal to display the spanning tree interface information. Press the Enter key.



2.2.14.4 How to Enable Spanning Tree per Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal. Press the Enter key.
3. Type the **no spanning-tree disable** command into the terminal. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
5. Type the **show spanning-tree summary** command into the terminal. Press the Enter key.



You can check/display the administrative and operational status for STP with the following terminals:

- show spanning-tree
- show spanning-tree summary
- show spanning-tree detail

2.3 LLDP

2.3.1 Managing LLDP

Feature Overview

The LLDP feature enables you to discover the neighbor devices. LLDP (Link Layer Discovery Protocol) is a link-layer protocol used by devices to advertise their identity and capabilities to their neighbors on a LAN.

Standards

- The protocol is standardized as IEEE 802.1ab and IEEE 802.3-2012 section 6 clause 79.

Scaling Numbers

- A maximum number of 256 neighbors are supported in this release.

Limitations

- LLDP-MED is not supported in this release.

Default Values

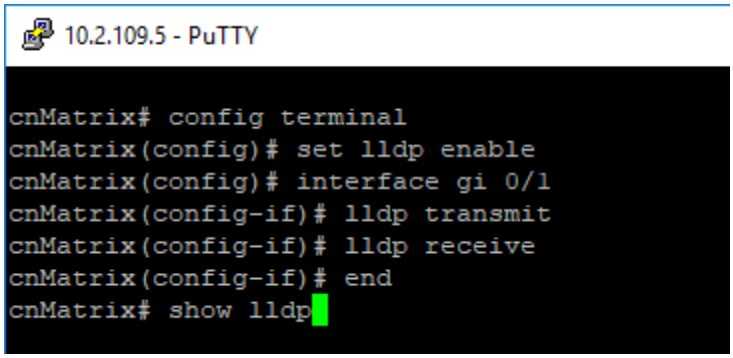
- The default transmission interval: 30 seconds.

- The default value for holdtime-multiplier: 4.
- The default value for reinitialization delay time: 2.
- Transmission / reception of LLDPU are enabled by default.
- The default LLDP version is v2.
- Port description, system name, system description and system capabilities TLVs are enabled on all ports.

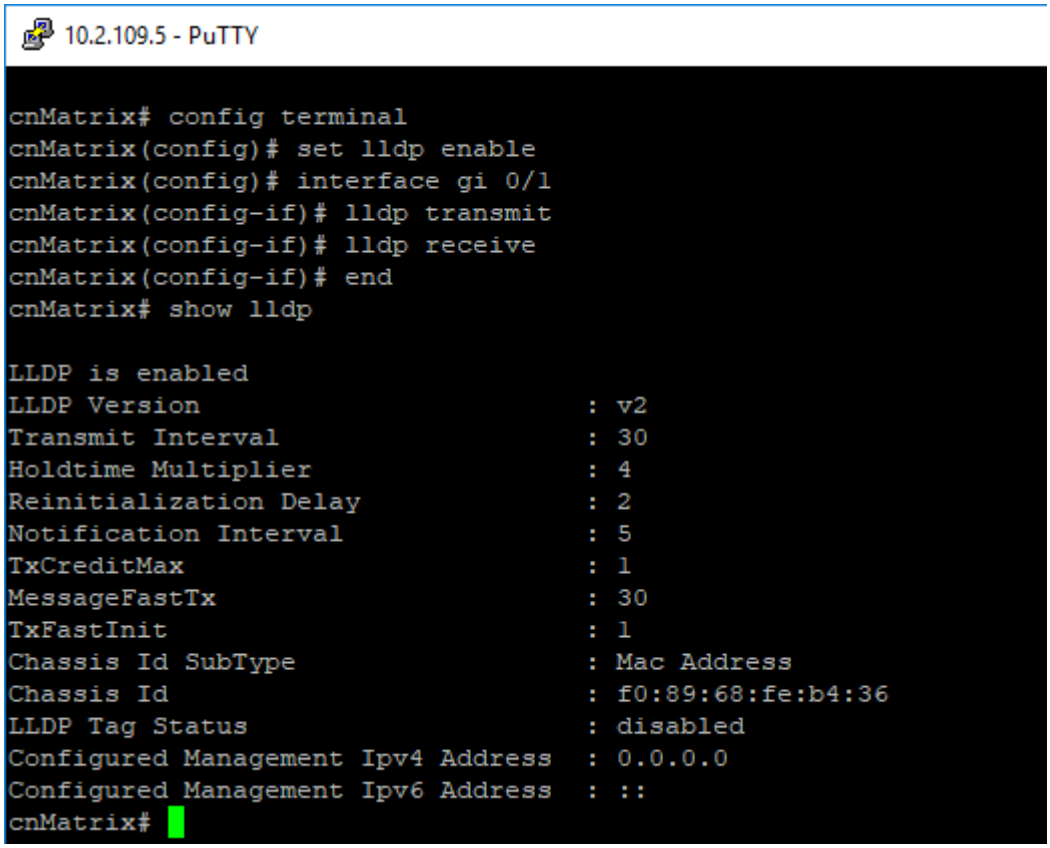
Prerequisites

- For the basic functionality, no user configuration is necessary. The reception and transmission of LLDPDUs are enabled by default on all ports.

2.3.2 How to Enable LLDP in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **set lldp enable** command into the terminal to enable LLDP in the system. Press the Enter key.
3. Type the **interface gi 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
4. Type the **lldp transmit** command into the terminal to set the admin status on an interface as transmit. Press the Enter key.
5. Type the **lldp receive** command into the terminal to set the admin status on an interface as receive. Press the Enter key.
6. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
7. Type the **show lldp** command into the terminal. Press the Enter key.



For the basic functionality, **no user configuration is necessary**.

For more information, see LLDP Parameters and Commands.

2.3.3 Managing LLDP-MED (Starting with version 2.1)

2.3.3.1 Feature Overview

Feature Overview

Starting with version 2.1, the **Media Endpoint Discovery** extension has been added to the LLDP protocol, which provides the following facilities:

- Discovery of network policies – allows the network administrator to set automatically-discoverable policies for phones, video streaming and video conferencing devices. A policy consists of a VLAN ID, a DSCP code point and a dot1p priority for the end device to use.
- Location discovery – support for Emergency Location Identification Number (ELIN).
- Extended Power-over-Ethernet management.
- Inventory management – for a better tracking of deployed network devices.

Standards

- ANSI/TIA-1057 - Telecommunications IP Telephony Infrastructure Link Layer Discovery Protocol for Media Endpoint Devices.

Scaling Numbers

- A maximum number of 256 neighbors are supported.

Limitations

- For the location TLV, only the “ELIN Location” subtype is supported.

Default Values

- By default, all ports send only MED Capability TLV.

Prerequisites

- To send and receive LLDP MED TLVs, the TX/RX of LLDPDUs must be enabled on the port.

2.3.3.2 Network Diagram

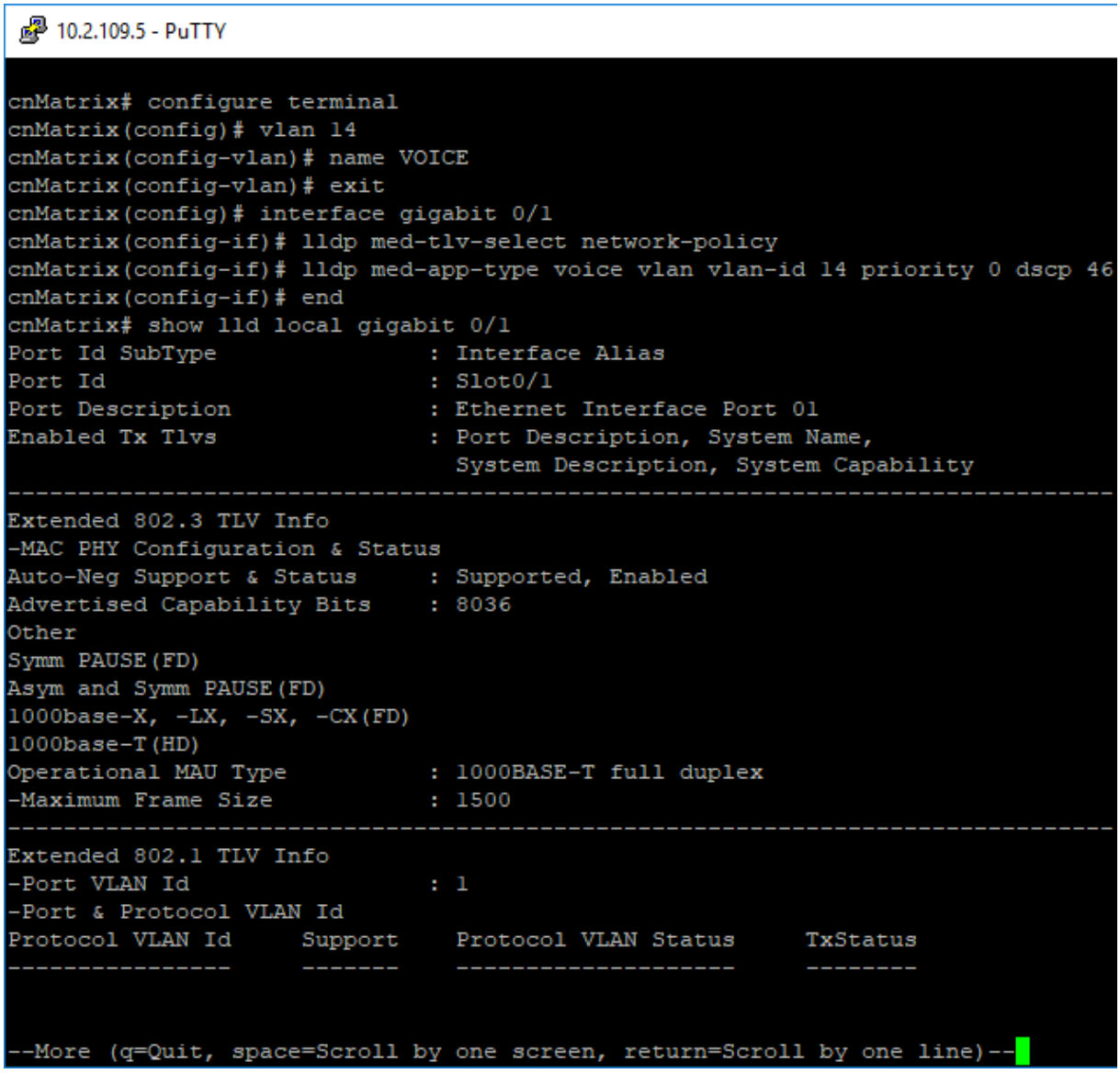
2.3.4 How to Configure Network Policy (Starting with version 2.1)

```
10.2.109.5 - PuTTY

cnMatrix# configure terminal
cnMatrix(config)# vlan 14
cnMatrix(config-vlan)# name VOICE
cnMatrix(config-vlan)# exit
cnMatrix(config)# interface gigabit 0/1
cnMatrix(config-if)# lldp med-tlv-select network-policy
cnMatrix(config-if)# lldp med-app-type voice vlan vlan-id 14 priority 0 dscp 46
cnMatrix(config-if)# end
cnMatrix# show lld local gigabit 0/1
```

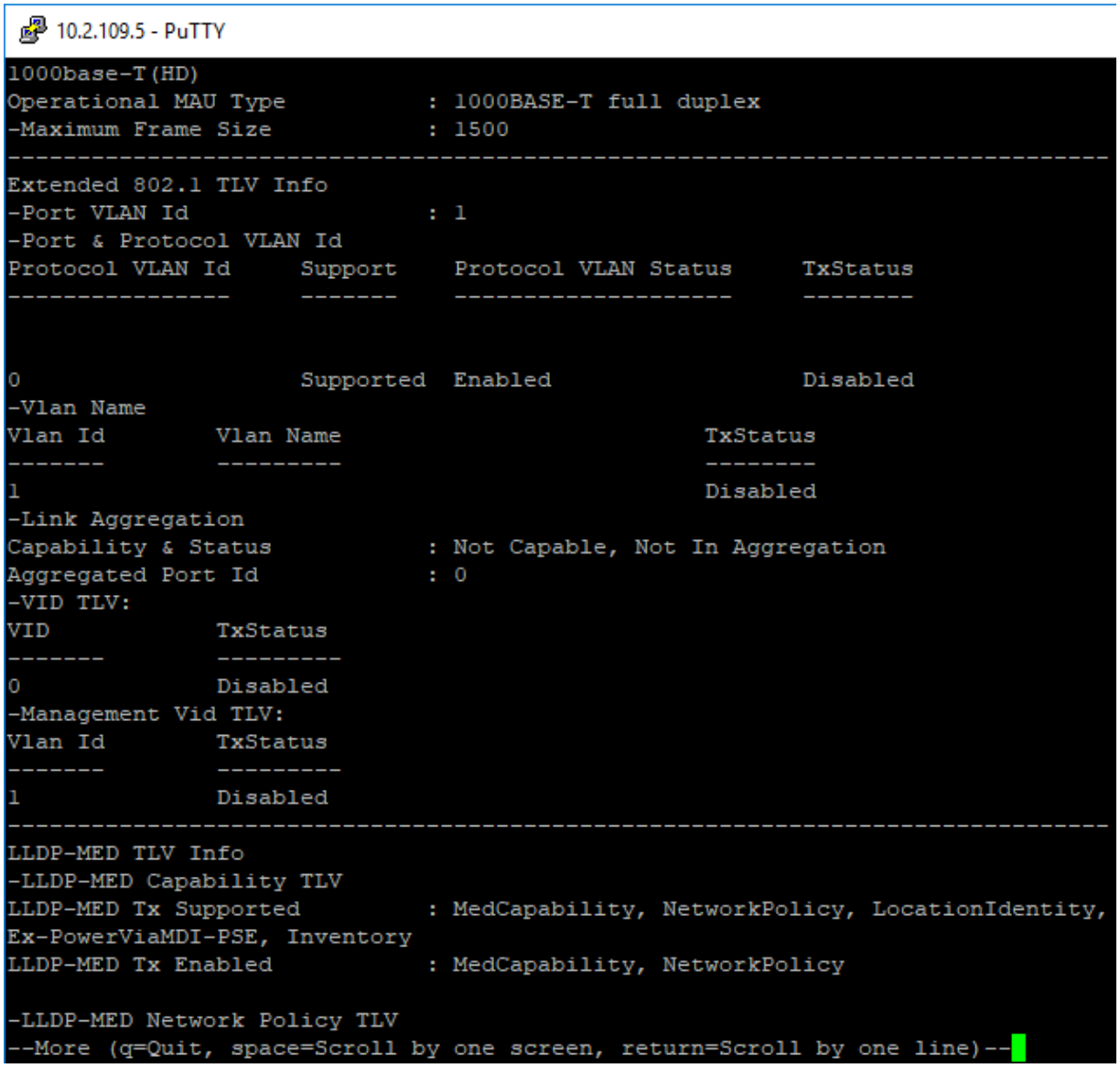
1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **vlan 14** command into the terminal to configure a VLAN. Press the Enter key.
3. Type the **name VOICE** command into the terminal to configure a name for the VLAN. Press the Enter key.
4. Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key.
5. Type the **interface gigabit 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
6. Type the **lldp med-tlv-select network-policy** command into the terminal to enable LLDP-MED TLV transmission on a given switch port. Press the Enter key.
7. Type the **lldp med-app-type voice vlan vlan-id 14 priority 0 dscp 46** command into the terminal to set the Network-policy TLV as Voice Application, configure the priority value for the selected VLAN and to set the DSCP value. Press the Enter key.

8 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

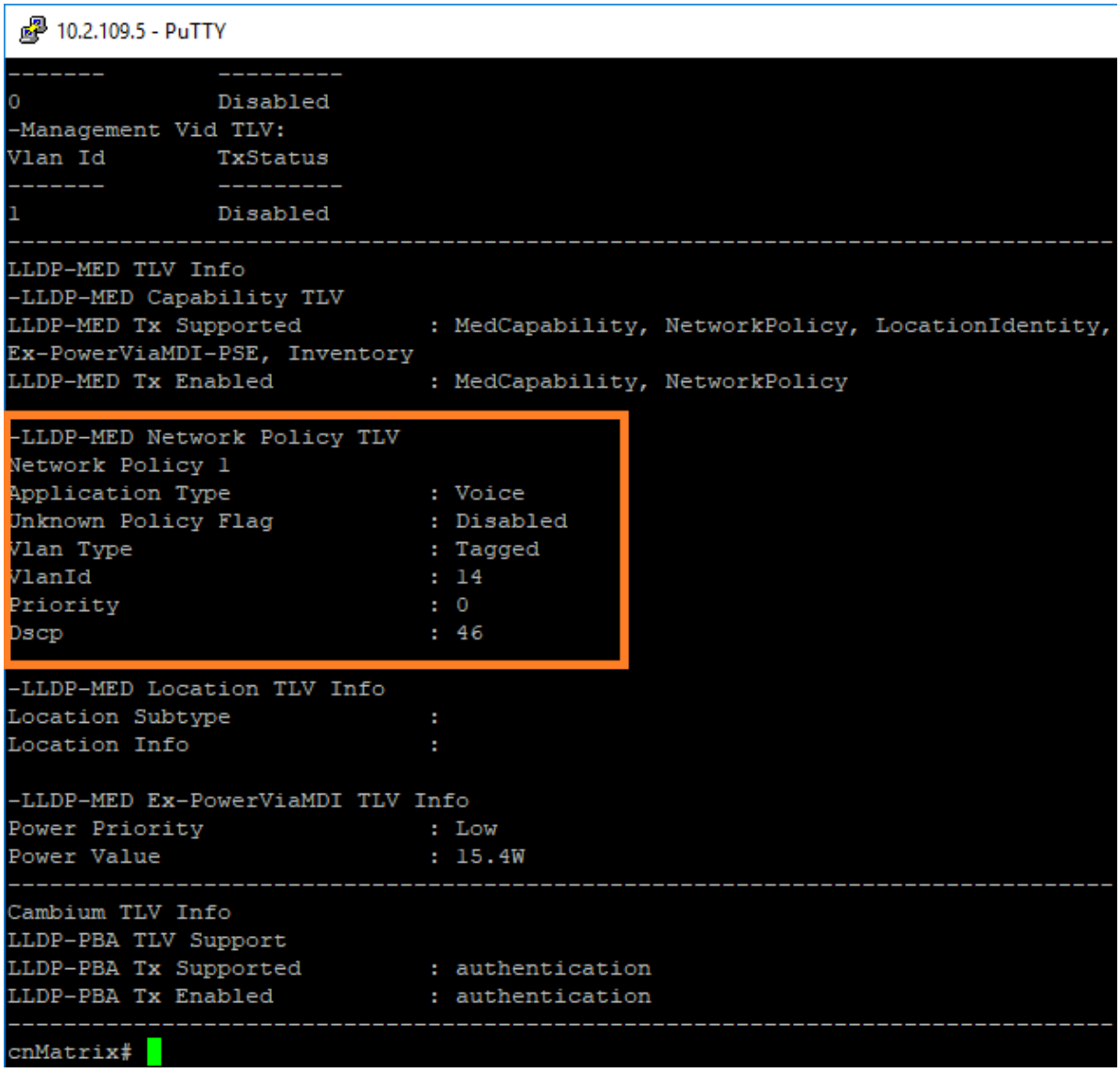
9 Type the **show lld local gigabit 0/1** command into the terminal to display the current switch information that will be used to populate outbound LLDP advertisements for a specific interface (verify if the above configurations were applied). Press the Enter key.



10 Press the Space key.

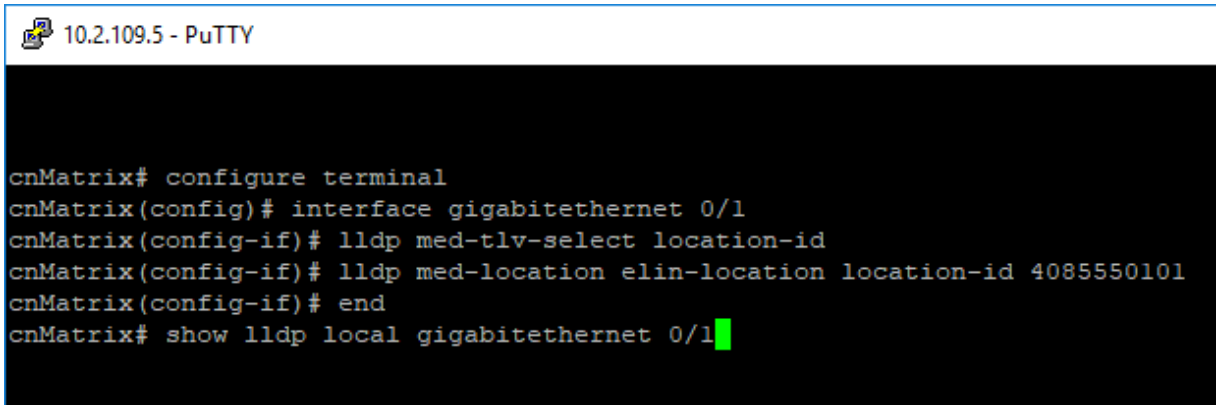


11 Press the Space key.



For more information, see LLDP-MED Parameters and Commands.

2.3.5 How to Enable Location ID (Starting with version 2.1)

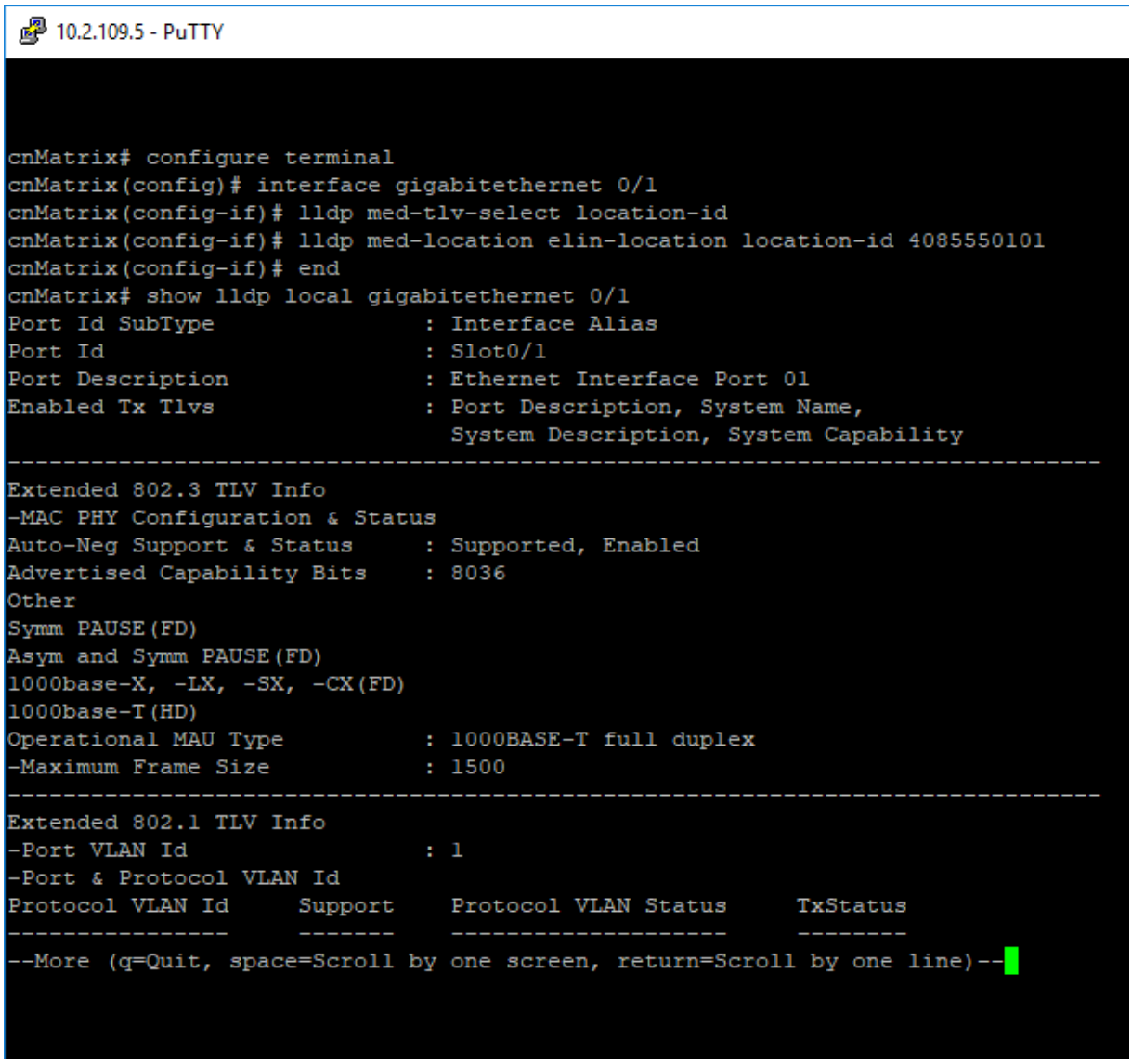


1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **lldp med-tlv-select location-id** command into the terminal to select LLDP-MED TLV and Location Identification TLV related configuration. Press the Enter key.

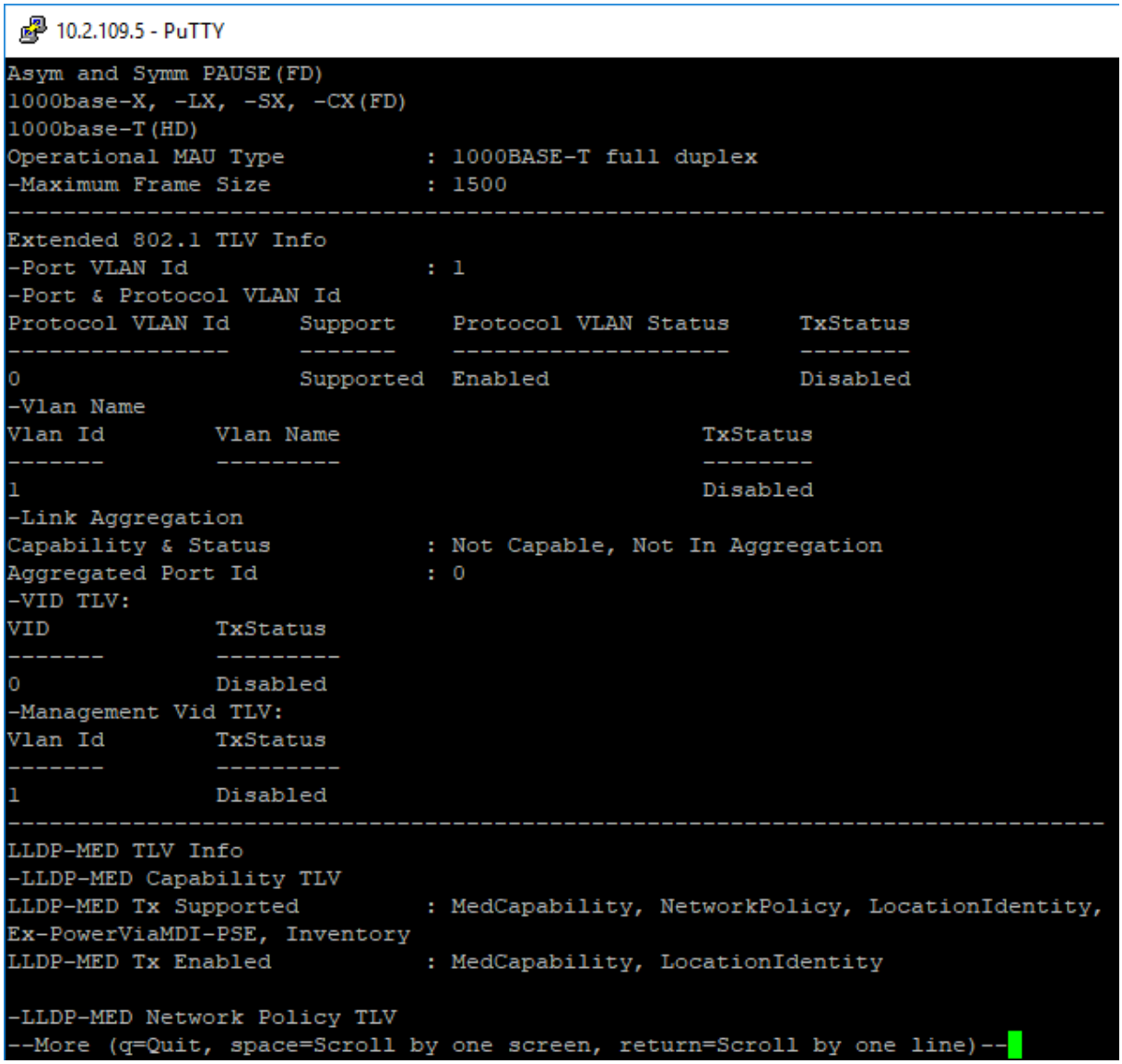
4. Type the **lldp med-location elin-location location-id 4085550101** command into the terminal to configure the Emergency Location Information Number (ELIN) location subtype information advertised by the endpoint. Press the Enter key.

5. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

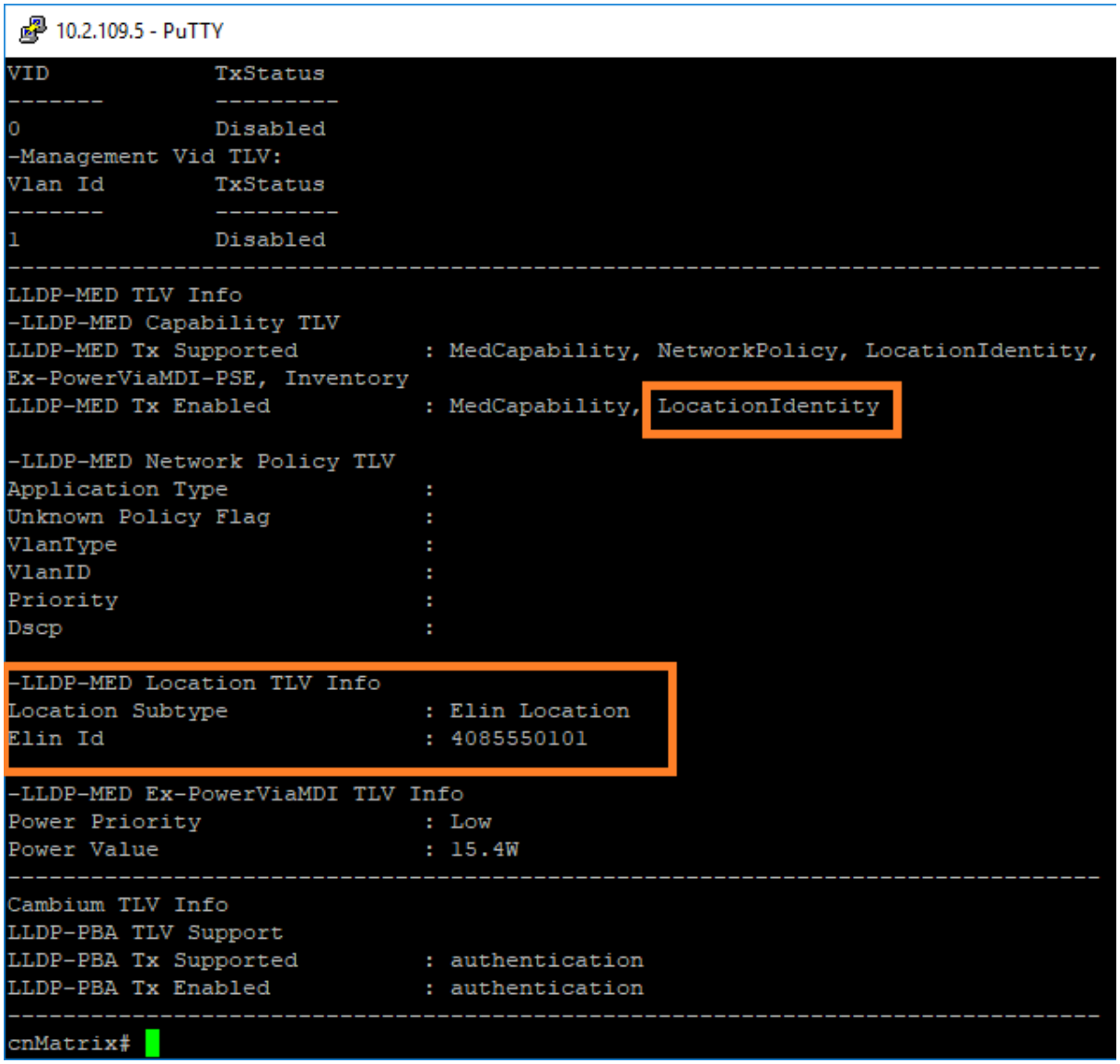
6. Type the **show lldp local gigabitethernet 0/1** command into the terminal to display the current switch information that will be used to populate outbound LLDP advertisements for a specific interface (verify if the above configurations were applied). Press the Enter key.



7. Press the Space key.

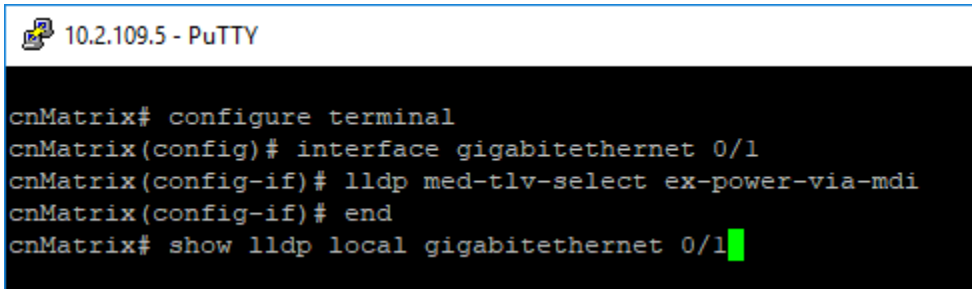


8 Press the Space key.



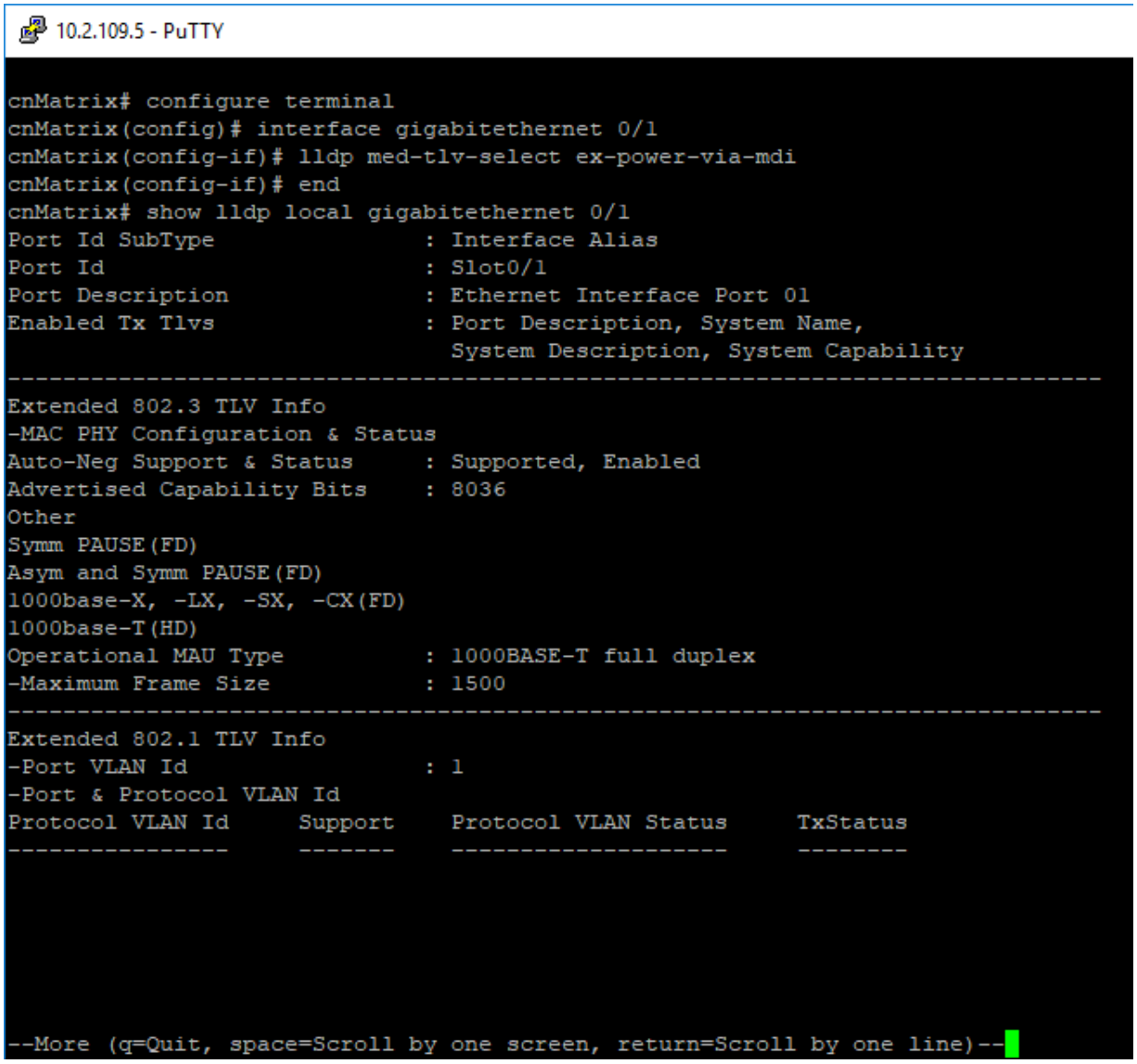
For more information, see LLDP-MED Parameters and Commands.

2.3.6 How to Enable Extended Power via MDI

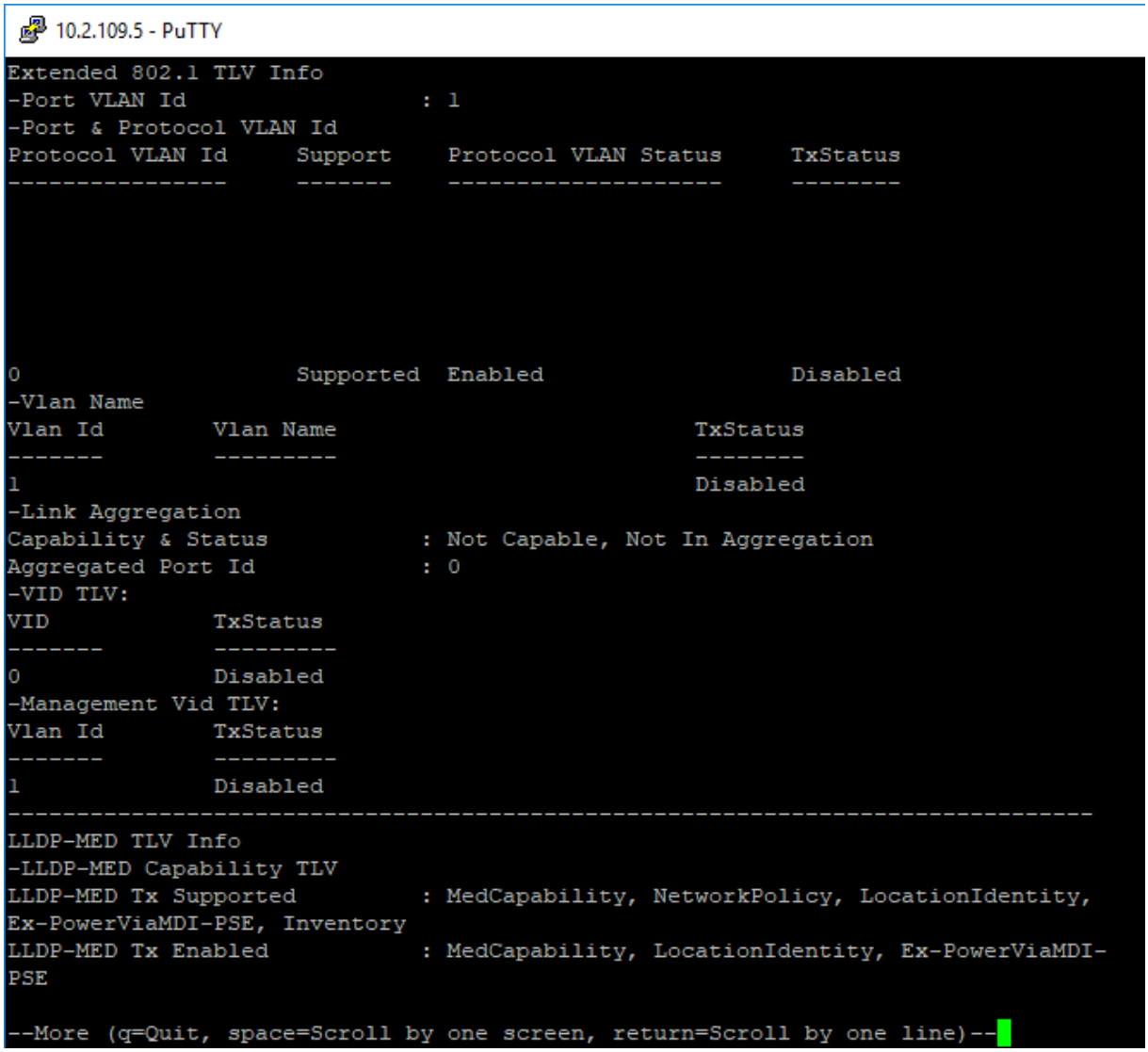


1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **lldp med-tlv-select ex-power-via-mdi** command into the terminal to configure the Extended power via MDI TLV related transmission for the LLDP module. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

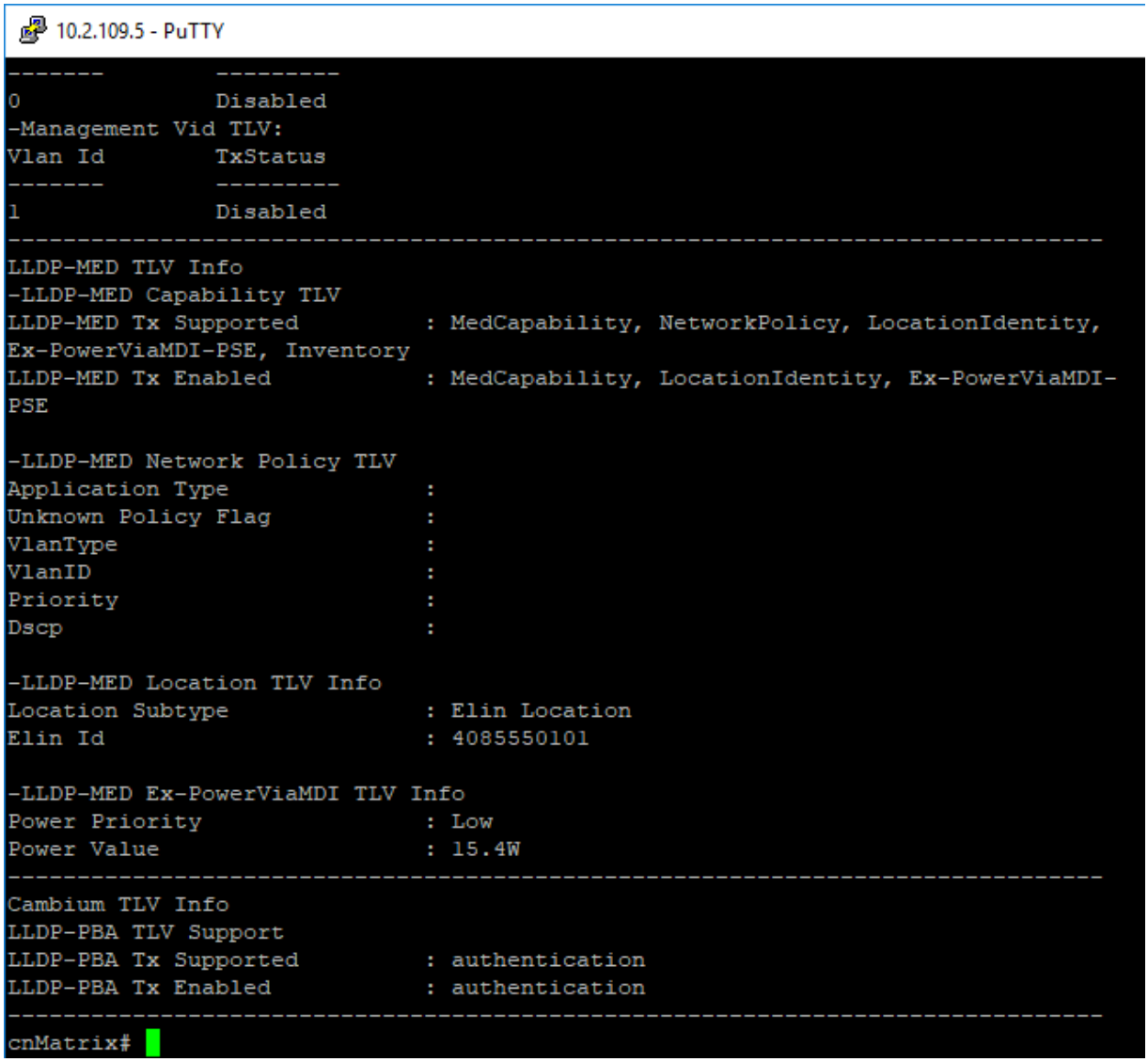
5 Type the **show lldp local gigabitethernet 0/1** command into the terminal to display the current switch information that will be used to populate outbound LLDP advertisements for a specific interface (verify if the above configurations were applied). Press the Enter key.



6 Press the Space key.



7 Press the Space key.



2.4 RMON

2.4.1 Managing RMON

The RMON feature defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes and enables various network monitors and console systems to exchange network-monitoring data.

Standards

- The RMON feature is documented in RFC 2819.

Scaling Numbers

- A maximum number of 50 RMON events can be created.
- A maximum number of 50 RMON alarms can be created.
- A maximum number of 74 history collection entries can be created.

Limitations

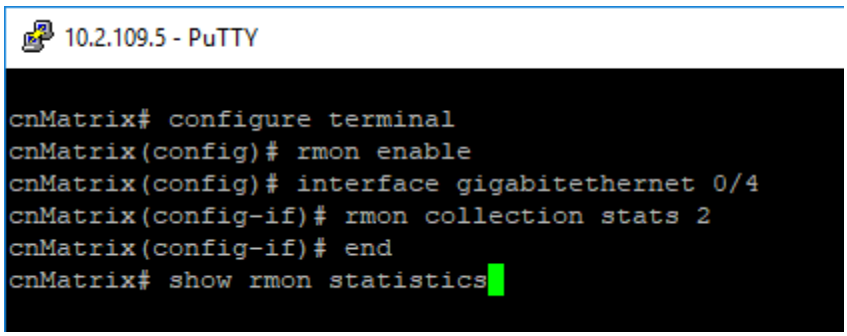
- User must configure an SNMP user and a notification receiver to use the SNMP notification events.
- The RMON alarm mib must be configured in its complete format, including final index. For example, 1.3.6.1.2.1.2.2.1.10.1 refers to ifInOctets for interface 1.

- RMON alarms can be configured only for MIB objects that resolve to an integer.

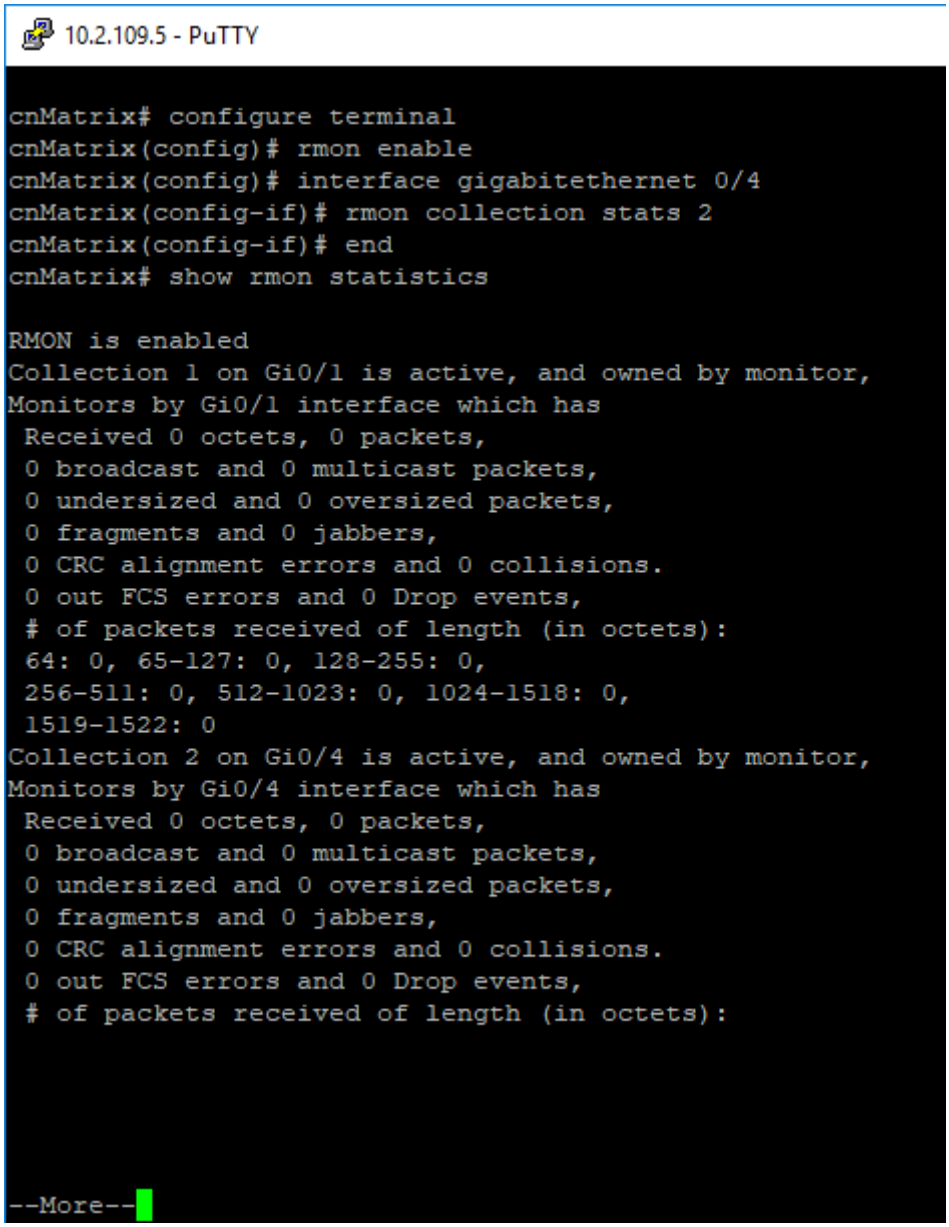
Default Values

- The RMON feature is disabled by default.
- By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

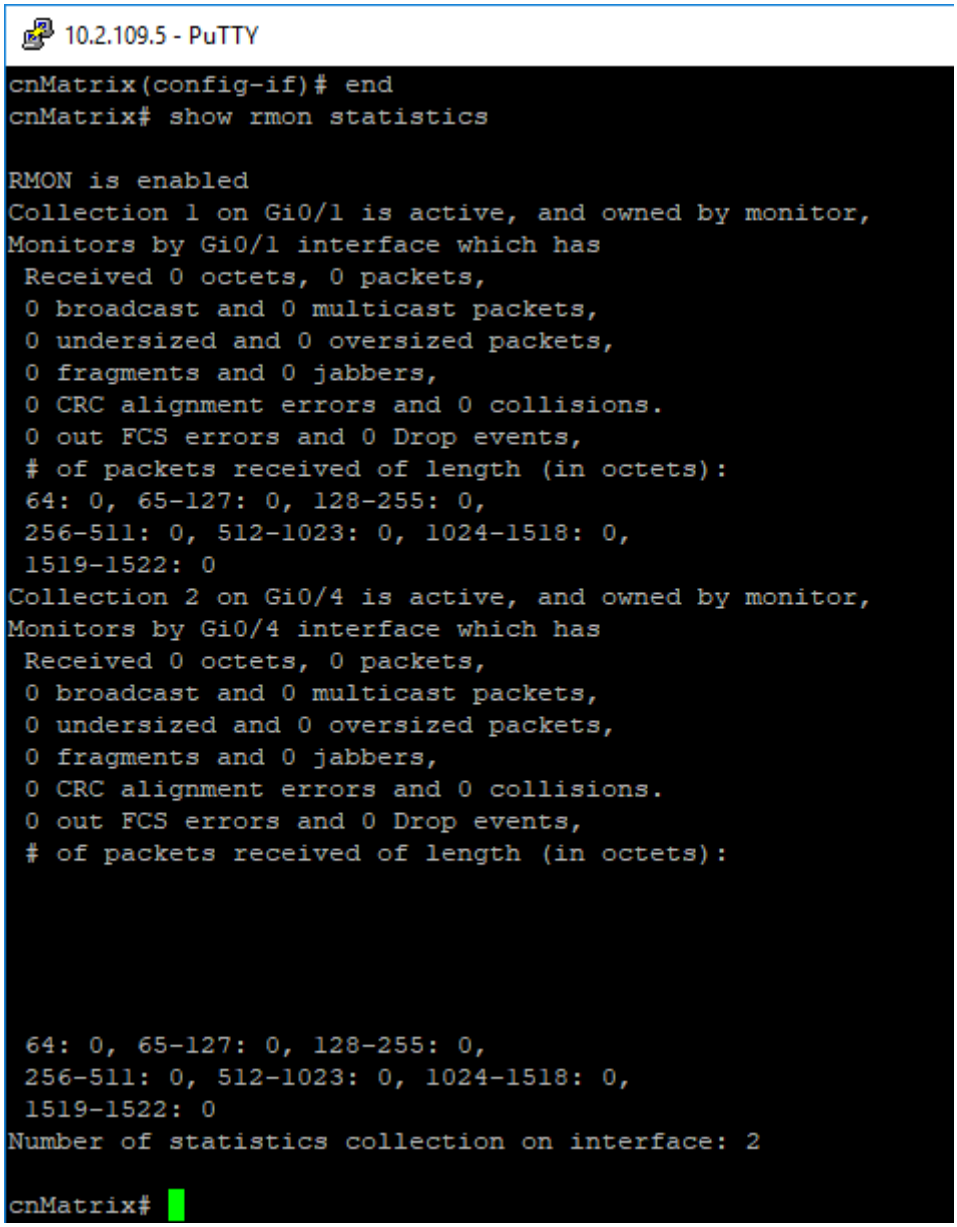
2.4.2 How to Enable and Configure RMON in CLI Interface (Interface Mode)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **rmon enable** command into the terminal to enable RMON. Press the Enter key.
3. Type the **interface gigabitethernet 0/4** command into the terminal to select an interface to be cofigured . Press the Enter key.
4. Type the **rmon collection stats 2** command into the terminal to enable RMON statistic collection on the interface. Press the Enter key.
5. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
6. Type the **show rmon statistics** command into the terminal to display RMON statistics. Press the Enter key.

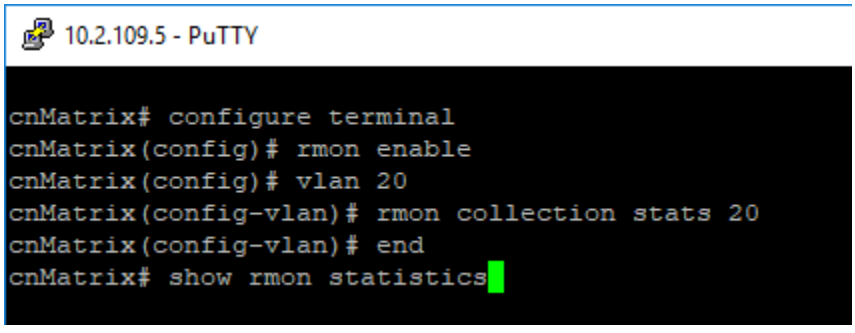


7 Press the Space key.



For more information, see RMON Parameters and Commands.

2.4.3 How to Enable and Configure RMON in CLI Interface (VLAN Mode)

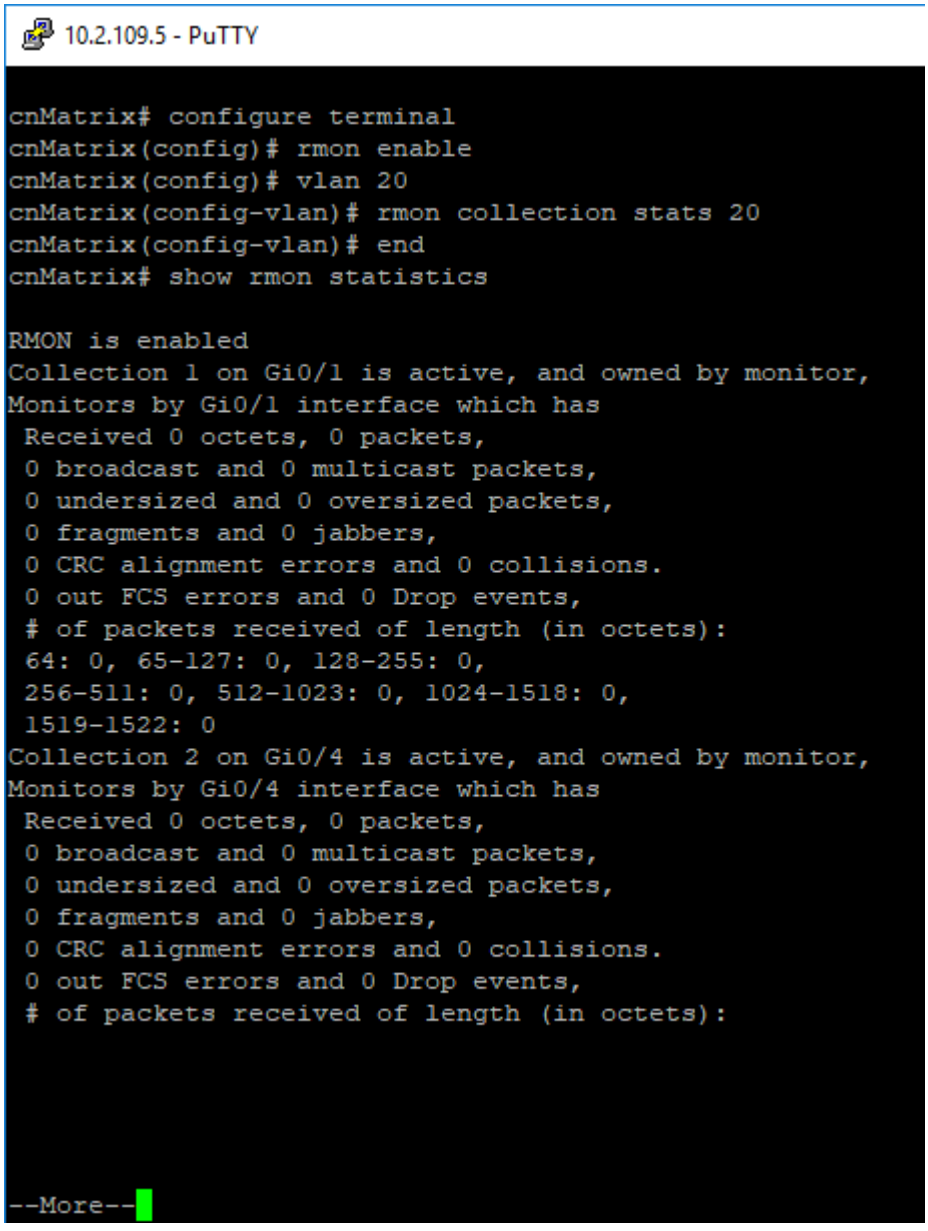


1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **rmon enable** command into the terminal to enable RMON. Press the Enter key.
3. Type the **vlan 20** command into the terminal to configure a VLAN. Press the Enter key.

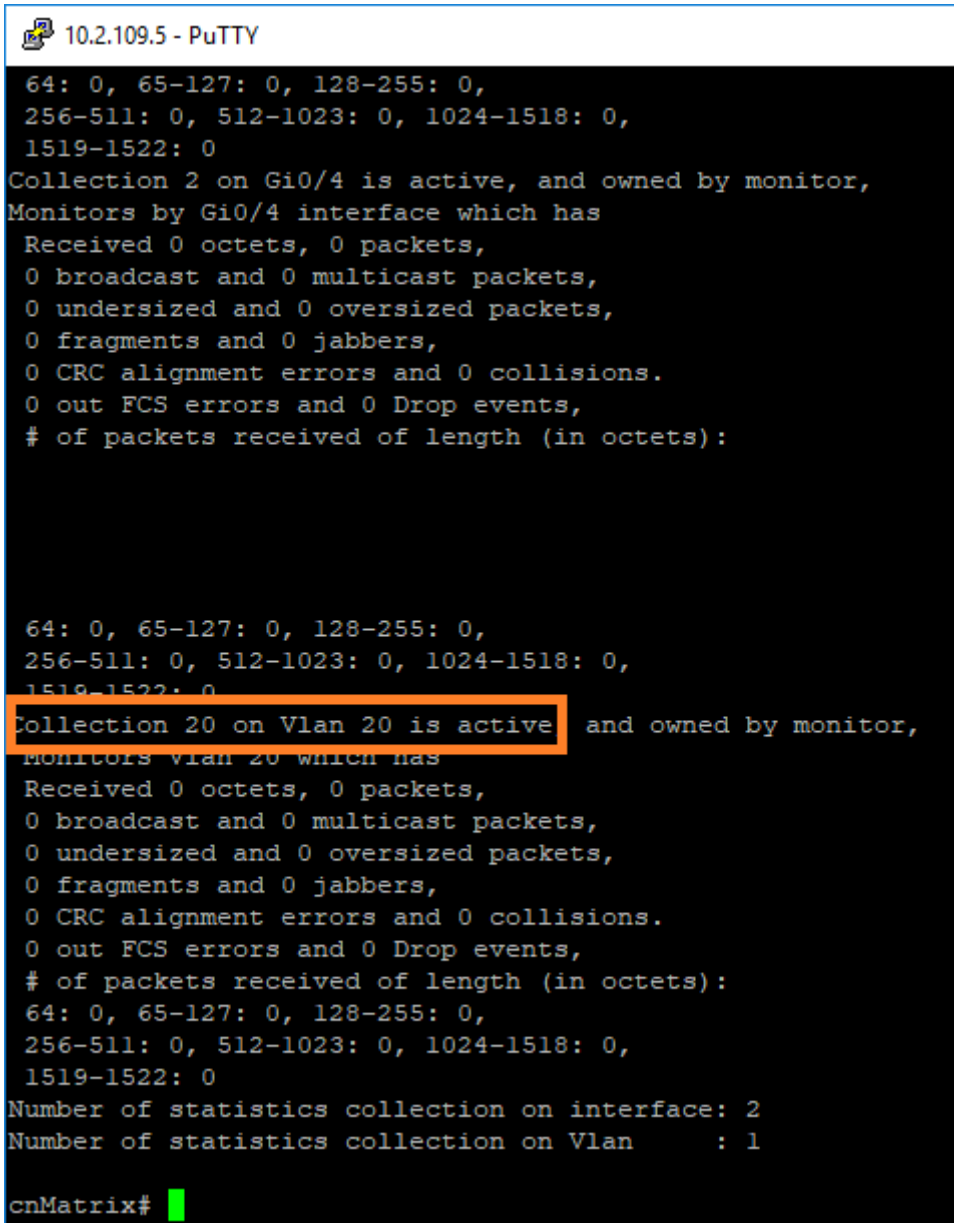
4. Type the **rmon collection stats 20** command into the terminal to enable RMON statistics collection on the VLAN. Press the Enter key.

5. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

6. Type the **show rmon statistics** command into the terminal to display RMON statistics. Press the Enter key.



7. Press the Space key.



For more information, see RMON Parameters and Commands.

2.4.4 Troubleshooting RMON

Useful commands for troubleshooting:

```
cnMatrix#show rmon statistics

cnMatrix#show rmon alarms

cnMatrix#show rmon history

cnMatrix#show rmon events
```

2.5 SNTP

2.5.1 Managing SNTP

2.5.1.1 Feature Description

The **SNTP** client feature enables you to synchronize the time and date in cnMatrix with a SNTP Server and to determine the time, roundtrip delay and local clock offset in reference to a SNTP server.

Standards

- cnMatrix SNTP client is RFC 4330 compliant.

Scaling Numbers

- cnMatrix SNTP is a client feature and depends only on scaling capabilities of the server.

Limitations

- SNTP client accesses a single server to synchronize with. For unicast mode, there is a back-up server in case the primary server fails.
- The software does not support SNTP symmetric mode.
- When configured to function in Unicast Addressing mode, the software delivers the functionality listed below:
  - Dinamically discovers the Version Number of the SNTP server.
  - Sets the transmit time field in the request packet to determine roundtrip delay and system clock offset relative to the server.
  - Avoids sending client request message with less than 1-minute periodic interval.
  - Stops sending request packets to a particular server while receiving a reply with stratum field set to zero.
  - Retransmits request packet using an exponential-back off algorithm, after receiving reply packet with stratum field set as zero.
  - Allows administrative configuration for two designated SNTP servers.
- When configured to function in Broadcast or Multicast Addressing Mode, the software delivers the functionality listed below:
  - Listens for a Broadcast or Multicast Address from one or more broadcast servers.
  - Allows configuration of the designated Broadcast or Multicast servers.
  - Sends request packet to measure the propagation delay and continues operation in listen-only mode.
  - Abandons the measurement and assumes a default value for the delay, if it does not receive a reply from the broadcast server.
- The software does not support any authentication schemes.
- When configured to function in Manycast Addressing Mode, the software delivers the functionality listed below:
  - Sends a client request packet to designated Manycast servers.
  - Adjusts the TTL field in the IP header for appropriate scope in the client request message.
  - Sets the message header to zero, except the Mode, Version Number and optional transmit Timestamp fields in the client request message.
  - Sets the Mode field to three (client) in the client request packet header.
  - Avoids sending any request packet with version number set as zero.
  - Allows the administrator to configure the version number field.
  - Discovers the version number of the server dynamically.
  - Sets the transmit time field in the request packet which allows to determine roundtrip delay and system clock offset relative to the server.
  - Sends client request messages periodically.
  - Avoids sending client request messages with less than 1-minute periodic interval.
  - Stops sending request packets to a particular server when receives a reply with stratum

field set to zero.

- Retransmits a request packet using an exponential-backoff algorithm, after receiving reply packet with start field set as zero.

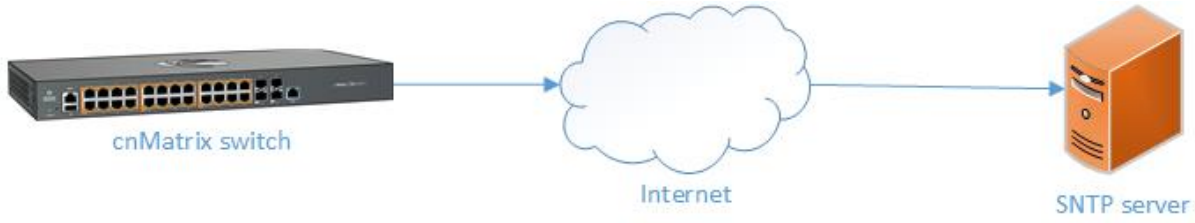
Default Values

- The default SNTP client version: v4.
- The default SNTP addressing mode is unicast.
- The SNTP to send status request is disabled by default.
- The default SNTP unicast server: IPv4.
- The default value for the maximum poll retries: 3.
- The default value for the maximum poll interval timeout: 5 seconds.
- The default unicast poll interval is: 64 seconds.
- The auto discovery option is enabled by default.
- The default time zone is: +00:00.
- The default clock format: hours.
- The default client port number is: 123.
- The default SNTP addressing mode: unicast.

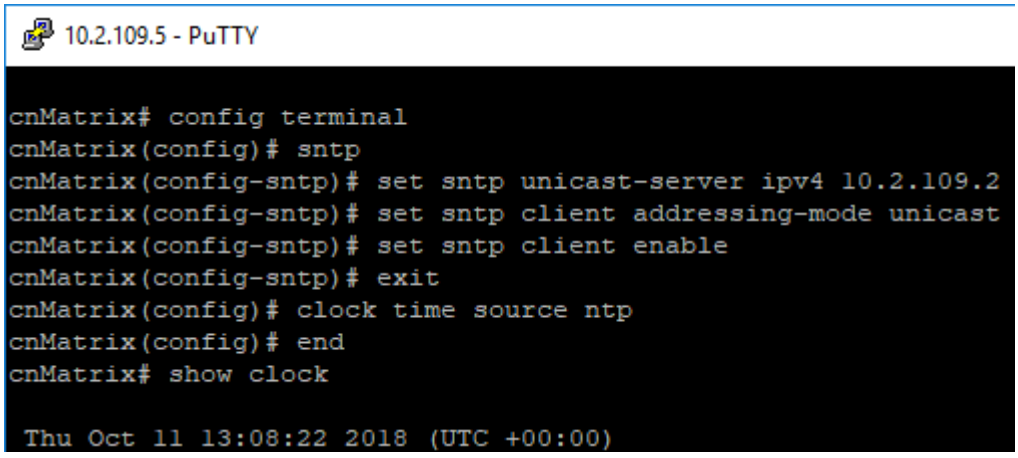
Prerequisites

- Network connectivity to a SNTP server.

2.5.1.2 Network Diagram



2.5.2 How to Enable and Configure SNTP in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **sntp** command into the terminal to Type the SNTP confihuration mode. Press the Enter key.

3 Type the **set sntp unicast-server ipv4 10.2.109.2** command into the terminal to configure SNTP unicast server. Press the Enter key.

4 Type the **set sntp client addressing-mode unicast** command into the terminal to set the addressing mode of the SNTP client as unicast. Press the Enter key.

5 Type the **set sntp client enable** command into the terminal to enable SNTP client module. Press the Enter key.

6 Type the **exit** command into the terminal to go back to the global configuration mode. Press the Enter key.

7 Type the **clock time source ntp** command into the terminal to configure the time source for the primary clock. Press the Enter key.

8 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

9 Type the **show clock** command into the terminal to display the system clock. Press the Enter key.

For more information, see SNTP Parameters and Commands.

2.6 Port Settings Feature

2.6.1 Managing Negotiation

Feature Overview

The **negotiation** setting enables the auto-negotiation on the interface so that the port can negotiate with the other end of port properties.

Standards

N/A

Scaling Numbers

N/A

Limitations

- Fiber ports do not support auto-negotiation.

Default Values

- The negotiation setting is enabled by default.

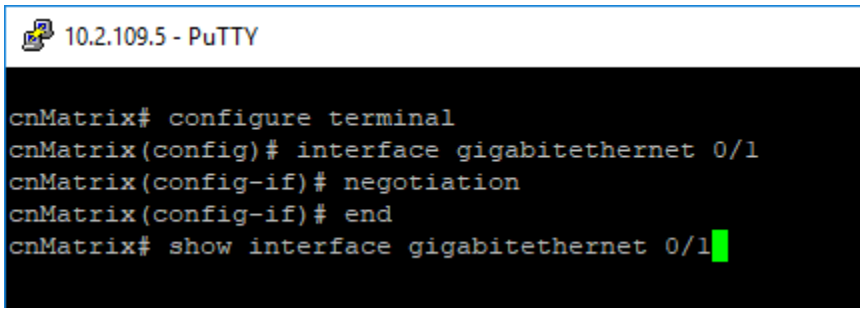
Prerequisites

- N/A

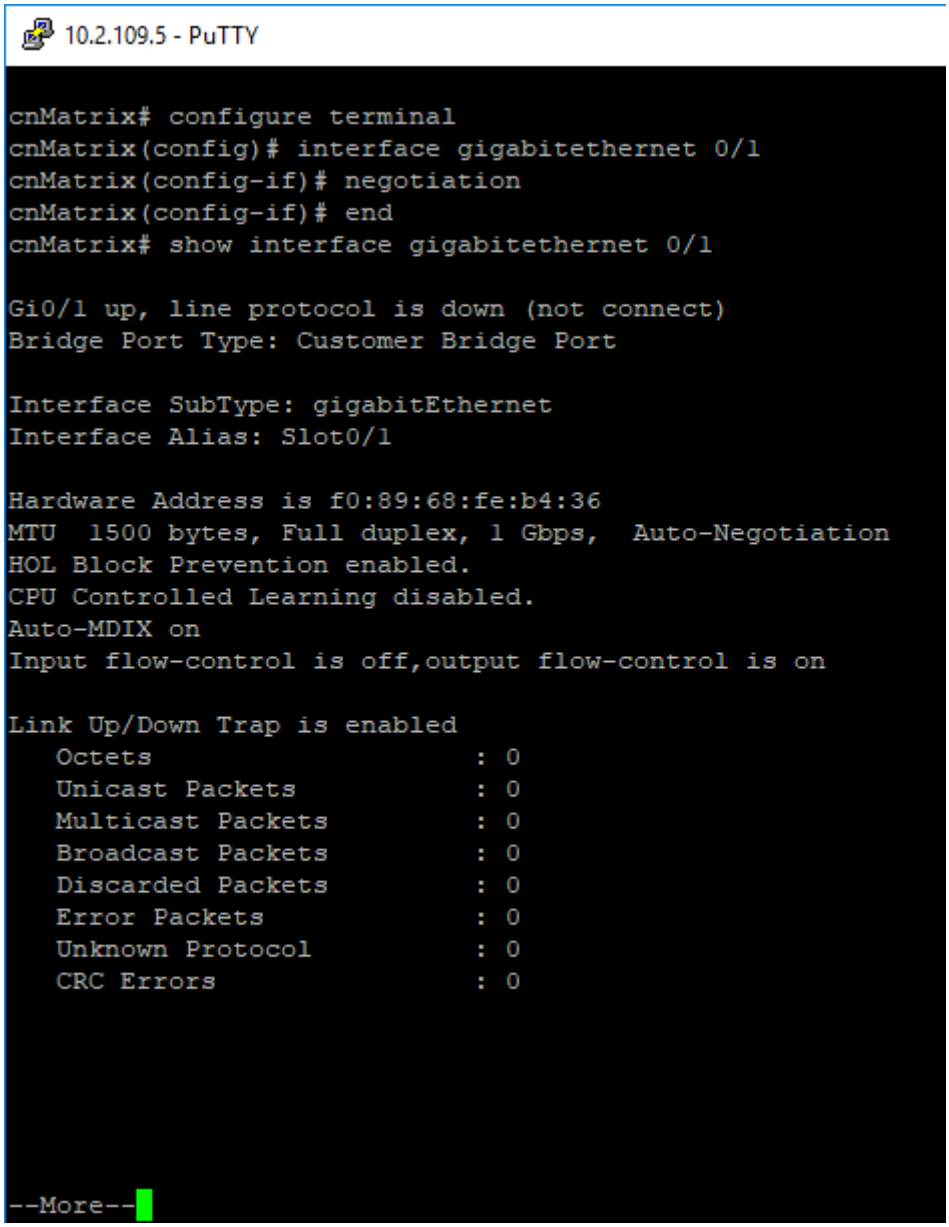
SNMP

- The object is called issPortCtrlMode and it is accompanied by an index which represents the port number. It is part of the issPortCtrlTable table.

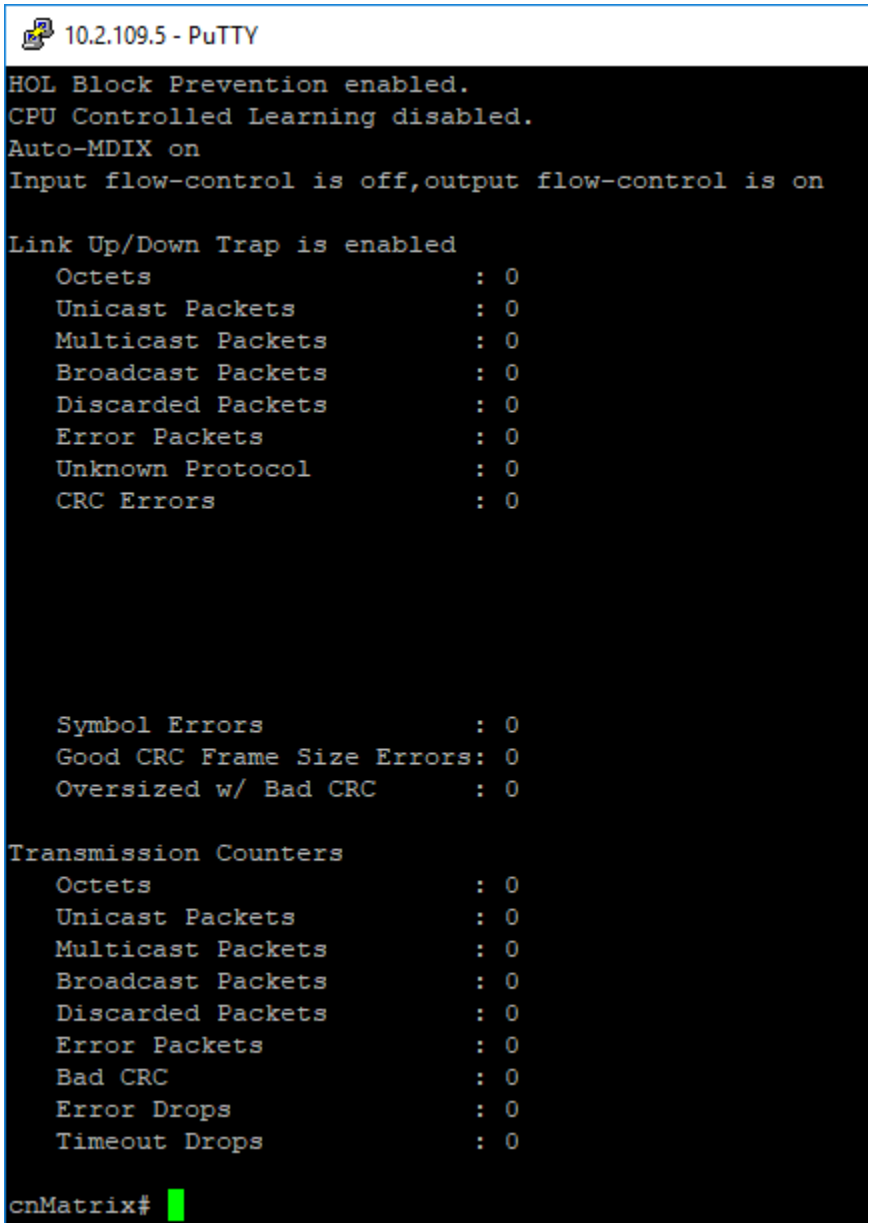
2.6.2 How to Enable and Configure Negotiation in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **negotiation** command into the terminal to enable auto-negotiation on the interface. Press the Enter key.
4. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
5. Type the **show interface gigabitethernet 0/1** command into the terminal to display the interface status and the configurations (verify if negotiation has been enabled).



6 Press the Space key.



For more information, see Port Settings Parameters and Commands.

2.6.3 Managing Speed

Feature Overview

The **speed** setting enables you to set the speed of the interface.

Standards

- N/A

Scaling Numbers

- N/A

Limitations

- Manual speed cannot be set if auto-negotiation is enabled.
- Manual speed can be set on fiber ports only if module is inserted.

Default Values

- The default speed: 1 Gbps (copper ports), 1Gbps/10Gbps(fiber ports).

Prerequisites

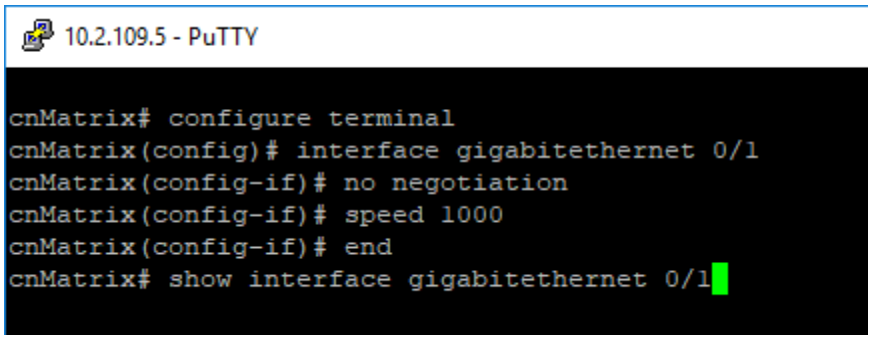
- N/A

SNMP

The object is called issPortCtrlSpeed and it is accompanied by an index which represents the port number. It is part of the issPortCtrlTable table.

The speed feature can be configured, only if the nogotiation **Mode** is set to **No Nego**.

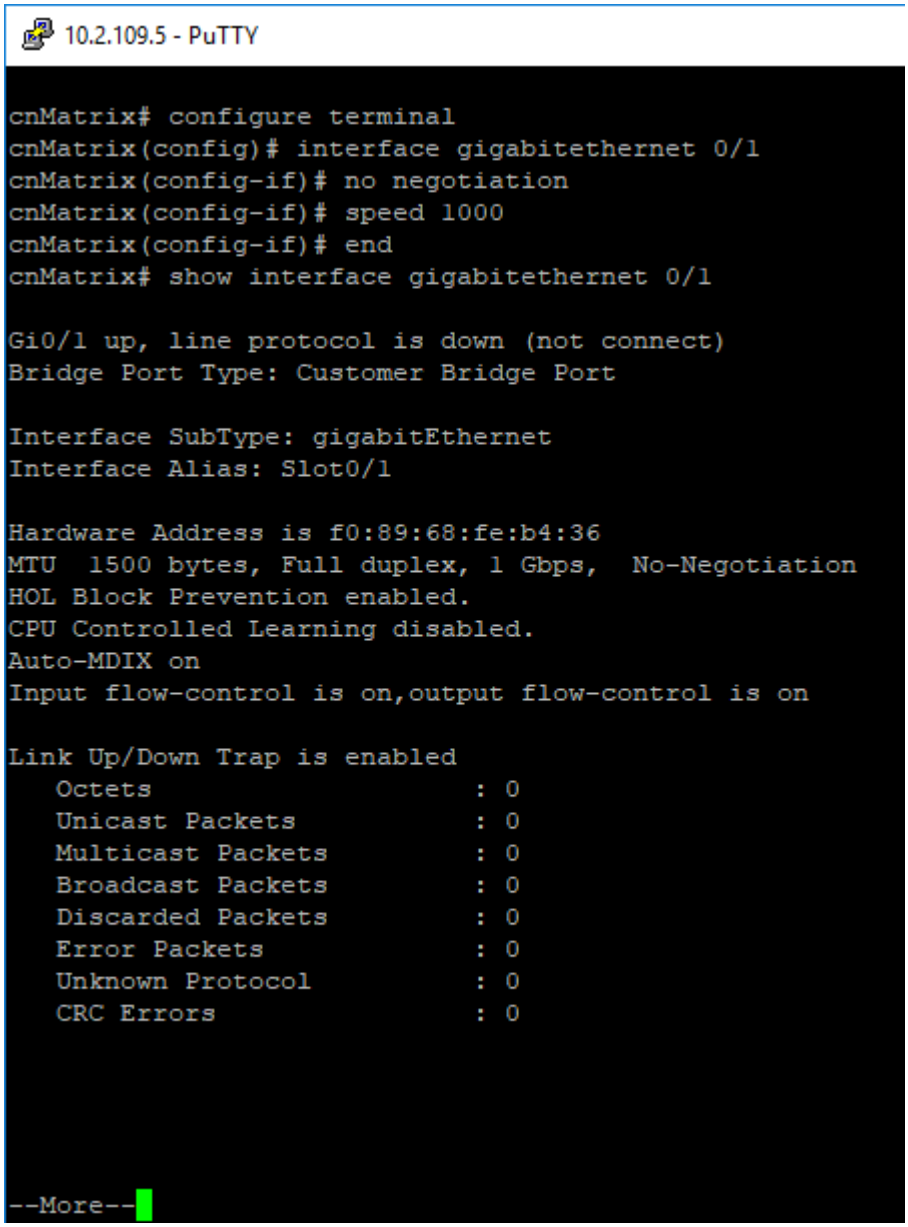
2.6.4How to Enable and Configure Speed in CLI Interface



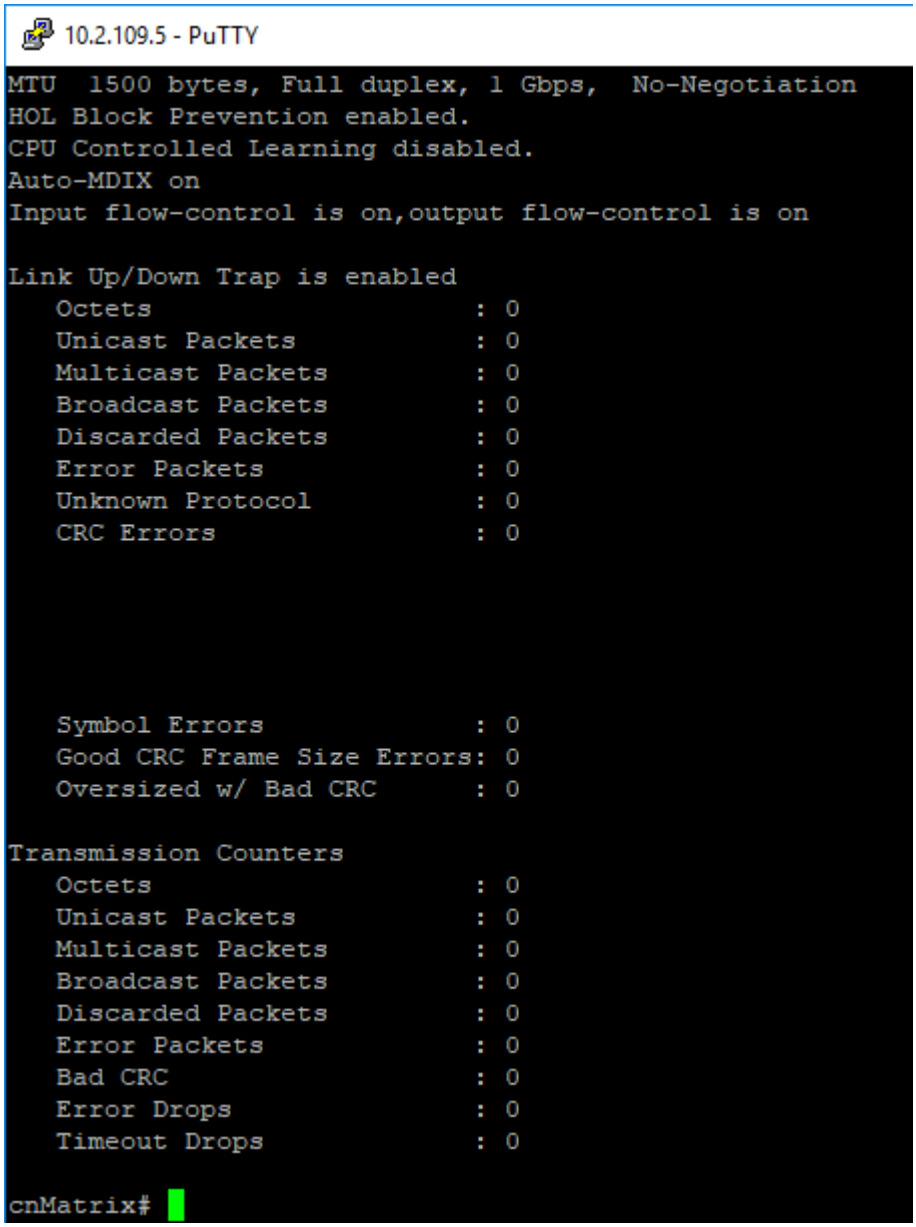
1. Enter **configure terminal** into the field. Press the Enter key.
2. Enter **interface gigabitethernet 0/1** into the field to select an interface to be configured. Press the Enter key.
3. Enter **no negotiation** into the field to disable auto-negotiation on the interface. Press the Enter key.

Speed cannot be set if auto-negotiation is enabled.

4. Enter **speed 1000** into the field to set the speed of the interface. Press the Enter key.
5. Enter **end** into the field. Press the Enter key.
6. Enter **show interface gigabitethernet 0/1** into the field to display interface status and configurations (verify if speed has been correctly set on the configured interface). Press the Enter key.



7 Press the Space key.



2.6.5 Managing MTU

Feature Overview

The **MTU** setting enables you to configure the maximum transmission unit size for all the frames transmitted and received on all the interfaces in a switch.

Standards

- N/A

Scaling numbers

- N/A

Limitations

- N/A

Default Values

- The default MTU value: 1500 bytes.

Prerequisites

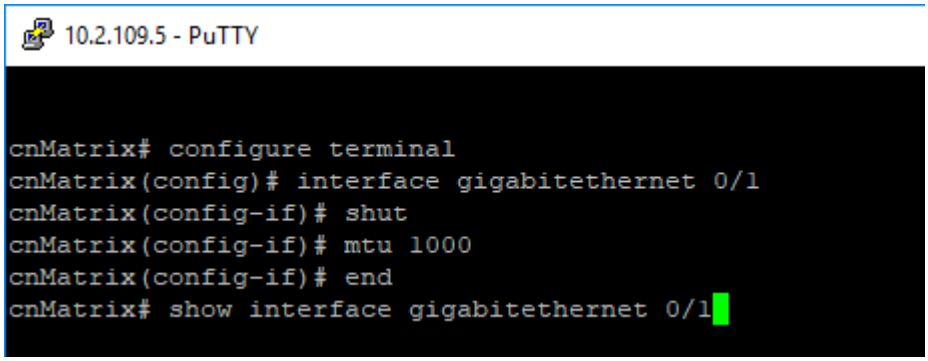
- N/A

SNMP

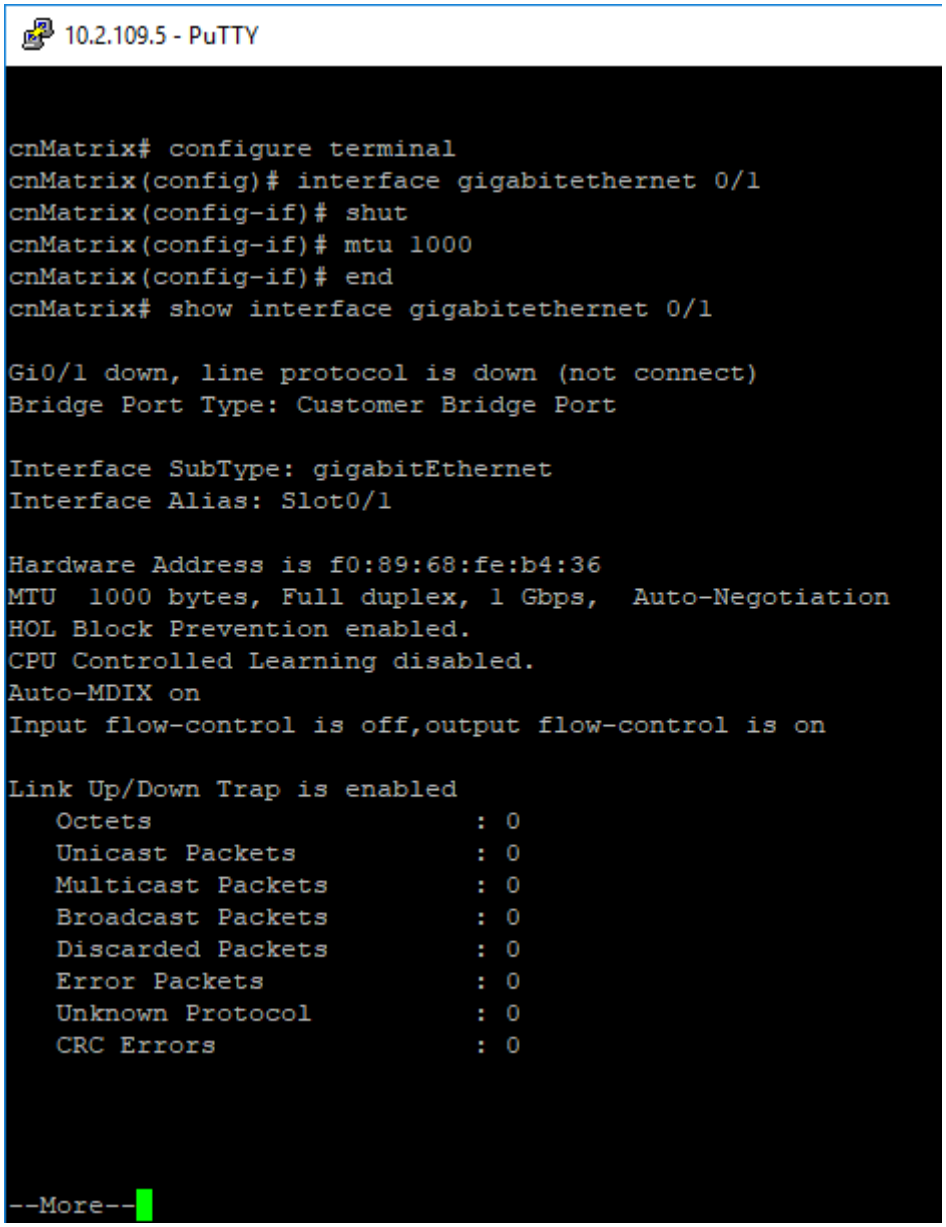
The object is called ifMainMtu, and it is accompanied by an index which represents the port number. It is part of the ifMainTable table.

The MTU value can be changed only if the **Admin State** is set as **Down**.

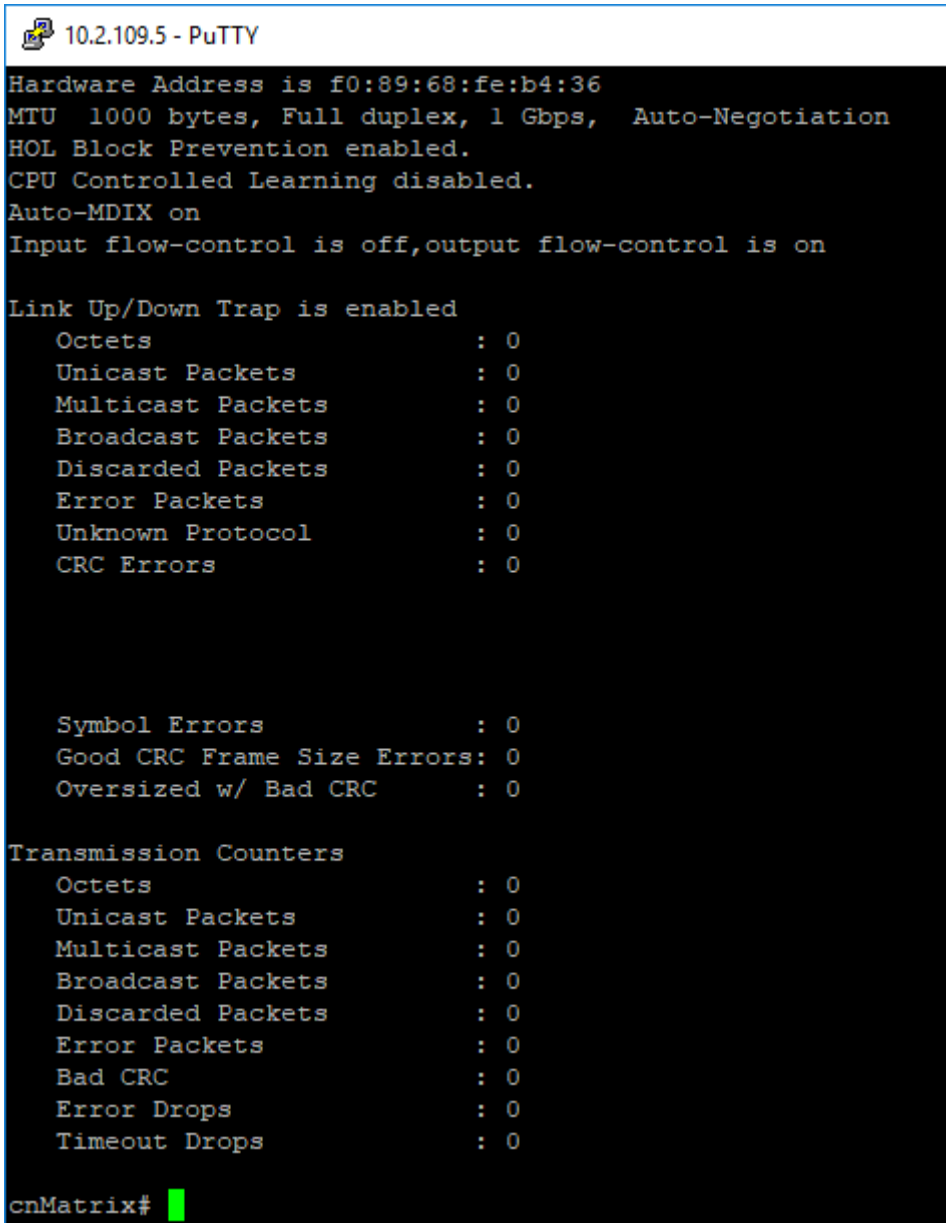
2.6.6 How to Enable and Configure MTU in CLI Interface



1. Enter **configure terminal** into the field. Press the Enter key.
2. Enter **interface gigabitethernet 0/1** into the field to select an interface to be configured. Press the Enter key.
3. Enter **shut** into the field to disable a physical interface. Press the Enter key.
4. Enter **mtu 1000** into the field to set the mtu of the interface. Press the Enter key.
5. Enter **end** into the field. Press the Enter key.
6. Enter **show interface gigabitethernet 0/1** into the field to display interface status and configuration (verify if mtu has been correctly set on the selected interface). Press the Enter key.



7 Press the Space key.



For more information, see Port Settings Parameters and Commands.

2.6.7 Managing Duplex

Feature Overview

The **duplex** setting enables you to set the port duplex mode.

Full-duplex communication improves the performance of a switched LAN. Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.

⚡ The duplex mode can be configured, only if the negotiation **Mode** is set to **NoNego**.

Limitations

- Full/Half duplex cannot be set when auto-negotiation is enabled.

Default Values

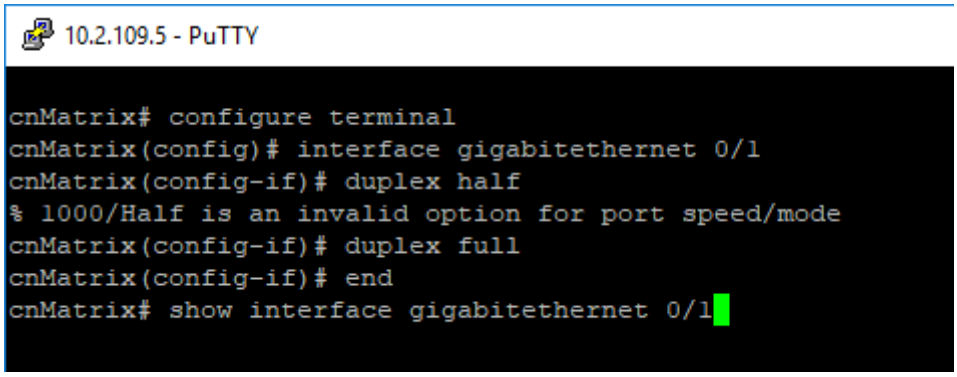
- The default value: full.

Prerequisites

- N/A

- The object is called **issPortCtrlDuplex** and it is accompanied by an index which represents the port number. It is part of the **issPortCtrlTable** table.

2.6.8 How to Enable and Configure Duplex in CLI Interface



1. Enter **configure terminal** into the field. Press the Enter key.
2. Enter **interface gigabitethernet 0/1** into the field. Press the Enter key.
3. Enter **duplex half** into the field to configure the duplexity of the interface. Press the Enter key.
4. Enter **duplex full** into the field (if speed was set to 1000, the mtu value cannot be set to half). Press the Enter key.
5. Enter **end** into the field. Press the Enter key.
6. Enter **show interface gigabitethernet 0/1** into the field to display interface status and configuration (verify if duplex has been correctly set on the selected interface). Press the Enter key.

For more information, see Port Settings Parameters and Commands.

2.6.9 Managing Flow Control

Feature Overview

Flow Control is a per-port feature that detects packet congestion at its end and notifies the link partner by sending a pause frame. By enabling Flow Control, both the Tx (sending of pause frames) and Rx (receiving and obeying pause frames originating from a partner) are enabled.Flow control can be enabled manually on a per-port basis, or by auto-negotiation with a compatible link partner.

Standards

- IEEE 802.3x

Scaling Numbers

- N/A

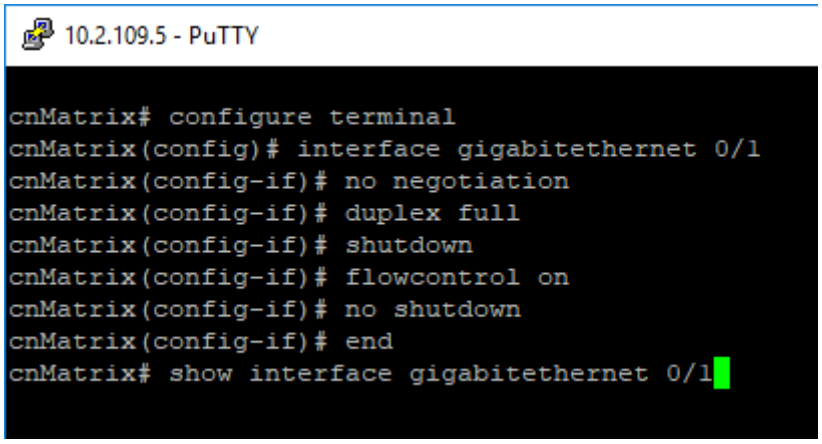
Limitations

- This feature requires the port to be down while the setting is changed.
- This feature only works in full-duplex mode.
- Flow control can be either disabled or enabled on both RX and TX, not separately on RX or TX.

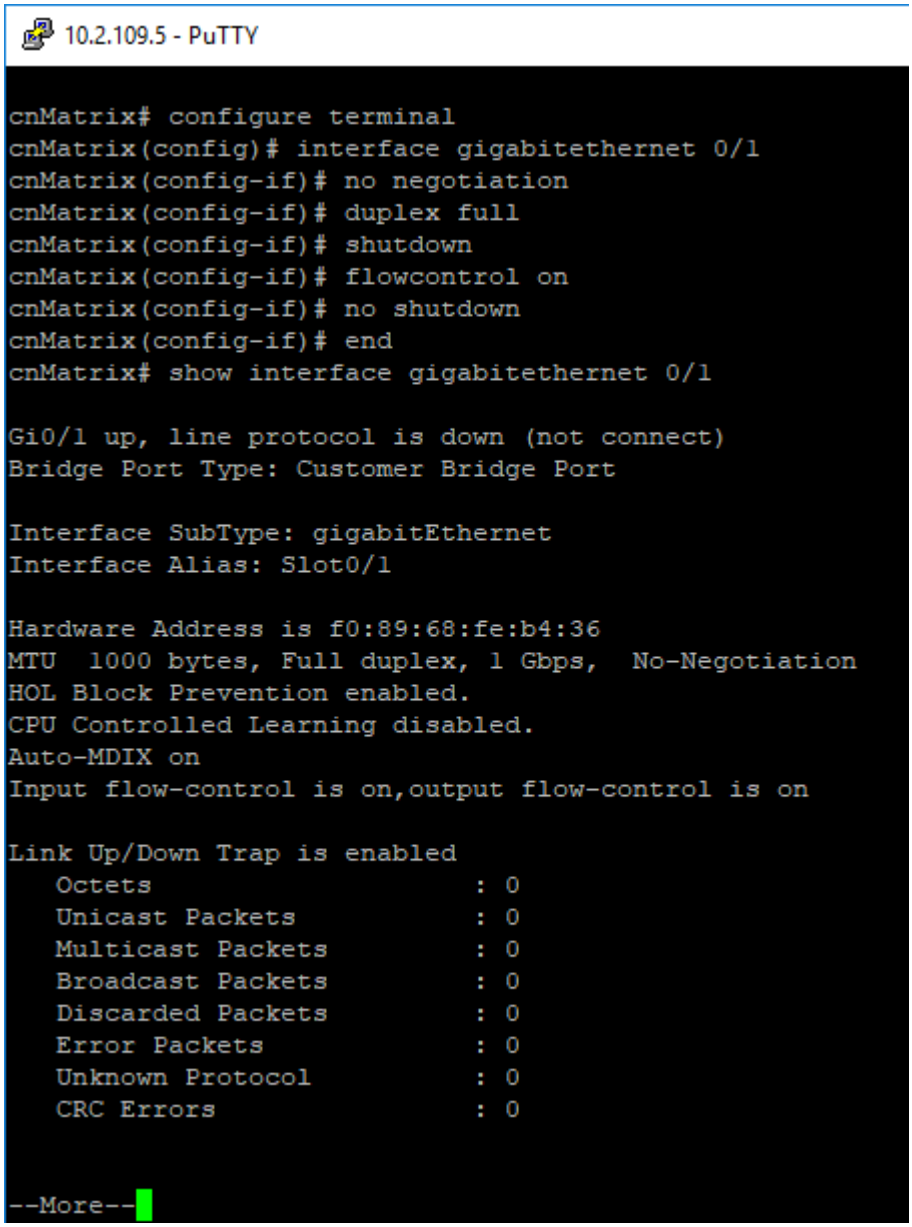
Default Values

- By default, auto-negotiation is enabled on all ports. If the compatible link partner advertises flow control capability, flow control will be operationally enabled.

2.6.10 How to Enable and Configure Flow Control in CLI Interface



1. Enter **configure terminal** into the field. Press the Enter key.
2. Enter **interface gigabitethernet 0/1** into the field to select an interface to be configured. Press the Enter key.
3. Enter **no negotiation** into the field to disable auto-negotiation on the interface. Press the Enter key.
4. Enter **duplex full** into the field to configure the duplexity of the interface. Press the Enter key.
5. Enter **shutdown** into the field to disable a physical interface. Press the Enter key.
6. Enter **flowcontrol on** into the field to enable flow control. Press the Enter key.
7. Enter **no shutdown** into the field to enable a physical interface. Press the Enter key.
8. Enter **end** into the field. Press the Enter key.
9. Enter **show interface gigabitethernet 0/1** into the field to display interface status and configuration (verify if flow control has been enabled). Press the Enter key.



For more information, see Port Settings Parameters and Commands.

2.6.11 How to Display Transceiver Information (Starting with version 2.1)

Feature Overview

- **Starting with version 2.1**, the users have the possibility to display vendor information regarding inserted transceivers by using the following command:

```
cnMatrix# show interfaces transceivers
```

- The ports do not need to have link-up in order to be able to display the information.
- The following information will be displayed:
  - TX status
  - Type
  - Wavelength
  - Vendor name
  - Vendor OUI
  - Vendor SN
  - Vendor PN

- Revision
- Date of manufacturing

Limitations

- The EX2010 model can only display information for SFP, while the EX2028 model supports SFP+.

Prerequisites

- Insert a transceiver in your cnMatrix switch.

2.7 Link Aggregation

2.7.1 Managing Link Aggregation

2.7.1.1 Feature Description

Feature Overview

The Link Aggregation feature enables you to combine physical network links into a single logical link so that you can have increased bandwidth, higher link availability and increased link capacity.

Standards

- IEEE 802.3ad

Scaling Numbers

- Maximum 8 Ports per Port Channel.
- Maximum 8 Port Channels on Switch.

Limitations

- Maximum 8 Ports per Port Channel.
- Maximum 8 Port Channels on Switch.

Default Values

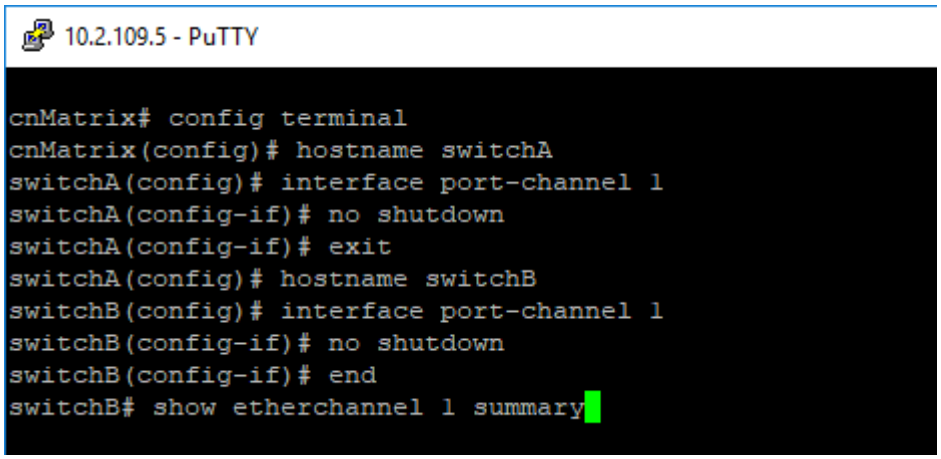
- The Link Aggregation feature is enabled by default.
- The admin status of the Link Aggregation Status in the switch is disabled by default.
- The default LACP wait-time: 2.
- The default LACP timeout period: long.
- The default LACP rate: normal.

Prerequisites

N/A

2.7.1.2 Network Diagram

2.7.2 How to Enable and Configure Link Aggregation in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **hostname switchA** command into the terminal to configure the name of the switch. Press the Enter key.

3 Type the **interface port-channel 1** command into the terminal to select the interface to be configured. Press the Enter key.

4 Type the **no shutdown** command into the terminal to enable a vlan interface. Press the Enter key.

5 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

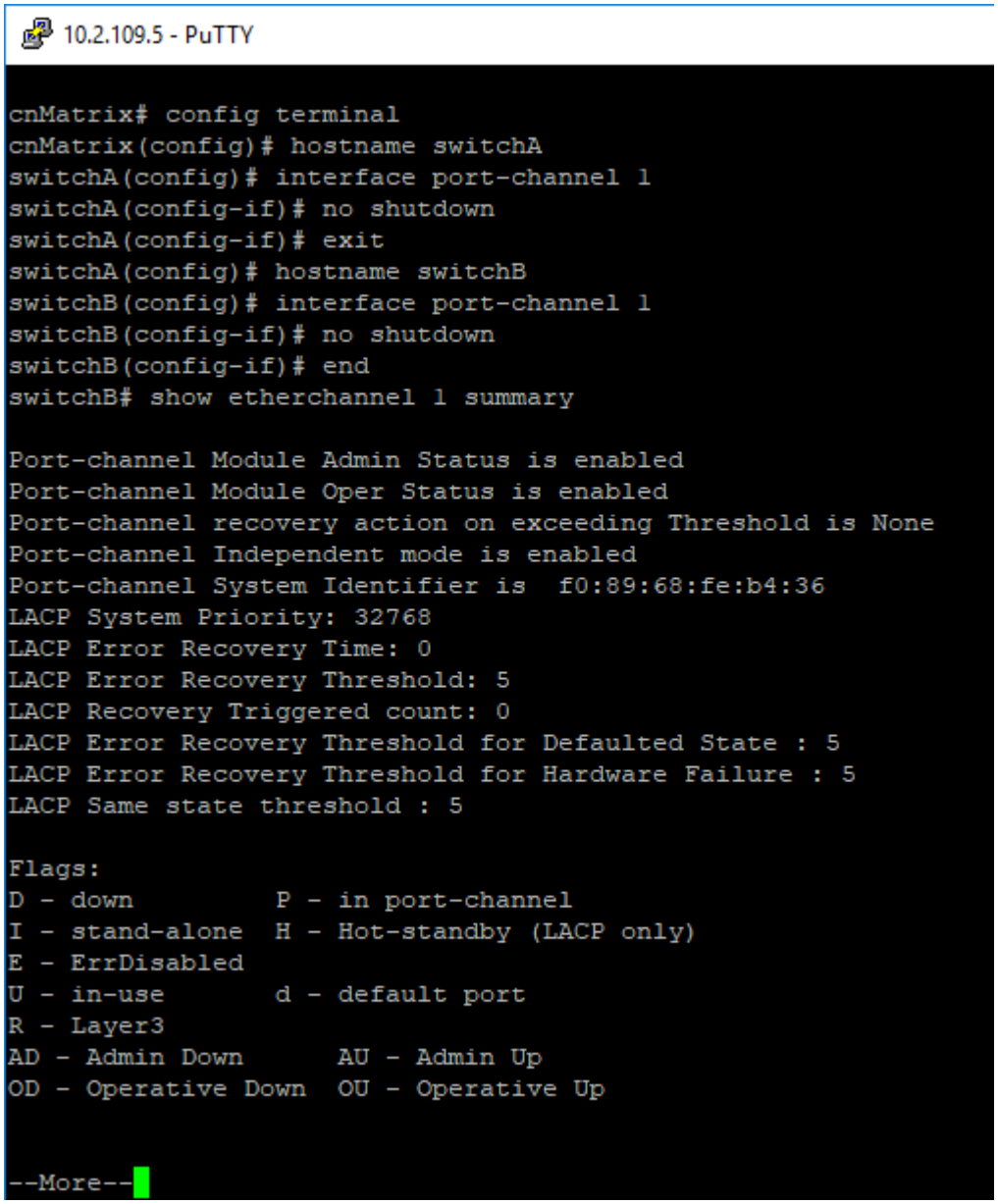
6 Type the **hostname switchB** into the terminal to configure the name of the second switch . Press the Enter key.

7 Type the **interface port-channel 1** into the terminal to select the interface to be configured. Press the Enter key.

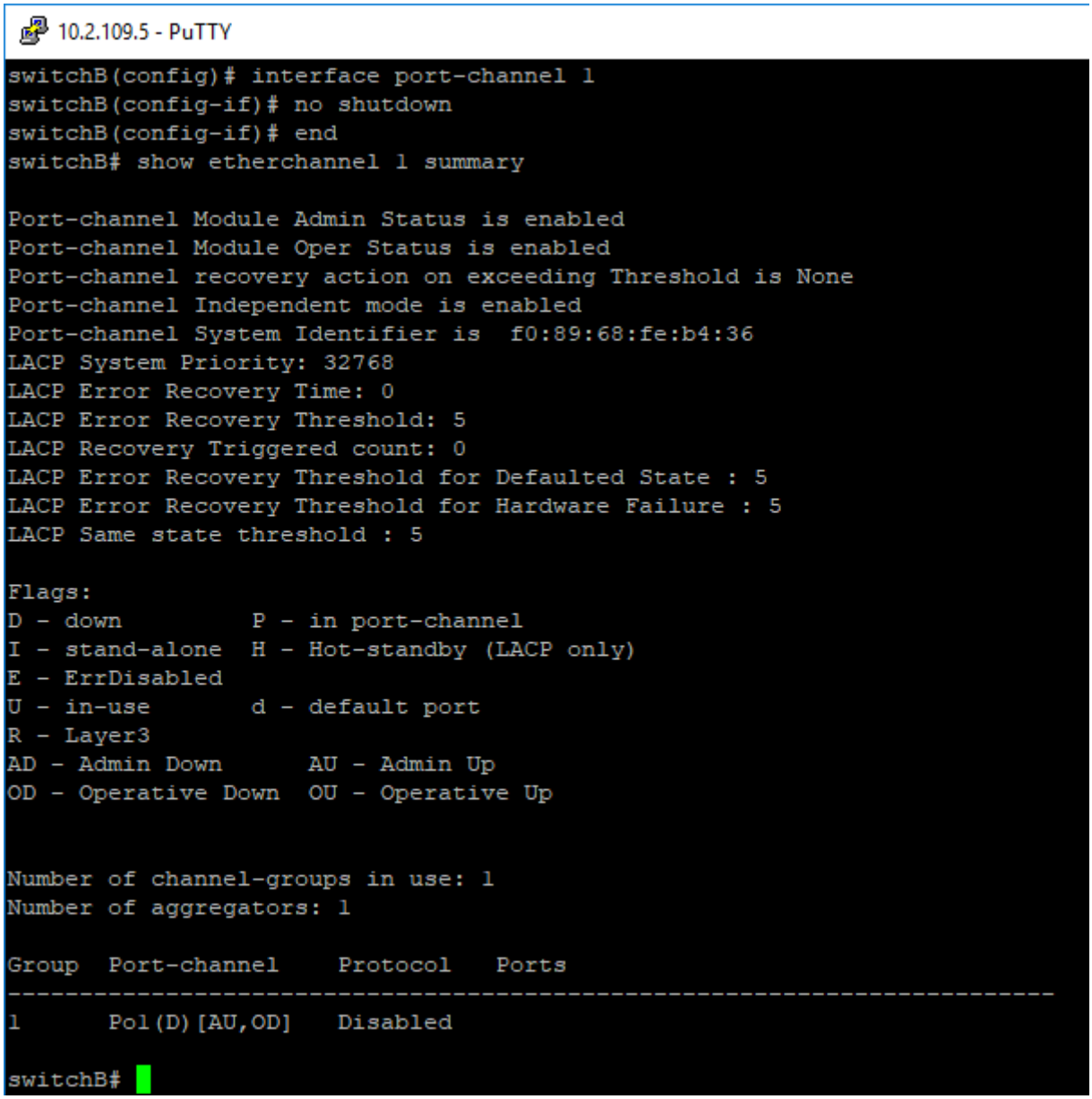
8 Type the **no shutdown** into the terminal to enable a vlan interface. Press the Enter key.

9 Type the **end** into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

10 Type the **show etherchannel 1 summary** into the terminal to display the etherchannel related information for the specified channel group number (in this example: channel group 1). Press the Enter key.



11 Press the Space key.



For more information, see Link Aggregation Parameters and Commands.

2.7.3 Troubleshooting Link Aggregation

Useful commands for troubleshooting:

```
cnMatrix#debug lacp [ { init-shutdown | mgmt | data | events | packet | os |
failall | buffer | all } ]
```

```
cnMatrix#show etherchannel
```

```
cnMatrix#show etherchannel <Channel group number> summary
```

```
cnMatrix#show etherchannel <Channel group number> details
```

2.8 Private VLAN Edge

2.8.1 Managing Private VLAN Edge

2.8.1.1 Feature Description

When a port has protected status, it no longer forwards any L2 traffic (unicast, multicast, broadcast)

to any other port that is also protected and on the same switch. The **Private VLAN Edge** feature enables you to control the flow of the Layer 2 traffic.

Standards

- N/A

Scaling Numbers

- All front panel ports can be set to have protected status.

Limitations

- N/A

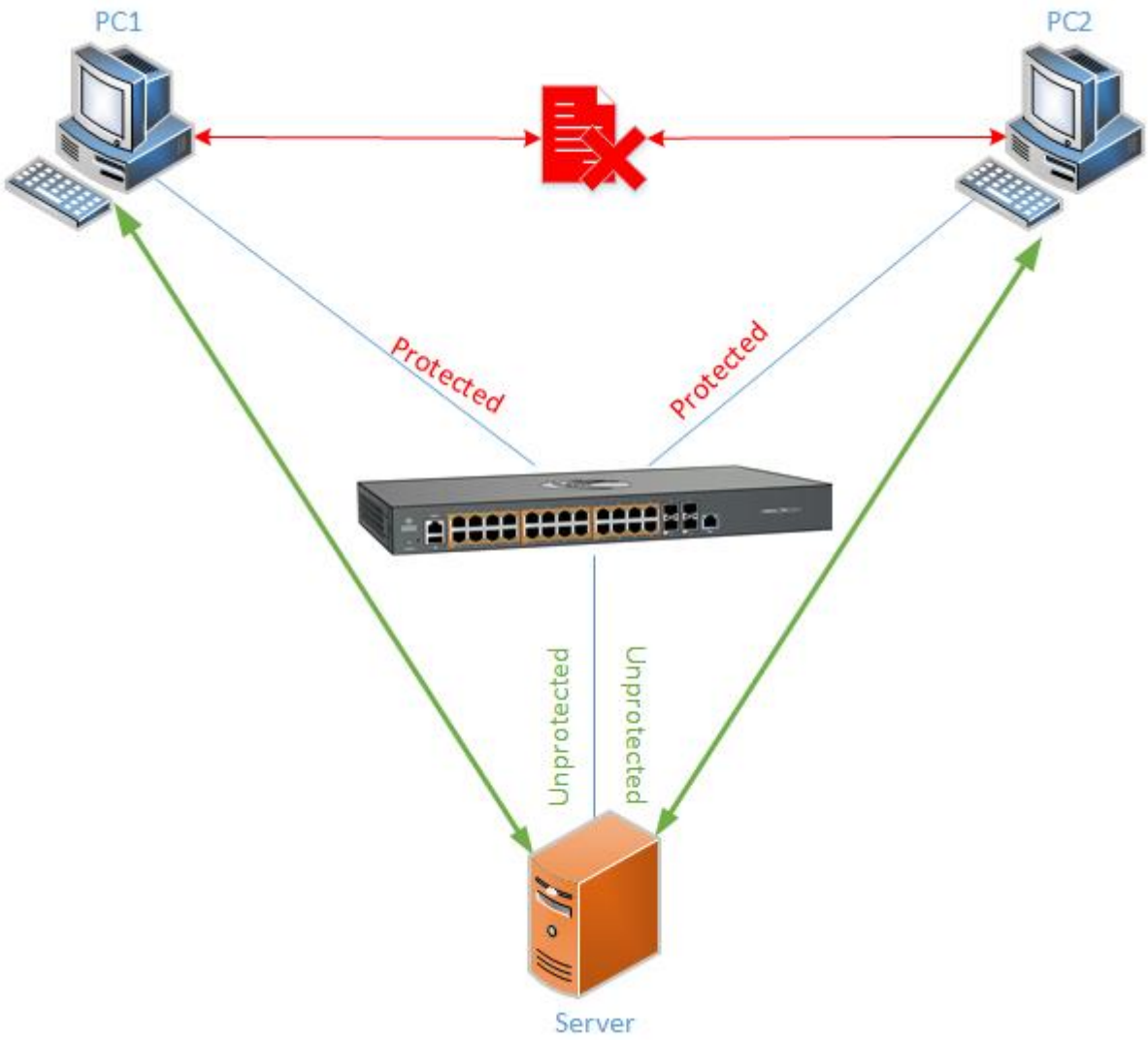
Default Values

- The switch boots having the protected status disabled on all ports.

Prerequisites

- N/A

2.8.1.2 Feature Description



2.8.2 How to Enable Private VLAN Edge in CLI Interface

```
10.2.109.5 - PuTTY

cnMatrix# config terminal
cnMatrix(config)# interface range gigabitethernet 0/1-4
cnMatrix(config-if-range)# switchport protected
cnMatrix(config-if-range)# end
cnMatrix# show vlan port gigabitethernet 0/1
```

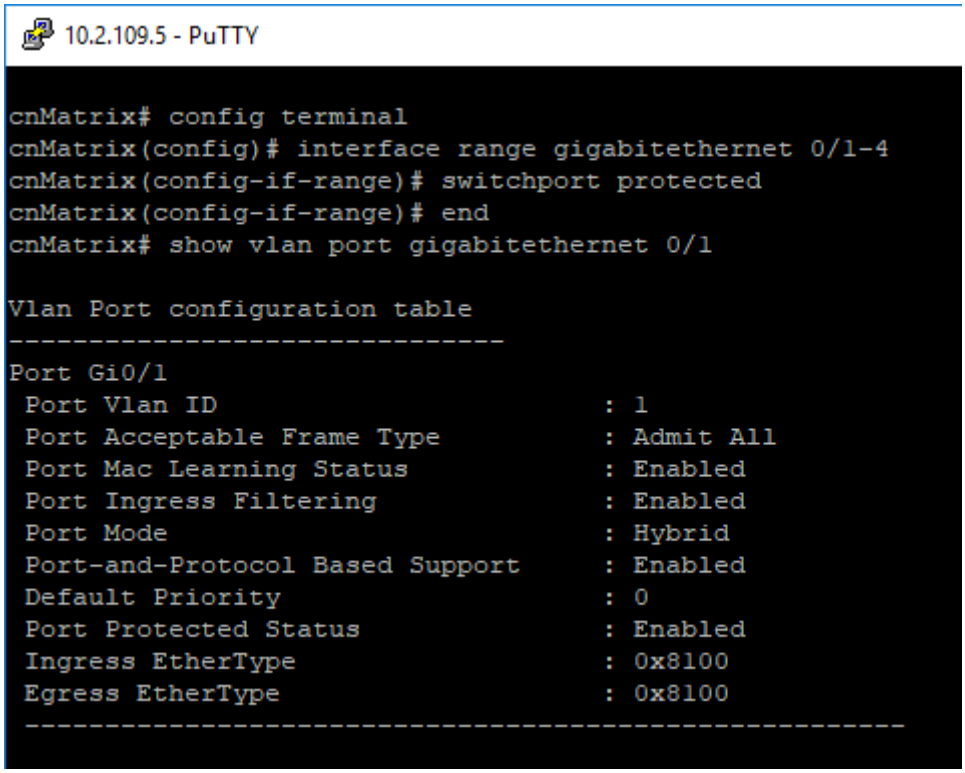
1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **interface range gigabitethernet 0/1-4** command into the terminal to select the range of L2 interfaces to be configured. Press the Enter key.

3 Type the **switchport protected** command into the terminal to enable the protected feature of a port. Press the Enter key.

4 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

5 Type the **show vlan port gigabitethernet 0/1** command into the terminal to display the interface information (verify if the port protected status is enabled). Press the Enter key.



For more information, see Private VLAN Edge Parameters and Commands.

2.8.3 Troubleshooting Private VLAN Edge

Useful commands for troubleshooting:

```
cnMatrix# show vlan port gigabitethernet 0/1
```

2.9 Power over Ethernet

2.9.1 Managing PoE (Power over Ethernet)

Feature Overview

The **PoE** feature enables data connection and electric power to be transmitted to devices such as wireless access points, IP cameras and VOIP phones. Power over Ethernet technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network.

Standards

- IEEE 802.3af
- IEEE802.3at

Scaling Numbers

N/A

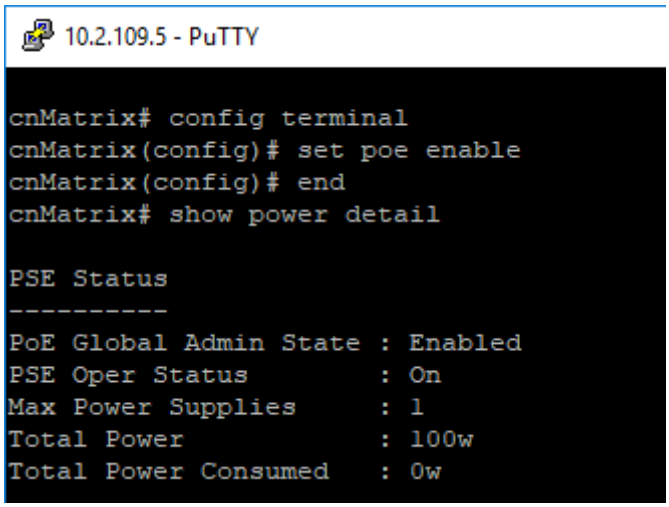
Limitations

N/A

Default Values

- The PoE feature is enabled by default, both globally and per-port.
- The power inline priority is set to low by default.

2.9.2 How to Enable PoE in CLI Interface (Power over Ethernet)



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **set poe enable** command into the terminal to enable Power Over Ethernet module on the switch. Press the Enter key.
3. **Type the end command into the terminal to go back to Privileged EXEC mode. Press the Enter key.**
4. Type the **show power detail** command into the terminal to display the Power Over Ethernet power supply status. Press the Enter key.

For more information, see Power over Ethernet Parameters and Commands.

2.9.3 Troubleshooting PoE

Useful commands for troubleshooting:

```
cnMatrix# show power detail
cnMatrix# show power inline
cnMatrix# show power inline measurements
```

2.10 Port Mirroring

2.10.1 Managing Port Mirroring

2.10.1.1 Feature Description

The **Port Mirroring** feature is used on the switch to send a copy of network packets available on one switch port (or an entire VLAN) to a network monitoring connection on another switch port or local sniffer device.

The following port mirroring modes are supported:

- Port based – mirror ingress/egress/ingress and egress packets from one source interface or multiple source interfaces to a destination interface.
- VLAN based – mirror packets tagged with a specific VLAN ID to a destination interface.
- IP/MAC ACL based – any packets that match an ACL rule are also forwarded to a mirroring interface.

Standards

- N/A

Scaling Numbers

- A maximum of 7 monitoring sessions can exist at once.

Limitations

- Only one ACL based mirroring session is supported.
- Port-channel can NOT be source or destination in monitor session.

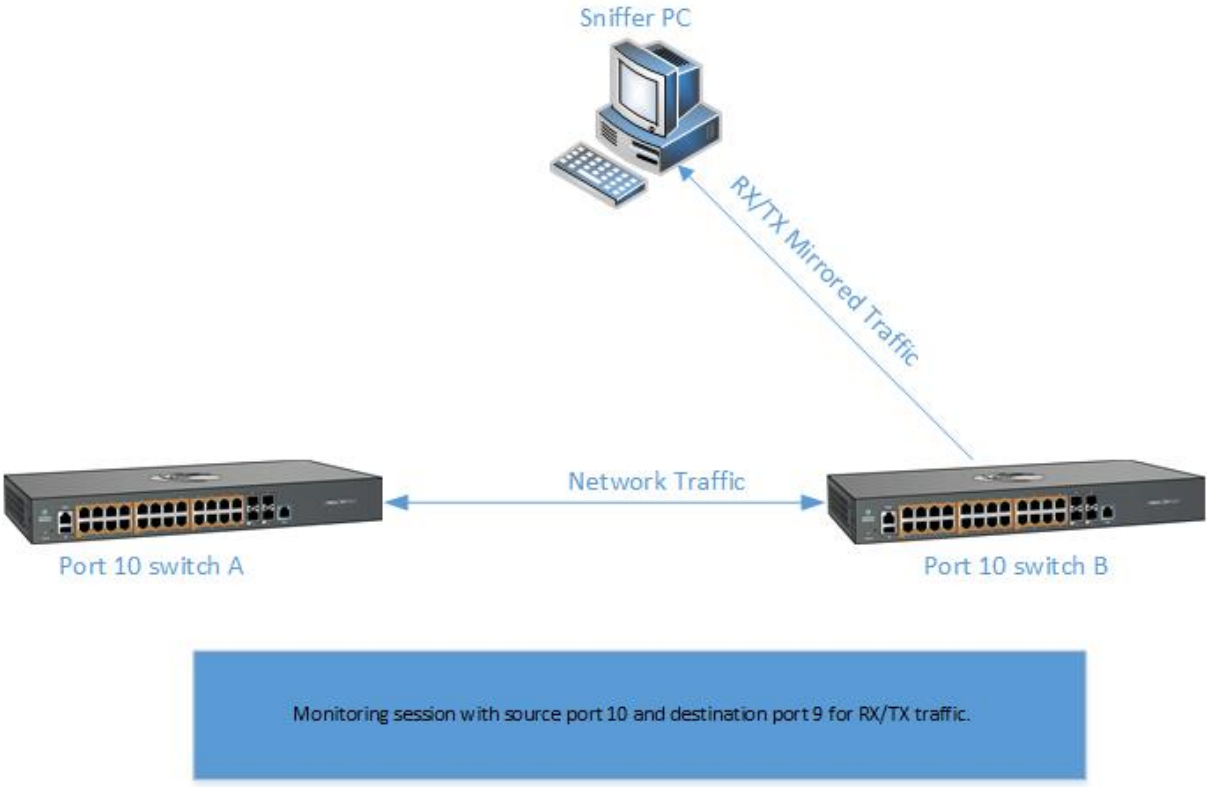
Default Values

- The Port Mirroring feature is enabled by default.

Prerequisites

- N/A

2.10.1.2 Network Diagram



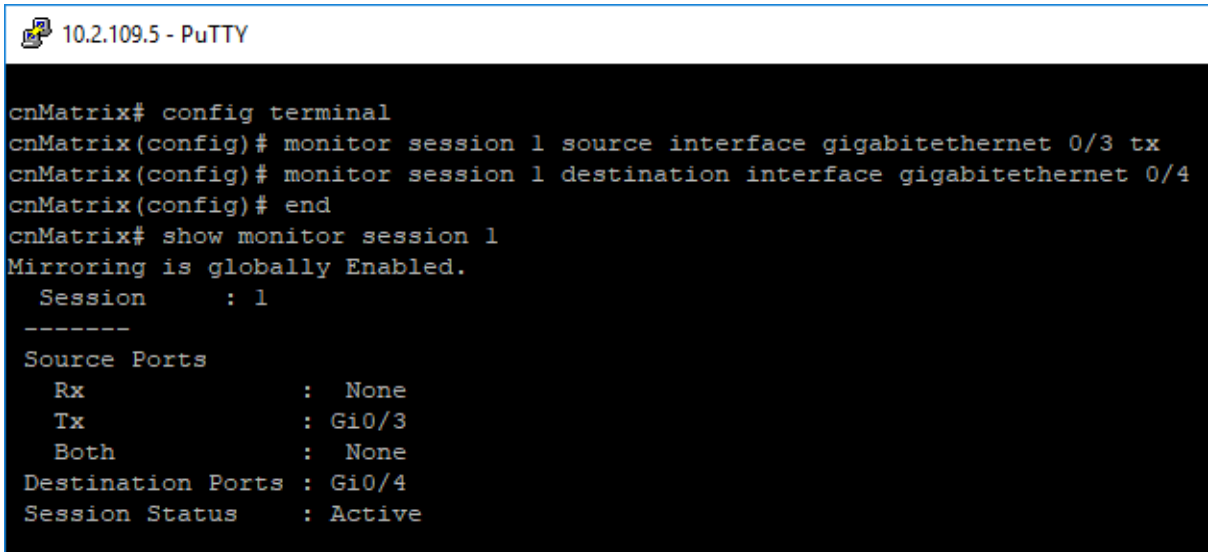
Destination port:

- Can be any Ethernet psysical port.
- Cannot be a source port.
- Cannot be an EtherChannel group.

Source port:

- Cannot be a destination port.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- Can be in the same or different VLANs.

2.10.2 Configuring Port Mirroring - Port Based in CLI Interface (Example)



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **monitor session 1 source interface gigabitethernet 0/3 tx** command into the terminal to configure the source for the mirroring session. Press the Enter key.

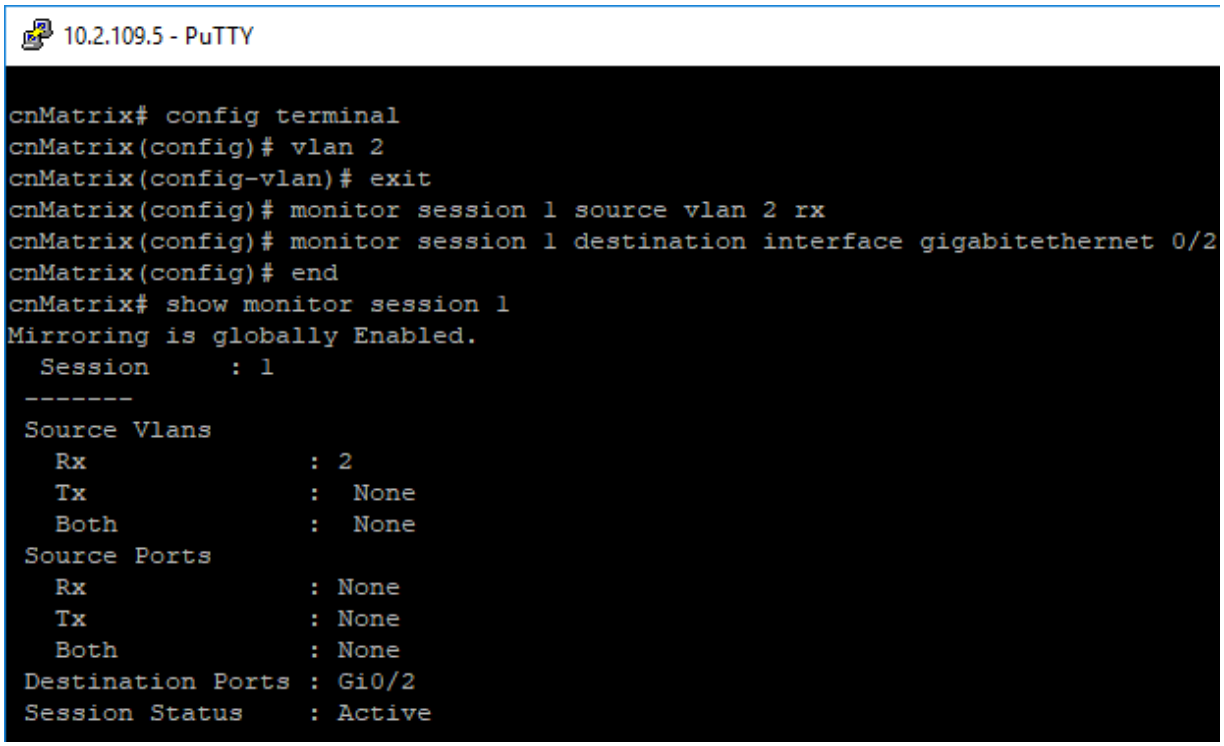
3 Type the **monitor session 1 destination interface gigabitethernet 0/4** command into the terminal to configure the source for the mirroring session. Press the Enter key.

4 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

5 Type the **show monitor session 1** command into the terminal to display the mirroring information. Press the Enter key.

For more information, see Port Mirroring Parameters and Commands.

2.10.3 Configuring Port Mirroring - VLAN Based in CLI Interface (Example)



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **vlan 2** command into the terminal to configure a VLAN. Press the Enter key.
3. Type the **exit** command into the terminal. Press the Enter key.
4. Type the **monitor session 1 source vlan 2 rx** command into the terminal to configure the source for the mirroring session. Press the Enter key.
5. Type the **monitor session 1 destination interface gigabitethernet 0/2** command into the terminal to configure the destination for the mirroring session. Press the Enter key.
6. Type the **end** command into the terminal to back to the Privileged EXEC mode. Press the Enter key.
7. Type the **show monitor session 1** command into the terminal. Press the Enter key.

For more information, see Port Mirroring Parameters and Commands.

2.10.4 Troubleshooting Port Mirroring

Useful commands for troubleshooting:

```
cnMatrix# show monitor session all
```

2.11 Storm Control

2.11.1 Managing Storm Control

Feature Overview

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broad-

cast, multicast, or unicast traffic storm on physical interfaces.

The traffic **storm control** (also called traffic suppression) feature has been added to monitor incoming traffic levels over a fixed interval, and during the interval it compares the traffic level with the traffic storm control level that you configure. Each port has a single traffic storm control level that is used for all types of traffic (broadcast, multicast, and unicast).

Standards

- N/A

Scaling Numbers

- N/A

Limitations

- Regardless of the value configured by the user in hardware, the actual configured value is rounded-down to the closest multiple of 640pkts/sec (for 100M speed), of 6400pkts/sec (for 1G speed) and for 64000pkts/sec (for 10G speed).

Default Values

- DLF Storm Control – Disabled by default.
- Broadcast Storm Control – Disabled by default.
- Multicast Storm Control – Disabled by default.

2.11.2 How to Enable Storm Control in CLI Interface

1 Type the **configure terminal** command into the terminal. Press the Enter key.

2 Type the **interface gigabitethernet 0/1** command into the terminal to select the interface to be configured. Press the Enter key.

3 Type the **storm-control broadcast level 100** command into the terminal to set the storm control rate for broadcast packets. Press the Enter key.

4 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

5 Type the **show interfaces gigabitethernet 0/1 storm-control** command into the terminal to display the interface status and configuration (verify if broadcast storm control is enabled). Press the Enter key.

For more information, see Storm Control Parameters and Commands.

2.12 Quality of Service

2.12.1 Managing QoS

QoS works in tight conjunction with the ACL module, which provides a way for the user to classify traffic using custom parameters and feed it to the QoS module.

The QoS module revolves about the concept of “class”. Traffic can be assigned to classes, based on the QoS information in the packet (dot1p priority or DSCP bits), based on per-port settings (default user-priority) or via an Access Control List (ACL). A policy can then be applied to that class to enforce a certain traffic profile. In the same manner, a meter can be applied to a class and have the corresponding traffic policed.

QoS provides means of doing the following:

- Traffic policing on ingress and egress
- Priority remarking - via priority maps or via traffic policers
- Class-based queueing and scheduling
- Traffic shaping
  - **Traffic policing** is a process applied to a flow of traffic that enforces configured parameters regarding the maximum throughput for that flow. In this context, a traffic flow is an ACL-based class, to which a policy containing a meter is applied. Traffic policing acts on ingress or egress traffic, according to the way the ACL was configured.

Feature Overview

A **meter** is used to classify packets into three conformance levels: Green, Yellow and Red. Traffic that is below the committed information rate is considered conforming, and marked as Green. Traffic that is over the committed information rate, but still conforming to a committed burst size is considered “exceeding” or yellow. Traffic non-conforming to the meter is called violating and it’s marked Red. The configured policy determines then what actions should be applied on the packet, depending on this conformance level: allow, remark its priority, or drop.

- **Priority remarking** allows packets to have their dot1p priority or IP DSCP priority field modified by being remapped to a “regenerated” value. When a packet has its dot1p priority remarked, it will be queued according to the new “regenerated” priority. Priority remarking is accomplished via a “priority map”, which is a system-wide setting, therefore, a configured priority map will be by default applied to all ports.

In order to configure which priority information should be used as an input for the QoS application and the priority remapping mechanism, the **qos trust mode** has to be selected. The user can configure QoS trust mode as none, in which case the packet is assigned the port’s default dot1p priority regardless of any priority information in the packet, or he can select dot1p and DSCP. This is a per-port setting.

Upon ingress, the switch needs to assign certain QoS properties to the packet. These properties will determine what policies will be assigned to the packet, and, in the end, which queue of the egress port will be used - how the packet will be scheduled, and which shapers will be applied.

These properties, which are initially assigned to the packet can be modified by configuring a class map, which will use either priority maps or ACLs (dot1p priorities can be changed at this stage, and a traffic class is assigned).

QoS properties can be re-assigned at the ingress stage by a policy map, which will use a meter to determine the packet's compliance to a configure rate, according to the packet's traffic class.

The user can configure which data the switch should use to determine the initial QoS properties of a packet:

- setting the trust mode to **dot1p** indicates that if a frame includes both 802.1p and a DSCP

field, then the pbit field takes precedence. If the frame doesn't include a 802.1p field, the ingress port's priority is used to determine the packet's QoS properties.

- setting the trust mode to **DSCP** indicates that if a frame includes both 802.1p and a DSCP field, then the DSCP field takes precedence. For non-IP packets, the ingress port's priority is used to determine the packet's QoS properties.
- setting the trust mode to **None** indicates that the content of the frame is ignored, and the QoS properties of the packet are assigned by using the ingress port's default priority.

The cnMatrix switch supports eight **egress queues**. By default, traffic marked with dot1p priority 0 is mapped to queue 1, priority 1 to queue 2, and so on. Default queue assignment can be changed using the "queue-map" command. A priority map can be used to send a specific class of traffic to a particular egress queue without actually remapping the dot1p priority value. In this case, the ingress priority must be the same as the regenerated priority.

- A **scheduler** is an algorithm that decides the sequence in which frames from different egress queue should be forwarded. Four types of scheduling algorithms are supported: strict-priority, round robin, weighted round robin, and strict-wrr.

- **Traffic shaping** is an algorithm that controls the sending of frames, by inserting delays, in such a way that the output bandwidth conforms to a configured traffic profile. The switch uses a token bucket shaper with CIR and CBS parameters to compare outgoing traffic to.

In order for the packet to be taken out of a transmit queue and to be forwarded, a packet has to be scheduled for transmission by the scheduler and to conform to the shaper attributes. Non-conforming packets remain queued until they will conform, even when the link is available for transmission.

Standards

- RFC 2474 defines the differentiated services field in the IP header.
- IEEE 802.1D incorporates the 802.1p definition of the user priority field.
- RFC 2697 defines srTCM (single rate Three Color Marker).
- RFC 2698 defines trTCM (two rate Three Color Marker).

Scaling Numbers

- Up to 120 classes can be defined.

Limitations

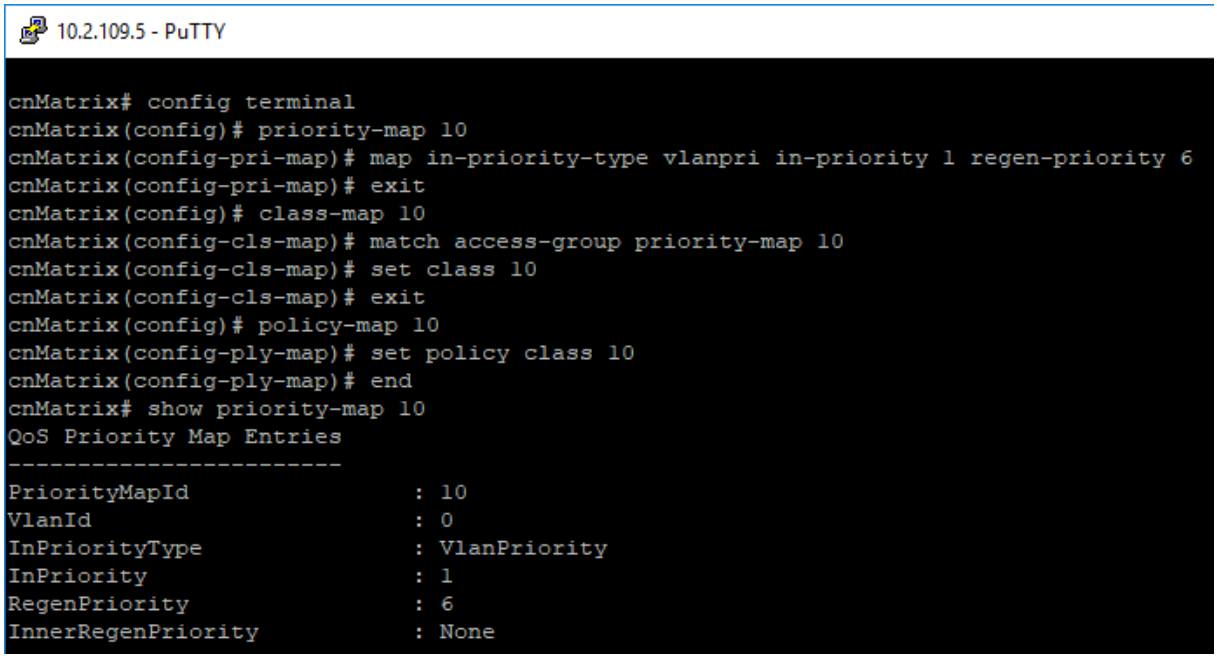
- Although DSCP remarking is supported with the priority-map, mapping of the traffic to the updated queue is not supported, and all remarked priority packets will be transmitted via queue 1 only.
- Traffic policing is not supported for classes that use priority maps.
- Two types of meters are supported: srTCM and trTCM.
- Four types of scheduling algorithms are supported: strict-priority, round robin, weighted round robin, strict-wrr.
- The WRR scheduler will not be effective if we send multiple priority traffic from same port. However, if multiple ports are sending traffic with unique priority traffic then the WRR scheduling works as per the configured weights.
- Remarking of flows under violate actions is not supported.
- Shapers support only CIR and CBS parameters.
- Modifying the Queue weight is applicable to all the ports where the scheduler is mapped.
- Priority maps are only applied to trusted interfaces. For untrusted interfaces, the initial QoS properties of the packet can be changed only by the use of ACL rules.

Default Values

- There are eight egress queues for every port, the default scheduling algorithm is strict-

priority. Queue 1 is the top priority queue.

2.12.2 Remarking with Priority Maps (QoS)



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **priority-map 10** command into the terminal to add a priority map entry. Press the Enter key.

3 Type the **map in-priority-type vlanpri in-priority 1 regen-priority 6** command into the terminal (mapping incoming priority to regen priority). Press the Enter key.

4 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

5 Type the **class-map 10** command into the terminal to add a class map. Press the Enter key.

6 Type the **match access-group priority-map 10** command into the terminal to set class map parameters. Press the Enter key.

7 Type the **set class 10** command into the terminal to set class for L2 and/or L3. Press the Enter key.

8 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

9 Type the **policy-map 10** command into the terminal to create a policy map. Press the Enter key.

10 Type the **set policy class 10** command into the terminal to set class for policy. Press the Enter key.

11 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

12 Type the **show priority-map 10** command into the terminal to display the priority map entries. Press the Enter key.

For more information, see QoS Parameters and Commands.

2.12.3 Remarking with ACL (QoS)

10.2.109.5 - PuTTY

```
cnMatrix(config-ext-nacl)# exit
cnMatrix(config)# interface gi 0/1
cnMatrix(config-if)# ip access-group 1001 in
cnMatrix(config-if)# exit
cnMatrix(config)# class-map 11
cnMatrix(config-cls-map)# match access-group ip-access-list 1001
cnMatrix(config-cls-map)# set class 11
cnMatrix(config-cls-map)# exit
cnMatrix(config)# policy-map 11
cnMatrix(config-ply-map)# set policy class 11 default-priority-type dot1P 7 0
cnMatrix(config-ply-map)# end
cnMatrix# show access-lists ip 1001

Extended IP Access List 1001
----------------------------
 Filter Priority                 : 1
 Filter Protocol Type            : TCP
 IP address Type                 : IPV4
 Source IP address               : 0.0.0.0
 Source IP address mask          : 0.0.0.0
 Source IP Prefix Length         : 0
 Destination IP address          : 0.0.0.0
 Destination IP address mask     : 0.0.0.0
 Destination IP Prefix Length    : 0
 Flow Identifier                 : 0
 In Port List                    : Gi0/1
 Out Port List                   : NIL
 Filter TOS                      : NIL
 Filter DSCP                     : NIL
 Filter Source Ports From        : 0
 Filter Source Ports Till        : 65535
 Filter Destination Ports From   : 443
 Filter Destination Ports Till   : 443
 Service Vlan                    : 0
 Service Vlan Priority           : None
```

1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **ip access-list extended 1001** command into the terminal. Press the Enter key.
3. Type the **permit tcp any any eq 443** command into the terminal to specify the TCP packets to forward based on the associated parameters. Press the Enter key.
4. Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
5. Type the **interface gi 0/1** command into the terminal to specidy the interface to be configured. Press the Enter key.
6. Type the **ip access-group 1001 in** command into the terminal to apply ACL on inbound packets. Press the Enter key.
7. Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
8. Type the **class-map 11** command into the terminal to add a class map entry. Press the

Enter key.

9 Type the **match access-group ip-access-list 1001** command into the terminal to set the L3 class map ID. Press the Enter key.

10 Type the **set class 11** command into the terminal to set class. Press the Enter key.

11 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

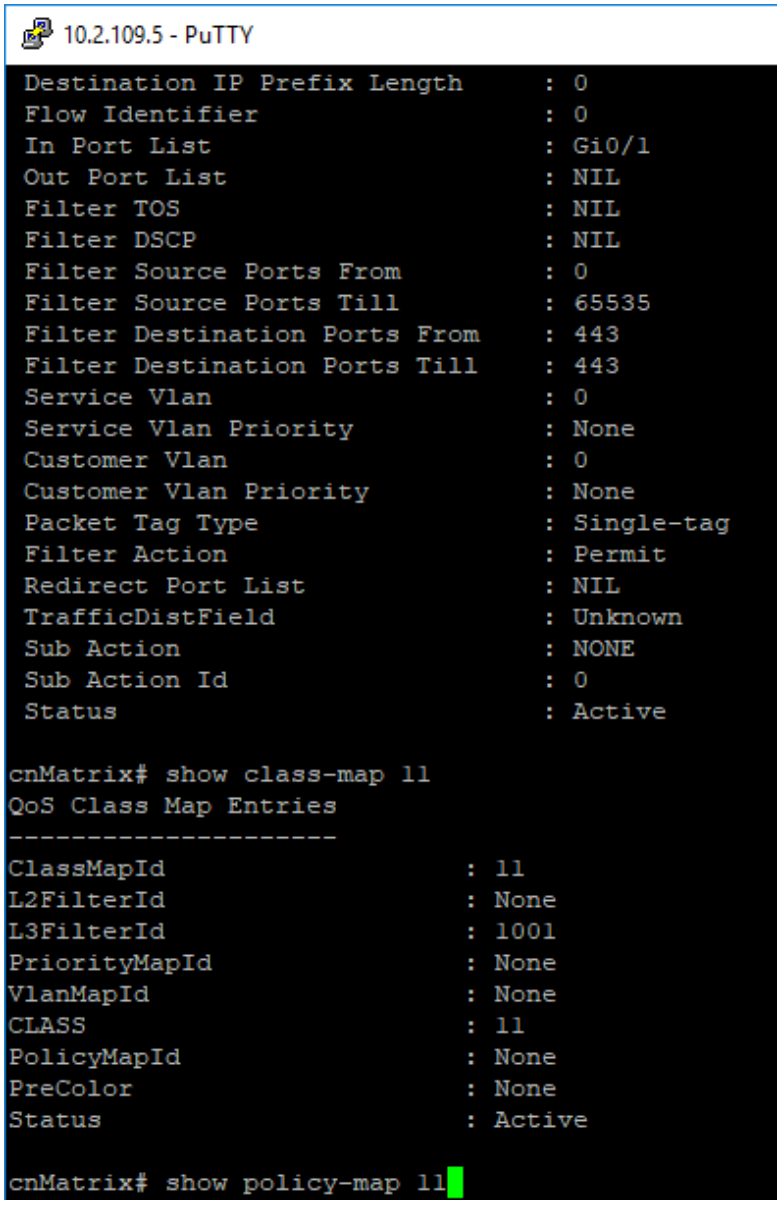
12 Type the **policy-map 11** command into the terminal to create a policy map. Press the Enter key.

13 Type the **set policy class 11 default-priority-type dot1P 7 0** command into the terminal. Press the Enter key.

14 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

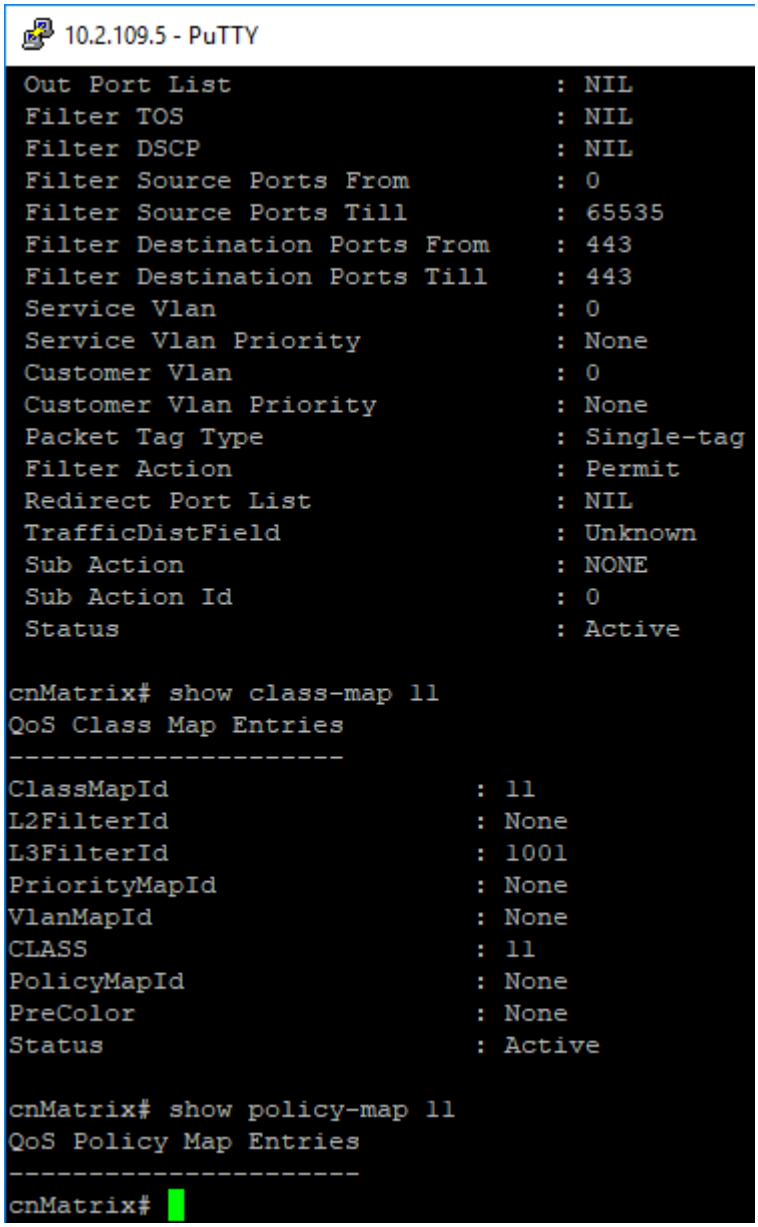
15 Type the **show access-lists ip 1001** command into the terminal to display the access lists configuration. Press the Enter key.

16 Press the Space key.



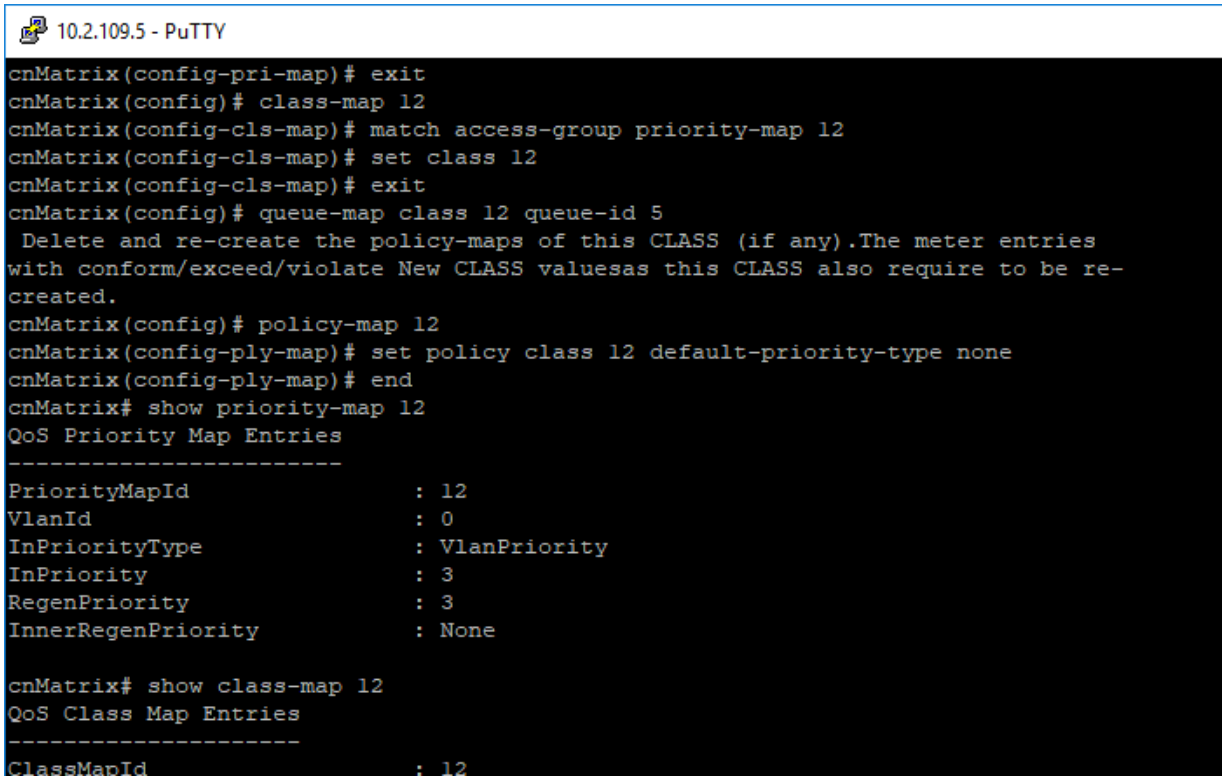
17 Type the **show class-map 11** command into the terminal to display the QoS class map entries. Press the Enter key.

18 Type the **show policy-map 11** command into the terminal to display the QoS policy map entries. Press the Enter key.



For more information, see QoS Parameters and Commands.

2.12.4 Queue Map(QoS)



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **priority-map 12** command into the terminal to add the priority map ID. Press the Enter key.

3 Type the **map in-priority-type vlanPri in-priority 3 regen-priority 3** command into the terminal to set the incoming priority and the regenerated priority. Press the Enter key.

4 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

5 Type the **class-map 12** command into the terminal to add a class map ID. Press the Enter key.

6 Type the **match access-group priority-map 12** command into the terminal to associate the priority map 12 to class map 12. Press the Enter key.

7 Type the **set class 12** command into the terminal to set the traffic class. Press the Enter key.

8 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

9 Type the **queue-map class 12 queue-id 5** command into the terminal to create a map for a queue with class 12 (previously created class). Press the Enter key.

10 Type the **policy-map 12** command into the terminal to create a policy map with ID=12. Press the Enter key.

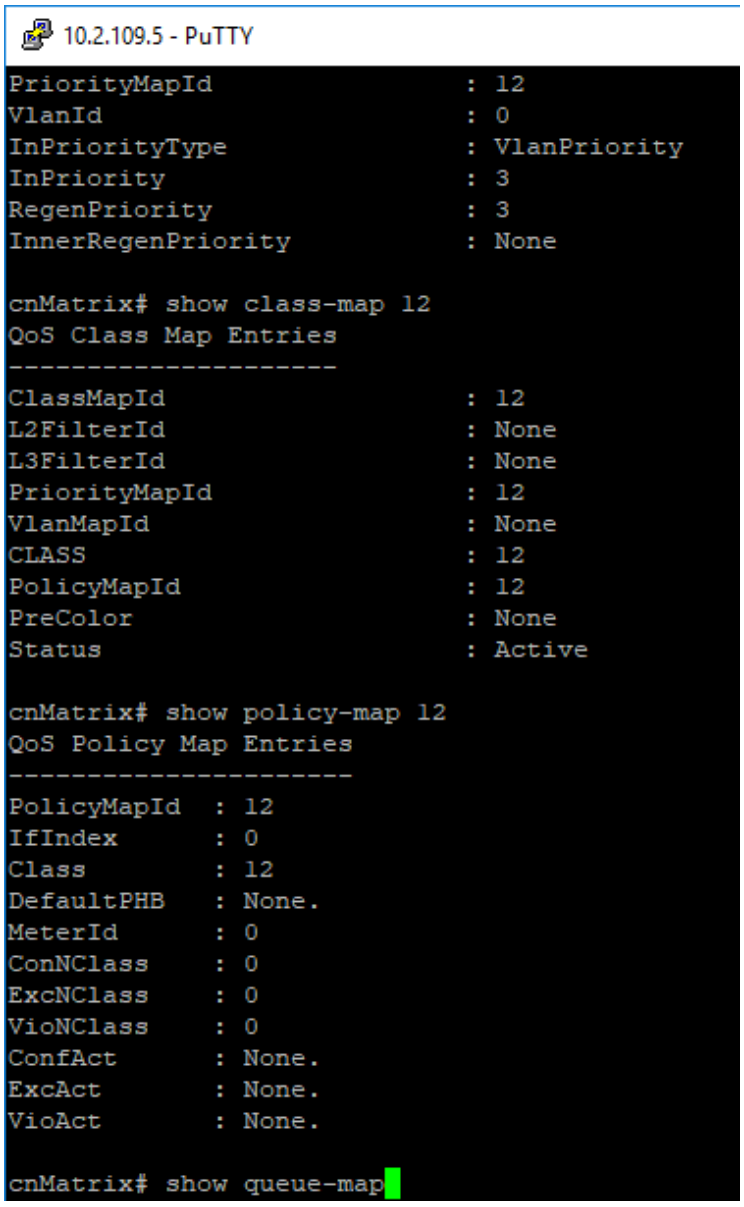
11 Type the **set policy class 12 default-priority-type none** command into the terminal to set class for priorirty with a none per-hop behavior type . **Press the Enter key.**

12 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

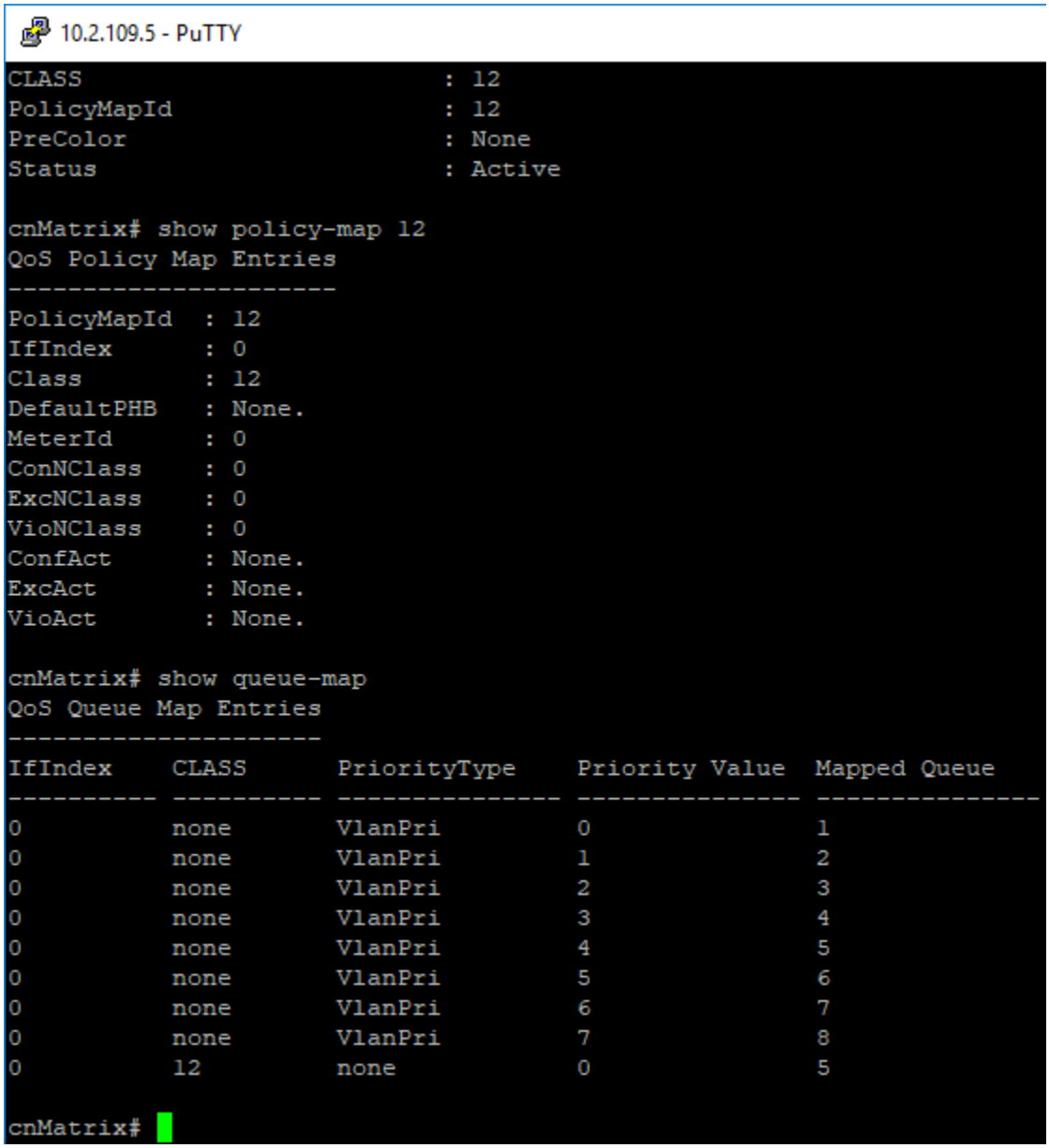
13 Type the **show priority-map 12** command into the terminal to display the priority map entries. Press the Enter key.

14 Type the **show class-map 12** command into the terminal to display the class map entries. Press the Enter key.

15 Type the **show policy-map 12** command into the terminal to display the policy map entries. Press the Enter key.

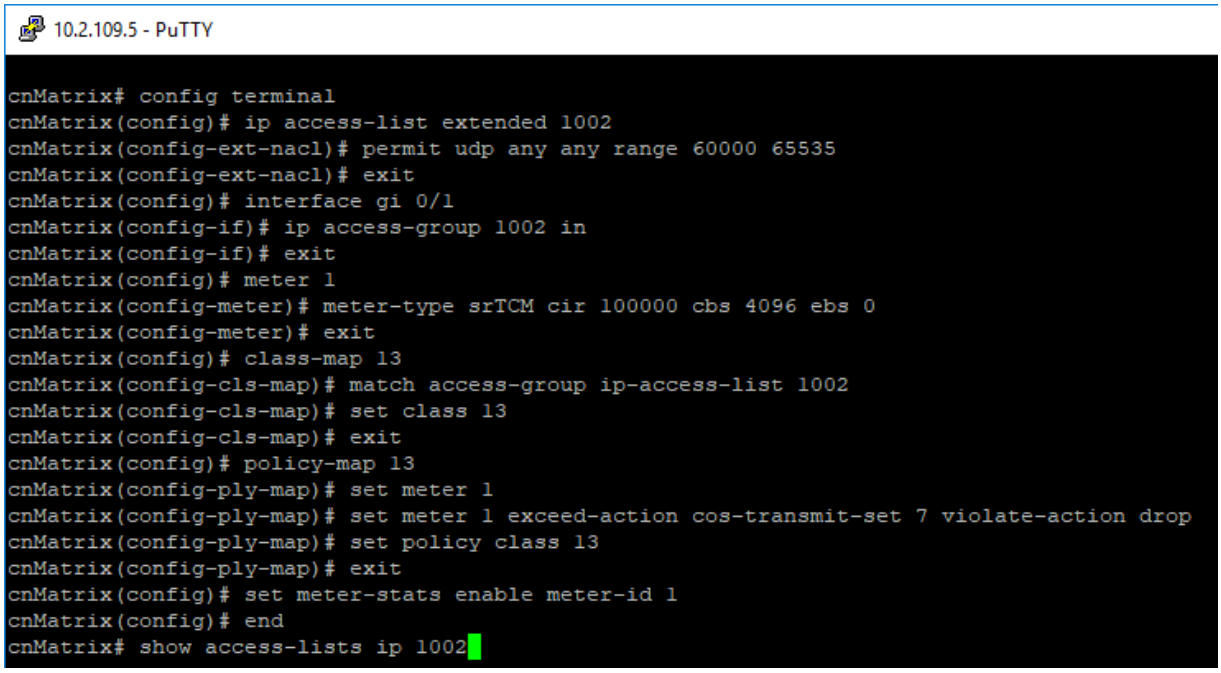


16 Type the **show queue-map** into the terminal to display the queue map entries. Press the Enter key.



For more information, see QoS Parameters and Commands.

2.12.5 Ingress Metering with ACL +Enable Metering(QoS)



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **ip access-list extended 1002** command into the terminal to create an IP access-list. Press the Enter key.

3 Type the **permit udp any any range 60000 65535** command into the terminal to specify the UDP port range of the packets to be allowed . Press the Enter key.

4 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

5 Type the **interface gi 0/1** command into the terminal to select the interface to be configured. Press the Enter key.

6 Type the **ip access-group 1002 in** command into the terminal to enable IP access control list on the interface. Press the Enter key.

7 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

8 Type the **meter 1** command into the terminal to create a meter and to go to the configuration-meter mode. Press the Enter key.

9 Type the **meter-type srTCM cir 100000 cbs 4096 ebs 0** command into the terminal to set the meter type as single rate three color marker metering and the committed information size as 100000, the committed burst size as 4096 and the excess burst size as 0. Press the Enter key.

10 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

11 Type the **class-map 13** command into the terminal to add a class map ID and to go to the config-cls-map mode. Press the Enter key.

12 Type the **match access-group ip-access-list 1002** command into the terminal to associate the IP access control list 1002 to class map 13. Press the Enter key.

13 Type the **set class 13** command into the terminal to set the traffic class. Press the Enter key.

14 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

15 Type the **policy-map 13** command into the terminal to create a policy map with ID=13 and to go to the config-ply-map mode. Press the Enter key.

16 Type the **set meter 1** command into the terminal to specify the policy meter to be applied by the policy to the class of traffic. Press the Enter key.

17 Type the **set meter 1 exceed-action cos-transmit-set 7 violate-action drop** command into the terminal to configure the action to be performed on the packet, the VLAN priority of the out-going packets as 7 and the action to be performed on the packet, when the packets are found to be out of profile as drop. Press the Enter key.

18 Type the **set policy class 13** command into the terminal to set class for policy. Press the Enter key.

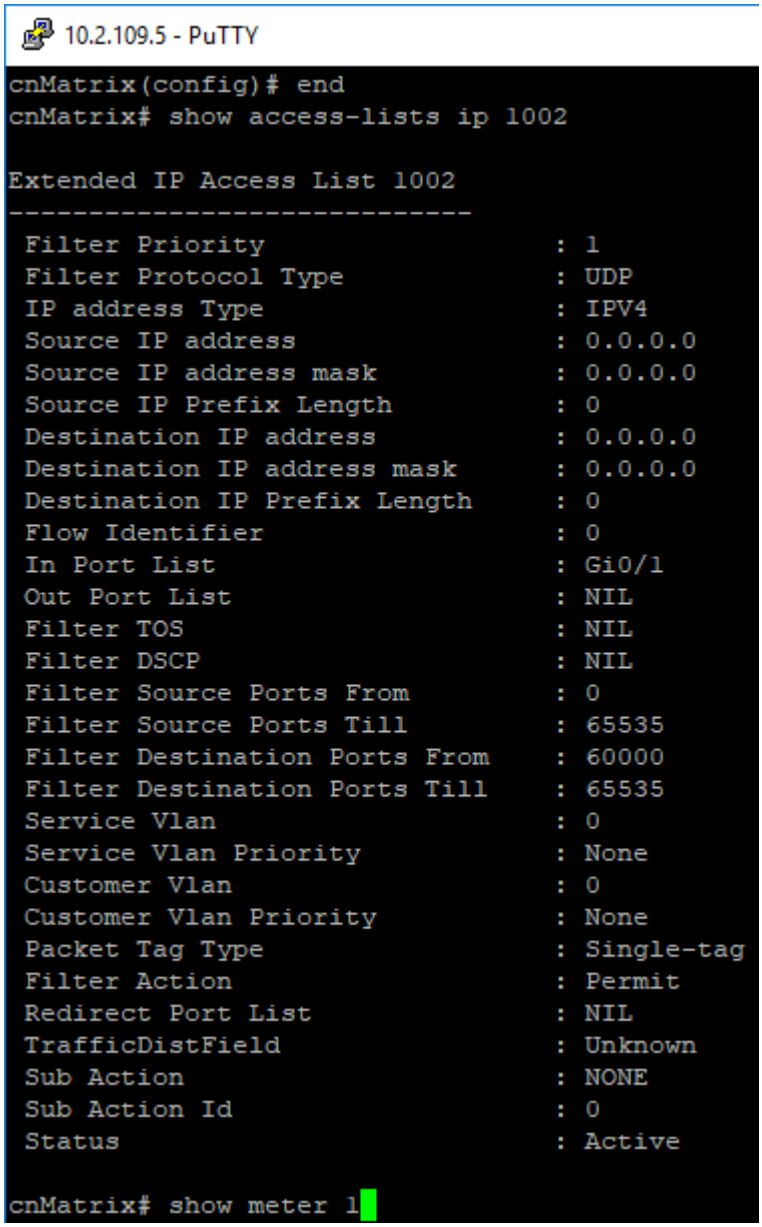
19 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

20 Type the **set meter-stats enable meter-id 1** command into the terminal. Press the Enter key.

Note: **Starting with version 2.1**, this command has been removed because the meters stats are now enabled by default.

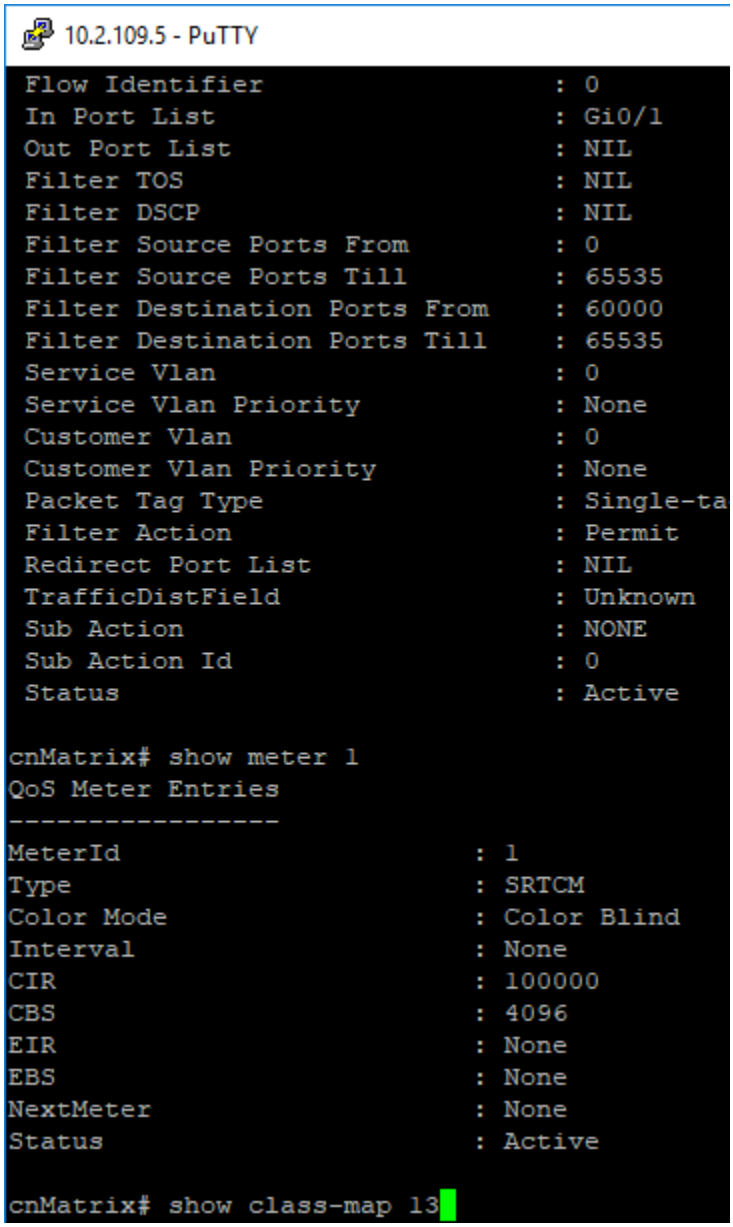
21 Type the **end** into the terminal to go to the Privileged EXEC mode. Press the Enter key.

22 Type the **show access-lists ip 1002** command into the terminal to display the configured IP access list. Press the Enter key.

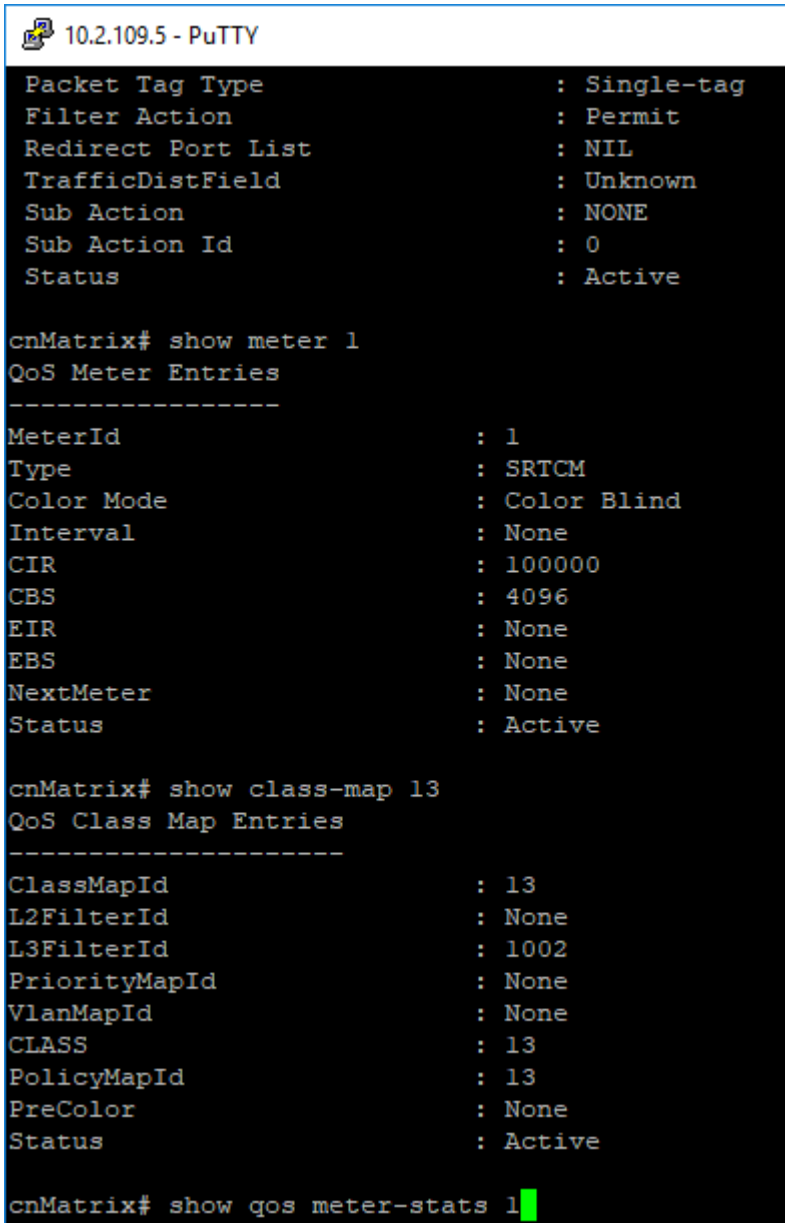


23 Press the Space key.

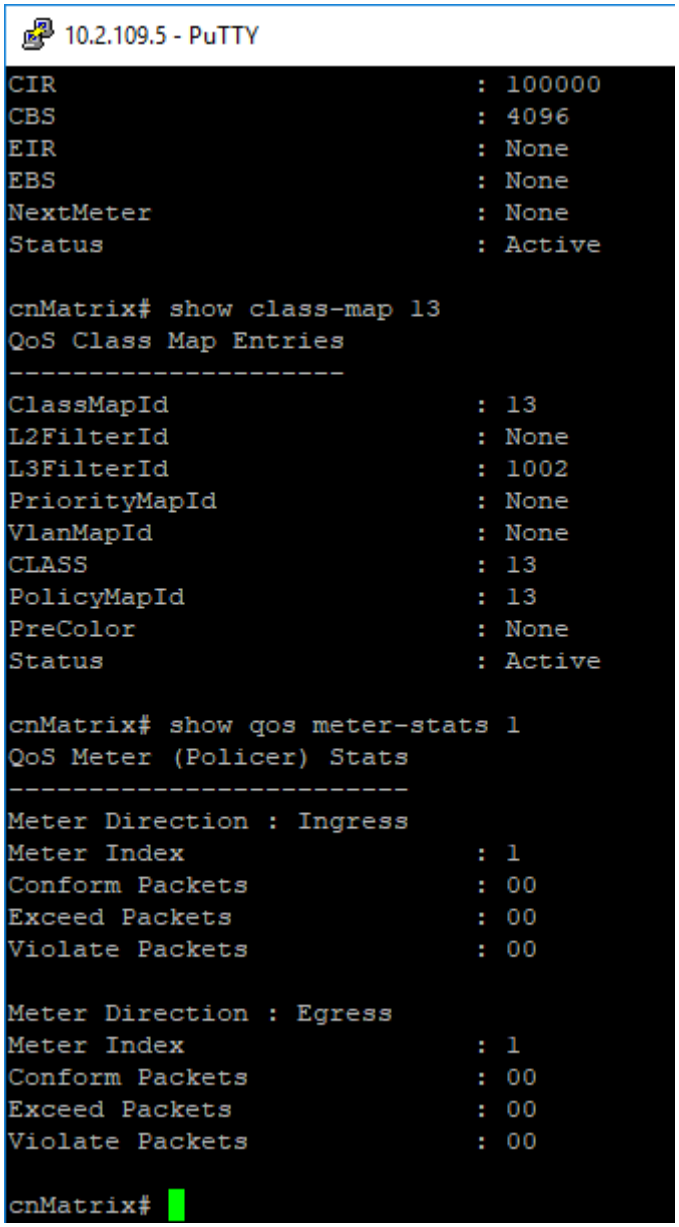
24 Type the **show meter 1** command into the terminal to display the QoS meter entries. Press the Enter key.



25 Type the **show class-map 13** command into the terminal to display the class map entries. Press the Enter key.

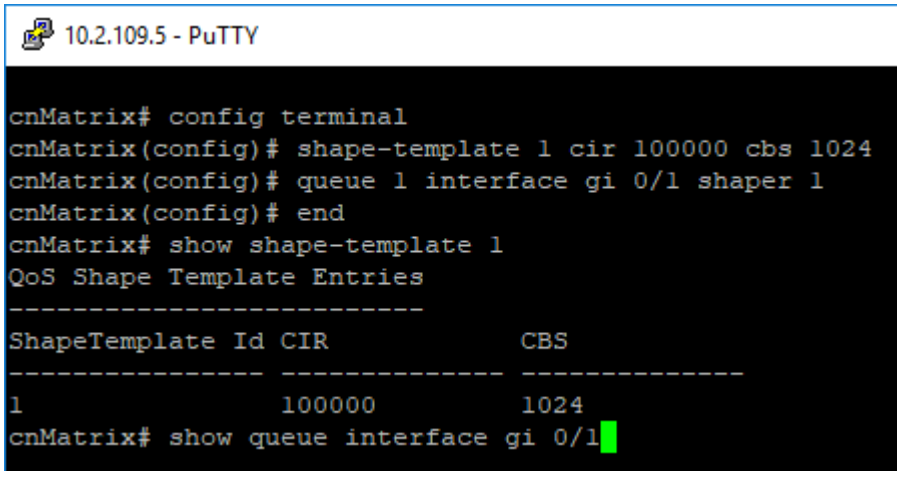


26 Type the **show qos meter-stats 1** command into the terminal to display the meter (policer) stats. Press the Enter key.



For more information, see QoS Parameters and Commands.

2.12.6 Queues + Shapers (QoS)



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **shape-template 1 cir 100000 cbs 1024** command into the terminal to create a

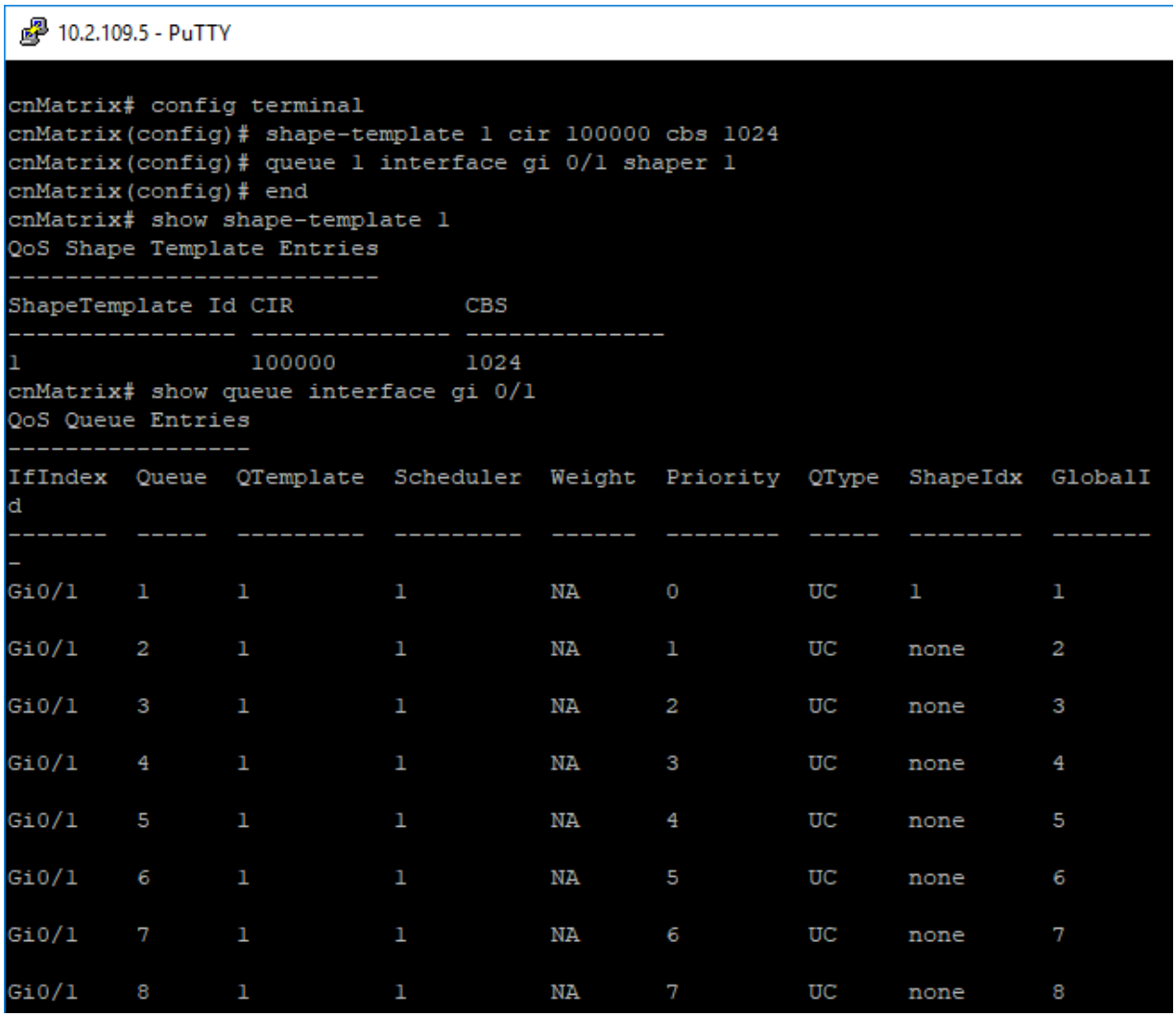
shape template , to set the committed information rate for packets through the queue in Kbps and to set the committed burst size for packets through the queue. Press the Enter key.

3 Type the **queue 1 interface gi 0/1 shaper 1** command into the terminal to create a queue and to set the shaper that specifies the bandwidth requirements for the scheduler. Press the Enter key.

4 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

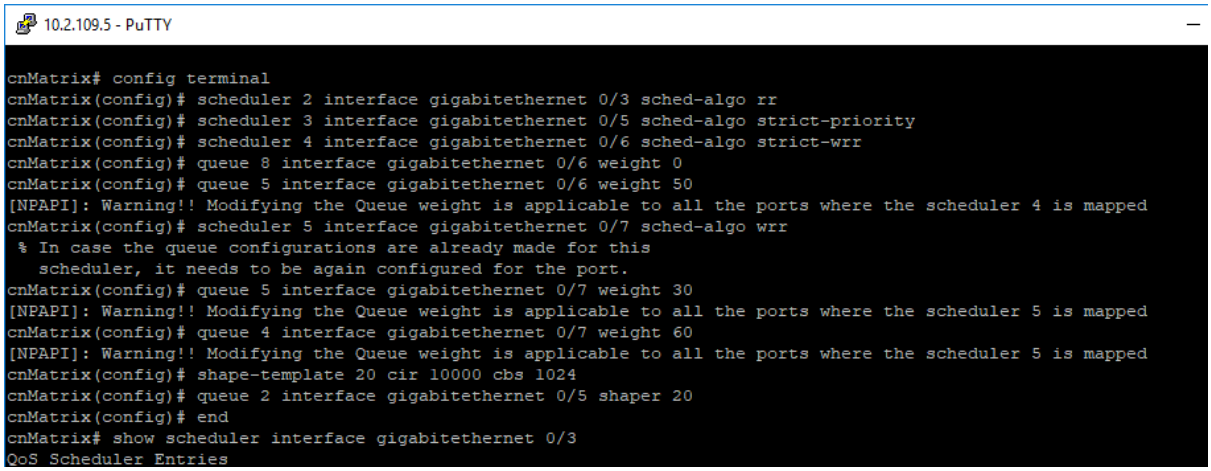
5 Type the **show shape-template 1** command into the terminal to display the shape template configuration. Press the Enter key.

6 Type the **show queue interface gi 0/1** command into the terminal to display the queue entries for a specific configured interface. Press the Enter key.



For more information, see QoS Parameters and Commands.

2.12.7 Configuring Schedulers (QoS)

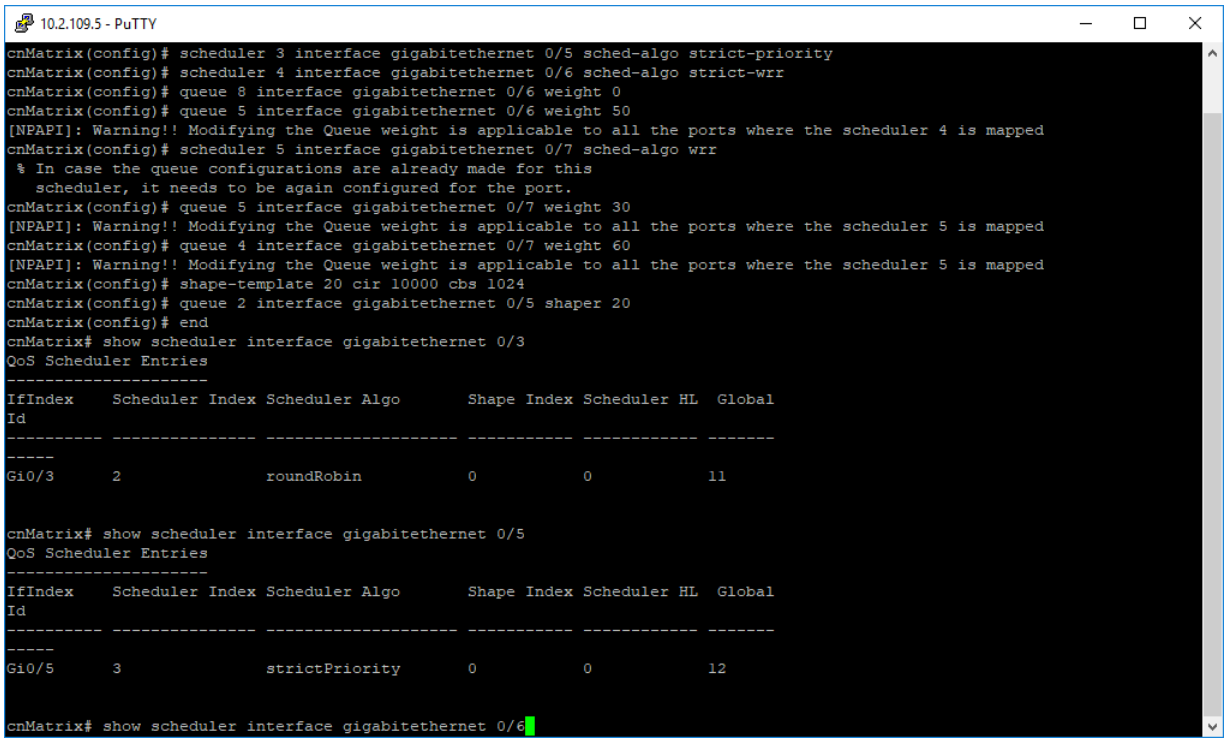


1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **scheduler 2 interface gigabitethernet 0/3 sched-algo rr** command into the terminal to create the scheduler 2 on a certain interface and to configure the packet scheduling algorithm as round robin. Press the Enter key.
3. Type the **scheduler 3 interface gigabitethernet 0/5 sched-algo strict-priority** command into the terminal to create the scheduler 3 on a certain interface and to configure the packet scheduling algorithm as strict scheduling. Press the Enter key.
4. Type the **scheduler 4 interface gigabitethernet 0/6 sched-algo strict-wrr** command into the terminal to create the scheduler 4 on a certain interface and to configure the packet scheduling algorithm as weighted round robin. Press the Enter key.
5. Type the **queue 8 interface gigabitethernet 0/6 weight 0** command into the terminal to set the weight to the configured scheduling algorithm. Press the Enter key.

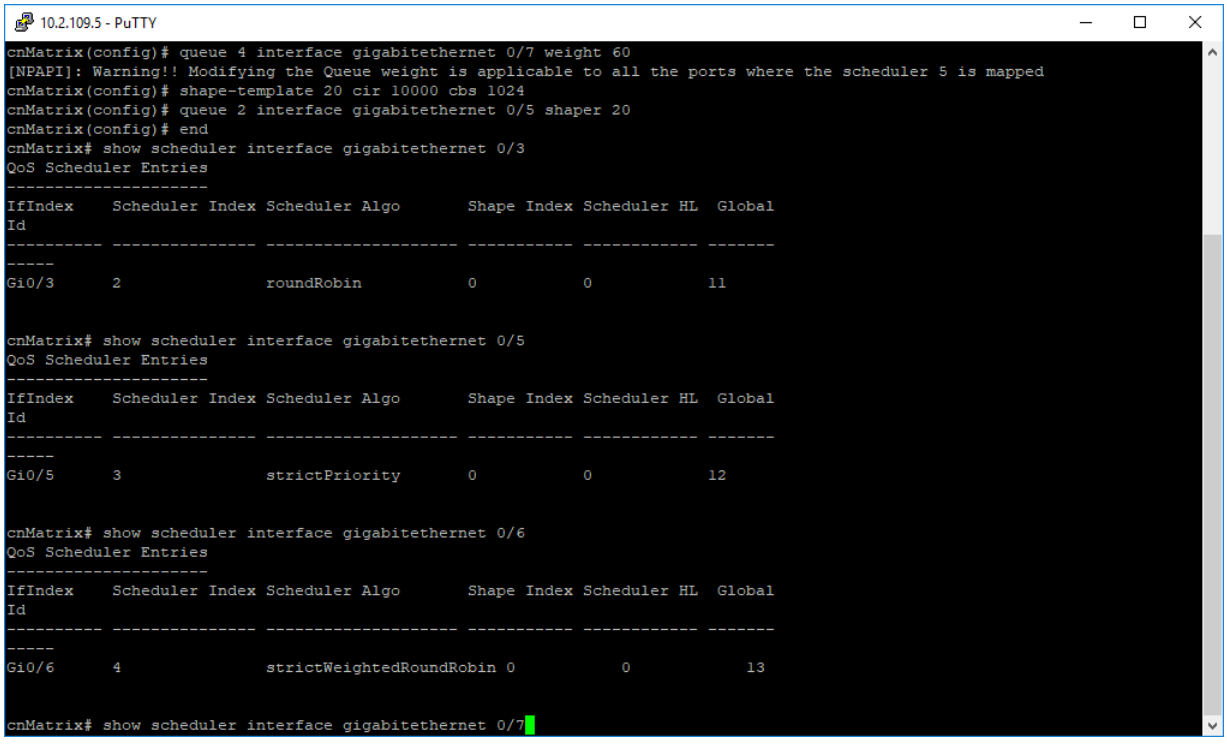
> Note: The weight parameter can only be configured for weighted round robin and strict weighted round robin algorithms.

6. Type the **queue 5 interface gigabitethernet 0/6 weight 50** command into the terminal. Press the Enter key.
7. Type the **scheduler 5 interface gigabitethernet 0/7 sched-algo wrr** command into the terminal. Press the Enter key.
8. Type the **queue 5 interface gigabitethernet 0/7 weight 30** command into the terminal. Press the Enter key.
9. Type the **queue 4 interface gigabitethernet 0/7 weight 60** command into the terminal. Press the Enter key.
10. Type the **shape-template 20 cir 10000 cbs 1024** command into the terminal. Press the Enter key.
11. Type the **queue 2 interface gigabitethernet 0/5 shaper 20** into the terminal. Press the Enter key.
12. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
13. Type the **show scheduler interface gigabitethernet 0/3** into the terminal to display the configured scheduler for interface gi 0/3 . Press the Enter key.

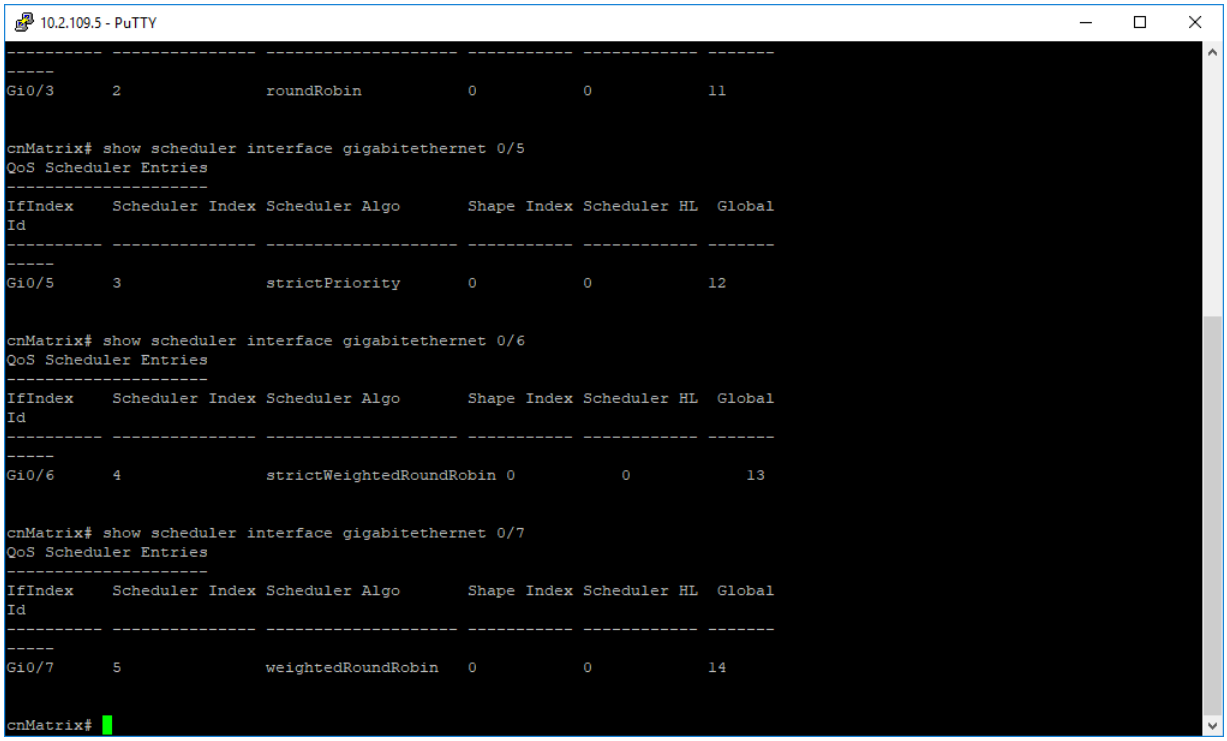
14 Type the **show scheduler interface gigabitethernet 0/5** command into the terminal. Press the Enter key.



15 Type the **show scheduler interface gigabitethernet 0/6** command into the terminal. Press the Enter key.



16 Type the **show scheduler interface gigabitethernet 0/7** command into the terminal. Press the Enter key.



For more information, see QoS Parameters and Commands.

2.13 Rate Limit Output

2.13.1 Managing Rate-Limit-Output

The **Rate-Limit-Output** feature enables the rate limiting and burst size rate. Burst size is the actual amount of “burstable” data that is allowed to be transmitted at the peak bandwidth rate in kilobytes. You can set the limit by configuring the egress packet rate of an interface.

Standards

N/A

Scaling Numbers

N/A

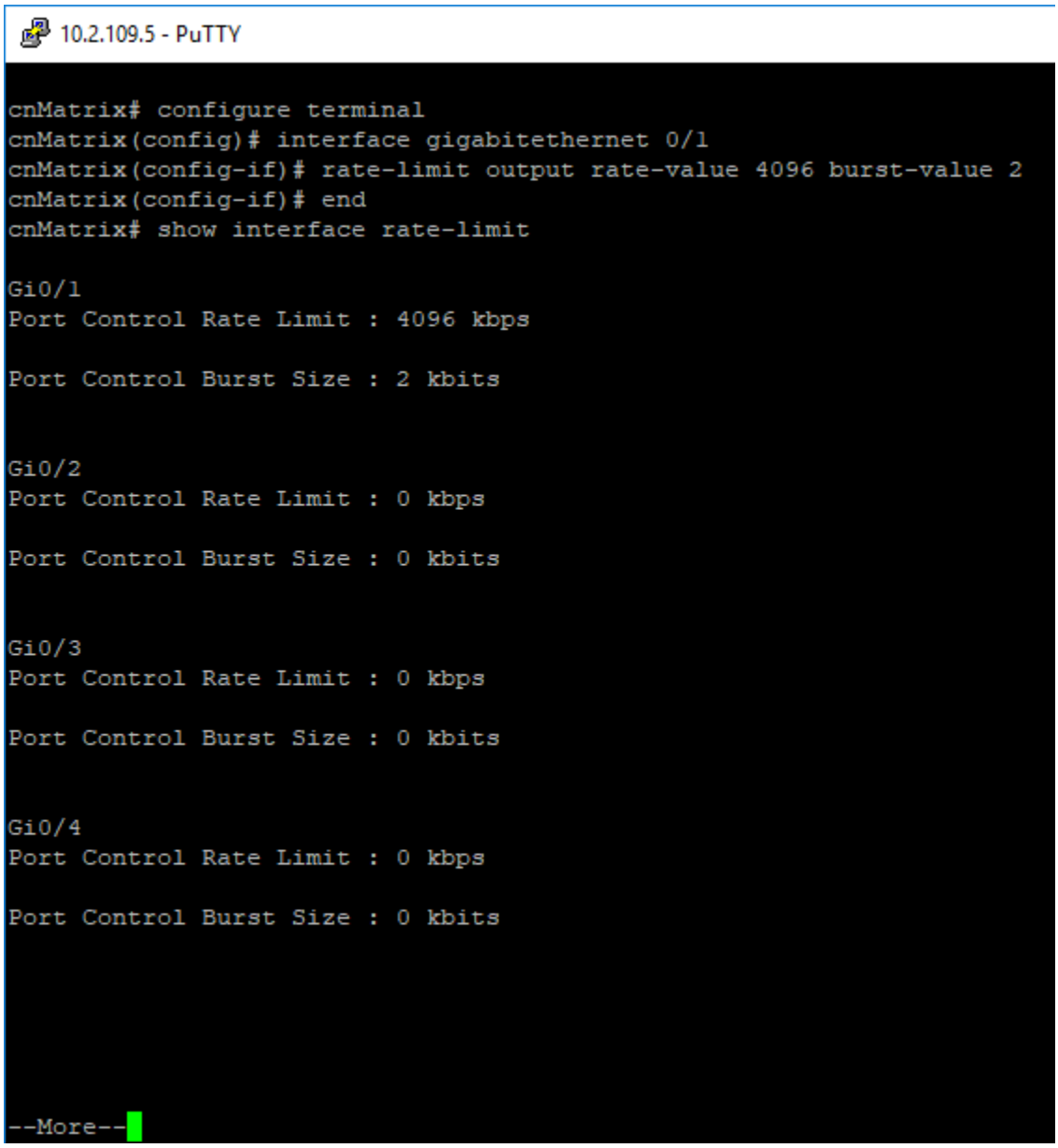
Limitations

N/A

Default Values

- The default value for rate and burst value: 0.

2.13.2 Configuring Rate-Limit-Output in CLI Interface (Example)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select the interface to be configured. Press the Enter key.
3. Type the **rate-limit output rate-value 4096 burst-value 2** command into the terminal to configure the rate limiting and the burst packet rate for the interface. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show interface rate-limit** into the terminal to display the interface status and configurations (verify if rate limit and burst size are displayed in the output with the previously configured values). Press the Enter key.

2.14 Policy-Based Automation with Dynamic Configuration

2.14.1 Managing Policy Based Automation Using Auto Attach

2.14.1.1 Feature Description

Feature Overview

The core goal of the Auto Attach (AA) feature is to support automated device deployment at the network edge for networks with a high number of directly attached devices, such as Access Points (APs), video cameras, IP phones and laptops/PCs.

A typical deployment scenario would consist of the following components:

- Access (access/hybrid-mode edge) switch ports.
- Uplink (trunk-mode) ports/LAGs.
- End-devices (APs, video cameras, IP phones, laptops/PCs).

This type of deployment can be handled by manually configuring the network access switch through management interfaces such as CLI, HTTP (web) or SNMP. This type of configuration is static and requires knowledge of the network topology ahead of time, such as which ports are associated with specific VLANs, the related native VLAN (i.e., PVID) and egress tagging mode for each VLAN. A static configuration requires continuous and error-prone manual configuration updates when devices are moved or new devices are added to the network (i.e., for all device moves, adds and changes).

The Auto Attach feature is intended to overcome the burden of constant manual reconfiguration. With Auto Attach, end-devices are automatically detected based on specific device criteria (e.g., LLDP device identification data) and device-specific settings are automatically installed or updated based on predefined Auto Attach policies.

Settings that may be updated based on device discovery include:

- VLAN presence and membership.
- Switch port mode (Access/Hybrid/Trunk).
- Port Native VLAN (PVID) value.

When an end-device is detected on a port, AA is passed the device data (e.g., LLDP-based device data) and the ingress port. If the end-device data matches device identification criteria in a configured AA policy, the associated AA policy actions are initiated, potentially creating VLANs and dynamically updating settings associated with the ingress port (i.e., conditioning the ingress data path).

The automatically applied settings are dynamic and are cleared (with the previous settings restored) when the end-device disconnects, device identification data expires (e.g., LLDP data timeout) or when the switch reboots.

Auto Attach Release 2.0.1 Capabilities

- Device Identification
  - LLDP Core TLVs (user-specified string matching of TLV data):
    - Chassis ID (TLV Type 1)
    - Port ID (TLV Type 2)
    - Port Description (TLV Type 4)
    - System Name (TLV Type 5)
    - System Description (TLV Type 6)
    - System Capabilities (TLV Type 7)
- Dynamic Actions
  - VLAN creation and port association.

- Port PVID update.
- Switch port mode (Hybrid only) update.

- AA Monitoring/Configuration
  - CLI
  - SNMP

Limitations

User Interface Limitations:

- **Starting with version 2.1**, the Auto Attach feature can be configured in Web GUI.
- No support for cnMaestro GUI and JSON files. Templates will be available in the first release and CLI commands can be pushed down to the switch.

Feature Interaction Limitations:

- Interactions with authentication (EAP) support are not supported.
- Setting the port as QoS Trusted/Untrusted is not supported.
- Setting the port default 802.1 User Priority is not supported.
- Auto Attach agent cannot run while Spanning Tree mode PVRST is enabled.

Feature Limitations:

- MAC-based device detection is not supported.
- Only core LLDP TLVs will be supported for device discovery.
- AA policies will not be applied to port channels in the first release.
- Switch port mode updates will be limited to 'hybrid' in the first release and updates will be static if data is saved by the user while dynamic updates are present.
- **Starting with version 2.1**, the following enhancements have been implemented for the **Policy Based Automation** feature:
  - Support for the standard Management Address TLV is available.
  - Device detection based on the MAC address data is supported.
  - With the initial cnMatrix release 2.0, administrator operations may supersede PBA-associated (i.e., dynamic) actions. For example, an administrator can manually update dynamic VLAN associations or update a PVID if required. PBA will not block administrator requests. Starting with cnMatrix version 2.1, the administrator can no longer alter most settings that have been updated by PBA. Administrator operations on ports that are associated with an active PBA policy are limited to those not potentially under PBA control. This means that VLAN membership updates are blocked as are PVID and switch port mode modifications. Furthermore, VLANs that are dynamically created though PBA operations are owned by PBA and can't be manipulated (e.g., deleted, associated with other ports) by the user. Administrator modifications to these settings are permitted once PBA settings are cleared from the port.
  - Traffic associated with the PVID egresses the switch as untagged traffic (i.e., the port is made an untagged member of the VLAN).
  - PBA support for all switch port mode options (i.e., Access/Hybrid/Trunk) and dynamic switch port mode updates is available. The PBA support for transitioning to/from Access and Trunk port modes has the following restrictions/behavior:

    ==>Access
  - Action data with a single VLAN and a matching PVID value must also be specified.
  - All VLANs associated with the applied PBA policy interface are removed (only the single action VLAN is associated with the port) while the policy is active. The removed VLAN memberships are reinstated when the PBA policy is no longer active on the port.

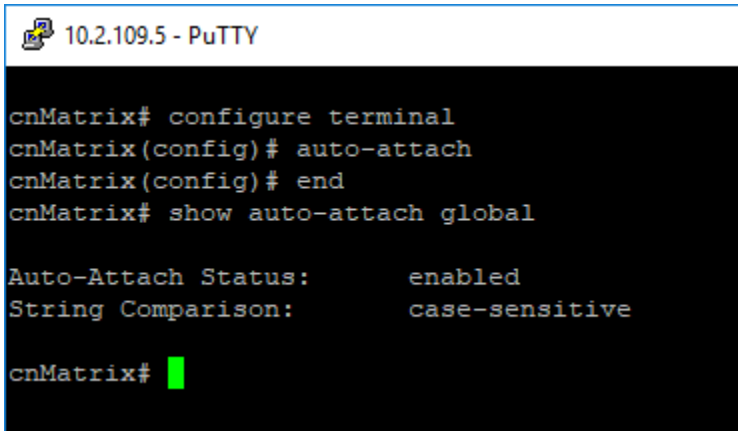
    ==>Trunk

- Action data can include a VLAN list. A PVID can't be specified.
- The QoS Trust mode (i.e., Trust 802.1p/Trust DSCP/Untrusted) for a port can be updated based on device discovery. The QoS Trust mode setting is restored to the previous statically configured value during the device cleanup phase.
- The default port 802.1p user priority value (0 to 7) can be updated based on device discovery. The default port 802.1p user priority value setting is restored to the previous statically configured value during the device cleanup phase.
- The administrator can identify up to four device ports to act as PBA uplinks. VLANs (newly created or existing) that are applied to the port on which the matching device was detected are also associated with the uplink ports. The VLAN membership update remains in effect while the related PBA policy is active. Uplink ports must be operating in hybrid switch port mode to be valid. Uplinks are identified using the interface type and the slot/port naming convention (e.g., 'Gi0/5,Ex0/1'). An action that includes uplink data must also include VLAN data for port membership updates.
- The PoE priority setting (i.e., Critical/High/Low) for a port can be updated based on device discovery. The PoE priority setting is restored to the previous statically configured value during the device cleanup phase. Requesting this action returns an error on devices that are not PoE-capable.

For more information, see Auto Attach Feature Description.

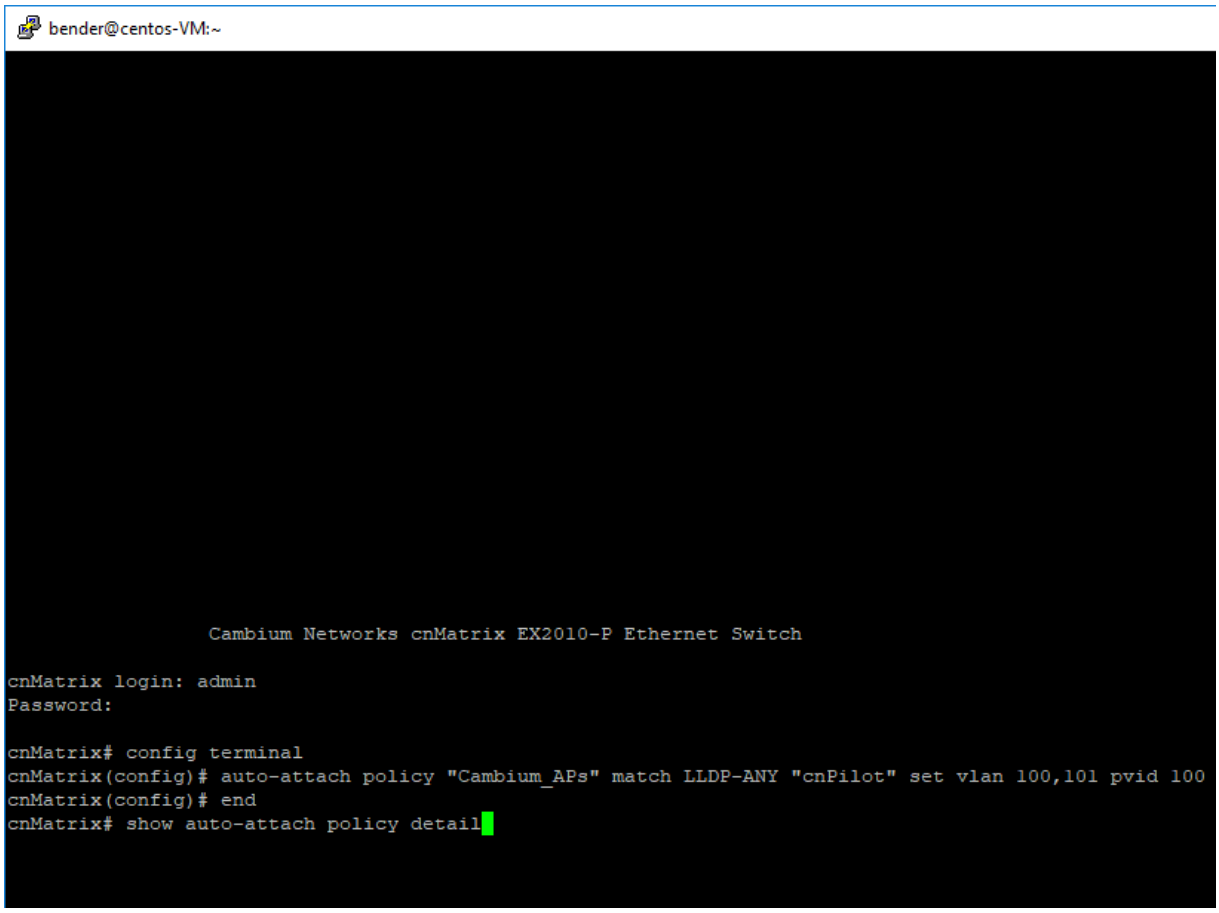
2.14.1.2 Network Diagram

2.14.2 How to Enable Auto Attach in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **auto-attach** command into the terminal to enable the Auto Attach feature. Press the Enter key.
3. Type the **end** command into the terminal. Press the Enter key.
4. Type the **show auto-attach global** command into the terminal to display the Auto Attach global configuration details (verify if the Auto Attach status is enabled). Press the Enter key.

2.14.3 Configuration Auto Attach (Policy) in CLI Interface (Example)



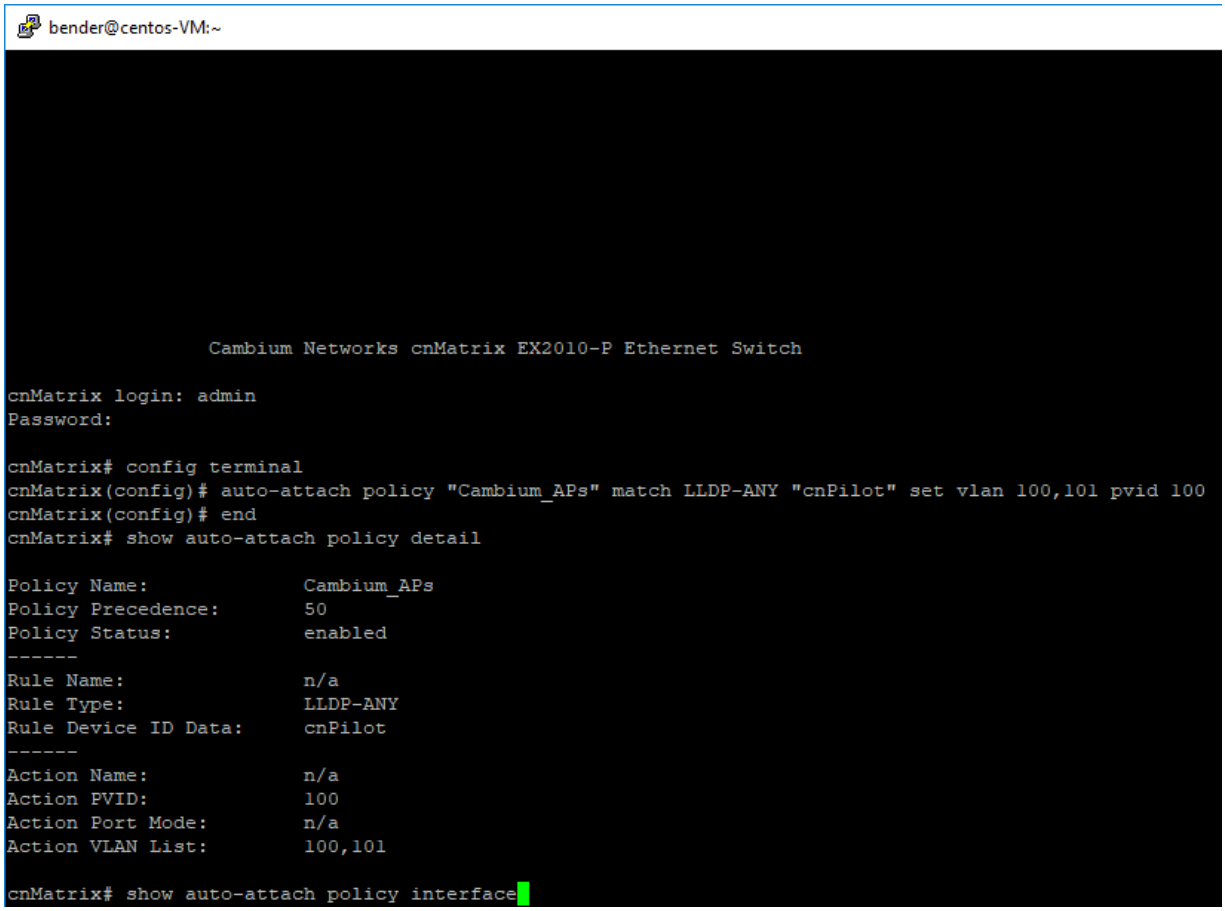
1. Type the **config terminal** command into the terminal. Press the Enter key.

2. Type the **auto-attach policy "Cambium_APs" match LLDP-ANY "cnPilot" set vlan 100,101 pvid 100** command into the terminal to configure Auto-Attach policy information. Press the Enter key.

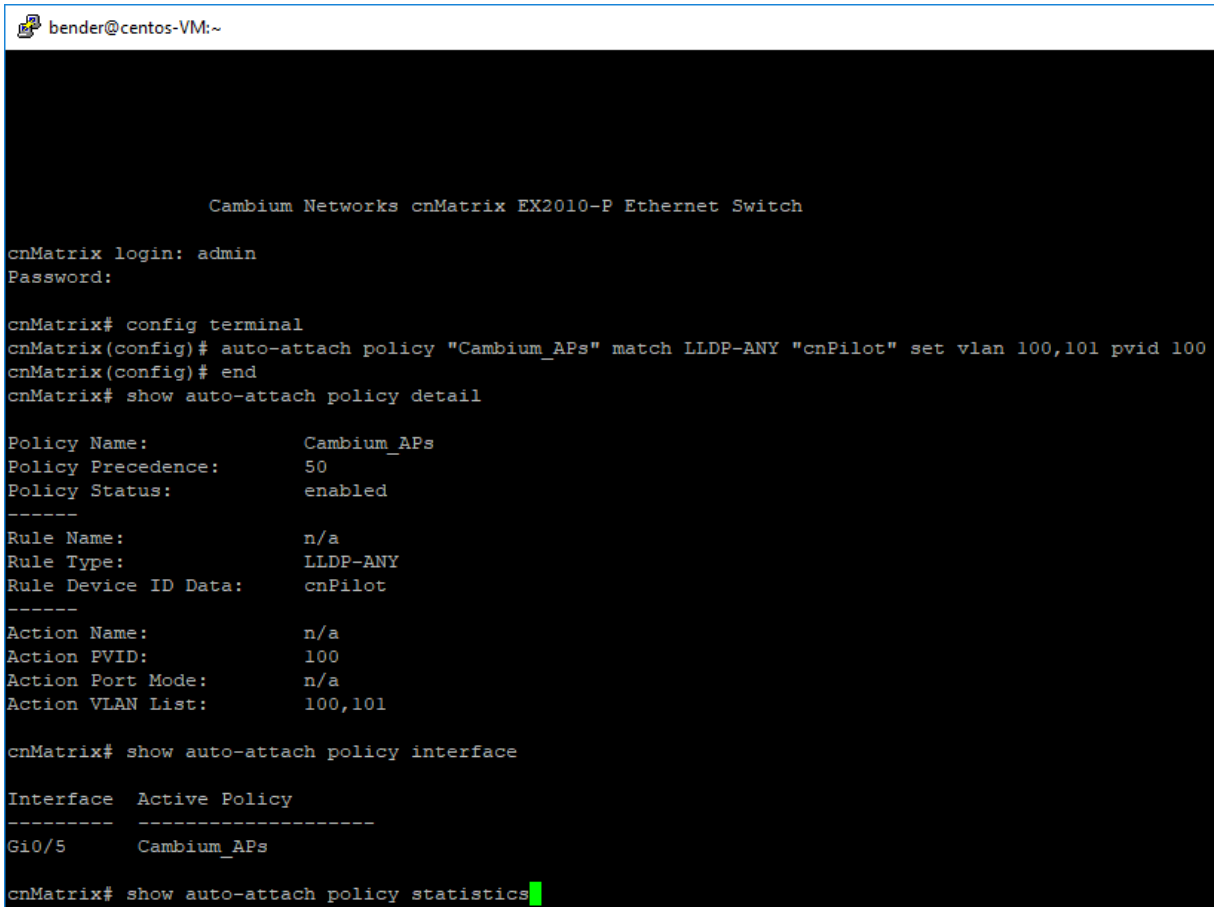
- Cambium_APs = unique policy name.
- cnPilot = previously configured matching rule.
- vlan 100, 101 = list of VLANs to be created.
- pvid 100 = pvid value; this has to be a value specified in the VLAN list.

3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

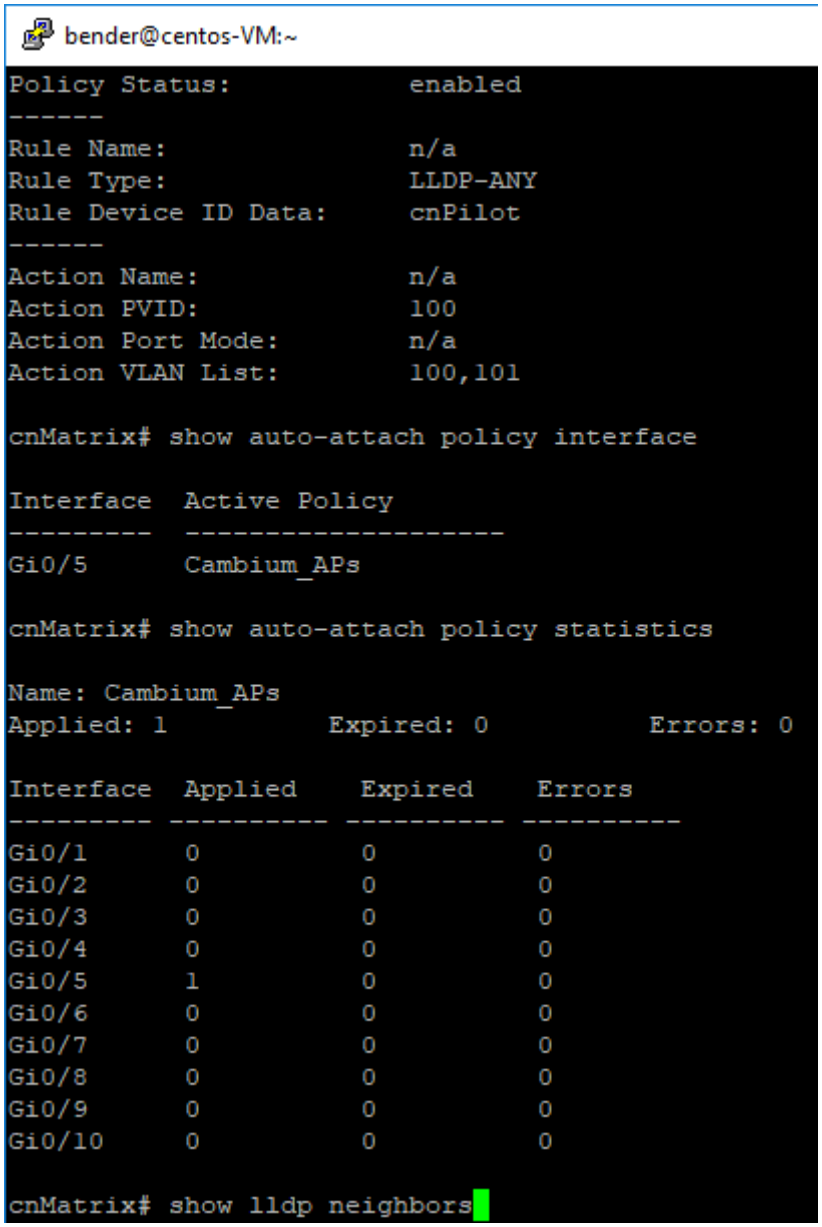
4. Type the **show auto-attach policy detail** command into the terminal to display the Auto-Attach policy information. Press the Enter key.



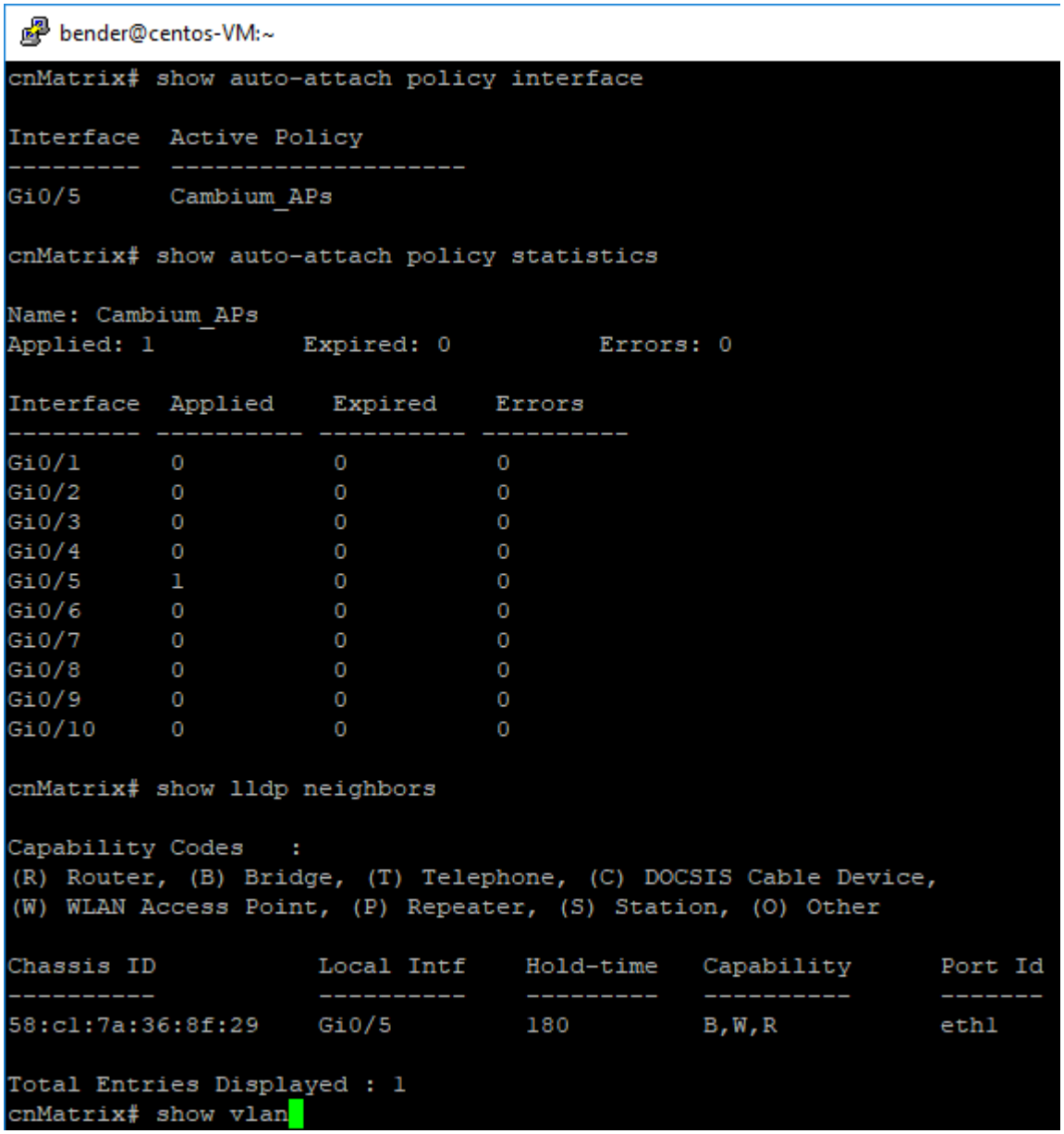
5 Type the **show auto-attach policy interface** command into the terminal to display current policy interface associations. Press the Enter key.



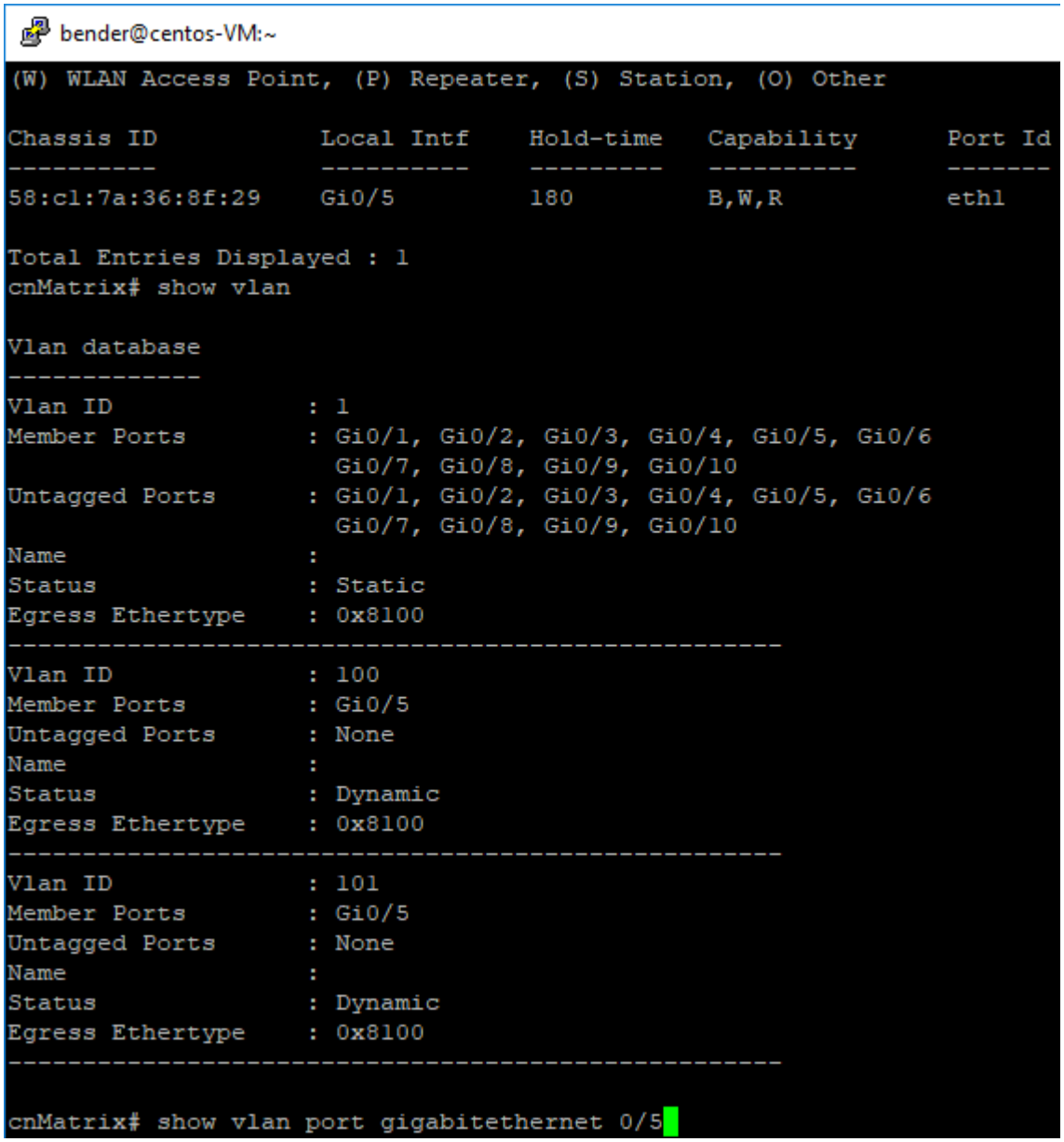
6 Type the **show auto-attach policy statistics** command into the terminal to display policy usage statistics. Press the Enter key.



7 Type the **show lldp neighbors** command into the terminal to display all neighbors learned on certain interface. Press the Enter key.



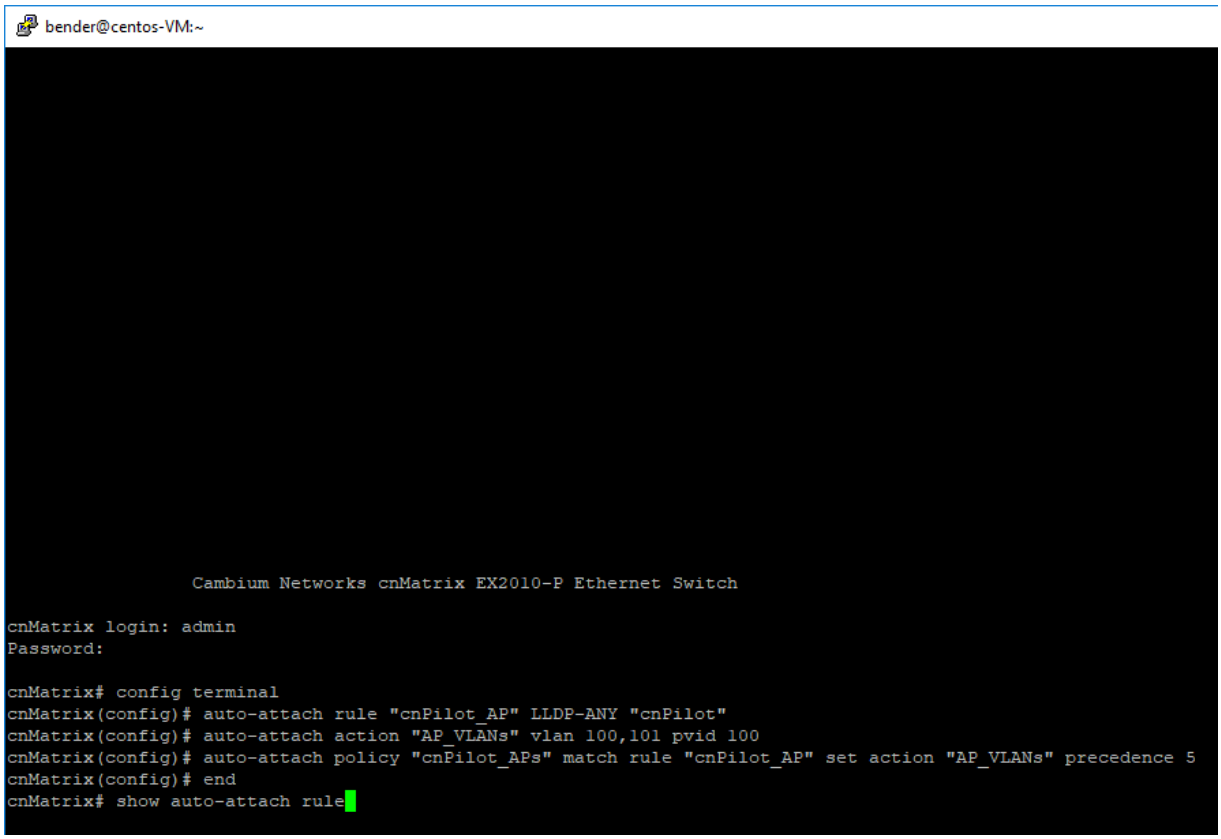
8 Type the **show vlan** command into the terminal to display VLAN global status. Press the Enter key.



9 Type the **show vlan port gigabitethernet 0/5** command into the terminal to display VLAN related information specific to member ports. Press the Enter key.

For more information, see Auto Attach Parameters and Commands.

2.14.4 Configuring Auto Attach (Rule and Action) in CLI Interface (Example)



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **auto-attach rule "cnPilot_AP" LLDP-ANY "cnPilot"** command into the terminal to configure Auto-Attach rule information. Press the Enter key.

- cnPilot_AP = rule name; with this rule we match cnPilot Access Points.
- cnPilot = matching string to be searched in all LLDP TLVs.

3 Type the **auto-attach action "AP_VLANs" vlan 100,101 pvid 100** command into the terminal to configure Auto-Attach action information. Press the Enter key.

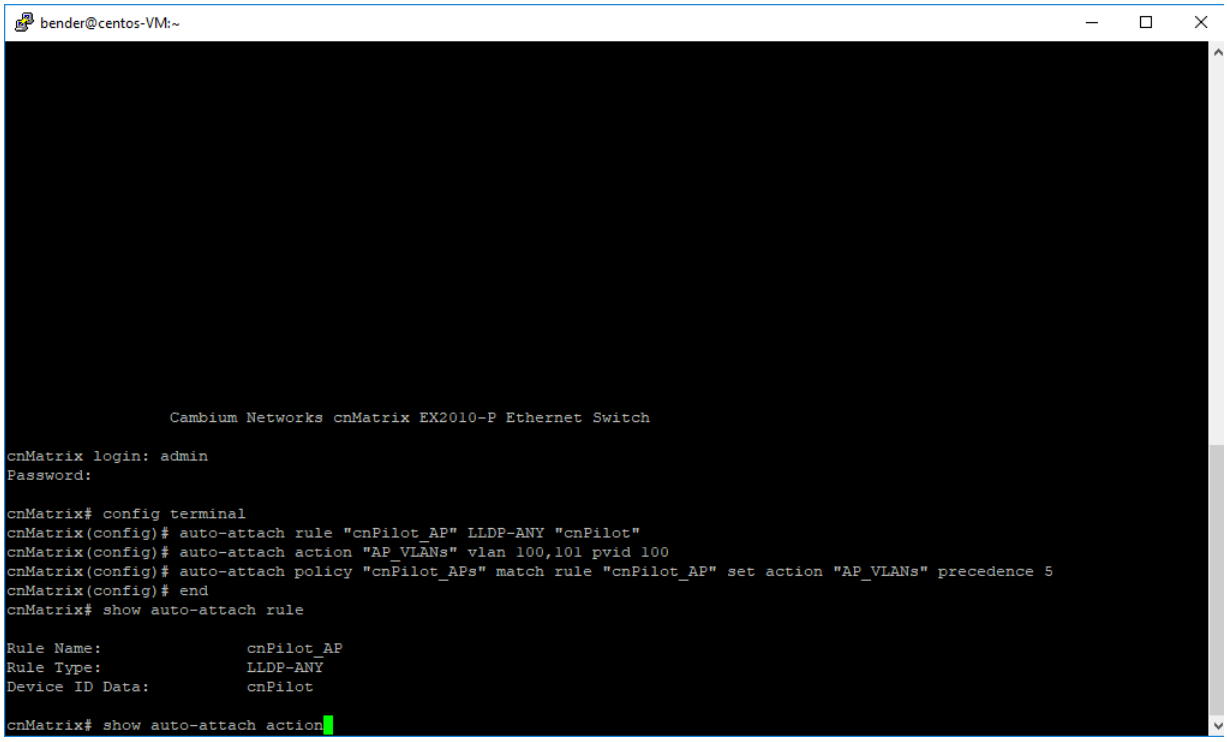
- AP_VLANs = unique action name.
- vlan 100, 101 = list of VLANs to be created.
- pvid 100 = pvid value; this has to be a value specified in the VLAN list.

4 Type the **auto-attach policy "cnPilot_APs" match rule "cnPilot_AP" set action "AP_VLANs" precedence 5** command into the terminal to configure Auto-Attach policy information. Press the Enter key.

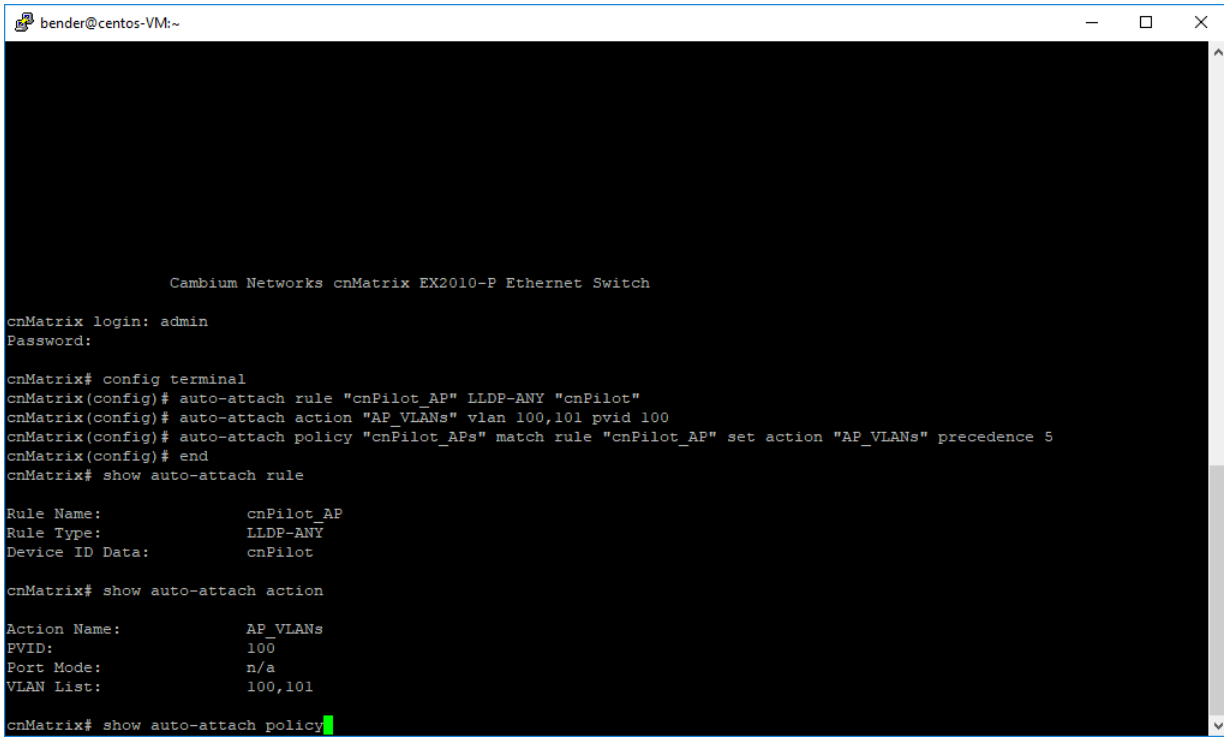
- cnPilot_APs = unique policy name.
- cnPilot_AP = previously configured matching rule.
- AP_VLANs = previously configured action.
- 5 = policy precedence value.

5 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

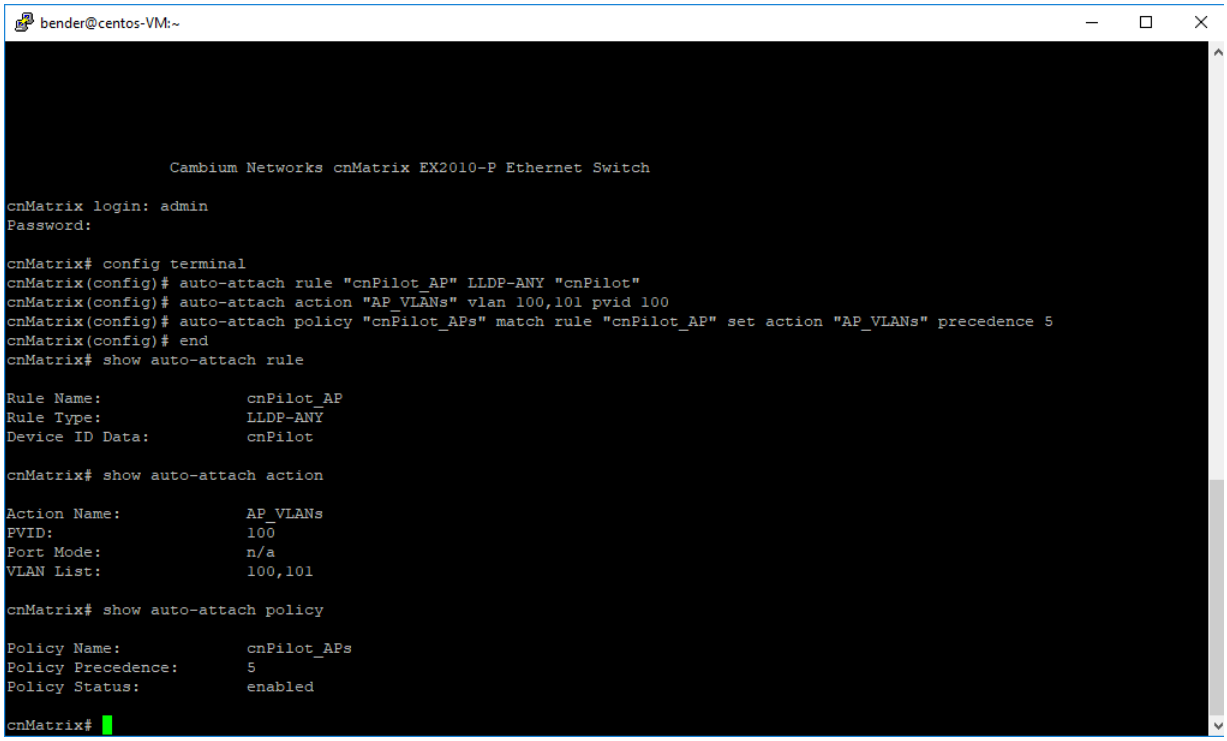
6 Type the **show auto-attach rule** command into the terminal to display Auto-Attach rule information. Press the Enter key.



7 Type the **show auto-attach action** command into the terminal to display Auto-Attach action information. Press the Enter key.



8 Type the **show auto-attach policy** command into the terminal to display Auto-Attach policy information. Press the Enter key.



For more information, see Auto Attach Parameters and Commands.

2.15 Dynamic ARP Inspection (Starting with version 2.1)

2.15.1 Managing Dynamic ARP Inspection

2.15.1.1 Feature Overview

Feature Overview

The **Dynamic ARP Inspection (DAI)** protocol has been added for the security of your cnMatrix switch and in order for your ARP response packets to be securely validated in the network. Without Dynamic ARP Inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet.

Scaling Numbers

The **DAI** feature can be enabled on a per-VLAN basis. It can be enabled on all the VLANs in the system at a time, although we have to take into consideration the CPU utilization which will increase with the number of VLANs on which the DAI is enabled and the rate of the ARP packets the switch will have to process.

Limitations

- The DAI feature is limited to the number of VLANs in the system.
- Number of entries in the binding database.
- The DAI feature is not supported for *port-channel* interfaces in version 2.1.

Default Values

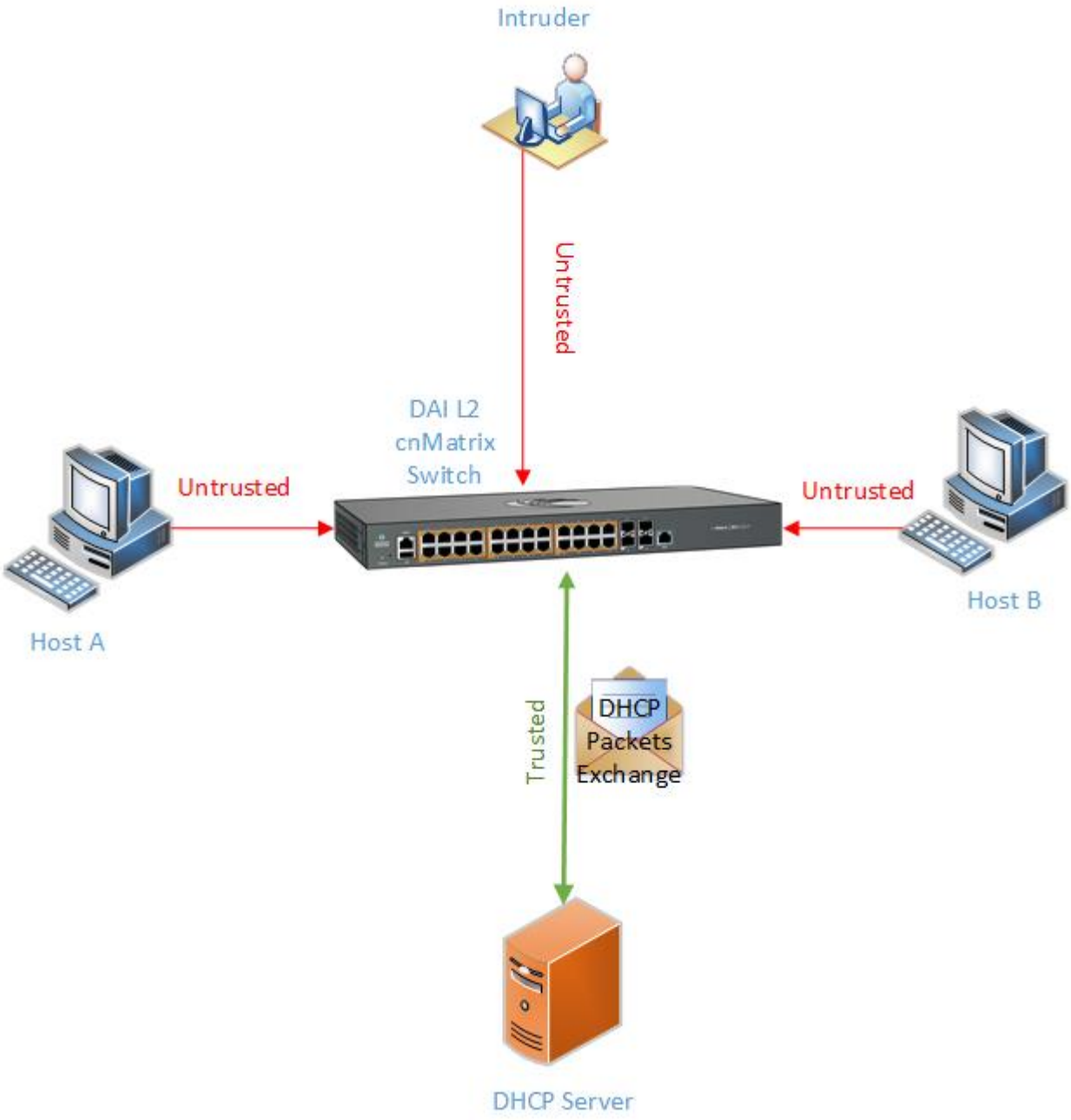
- The DAI feature is disabled on all VLANs.
- The DAI trust state is set as untrusted on all the physical interfaces.
- The DAI feature does not perform any validation checks.

Prerequisites

- In order for the DAI validation process to be initiated, the DAI has to be enabled on the VLAN on which the DAI is required to validate the ARP packets. DAI associates a trust state with each interface on the switch. ARP response packets received on trusted interfaces will skip the DAI validation process, and those arriving on untrusted interfaces will be subject to the DAI validation checks. In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches or servers as trusted. With this configuration, all ARP packets entering the network from a given switch or server bypass all the DAI security check. Although, the trust state must be used with caution since configuring an interface to be trusted when it is actually untrusted could impact the security of a network.
- The validity of ARP response packets arriving on the untrusted interfaces of the switch is determined by comparing the sender's hardware (MAC) - protocol (IP) addresses pair from each ARP packet against each MAC address – IP address binding stored in a trusted database from the switch. This trusted database is called the binding table and it can be populated dynamically when DHCP packets are exchanged between the switch and the DHCP server or statically, users being able to manually add entries in this binding table.

In order to populate the IP binding table dynamically, the DHCP Snooping module has to be enabled globally after enabling the DAI module on a previously created VLAN.

2.15.1.2Network Diagram



2.15.2 How to Enable Dynamic ARP Inspection on VLANs in CLI Interface

10.2.109.5 - PuTTY

```
cnMatrix# configure terminal
cnMatrix(config)# vlan 100
cnMatrix(config-vlan)# ip arp inspection
cnMatrix(config-vlan)# end
cnMatrix# show ip arp inspection vlan 100
```

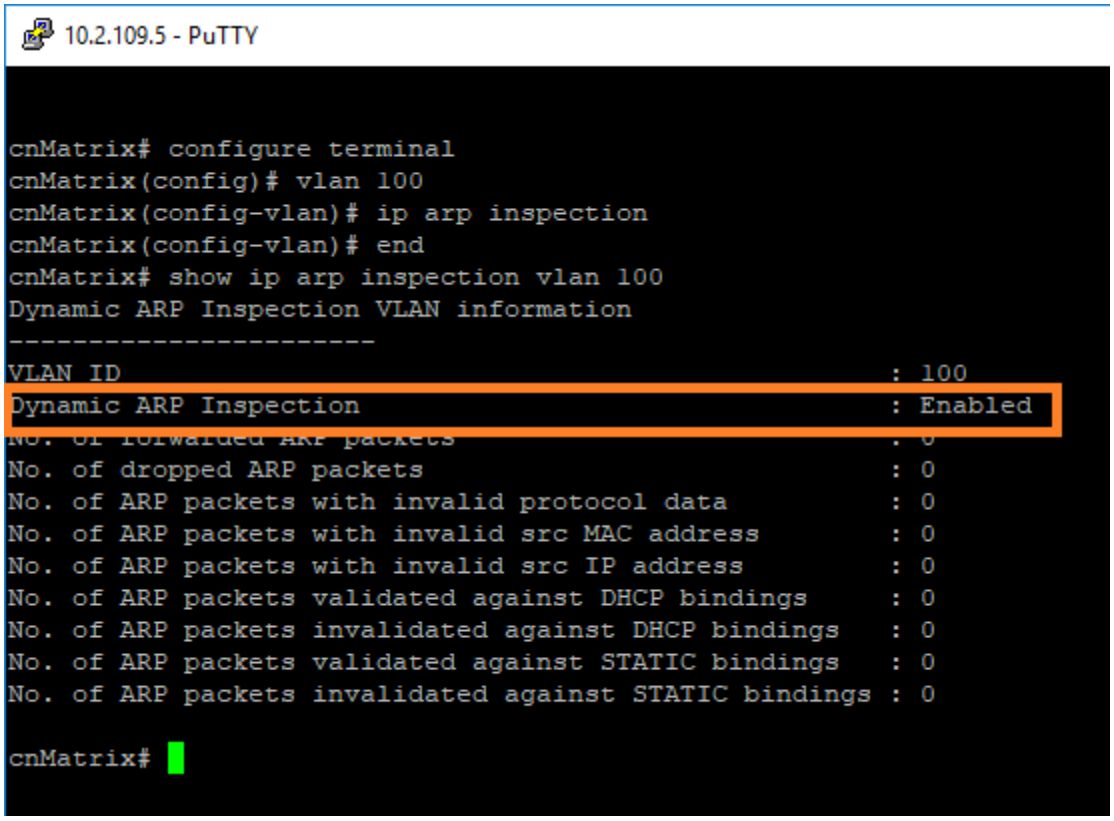
1 Type the **configure terminal** command into the terminal. Press the Enter key.

2 Type the **vlan 100** command into the terminal to configure vlan 100 . Press the Enter key.

3. Type the **ip arp inspection** command into the terminal to enable Dynamic ARP Inspection on the selected VLAN. Press the Enter key.

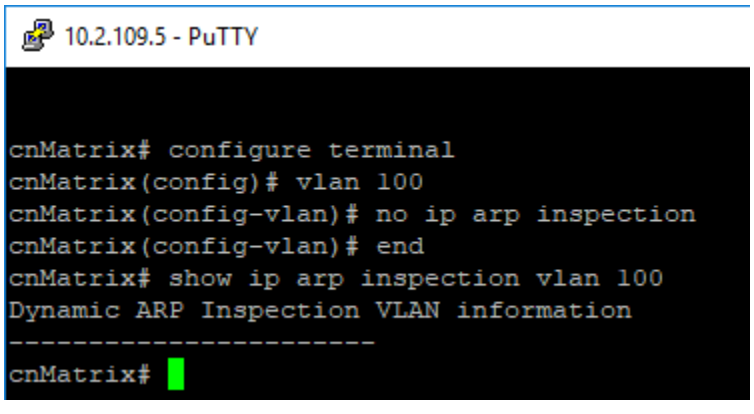
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

5. Type the **show ip arp inspection vlan 100** command into the terminal to display the Dynamic ARP Inspection status for vlan 100 (verify if Dynamic ARP Inspection is enabled).



For more information, see Dynamic ARP Inspection Parameters and Commands.

2.15.3 How to Disable Dynamic ARP Inspection on VLANs in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.

2. Type the **vlan 100** command into the terminal to configure vlan 100. Press the Enter key.

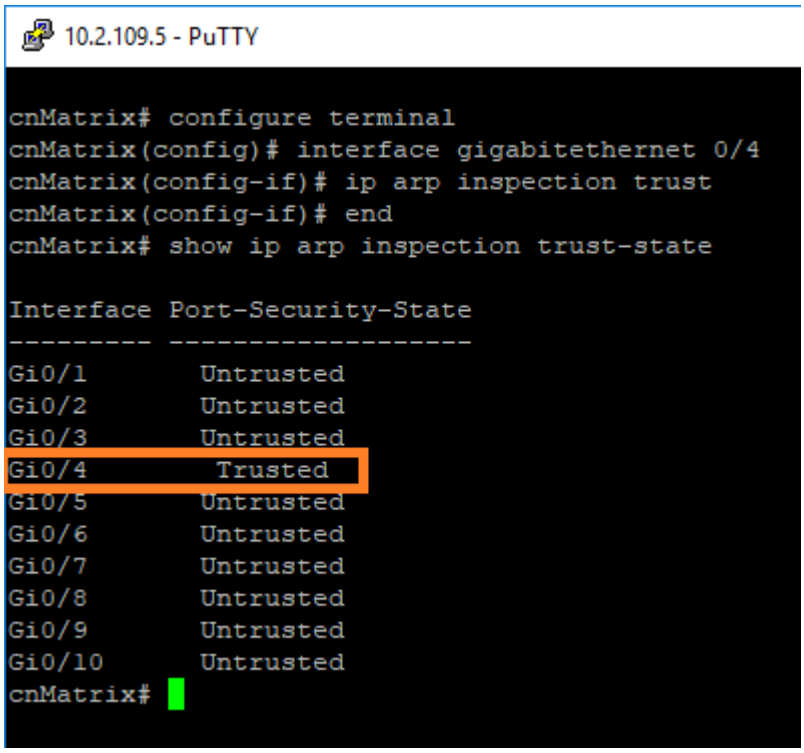
3. Type the **no ip arp inspection** command into the terminal to disable Dynamic ARP Inspection on the selected VLAN. Press the Enter key.

4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

5. Type the **show ip arp inspection vlan 100** command into the terminal to display the Dynamic ARP Inspection status for vlan 100 (verify if the DAI information for the selected VLAN is still displayed). Press the Enter key.

For more information, see Dynamic ARP Inspection Parameters and Commands.

2.15.4 Configuring the Dynamic ARP Inspection Trust State on an Interface in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.

2. Type the **interface gigabitethernet 0/4** command into the terminal to select an interface to be configured. Press the Enter key.

3. Type the **ip arp inspection trust** command into the terminal to configure the interface as a trusted port. Press the Enter key.

4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

5. Type the **show ip arp inspection trust-state** command into the terminal to display the Dynamic ARP Inspection trust state for all the physical interfaces (verify if gi0/4 is set as trusted). Press the Enter key.

For more information, see Dynamic ARP Inspection Parameters and Commands.

3 L3 Features

3.1 DHCP Relay

3.1.1 Managing DHCP Relay

3.1.1.1 Feature Description

DHCP Relay agent allows the DHCP client and DHCP server in different subnets to communicate with each other so that the DHCP client can obtain its IP address and configuration. The relay agent receives packets from the Client, inserts information such as network details, and forwards the modified packets to the Server. The Server identifies the Client's network from the received packets, allocates the IP address accordingly, and sends a reply to the Relay. The Relay strips the information inserted by the Server and broadcasts the packets to the Client's network.

Standards

- RFC 3046
- RFC 2131

Scaling Numbers

- Maximum 200 clients can use this feature simultaneously.

Limitations

- The cnMatrix switch cannot be a DHCP Relay and Server simultaneously.
- When enabled, the DHCP Relay feature is active on all VLANs/networks.
- DHCP Snooping and DHCP Relay are mutually exclusive.

Default Values

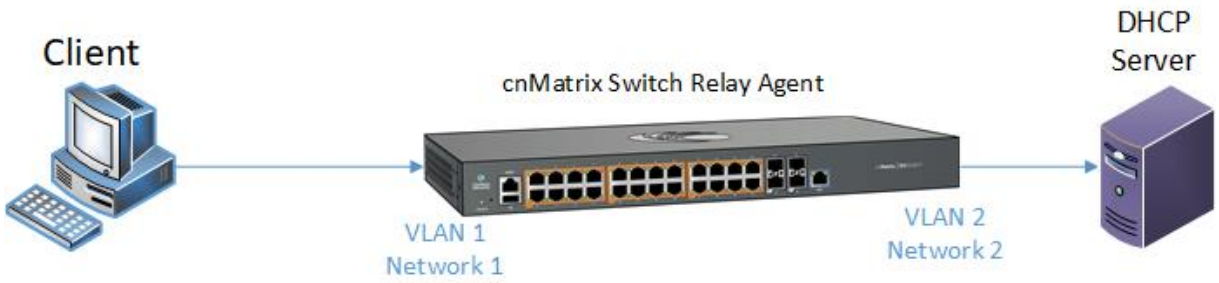
- The DHCP Relay feature, and also option 82 are disabled by default.

Prerequisites

- Enable IP routing globally.
- Create VLANs and assign ports to VLANs.
- Assign IP addresses to the VLANs.

Even though the feature can be enabled on a VLAN or port, it will relay packets from all VLANs.

3.1.1.2 Network Diagram



3.1.2 How to Enable DHCP Relay in CLI Interface

10.2.109.5 - PuTTY

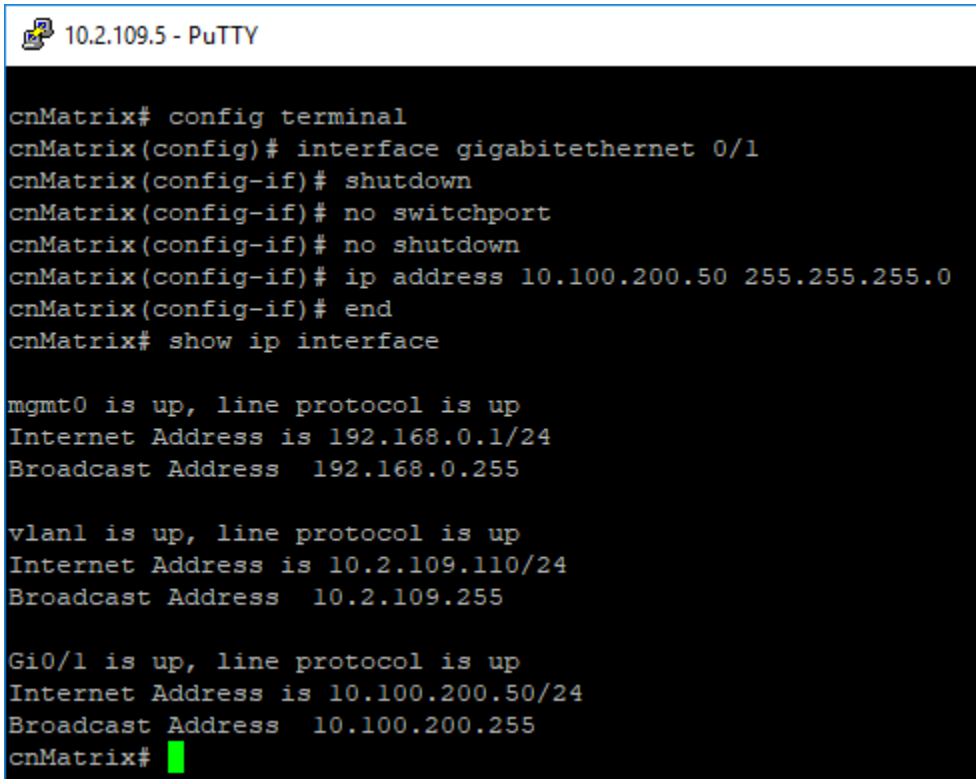
```
cnMatrix# config terminal
cnMatrix(config)# service dhcp-relay
cnMatrix(config)# ip dhcp server 10.100.100.10
cnMatrix(config)# end
cnMatrix# show ip dhcp relay information

Context Name : default
------------

Dhcp Relay                  : Enabled
Dhcp Relay Servers only     : Enabled

DHCP server 1:  10.100.100.10

Dhcp Relay RAI option       : Disabled
Default Circuit Id information : router-index
Debug Level                 : 0x0

No of Packets inserted RAI option               : 0
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
```

1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **service dhcp-relay** command into the terminal to enable DHCP Relay Agent. Press the Enter key.
3. Type the **ip dhcp server 10.100.100.10** command into the terminal to set an IP address for the DHCP server. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show ip dhcp relay information** command into the terminal to display the DHCP Relay Agent configuration (verify if the status for the DHCP Relay feature is enabled). Press the Enter key.

For more information,see DHCP Relay Parameters and Commands.

3.2 Routed Interface

3.2.1 How to Enable Routed Interfaces in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the Enter key.

3 Type the **shutdown** command into the terminal to disable a physical interface. Press the Enter key.

4 Type the **no switchport** command into the terminal to set the interface as a routed port and to erase all L2 interface configurations. Press the Enter key.

5 Type the **no shutdown** command into the terminal to enable a physical interface. Press the Enter key.

6 Type the **ip address 10.100.200.50 255.255.255.0** command into the terminal to set the IP address of the configured interface. Press the Enter key.

7 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

8 Type the **show ip interface** into the terminal to display the IP interface status and configuration. Press the Enter key.

3.3 IP Routing

3.3.1 Managing IP Routing

IPv4 Static Routing enables routing of IPv4 unicast traffic based on configured IPv4 Static Routes or programmed Directly Connected routes.

IP Interfaces must be created, and IP addresses and netmasks should be assigned to them.

Standards

- RFC791

Scaling Numbers

- A maximum of 64 IPv4 interfaces is supported.

Limitations

- IP routing cannot be disabled on the system.

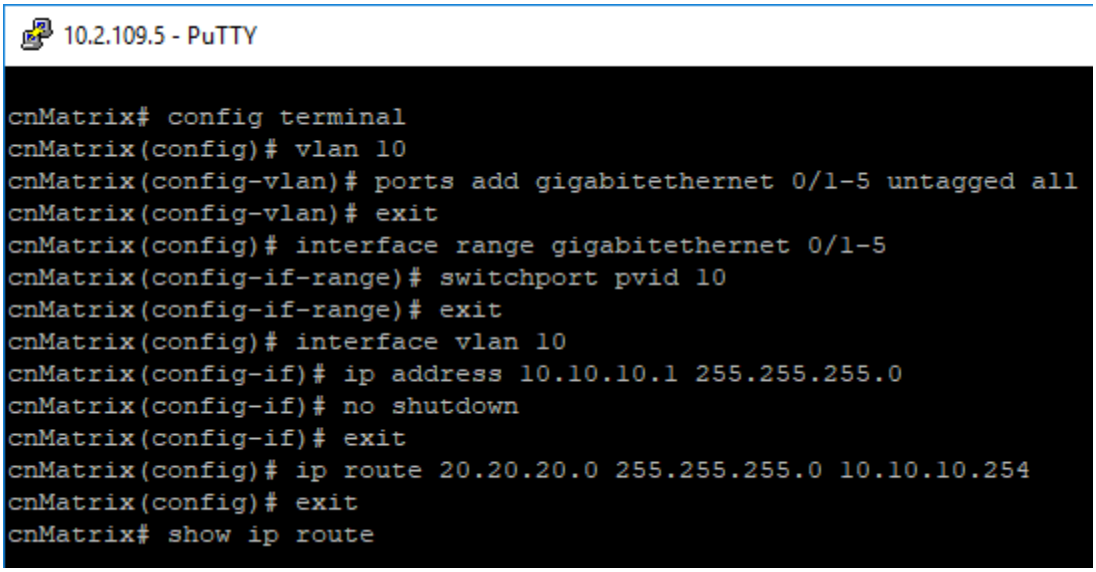
Default Values

- IP Routing is enabled by default.
- TTL value is 64 by default.
- ICMP redirect option is enabled by default.
- ICMP unreachable option is enabled by default.
- ICMP echo reply option is enabled by default.
- ICMP mask reply option is enabled by default.
- Path MTU discovery is disabled by default.

Prerequisites

- N/A

3.3.2 How to enable IP Routing in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **vlan 10** command into the terminal to go to the configuration vlan mode. Press the Enter key.

3 Type the **ports add gigabitethernet 0/1-5 untagged all** command into the terminal to configure the port list for the selected VLAN. Press the Enter key.

4 Type the **exit** command into the terminal to go back to the configuration mode. Press the

Enter key.

5 Type the **interface range gigabitethernet 0/1-5** command into the terminal to select the range of Layer 2 interfaces to be configured and to go to the configure interface range mode. Press the Enter key.

6 Type the **switchport pvid 10** command into the terminal to set pvid for the port. Press the Enter key.

7 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

8 Type the **interface vlan 10 command** into the terminal to select an interface to be configured and to go to the configuration interface mode. Press the Enter key.

9 Type the **ip address 10.10.10.1 255.255.255.0** command into the terminal to set an IP address for the configured interface. Press the Enter key.

10 Type the **no shutdown** command into the terminal to enable an interface. Press the Enter key.

11 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

12 Type the **ip route 20.20.20.0 255.255.255.0 10.10.10.254** command into the terminal to configure a static route. Press the Enter key.

13 Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

14 Type the **show ip route** command into the terminal to display the IP Routing table and to verify if the previously performed configuration was successful. Press the Enter key.

For more information, see IP Routing Parameters and Commands.

3.4 RIP (Starting with version 2.1)

3.4.1 Managing RIP

3.4.1.1 Feature Overview

Feature Overview

The **RIP (Routing Information Protocol)** is a dynamic protocol used to find the best route or path from end-to-end (source to destination) over a network by using a routing metric/hop count algorithm. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time.

This dynamic protocol represents a distance vector routing protocol, which has the default AD (Administrative Distance) value of 120, and it works on the application layer of the OSI model.

Note: RIP uses port number 520.

Scaling Numbers

- The switch can store a maximum of 512 RIP Routes.

Limitations

- If the hop count is below 15, the routes will drop.
- Variable Length Subnet Masks are not supported by RIP version 1 (which is obsolete).
- RIP has slow convergence.

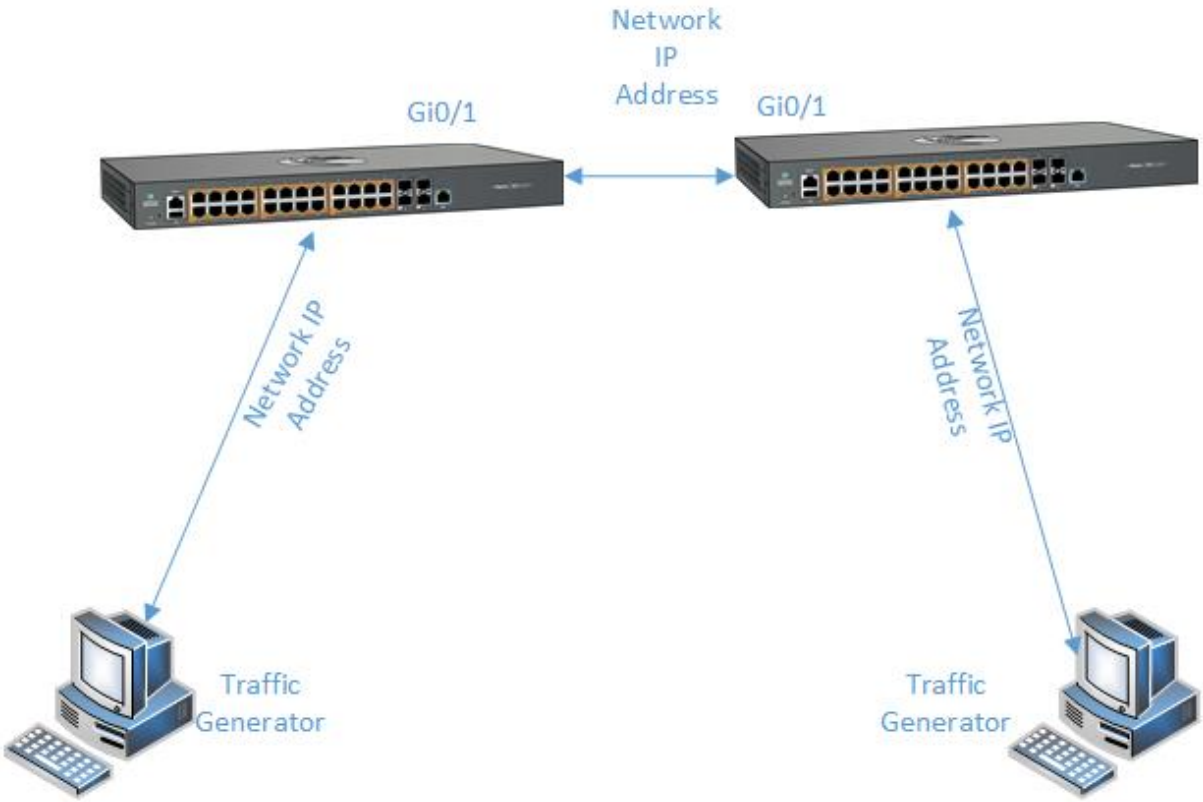
Default Values

- Router RIP is disabled by default.
- The security level of the RIP feature is set to maximum by default.
- Route Redistribution is disabled by default.
- The Administrative Distance (AD) is 120.
- Auto-summary is enabled.
- The installation of default route to the RIP database is restricted.
- The timers basic default values are:
  - Update-value - 30
  - Routeage-value - 180
  - Garbage-value - 120
- Split horizon with poison reverse is enabled.
- No authentication mode is set for RIP packets.
- The authentication type is set to md5 by default.
- Default version is version 1 compatibility.

Prerequisites

- Before configuring RIP on the desired SVIs (switched virtual interfaces) or routed ports, IP addresses should be configured on the same SVIs or routed ports.

3.4.1.2 Network Diagram

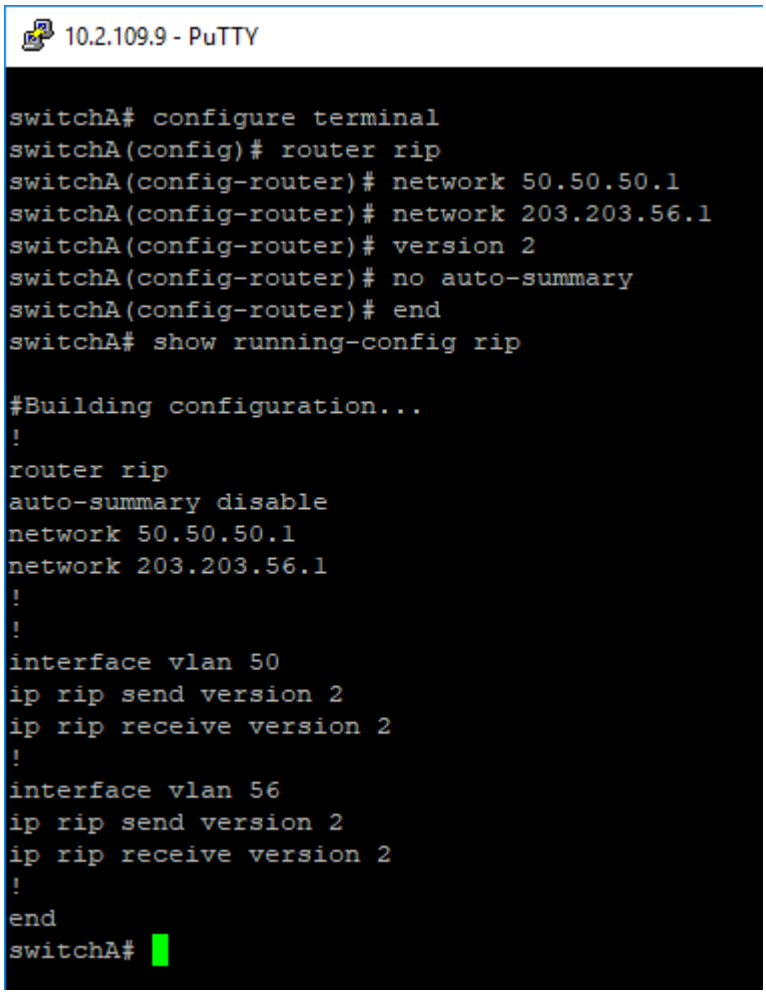


3.4.2How to Enable RIP in CLI Interface

```
10.2.109.5 - PuTTY

cnMatrix# configure terminal
cnMatrix(config)# router rip
cnMatrix(config-router)# end
cnMatrix# show run rip

#Building configuration...
!
router rip
!
!
end
cnMatrix#
```

1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **router rip** command into the terminal to enable the RIP feature and to go to the router configuration mode. Press the Enter key.
3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show run rip** command into the terminal to display the currently operating configuratin. Press the Enter key.

3.4.3How to Configure RIP in CLI Interface (example)



Before configuring RIP, please make sure that you previously configured the following:

On switch A:

```
vlan 50
ports gigabitethernet 0/4 untagged gigabitethernet 0/4

vlan 1
no ports gigabitethernet 0/4 untagged gigabitethernet 0/4

interface gigabitethernet 0/4
switchport pvid 50
no shutdown

vlan 56
ports gigabitethernet 0/2 untagged gigabitethernet 0/2

vlan 1
no ports gigabitethernet 0/2 untagged gigabitethernet 0/2

interface gigabitethernet 0/2
switchport pvid 56
no shutdown

interface vlan 50
```

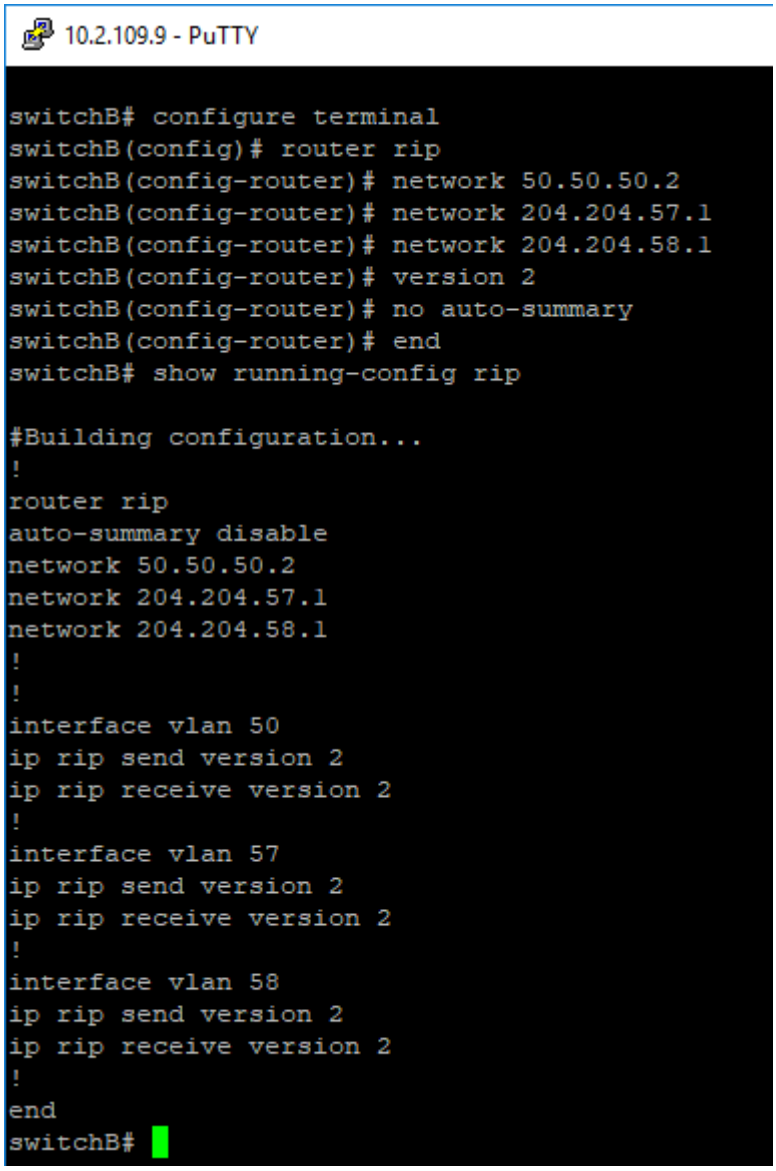
```
ip address 50.50.50.1 255.255.255.0
no shutdown

interface vlan 56
ip address 203.203.56.1 255.255.255.0
no shutdown
```

On switch B:

```
vlan 50
ports gigabitethernet 0/4 untagged gigabitethernet 0/4

vlan 1
no ports gigabitethernet 0/4 untagged gigabitethernet 0/4

interface gigabitethernet 0/4
switchport pvid 50
no shutdown

vlan 57
ports gigabitethernet 0/2 untagged gigabitethernet 0/2

vlan 1
no ports gigabitethernet 0/2 untagged gigabitethernet 0/2

interface gigabitethernet 0/2
switchport pvid 57
no shutdown
```

SWITCH A

1. Type the **configure terminal** command into the terminal. Press the Enter key.
1. Type the **router rip** command into the terminal to enable the RIP feature and to enter the router configuration mode. Press the Enter key.
2. Type the **network 50.50.50.1** command into the terminal to enable RIP on the 50.50.50.1 IP network. Press the Enter key.
3. Type the **network 203.203.56.1** command into the terminal to enable RIP on the 203.203.56.1 IP network. Press the Enter key.
4. Type the **version 2** command into the terminal to configure the global version of the RIP feature. Press the Enter key.
5. Type the **no auto-summary** command into the terminal to disable auto summarization in RIP. Press the Enter key.
6. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
7. Type the **show running-config rip** command into the terminal. Press the Enter key.



SWITCH B

8 Type the **configure terminal** command into the terminal. Press the Enter key.

9 Type the **router rip** command into the terminal. Press the Enter key.

10 Type the **network 50.50.50.2** command into the terminal. Press the Enter key.

11 Type the **network 204.204.57.1** command into the terminal. Press the Enter key.

12 Type the **network 204.204.58.1** command into the terminal. Press the Enter key.

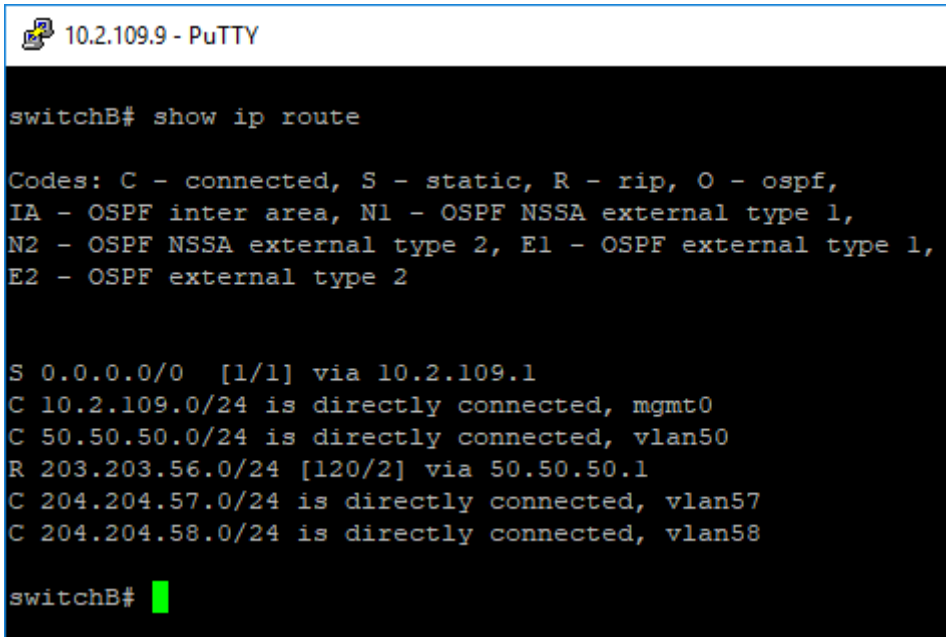
13 Type the **version 2** command into the terminal. Press the Enter key.

14 Type the **no auto-summary** command into the terminal. Press the Enter key.

15 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

16 Type the **show running-config rip** command into the terminal. Press the Enter key.

17 Type the **show ip route** command into the terminal. Press the Enter key.



3.5 OSPF (Starting with version 2.1)

3.5.1 Managing OSPF

3.5.1.1 Feature Overview

Feature Overview

Starting with version 2.1, the **OSPF (Open Shortest Path First)** feature has been added so that the routing information can be scattered within a single Autonomous System. The shortest path to each node will be calculated based on the topography of the Internet constructed by each node.

Before configuring the OSPF feature, the RRD option must be enabled.

Standards

- RFC 1583
- RFC 3509
- RFC 2328

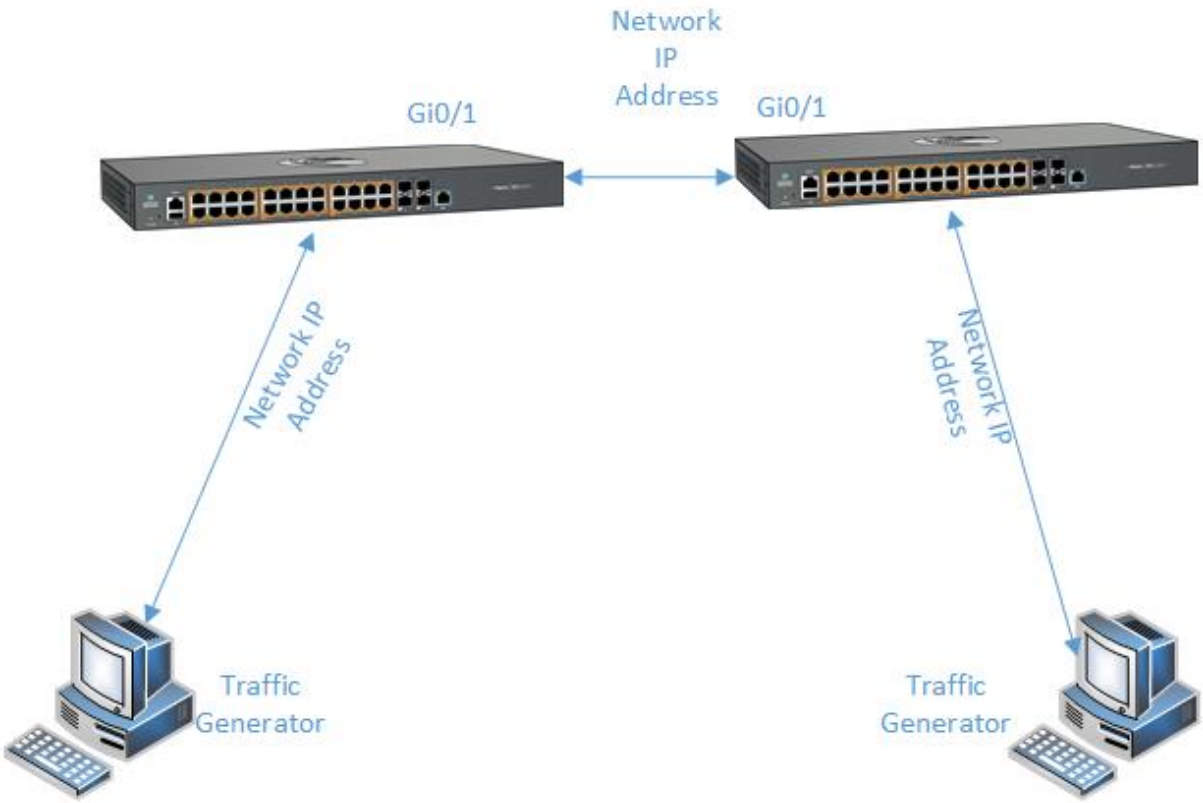
Default Values

- The Alternative ABR Type is set to standard by default.
- The capability of storing opaque LSAs is disabled by default.
- The helper support is enabled by default.
- The strict LSA check option is disabled by default in helper support.
- The OSPF route calculation staggering option is enabled by default.
- The router priority is set to 1 by default.
- The cost of sending a packet on an interface is set to 0 by default.
- The default OSPF network type is set to broadcast by default.
- The delay time between two consecutive SPF calculations is set to 5 seconds by default.
- The hold time between two consecutive SPF calculations is set to 10 seconds by default.

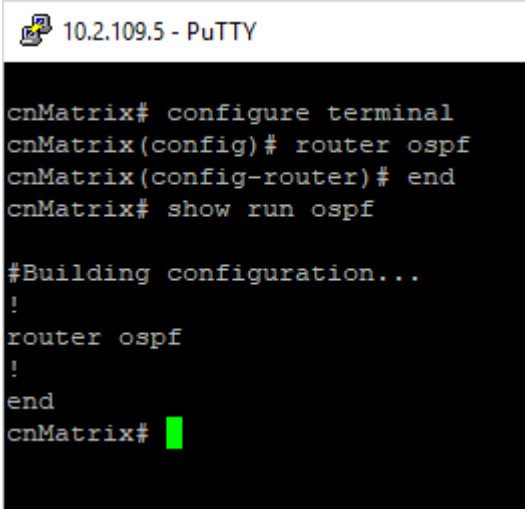
Prerequisites

- N/A

3.5.1.2 Network Diagram



3.5.2 How to Enable OSPF in CLI Interface



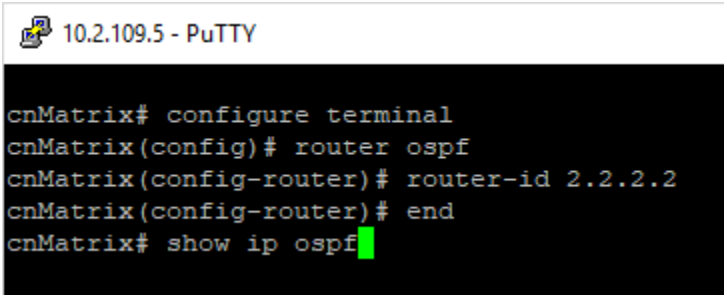
1 Type the **configure terminal** command into the terminal. Press the Enter key.

2 Type the **router ospf** command into the terminal to enable the OSPF feature. Press the Enter key.

3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

4. Type the **show run ospf** command into the terminal to display the OSPF related configuration (verify if OSPF was successfully enabled). Press the Enter key.

3.5.3 How to Configure OSPF Router-ID in CLI Interface



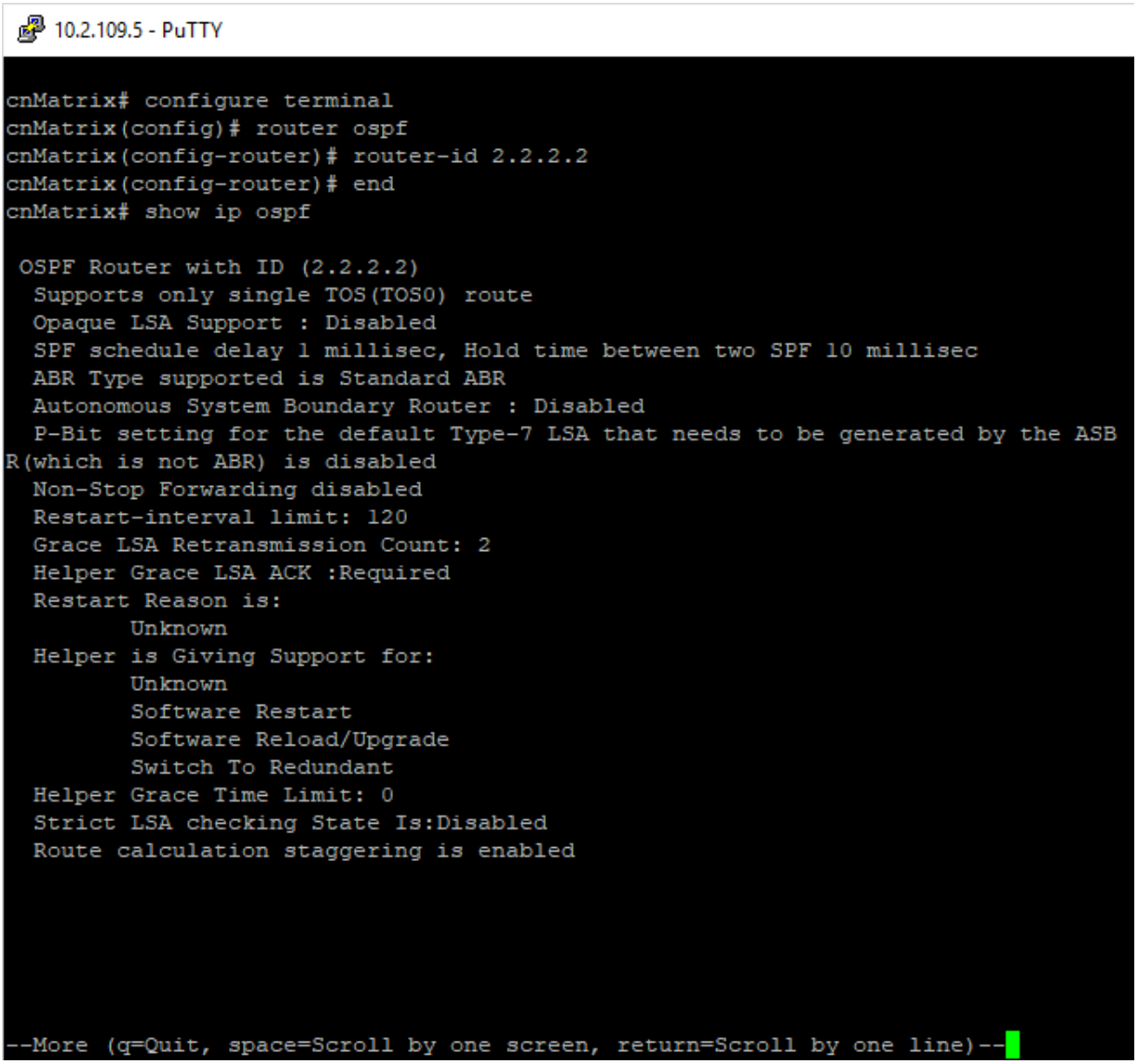
1. Type the **configure terminal** command into the terminal. Press the Enter key.

2. Type the **router ospf** command into the terminal to enable the OSPF feature. Press the Enter key.

3. Type the **router-id 2.2.2.2** command into the terminal to set the router ID for the OSPF process. Press the Enter key.

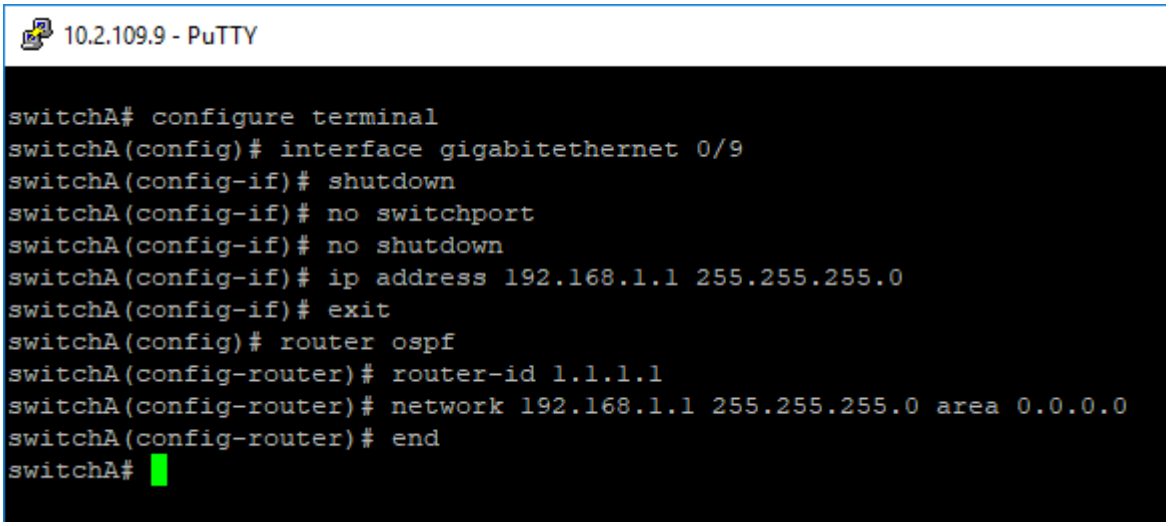
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

5. Type the **show ip ospf** command into the terminal to display the OSPF related configuration (verify if Router OSPF ID is 2.2.2.2).



For more information, see OSPF Parameters and Commands.

3.5.4 How to Configure OSPF in CLI Interface (example)



SWITCH A

1. Type the **configure terminal** command into the terminal. Press the Enter key.

2 Type the **interface gigabitethernet 0/9** into the terminal to select the interface to be configured. Press the Enter key.

3 Type the **shutdown** command into the terminal to disable a physical interface. Press the Enter key.

4 Type the **no switchport** command into the terminal to configure the interface as routed-interface. Press the Enter key.

5 Type the **no shutdown** command into the terminal to enable a physical interface. Press the Enter key.

6 Type the **ip address 192.168.1.1 255.255.255.0** command into the terminal to set the IP address of an interface. Press the

Enter key.

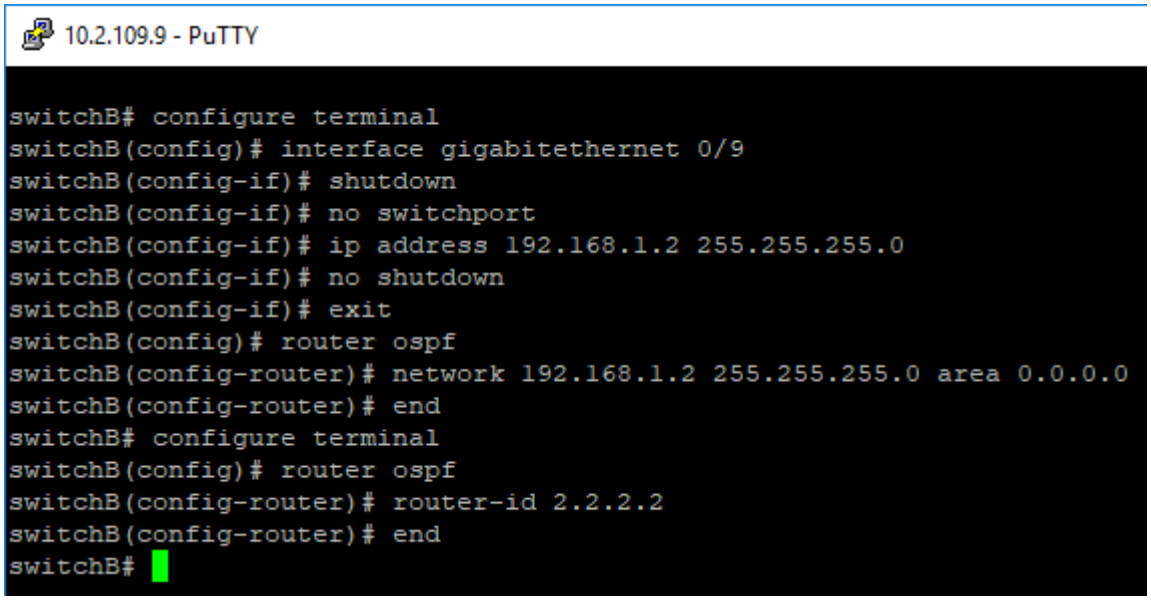
7 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

8 Type the **router ospf** command into the terminal to enable the OSPF routing process and to enter the configuration router mode. Press the Enter key.

9 Type the **router-id 1.1.1.1** command into the terminal to set the router ID for the OSPF process. Press the Enter key.

10 Type the **network 192.168.1.1 255.255.255.0 area 0.0.0.0** command into the terminal to define the interface on which the OSPF feature runs and the area idea for the select interface. Press the Enter key.

11 Type the **end** command into the terminal to go to the Pivileged EXEC mode on switch A. Press the Enter key.



SWITCH B

12 Type the **configure terminal** command into the terminal. Press the Enter key.

13 Type the **interface gigabitethernet 0/9** command into the terminal to select the interface to be configured on switch B. Press the Enter key.

14 Type the **shutdown** command into the terminal. Press the Enter key.

15 Type the **no switchport** command into the terminal. Press the Enter key.

16 Type the **ip address 192.168.1.2 255.255.255.0** command into the terminal. Press the Enter key.

17 Type the **no shutdown** command into the terminal. Press the Enter key.

18 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

19 Type the **router ospf** command into the field to enable the OSPF routing process and to enter the configuration router mode on switch B. Press the Enter key.

20 Type the **network 192.168.1.2 255.255.255.0 area 0.0.0.0** command into the terminal. Press the Enter key.

21 Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

If you forgot to create a router ID on switch B, you can go back in the configuration mode and create one even if you performed the configurations:

22 Type the **configure terminal** command into the terminal. Press the Enter key.

23 Type the **router ospf** command into the terminal. Press the Enter key.

24 Type the **router-id 2.2.2.2** command into the terminal. Press the Enter key.

25 Type the **end** command into the terminal to go back to the Privileged EXEC mode on switch B. Press the Enter key.

26 This is how you can verify if the configuration was successful on both switches:

Type the **show ip ospf neighbor** command into the terminal (in switch A and switch B) to display the OSPF neighbor information list (verify the adjacency on switch A and B, between switch A and switch B on area 0). Press the Enter key.

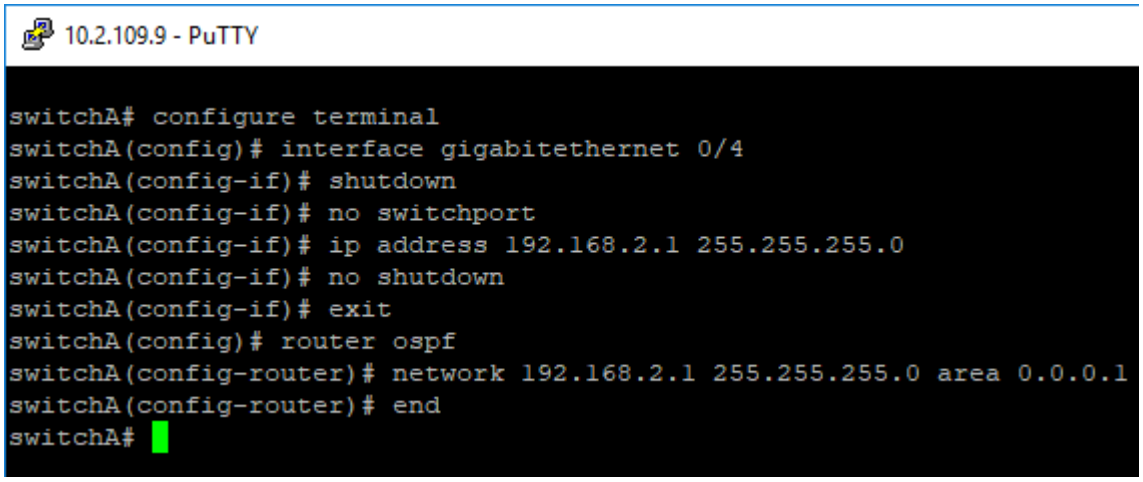
27 Type the **show ip ospf database** command into the terminal (in switch A and switch B) to display the OSPF Link State Database. Press the Enter key.

10.2.109.9 - PuTTY

```
switchA# show ip ospf neighbor

  Neighbor-ID     Pri   State           DeadTime   Address         Interface   H
elper      HelperAge     HelperER
  -----------     ---   -----           --------   -------         ---------   -
--------   ------------  ---------
  2.2.2.2         1     FULL/BACKUP     39         192.168.1.2     Gi0/9       N
ot Helping 0             None

switchA# show ip ospf database

OSPF Router with ID (1.1.1.1)
                 Router Link States (Area 0.0.0.0)
                 ----------------------------------------
Link ID          ADV Router       Age        Seq#          Checksum  Link count
-------          ----------       ---        ----          --------  ----------
1.1.1.1          1.1.1.1          106        0x80000004    0x82ce    1

2.2.2.2          2.2.2.2          109        0x80000002    0x4802    1

                 Network Link States (Area 0.0.0.0)
                 ----------------------------------------
Link ID          ADV Router       Age        Seq#          Checksum
-------          ----------       ---        ----          --------
192.168.1.1      1.1.1.1          107        0x80000001    0x328b

switchA#
```

10.2.109.9 - PuTTY

```
switchB# show ip ospf neighbor

  Neighbor-ID     Pri   State           DeadTime   Address         Interface   H
elper      HelperAge     HelperER
  -----------     ---   -----           --------   -------         ---------   -
--------   ------------  ---------
  1.1.1.1         1     FULL/DR         36         192.168.1.1     Gi0/9       N
ot Helping 0             None

switchB# show ip ospf database

OSPF Router with ID (2.2.2.2)
                 Router Link States (Area 0.0.0.0)
                 ----------------------------------------
Link ID          ADV Router       Age        Seq#          Checksum  Link count
-------          ----------       ---        ----          --------  ----------
1.1.1.1          1.1.1.1          250        0x80000004    0x82ce    1

2.2.2.2          2.2.2.2          249        0x80000002    0x4802    1

                 Network Link States (Area 0.0.0.0)
                 ----------------------------------------
Link ID          ADV Router       Age        Seq#          Checksum
-------          ----------       ---        ----          --------
192.168.1.1      1.1.1.1          250        0x80000001    0x328b

switchB#
```



SWITCH A

28 Type the **configure terminal** command into the terminal. Press the Enter key.

29 Type the **interface gigabitethernet 0/4** command into the terminal. Press the Enter key.

30 Type the **shutdown** command into the terminal. Press the Enter key.

31 Type the **no switchport** command into the terminal. Press the Enter key.

32 Type the **ip address 192.168.2.1 255.255.255.0** command into the terminal. Press the Enter key.

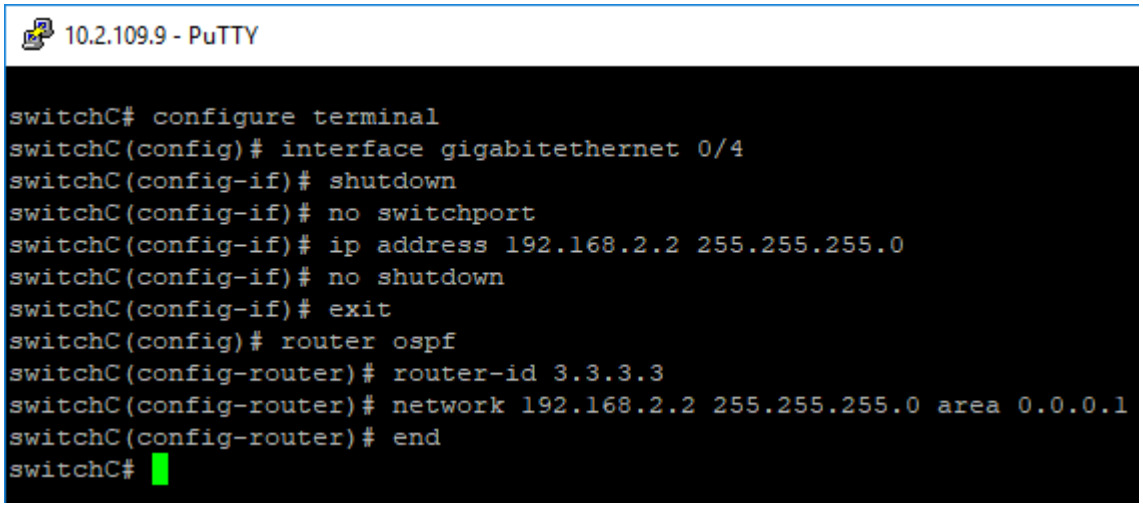
33 Type the **no shutdown** command into the terminal. Press the Enter key.

34 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

35 Type the **router ospf** command into the terminal. Press the Enter key.

36 Type the **network 192.168.2.1 255.255.255.0 area 0.0.0.1** command into the terminal. Press the Enter key.

37 Type the **end** command into the terminal to go back to the Privileged EXEC mode on switch A. Press the Enter key.



SWITCH C

38 Type the **configure terminal** command into the field. Press the Enter key.

39 Type the **interface gigabitethernet 0/4** command into the terminal. Press the Enter key.

40 Type the **shutdown** command into the terminal. Press the Enter key.

41 Type the **no switchport** command into the terminal. Press the Enter key.

42 Type the **ip address 192.168.2.2 255.255.255.0** command into the terminal. Press the Enter key.

43 Type the **no shutdown** command into the terminal. Press the Enter key.

44 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

45 Type the **router ospf** command into the terminal. Press the Enter key.

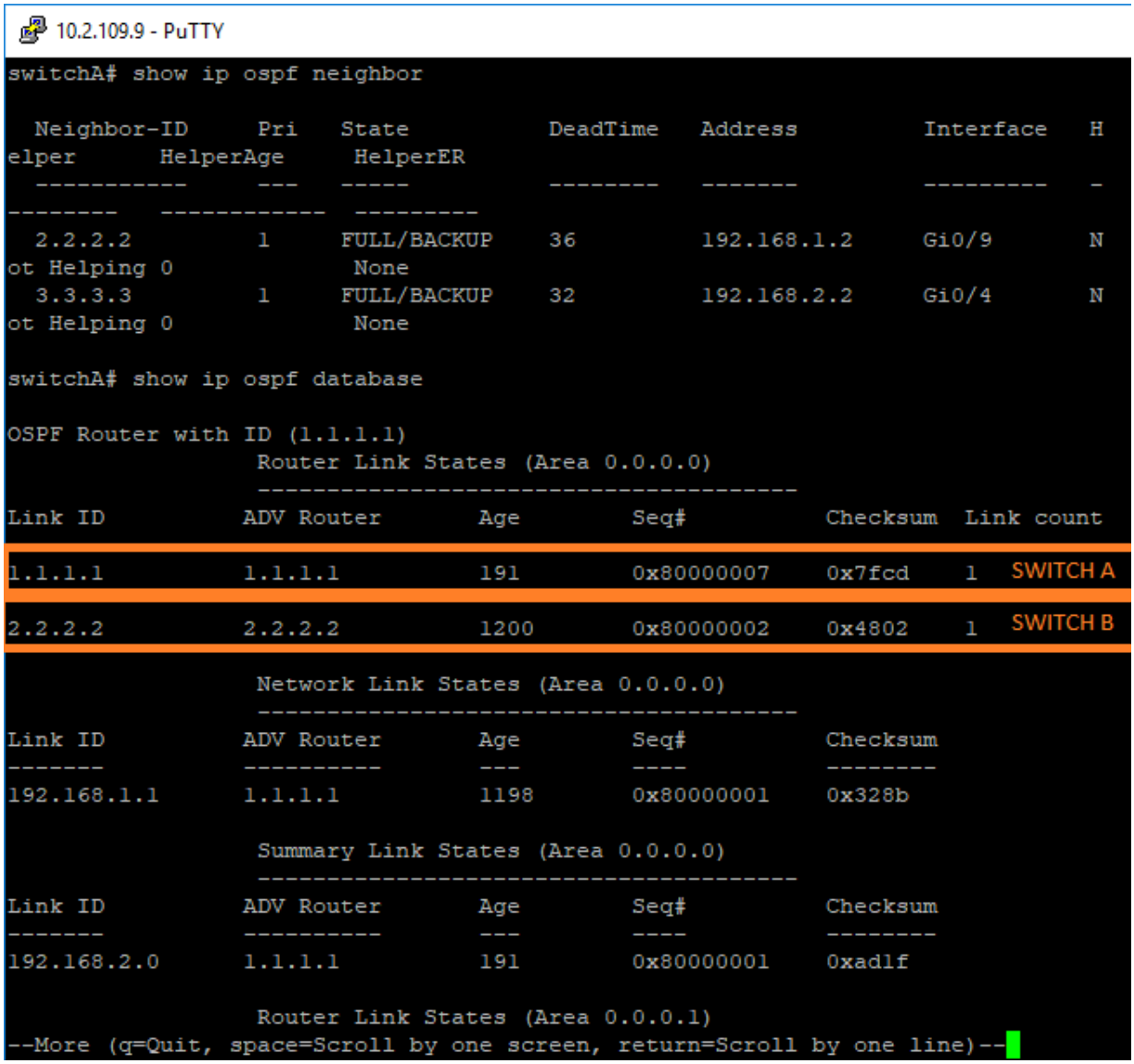
46 Type the **router-id 3.3.3.3** command into the terminal. Press the Enter key.

47 Type the **network 192.168.2.2 255.255.255.0 area 0.0.0.1** command into the terminal. Press the Enter key.

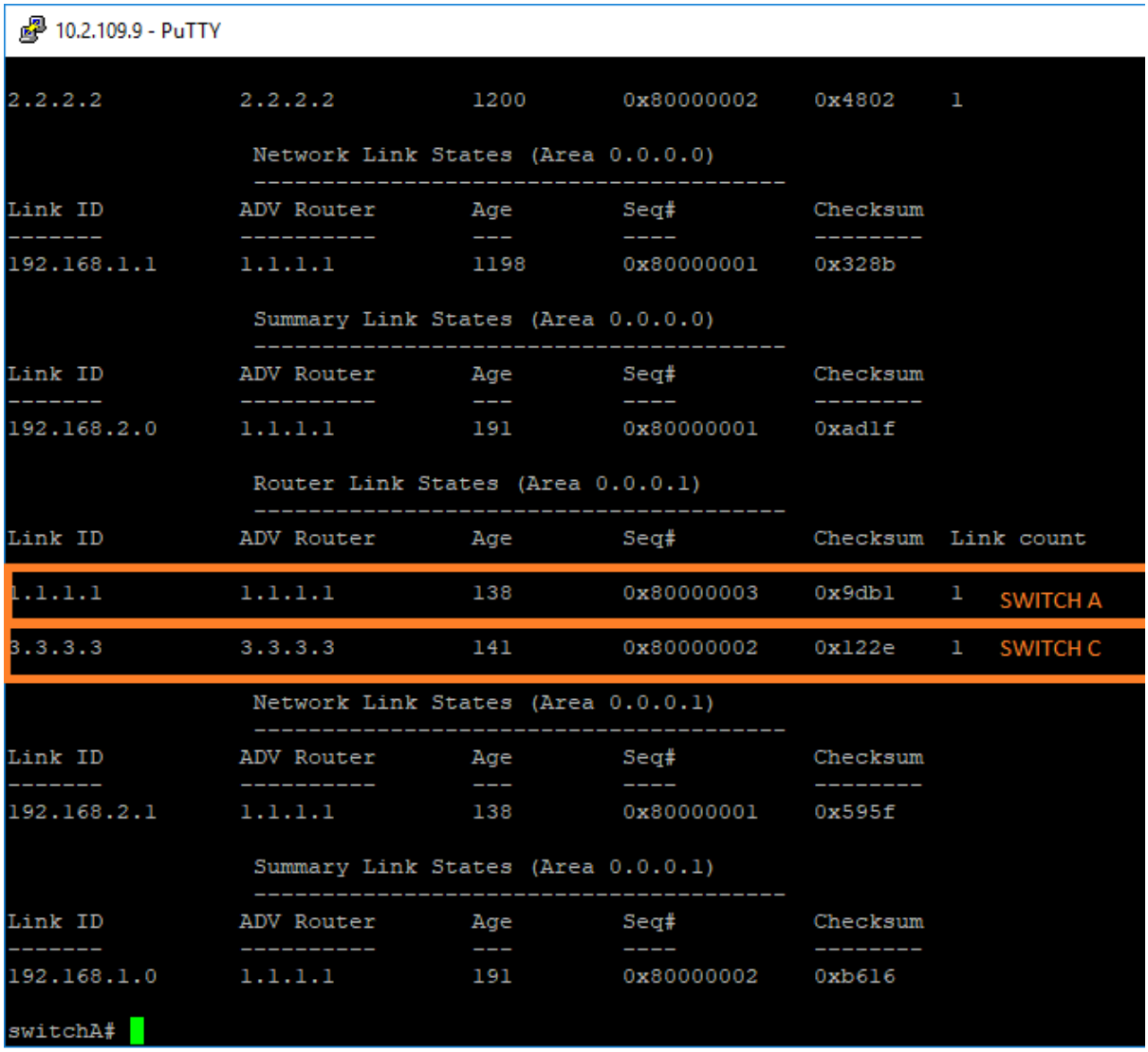
48 Type the **end** command into the terminal. Press the Enter key.

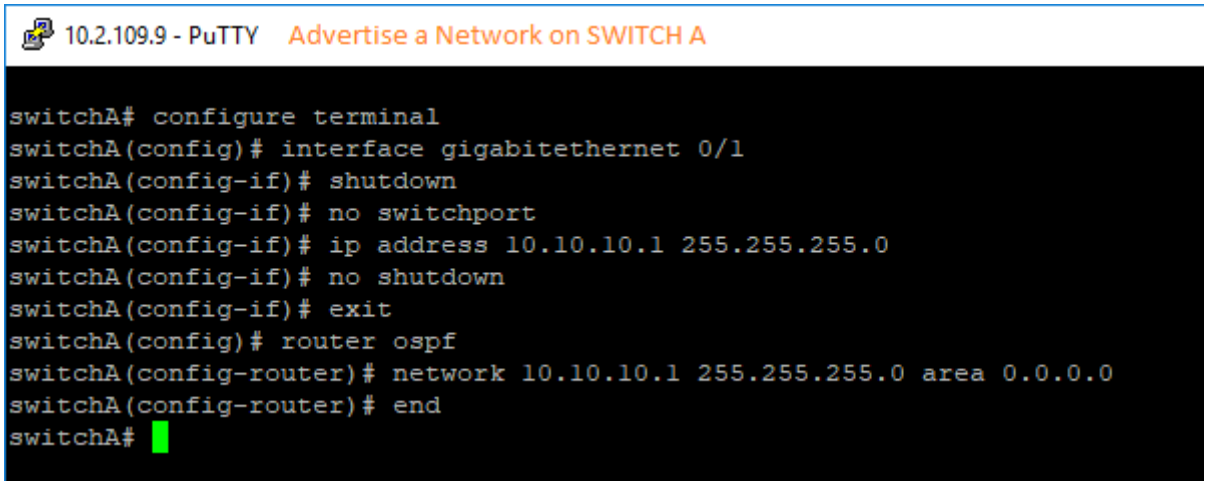
49 Type the **show ip ospf neighbor** command into the terminal (in switch A and switch C) to display the OSPF neighbor information list (verify the adjacency on switch A and C, between switch A and switch C on area 1). Press the Enter key.

50 Type the **show ip ospf database** command into the (in switch A and switch C) to display the OSPF Link State Database.



51 Press the Space key.





SWITCH A

52 Type the **configure terminal** command into the terminal. Press the Enter key.

53 Type the **interface gigabitethernet 0/1** command into the terminal. Press the Enter key.

54 Type the **shutdown** command into the terminal. Press the Enter key.

55 Type the **no switchport** command into the terminal. Press the Enter key.

56 Type the **ip address 10.10.10.1 255.255.255.0** command into the terminal. Press the Enter key.

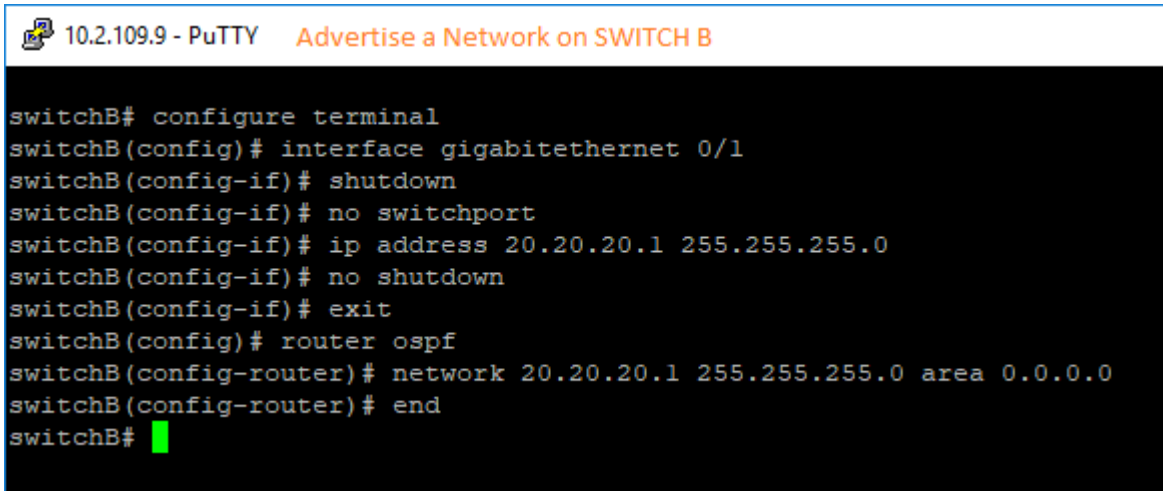
57 Type the **no shutdown** command into the terminal. Press the Enter key.

58 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

59 Type the **router ospf** command into the terminal. Press the Enter key.

60 Type the **network 10.10.10.1 255.255.255.0 area 0.0.0.0** command into the terminal. Press the Enter key.

61 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.



SWITCH B

62 Type the **configure terminal** command into the terminal. Press the Enter key.

63 Type the **interface gigabitethernet 0/1** command into the terminal. Press the Enter key.

64 Type the **shutdown** command into the terminal. Press the Enter key.

65 Type the **no switchport** command into the terminal. Press the Enter key.

66 Type the **ip address 20.20.20.1 255.255.255.0** command into the terminal. Press the Enter key.

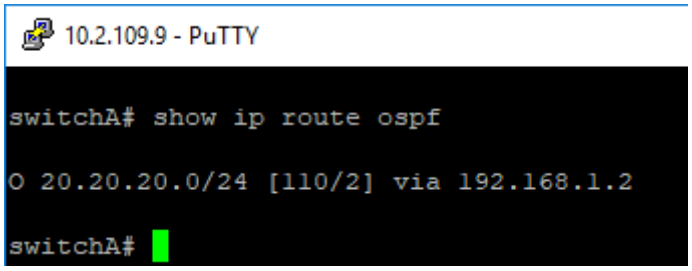
67 Type the **no shutdown** command into the terminal. Press the Enter key.

68 Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

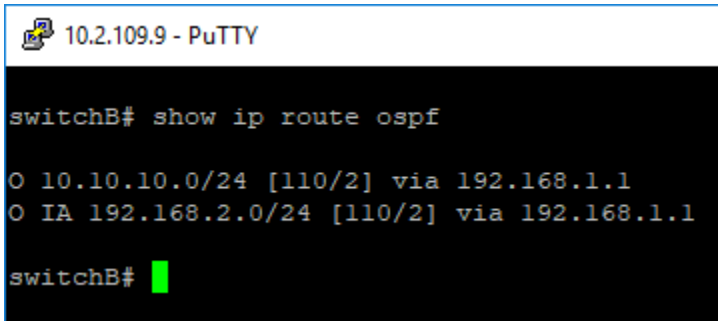
69 Type the **router ospf** command into the terminal. Press the Enter key.

70 Type the **network 20.20.20.1 255.255.255.0 area 0.0.0.0** command into the terminal. Press the Enter key.

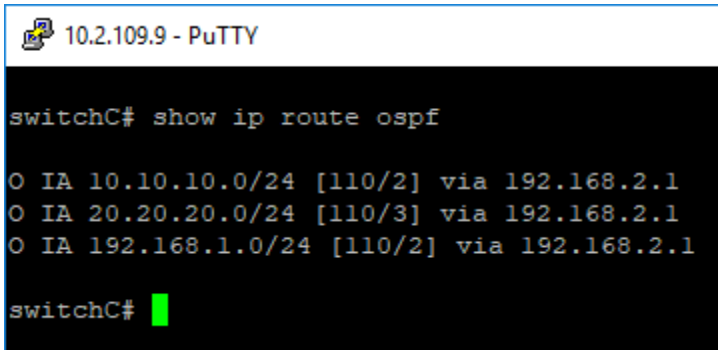
71 Type the **end** command into the terminal. Press the Enter key.



72 Type the **show ip route ospf** command into the terminal (on switch A) to display the IP routing table. Press the Enter key.



73 Type the **show ip route ospf** command into the terminal (on switch B). Press the Enter key.



74 Type the **show ip route ospf** command into the terminal (on switch C). Press the Enter key.

4 Management Features

4.1 DHCP Client

4.1.1 Managing DHCP Client

Feature Overview

DHCP Client uses DHCP protocol to temporarily receive a unique IP address for it from a DHCP server. It also receives other network configuration information such as default gateway IP address, DNS Server IP address, SNTP Server IP address from the DHCP server.

DHCP Client can be enabled on any IPv4 interface associated to existing VLANs, on Routed Interfaces or on the Out of Band interface.

Standards

- RFC 2131

Scaling Numbers

- DHCP Client can be enabled on 64 IPv4 Interfaces.

Limitations

N/A

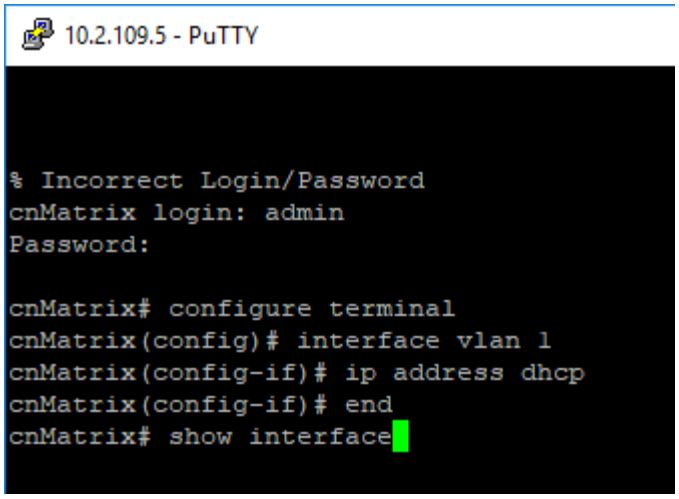
Default Values

- DHCP Client is enabled by default on VLAN 1.
- If DHCP fast mode is enabled, the default DHCP Client Discovery timer is 5.
- If DHCP fast mode is disabled, the default DHCP Client Discovery timer is 15.
- Tracking of the DHCP client operations is disabled.
- If DHCP fast mode is enabled, the default DHCP Client ARP check timer is 1.
- If DHCP fast mode is disabled, the default DHCP Client ARP check timer is 3.

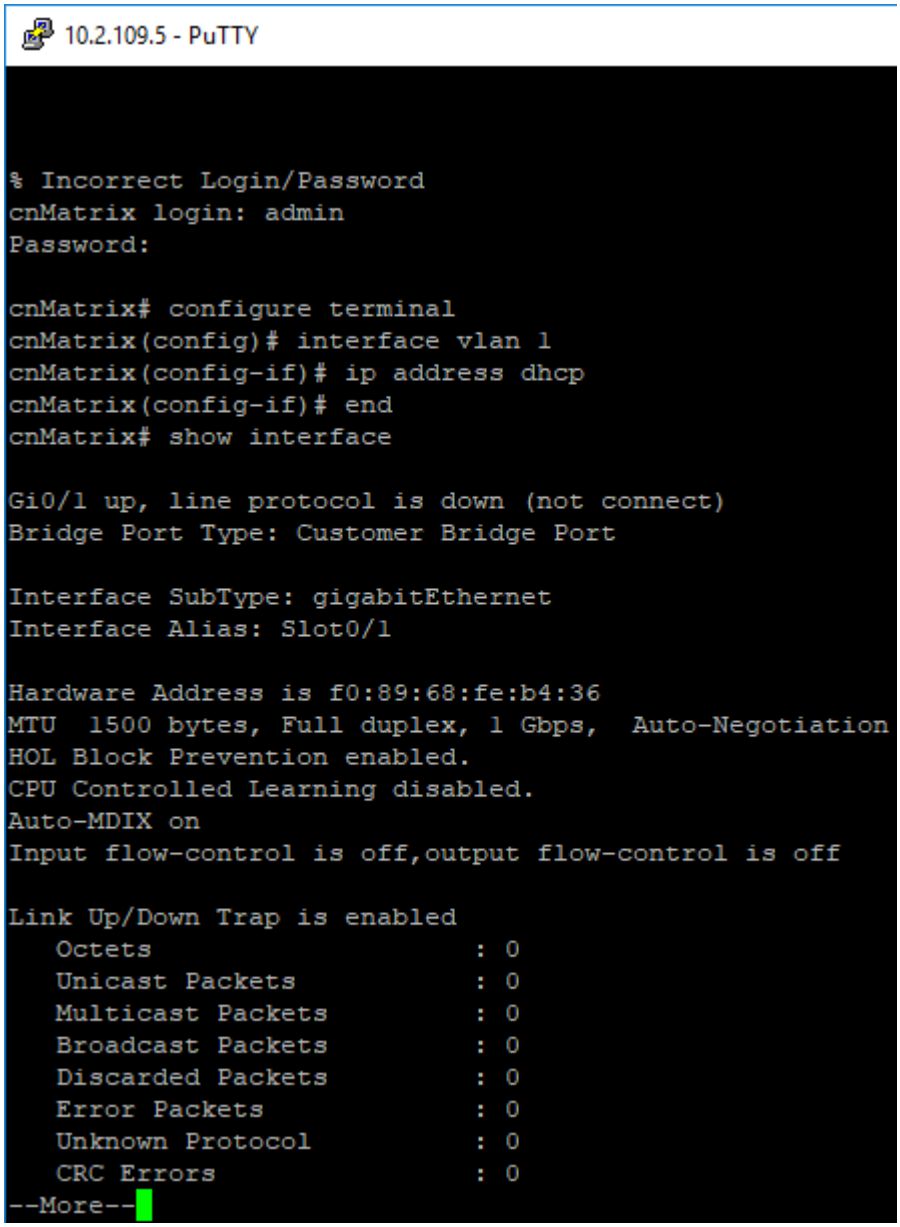
Prerequisites

N/A

4.1.2 How to Enable DHCP Client in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface vlan 1** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **ip address dhcp** command into the terminal to obtain an IP address through DHCP. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show interface** command into the terminal to display the interface status and configuration. Press the Enter key.



6 Press the Space key to move down with one page.

For more information, see DHCP Client Parameters and Commands.

4.2 DHCP Server

4.2.1 Managing DHCP Server

4.2.1.1 Feature Description

Feature Overview

DHCP Server maintains a configured set of IP address pools from which IP addresses are allocated to the DHCP Clients, whenever they request the Server dynamically.

Once the IP address is allocated, the Server will keep this IP as reserved until the lease time for that IP expires. If the Client does not renew the IP before the lease time expiry, this will be returned into the free pool and will be offered to new clients.

Standards

- RFC 2131
- RFC 2132

Scaling Numbers

- A maximum of 16 Address Pools can be configured.
- A maximum of 256 DHCP Clients per pool are supported.

Limitations

- DHCP Relay must be disabled before enabling the DHCP server.

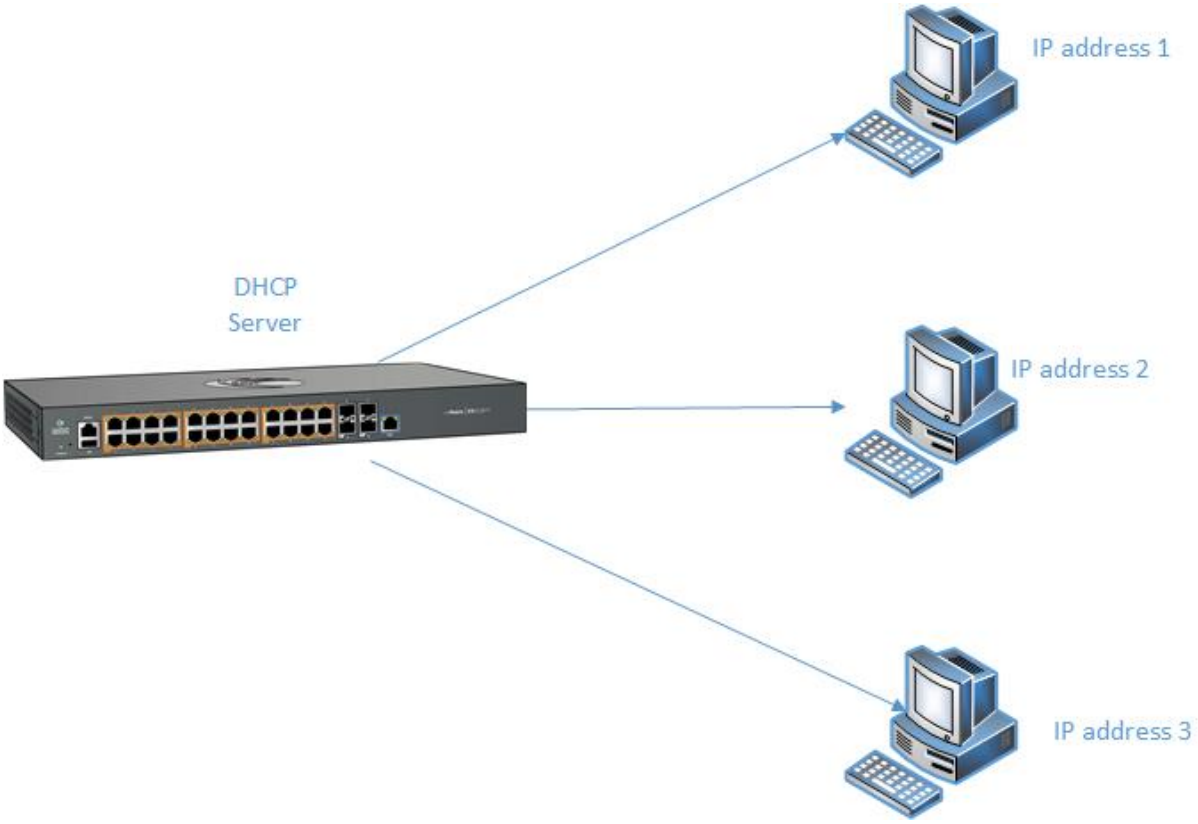
Default Values

- DHCP Server is disabled by default.
- ICMP echo is disabled by default.
- Offer reuse time out has a value of 5 seconds.
- DHCP server pool lease time is of 3600 seconds.
- DHCP server pool utilization threshold is 75%.

Prerequisites

- In order for the DHCP Server to respond to DHCP Clients requests from a certain subnet, the administrator must create a VLAN and a IPv4 interface with configured address associated to the DHCP Clients subnet.

4.2.1.2 Network Diagram



4.2.2 Configuring DHCP Static Mapping

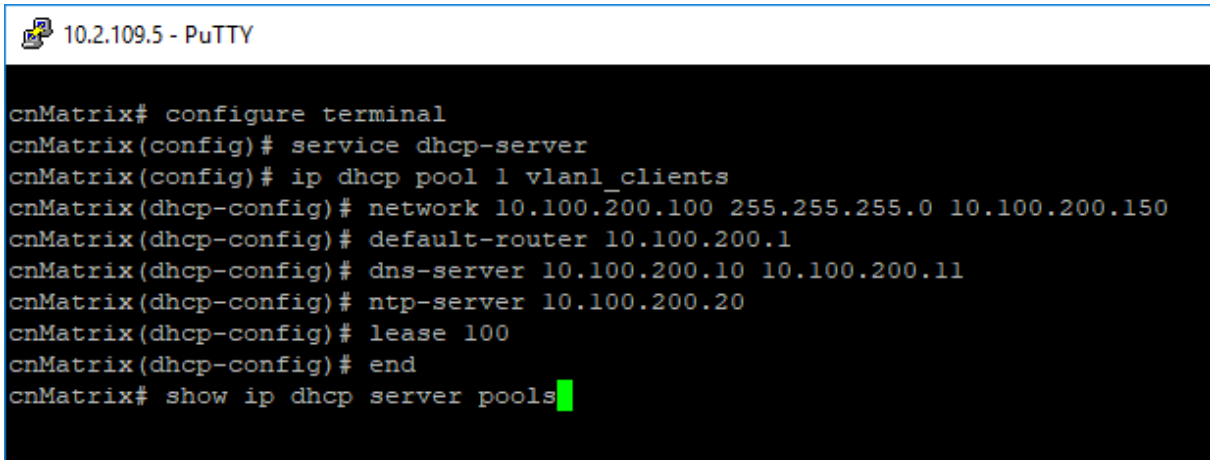
```
10.2.109.5 - PuTTY

cnMatrix# configure terminal
cnMatrix(config)# ip dhcp pool 1
cnMatrix(dhcp-config)# host hardware-type 1 client-identifier 00:11:22:33:44:04 ip 101.101.101.16
cnMatrix(dhcp-config)# end
cnMatrix# show ip dhcp server pools

Host Configurations
-------------------
Client Identifier             IP address
00:11:22:33:44:04             101.101.101.16

cnMatrix#
```

1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **ip dhcp pool 1** command into the terminal to create the DHCP address pool. Press the Enter key to create a DHCP address pool.
3. Type the **host hardware-type 1 client-identifier 00:11:22:33:44:04 ip 101.101.101.16** command into the terminal to set a host option. Press the Enter key.

- 00:11:22:33:44:04 = MAC address
- 101.101.101.6 = IP address

4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show ip dhcp server pools** command into the terminal to display the DHCP server pools. Press the Enter key.

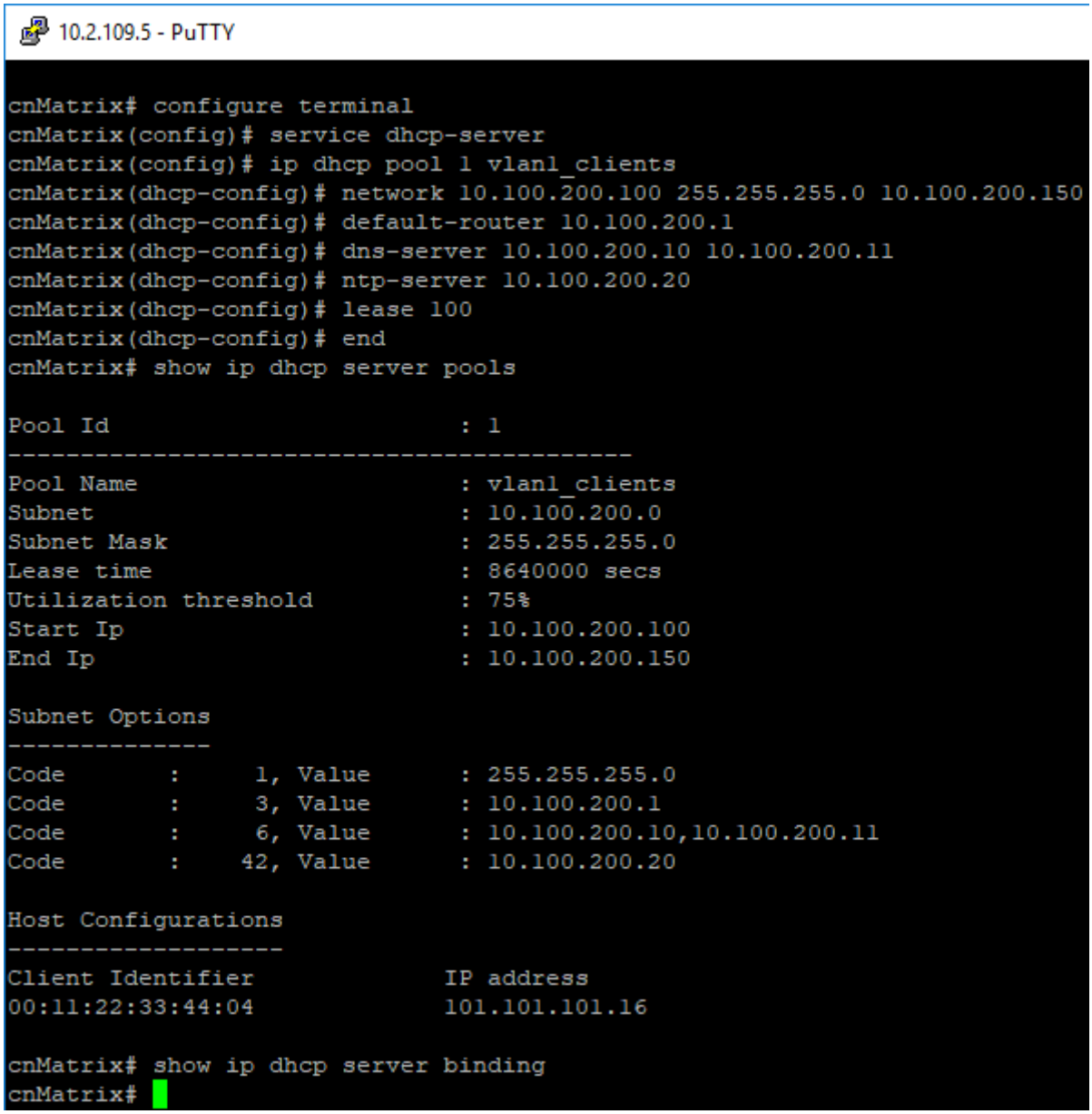
4.2.3 Configuring DHCP Address Pool



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **service dhcp-server** command into the terminal to enable the DHCP Server feature. Press the Enter key
3. Type the **ip dhcp pool 1 vlan1_clients** command into the terminal to create a name for the DHCP server address pool and to go to the dhcp configuration mode. Press the Enter key.
4. Type the **network 10.100.200.100 255.255.255.0 10.100.200.150** command into the terminal to specify the subnet network mask. Press the Enter key.
5. Type the **default-router 10.100.200.1** command into the terminal to specify the IP address of the default router for a DHCP client. Press the Enter key
6. Type the **dns-server 10.100.200.10 10.100.200.11** command into the terminal to specify the IP address of a DNS server that is available to a DHCP client. Press the Enter key
7. Type the **ntp-server 10.100.200.20** command into the terminal to specify the IP address of a NTP server that is available to a DHCP client. Press the Enter key.
8. Type the **lease 100** command into the terminal to specify the duration of the lease. Press the Enter key.

> The default duration of the lease: one day.

9. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
10. Type the **show ip dhcp server pools** command into the terminal to display the DHCP server pools. Press the Enter key.



11 Type the **show ip dhcp server binding** command into the terminal to display the DHCP server binding information. Press the Enter key.

For more information, see DHCP Server Parameters and Commands.

4.3 Out-of-Band Management

4.3.1 Managing Out-of-Band Ethernet Management

4.3.1.1 Feature Description

The **Out Of Band (OOB)** dedicated port provides management connectivity isolated from user – data plane - traffic.

Benefits:

- Separating user and management traffic provides extra security and reliability for the management traffic.
- Offers redundancy in management connectivity (dedicated network resources).
- Prevents data plane misconfiguration from impacting management connectivity.

Disadvantages of using OOB rather than in-band ports for management:

- Extra cost and effort are required for maintaining a separate network for management purposes only.

Standards

N/A

Scaling Numbers

N/A

Limitations

- IPv6 not supported on OOB port.

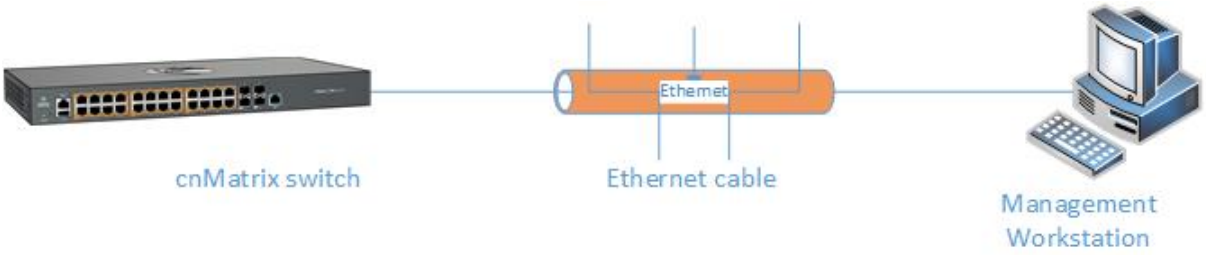
Default Values

- Default IP address on OOB port is 192.168.0.1, with a prefix length of 24.

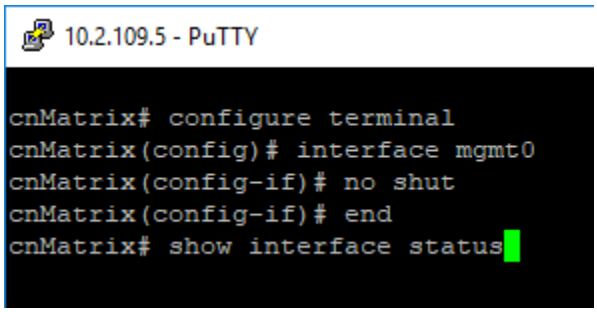
Prerequisites

N/A

4.3.1.2 Network Diagram

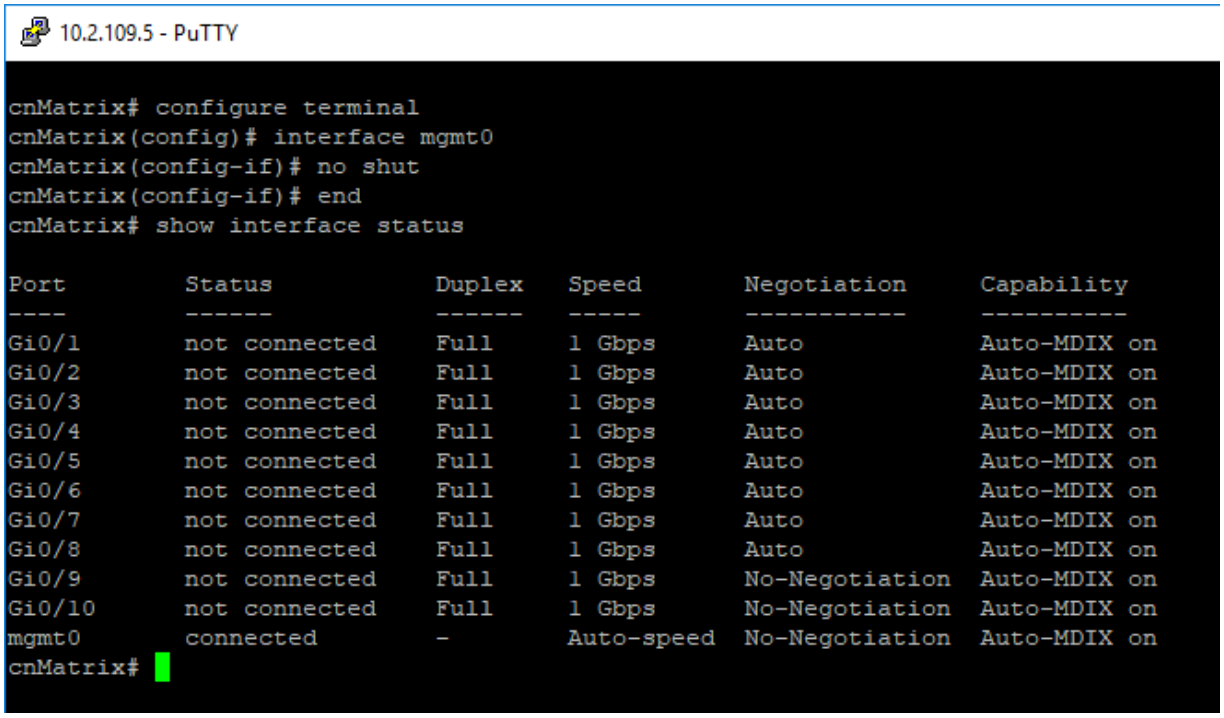


4.3.2 Configuring Out-of-band Ethernet Management in CLI Interface



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface mgmt0** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **no shut** command into the terminal to set the admin status of the interface as up. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

5 Type the **show interface status** into the terminal to display the interface status and configuration. Press the Enter key.



For more information, see Out of Band Ethernet Management Parameters and Commands.

4.4 Telnet Server

4.4.1 Managing Telnet Server

Feature Overview

Telnet is an industry standard protocol for accessing remote systems using TCP protocol. **Telnet Server** allows clients to authenticate using an user and a password and then provide access to a CLI session.

The Telnet protocol exchanges unencrypted data and is vulnerable to spoofing when used over public networks, thus it is recommended **NOT** to use it in live deployments.

Standards

- RFC 854

Scaling Numbers

- 8 sessions are accepted.

Limitations

N/A

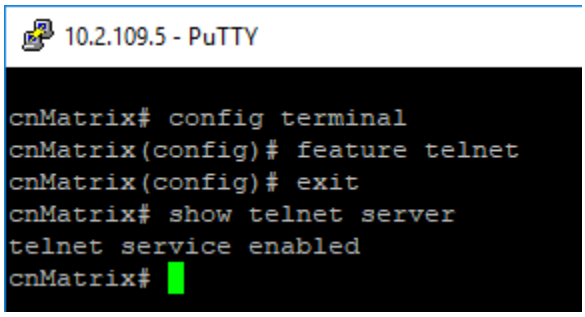
Default Values

- The Telnet Server feature is disabled by default.
- The TCP listening port is 23.

Prerequisites

N/A

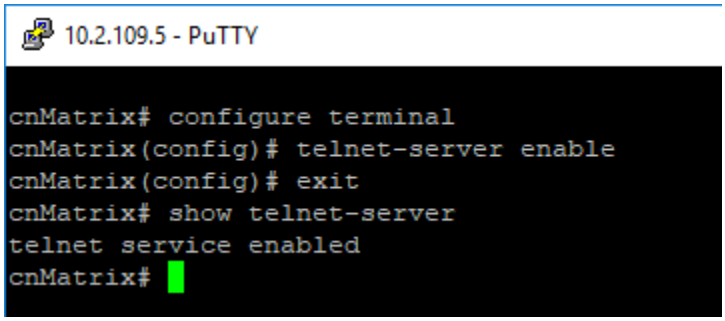
4.4.2 How to Enable Telnet Server in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **feature telnet** command into the terminal to enable the telnet service. Press the Enter key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.
4. Type the **show telnet server** command into the terminal to display the telnet server status. Press the Enter key.

For more information, see Telnet Client/Telnet Server Parameters and Commands.

4.4.3How to Enable Telnet Server in CLI Interface (Starting with version 2.1)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **telnet-server enable** command into the terminal to enable the telnet service. Press the Enter key..
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show telnet-server** into the terminal to display the telnet server status. Press the Enter key..

For more information, see Telnet Client / Telnet Server Parameters and Commands.

4.4.4 Troubleshooting Telnet Client/Telnet Server

Useful commands for troubleshooting:

```
cnMatrix#show telnet-client

cnMatrix#show telnet server

cnMatrix#show users – see active connections
```

4.5 System Resource Monitoring

4.5.1 Managing System Resource Monitoring

Feature Overview

The **System Resource Monitoring** feature enables the users to monitor the general status of the devices.

Standards

N/A

Scaling Numbers

N/A

Limitations

- Fan and temperature information is available only on EX2028-P.

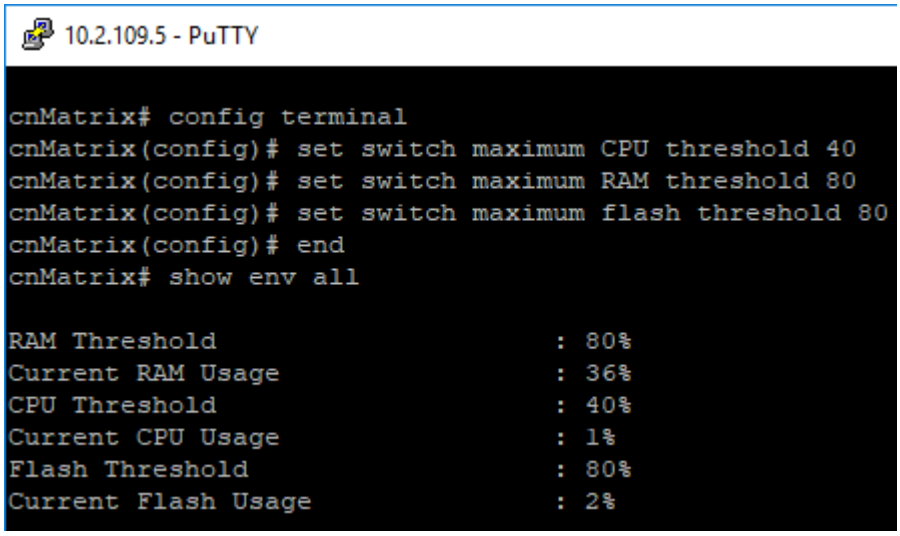
Default Values

- The default threshold RAM, CPU and Flash value is 100% by default.

Prerequisites

N/A

4.5.2 Configuring System Resource Monitoring in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **set switch maximum CPU threshold 40** command into the terminal to set the maximum CPU threshold value(in percentage). Press the Enter key.
3. Type the **set switch maximum RAM threshold 80** command into the terminal to set the maximum RAM threshold value (in percentage). Press the Enter key.
4. Type the **set switch maximum flash threshold 80** command into the terminal to set the maximum flash threshold value (in percentage). Press the Enter key.
5. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
6. Type the **show env all** into the terminal to display the switch related information, such as

CPU, Flash and RAM usages. Press the Enter key.

For more information, see System Resource Monitoring Parameters and Commands.

4.5.3 Troubleshooting System Resource Monitoring

Useful commands for troubleshooting:

```
cnMatrix#show env all
```

4.6 Syslog

4.6.1 Managing Syslog

Feature Overview

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

Standards

- The syslog protocol is described in RFC5424.

Scaling Numbers

- There are 8 severity levels: alerts, emergencies, critical, error, warnings, informational, notification, debugging.
- There are 8 available facilities (local0-7).

Limitations

- A maximum of 8 logging entries can created
- The maximum length of the DNS host name is 64 characters.

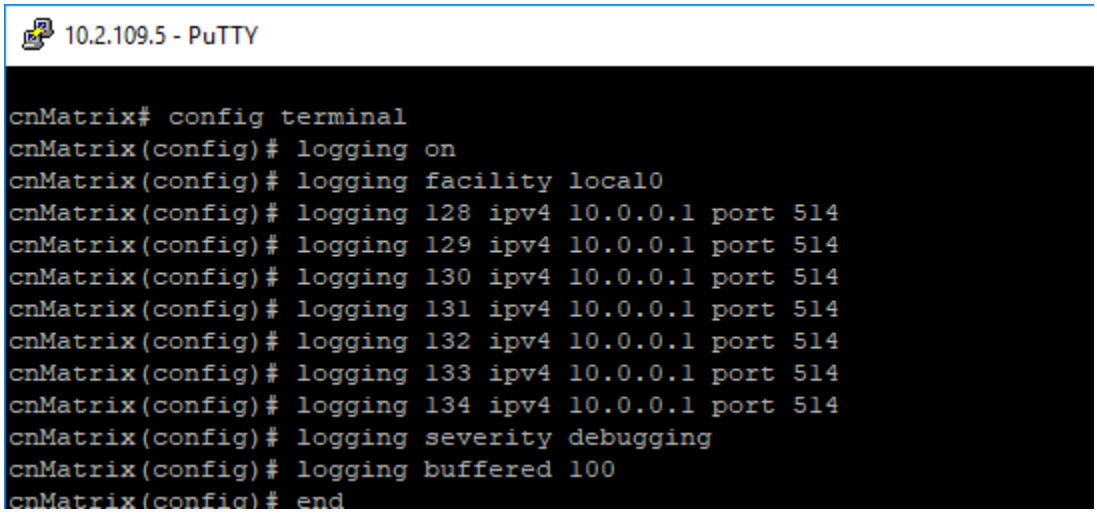
Default Values

- Syslog logging is enabled by default.
- Console logging is enabled by default.
- Severity logging is set to critical by default.
- Buffered size: 50 entries by default.
- The TimeStamp option is enabled by default.

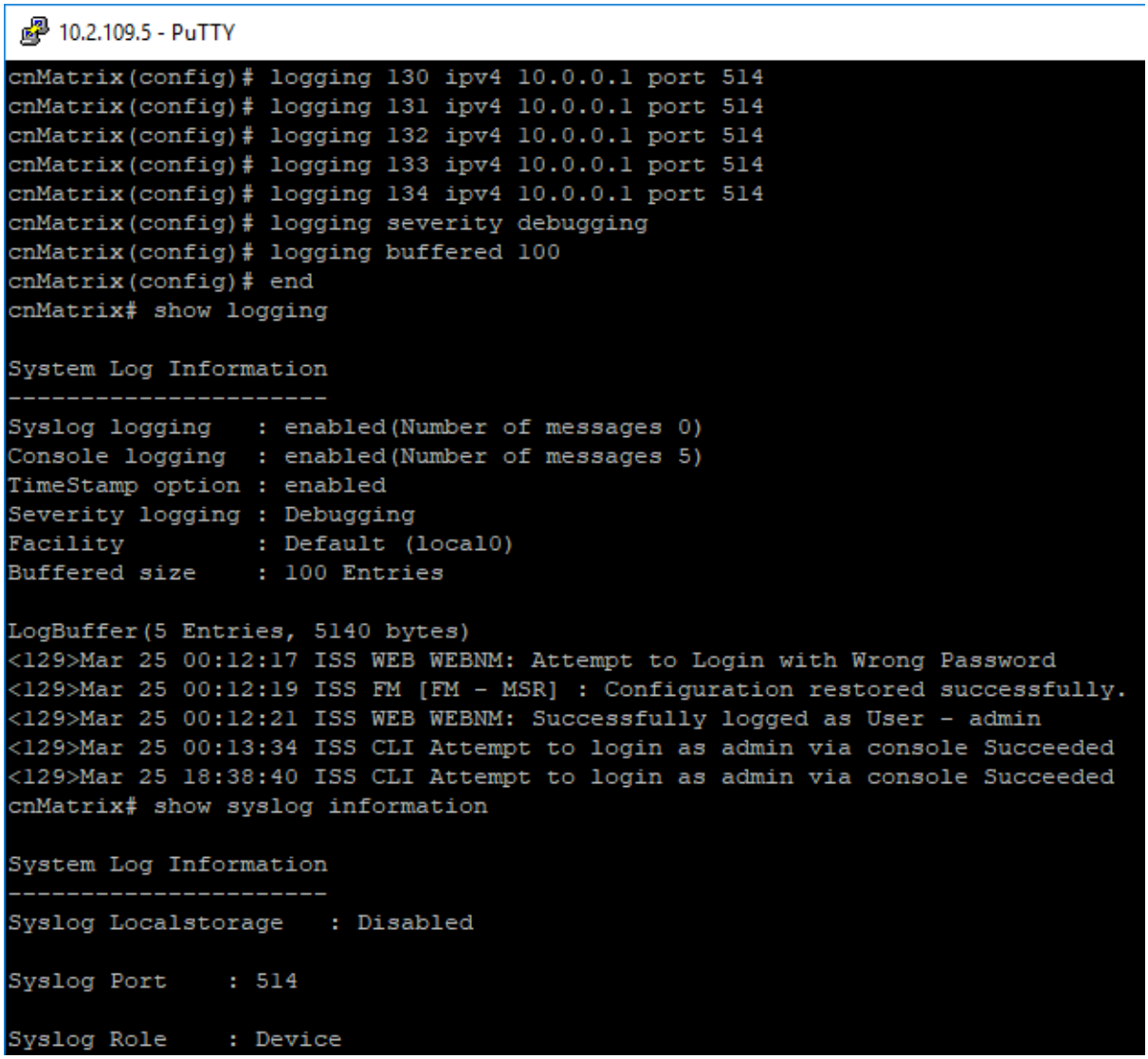
Prerequisites

- Before configuring a Cambium device to send syslog messages, the right time and date should be configured. When using NTP, a correct and synchronized system clock on all devices within the network is guaranteed.
- Before configuring a Cambium device to send syslog messages, the device should be able to reach the external device on which the messages will be stored.

4.6.2How to Enable and Configure Syslog in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **logging on** command into the terminal to enable the syslog server. Press the Enter key.
3. Type the **logging facility local0** command into the terminal. Press the Enter key.
4. Type the **logging 128 ipv4 10.0.0.1 port 514** command into the terminal to add an entry into the logging-server table. Press the Enter key.
5. Type the **logging 129 ipv4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
6. Type the **logging 130 ipv4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
7. Type the **logging 131 ipv4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
8. Type the **logging 132 ipv4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
9. Type the **logging 133 ip v4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
10. Type the **logging 134 ipv4 10.0.0.1 port 514** command into the terminal. Press the Enter key.
11. Type the **logging severity debugging** command into the terminal to set the severity logging syslog parameter. Press the Enter key.
12. Type the **logging buffered 100** command into the terminal to set the buffered size syslog parameter. Press the Enter key.
13. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
14. Type the **show syslog information** into the terminal to display the syslog information. Press the Enter key.



For more information, see SYSLOG Parameters and Commands.

4.6.3Troubleshooting Syslog

Useful commands for troubleshooting:

- cnMatrix# show syslog file-name
- cnMatrix# show syslog information
- cnMatrix# show syslog localstorage
- cnMatrix# show logging

4.7 SNMP

4.7.1 Managing SNMP

4.7.1.1 Feature Description

Feature Overview

SNMP (Simple Network Management Protocol) is the most widely used network management protocol on TCP/IP based networks.

SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as a part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. In addition, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models, etc. With SNMPv3, the SNMP communication is completely safe and secure.

Standards

- RFC 1157
- RFC 1901
- RFC 1908
- RFC 3416
- RFC 3410-3417

Scaling Numbers

- N/A_

Limitations

- N/A

Default Values

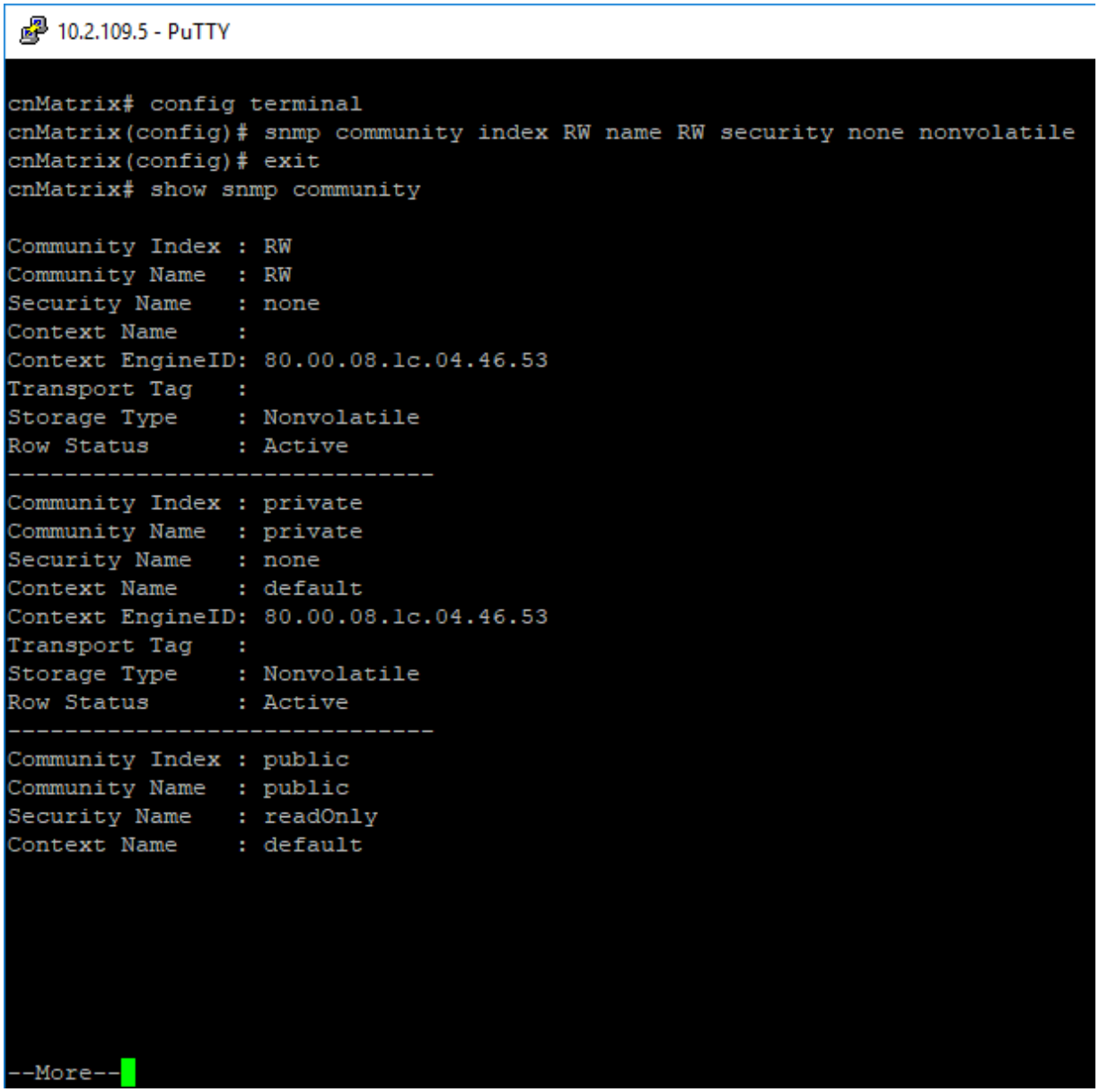
- SNMP agent is enabled by default.
- SNMP Coldstart trap is enabled by default.
- Storage Type: Non-Volatile by default.
- Row Status : Active by default.
- Sub-tree OID: 1 by default.
- Sub-tree Mask: 1 by default.
- Community names: private, public.
- Group security models: v1, v2c, v3.

4.7.1.2 Network Diagram

4.7.2 How to Enable and Configure SNMP V2 in CLI Interface

```
10.2.109.5 - PuTTY

cnMatrix# config terminal
cnMatrix(config)# snmp community index RW name RW security none nonvolatile
cnMatrix(config)# exit
cnMatrix# show snmp community
```

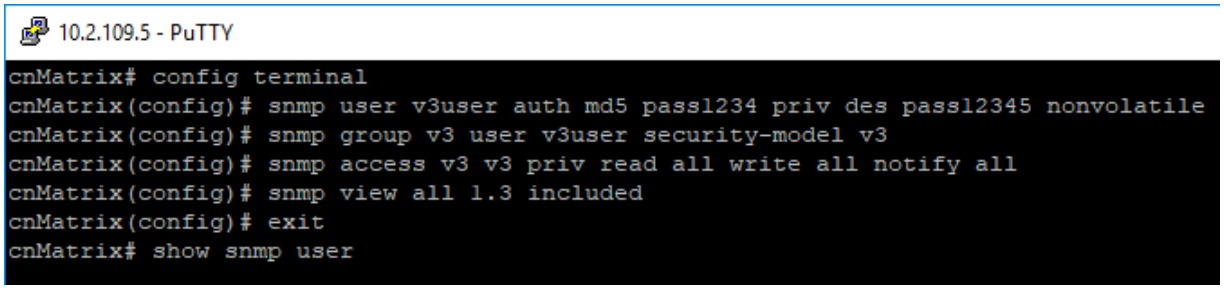
1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **snmp community index RW name RW security none nonvolatile** command into the terminal to configure the SNMP community details. Press the Enter key.
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show snmp community** command into the terminal to display the configured SNMP community details. Press the Enter key.



5 Press the Space key.

For more information, see SNMP Parameters and Commands.

4.7.3 How to Enable and Configure SNMP V3 in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **snmp user v3user auth md5 pass1234 priv des pass12345 nonvolatile** command into the terminal to configure the SNMP user details. Press the Enter key.

3 Type the **snmp group v3 user v3user security-model v3** command into the terminal to configure the details for the SNMP group. Press the Enter key.

4 Type the **snmp access v3 v3 priv read all write all notify all** command into the terminal to configure the SNMP group access details. Press the Enter key.

5 Type the **snmp view all 1.3 included** command into the terminal to configure SNMP view. Press the Enter key.

6 Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

7 Type the **show snmp user** command into the terminal to display the configured SNMP users. Press the Enter key.

8 Type the **show snmp group** command into the terminal to display the configured SNMP groups. Press the Enter key.

9 Type the **show snmp group access** command into the terminal to display configured SNMP group access details. Press the Enter key.

10 Type the **show snmp viewtree** command into the terminal to display configured SNMP tree views. Press the Enter key.

For more information, see SNMP Parameters and Commands.

4.8 SSH

4.8.1 Managing SSH

4.8.1.1 Feature Description

Secure Shell is a protocol for secure remote login and other secure network services over an insecure network. It runs on top of the transport layer and is basically a replacement for insecure telnet services to the switch.

The SSH protocol uses a client server model. cnMatrix contains both SSH server and SSH client implementations. The SSH server implementation is the OpenSSH version 7.9 server integrated into the cnMatrix software. The SSH server interoperates with the following SSH clients.

- PuTTY SSH 0.71 for Windows 95/98/2000/NT.
- TTSSH (TeraTerm) 1.5.4 for Windows 95/98/2000/NT.
- OpenSSH client for Linux.

Standards

- The SSH (IPv4/IPv6) client is RFC 1321 compliant.
- The SSH (IPv4/IPv6) server is RFC 4250 RFC 4251 RFC 4252 RFC 4253 RFC 4254 and RFC 4256 compliant.

Scaling Numbers

- The number of simultaneous supported SSH sessions is 8.

Default Values

- The SSH server and SSH client are enabled by default.
- The debugging option is disabled by default.
- The maximum number of bytes allowed in an SSH transport connection is set to 32768 by default.

- The default primary port number: 22.
- The following cipher algorithms are set by default: CHACHA20-POLY1305, 3DES-CBC, AES128-CBC, AES256-CBC, AES128-CTR, AES256-CTR, AES128-GCM, and AES256-GCM
- The default MAC algorithms: HMAC-SHA2-512-ETM, HMAC-SHA2-256-ETM, HMAC-SHA2-512, HMAC-SHA
  2-256.

Limitations

- Normally the SSH protocol allows cipher algorithms for the incoming and the outgoing direction to be configured independently. But in cnMatrix, SSH cipher configuration must be the same for both directions. This is to ensure that the configuration is simple.
- Compression is not supported.
- The key exchange algorithm, and the public key algorithm have default values and cannot be configured
- The SSH server is fairly resistant to any kind of security attack. But the Cipher Block Chaining (CBC) mode reveals information about the plain text if two cipher text blocks encrypted under the same key are equal. Since rekeying is not supported prolonged active session may lead to a security threat.
- The SSH server may be susceptible to the man-in-the-middle attacks when the server communicates with the client for the first time. When the server sends its public key for the first time to the client, the client does not have any binding of the server's public key to the identity of the server. In that case, an attacker can substitute his public key and signature in place of server's public key. The user in turn will send his password to the attacker thus resulting in a security break.
- The SSH client session cannot be established by providing the hostname. Also, SSH client does not support all the options available in normal SSH Client feature.
- cnMatrix does not store the keys used for creating SSH client sessions.
- The SSH client sessions cannot be established via SNMP and Web.

The SSH server provides a secure channel over which cnMatrix CLI is accessed and offers the following:

- Protocol version exchange for version compatibility check.
- Data integrity by including Message Authentication Code with each packet.
- Cipher and key exchange algorithms negotiation between two communicating entities.
- Key exchange mechanism.
- Encryption and server authentication.

The cnMatrix SSH server implementation supports the following:

- Algorithms:
  - Cipher algorithms – CHACHA20-POLY1305, 3DES-CBC, AES128-CBC, AES256-CBC, AES128-CTR, AES256-CTR, AES128-GCM, and AES256-GCM.
  - MAC algorithms - HMAC-SHA2-512-ETM, HMAC-SHA2-256-ETM, HMAC-SHA2-512, HMAC-SHA
    2-256.
  - Version compatibility flag (SSH 1.0 support) – a user can use this to change the protocol version support to SSH 1.0 or SSH 2.0.
  - The key exchange algorithms supported are Diffie-hellman-group1sha1 and Diffie-

hellman-group14-sha1. The SSH server uses the key generated during the key exchange for data encryption and providing data integrity.

- The Public Key algorithms supported are ssh-rsa and ssh-dss.

- Authentication using username and password.

- Timer for authentication and sends a disconnect message in case the timer expires. The timeout period is 10 minutes. The SSH server allows a maximum of 10 authentication attempts by the user. If the threshold is reached, the server sends a disconnect message to the client.

The SSH server implementation does not support the following:

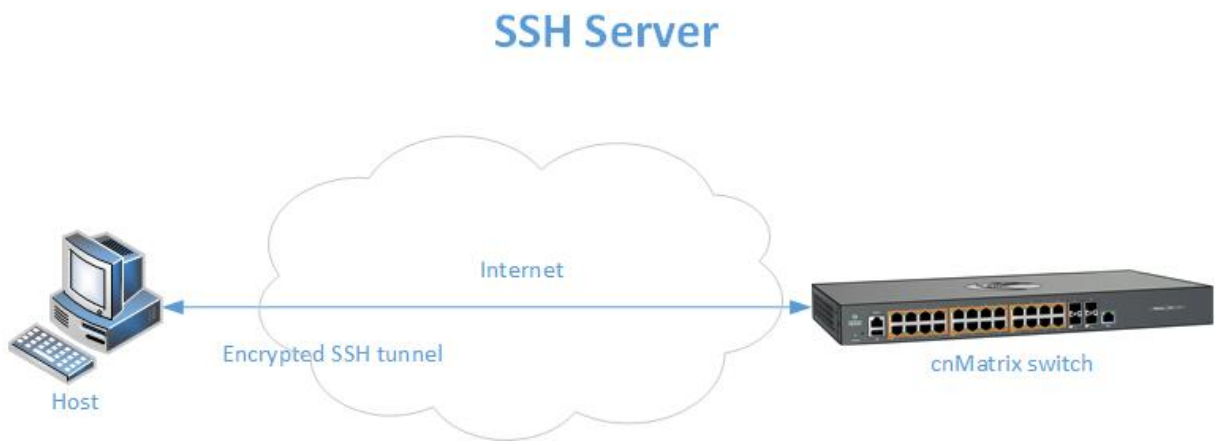
- Certificates for server and user authentication
- Session re-keying after a specified time interval or after a specified amount of data transfer.
- User authentication using public key, because it is mandatory for the server to validate the public key and also to verify the signature sent by the client. This is not possible without the out of band transfer of client's public key to the server or some trusted authority like certificate authorities.
- Host based authentication.
- TCP/IP forwarding or X11 forwarding.

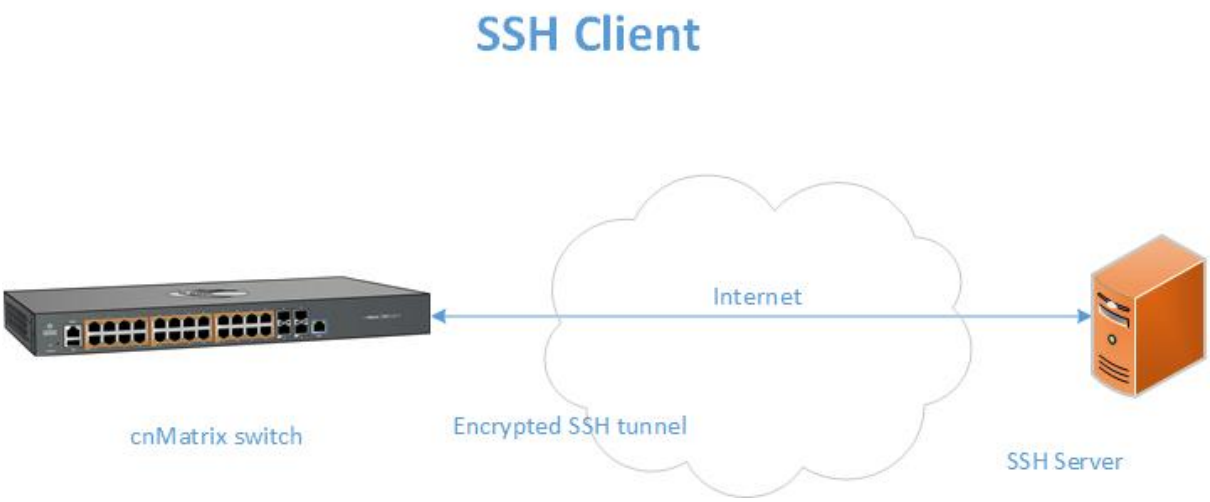
The SSH Client functionality is implemented in cnMatrix by integrating PuTTY (version 0.60) open source code. The SSH client session to any reachable host can be established from cnMatrix through CLI. SSH client feature can be enabled or disabled through SNMP and CLI. SSH client supports both Ipv4 and Ipv6 addresses.

Options supported in SSH client :

- - 1 - Forces SSH to try protocol version 1 only.
- - 2 - Forces SSH to try protocol version 2 only.
- - 4 - Forces SSH to use Ipv4 addresses only.
- - 6 - Forces SSH to use Ipv6 addresses only.
- - A - Enables forwarding of the authentication agent connection.
- - a - Disables forwarding of the authentication agent connection.
- - C - Requests compression of all data.
- -N - Do not execute a remote command.
- - s - The subsystem is specified as the remote command. (SSH-2 only).
- - T - Disables pseudo-tty allocation.
- - t - Enables pseudo-tty allocation.
- -v - show verbose messages.
- -V - print version information.
- -i identity_file – Specifies the private key file for authentication.
- -l login_name - Specifies the user to log in as on the remote machine.
- -p port - Specifies the port to connect on the remote host.

4.8.1.2 Network Diagram

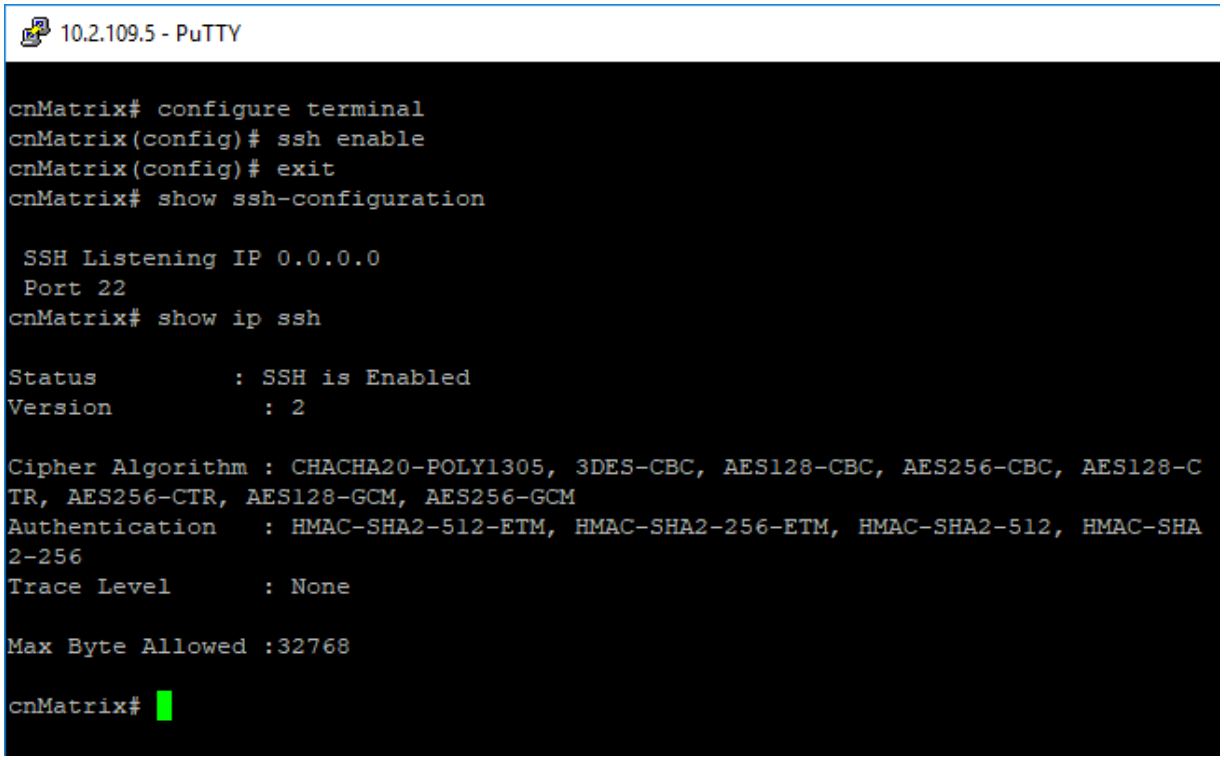




4.8.2How to Enable SSH in CLI Interface

1. Type the **configure terminal** command into the terminal.
3. Type the **ssh enable** command into the terminal to enable the SSH subsystem. Press the Enter key.
5. Type the **exit** command into the terminal to go back to the Privileged EXEC mode.
7. Type the **show ssh-configuration** command into the terminal to display the SSH server IP and port information. Press the Enter key.
9. Type the **show ip ssh** command into the terminal to display SSH server information. Press the Enter key.

Attention: The SSH feature is enabled by default



4.8.3 Troubleshooting SSH

Useful command for troubleshooting:

```
cnMatrix# show ssh-client

cnMatrix# show ssh-configurations

cnMatrix#show users – see active connections
```

4.9 IPv6 Management

4.9.1 Managing IPv6 Management

Feature Overview

Internet Protocol version 6 (IPv6) has been added as a successor of the Internet Protocol version 4, which expands the number of network address bits from 32 bits to 128 bits. After implementing this protocol in the cnMatrix switch, there is a clear improvement of the user experience and of the security when transitioning from IPv4 to IPv6.

Standards

- RFC2460

Scaling Numbers

- One IPv6 interface is supported.
- Multiple IPv6 link-local addresses on an interface are not supported.

Limitations

- IPv6 is not supported on routed interfaces.

Default Values

- ICMPv6 Error Rate Limiting option is enabled.
- ICMPv6 Rate-Limit interval value is 100.
- ICMPv6 Error Rate-Limit Bucket size is 10.
- ICMPv6 Redirect option is disabled.

Prerequisites

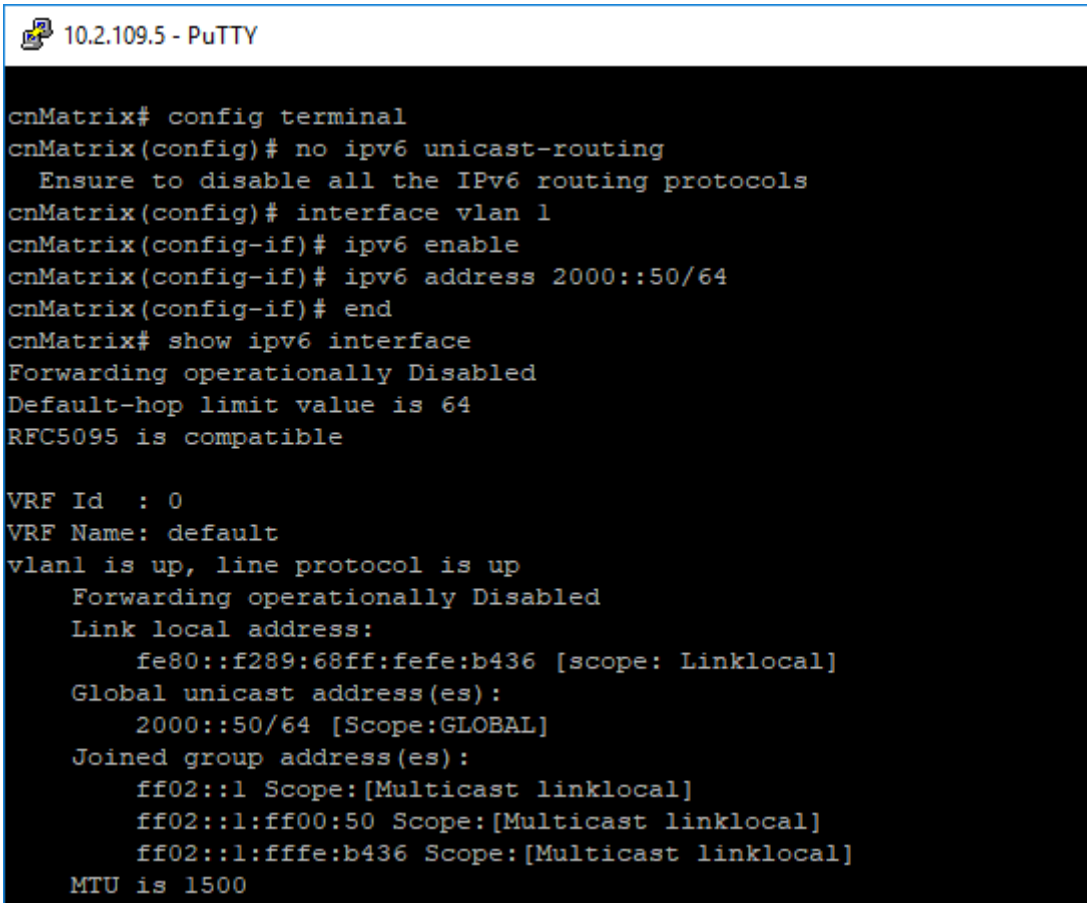
For the IPv6 interface to run in HOST mode and SLAAC to work properly, the administrator needs to perform the following command:

```
no ipv6 unicast-routing
```

The IPv6 addresses are not case-sensitive.

If the switch is linked to an IPv6 Router, capable of sending IPv6 Router Advertisements, an IPv6 address will be automatically configured. In order for you to assign a specific IPv6 address, you need to perform the following configuration: *ipv6 unicast-routing*.

4.9.2How to Enable and Configure IPv6 in CLI Interface



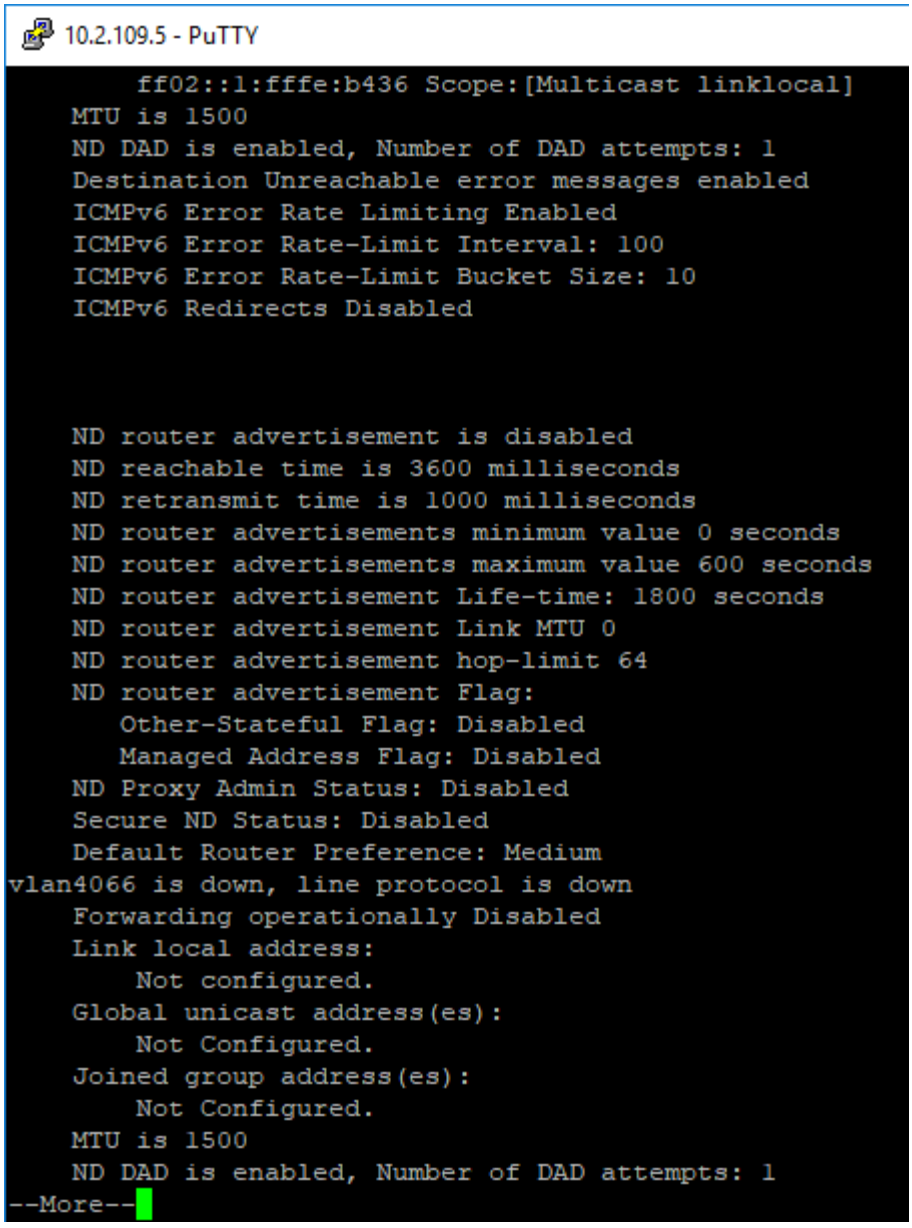
1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **no ipv6 unicast-routing** command into the terminal to run IPv6 in Host mode. Press the Enter key.
3. Type the **interface vlan 1** command into the terminal to select the interface to be configured. Press the Enter key.
4. Type the **ipv6 enable** command into the terminal to enable IPv6 on the selected interface. Press the Enter key.

5 Type the **ipv6 address 2000::50/64** command into the terminal to configure IPv6 address and Prefix lenght on the interface. Press the Enter key.

6 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

7 Type the **show ipv6 interface** command into the terminal to display the IPv6 interface information. Press the Enter key.

8 Press the Space key.



For more information, see IPv6 Management Parameters and Commands.

4.10 Reload (Starting with version 2.1)

4.10.1 Managing Reload

Feature Overview

The **Reload** feature has been added so that you can schedule a specific time for the switch to reboot

itself.

If you are configuring the switch remotely (cnMaestro, WEB Interface, SSH), and if the new configuration caused the loss of connectivity to the switch, a reload can be scheduled in order to reboot the switch and load the previous configuration form nvram.

There are two ways of scheduling a reload system:

- **Relative time** – reboots the switch after a specified time, starting from the moment when the schedule was created (independent of the system clock).
- **Absolute time** – reboots the switch at a specified time and assumes that the system clock is correct.

The reload time must be at least one minute in the future, and you have to verify if the clock is correct before scheduling a reload at a specific time.

Limitations

- If the device loses power during the boot process, the last reboot reason will not be changed to Power Cycle.

Default Values

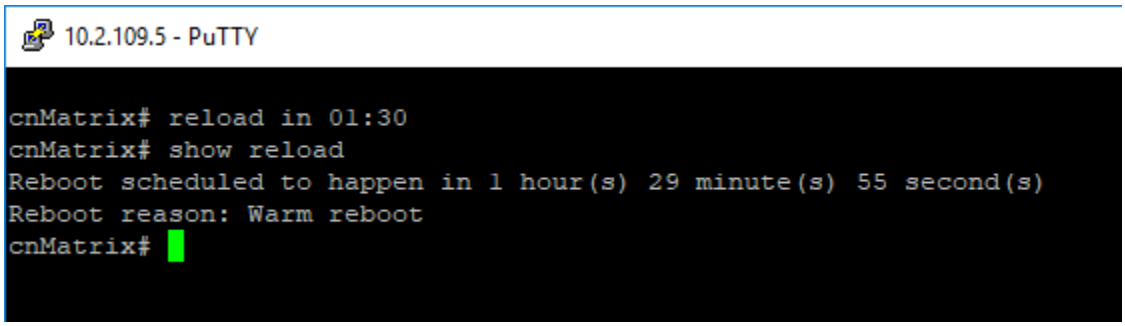
- No reload is scheduled by default.

Prerequisites

- N/A

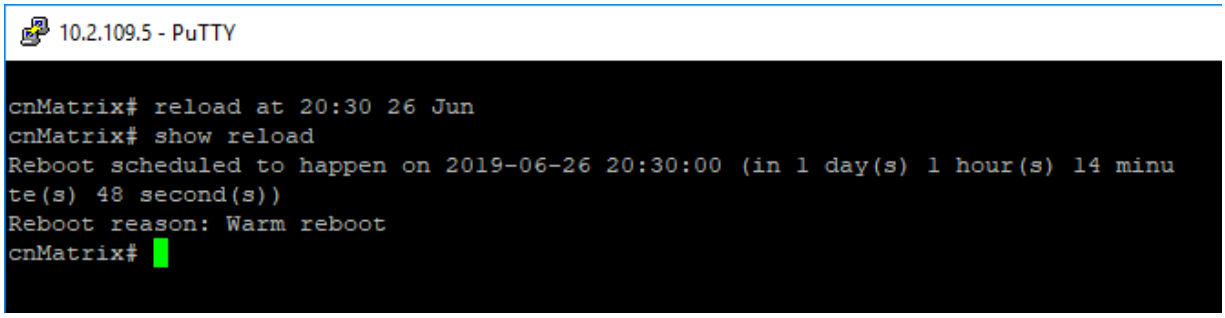
4.10.2 How to Schedule Reload on your cnMatrix Switch in CLI Interface

4.10.2.1 Schedule Reload in a Specific Amount of Time



1. Type the **reload in 01:30** command into the terminal to scehdule a reboot in 1 hour and 30 minutes. Press the Enter key.
2. Type the **show reload** command into the terminal to display the scheduled restart information and to verify if the switch will reboot itself in the requested amount of time. Press the Enter key.

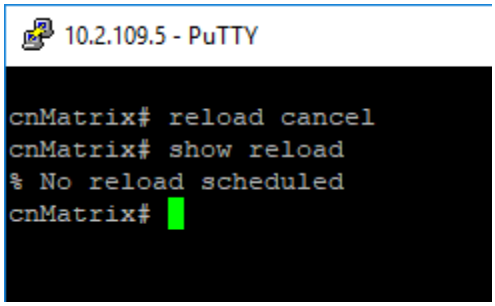
4.10.2.2 Schedule Reload at a Specific Time and Date



1. Type the **reload at 20:30 26 Jun** command into the terminal to schedule a reboot at 20:30 PM on June 26. Press the Enter key.
2. Type the **show reload** command into the terminal to display the scheduled restart information and to verify if the switch will reboot itself at the requested date and time. Press the Enter key.

For more information, see Reload Parameters and Commands.

4.10.3 How to Cancel a Scheduled Reload in CLI Interface



1. Type the **reload cancel** command into the terminal to cancel any scheduled reboot. Press the Enter key.
2. Type the **show reload** command into the terminal to verify if the scheduled reload has been successfully canceled. Press the Enter key.

4.11 USB (Starting with version 2.1)

4.11.1 Managing USB

Feature Overview

The USB feature enables you to perform different offline actions and gives you the possibility to interact with a flash storage device that is inserted in the USB port of a switch.

The USB has the following capabilities:

1. Software upgrades/downgrades from the USB device.
2. Switch configurations can be applied from a USB device.
3. Switch configurations can be copied on an USB device.
4. Access the files and folders that are on the USB device.
5. Access device information and vendor information (Vendor Name, Product ID, Total Capacity, etc).

The USB feature can be used as a backup solution for software upgrades.

After a USB is inserted in the designated USB port, the device can be manually mounted.

Manually mounting the device is not mandatory.

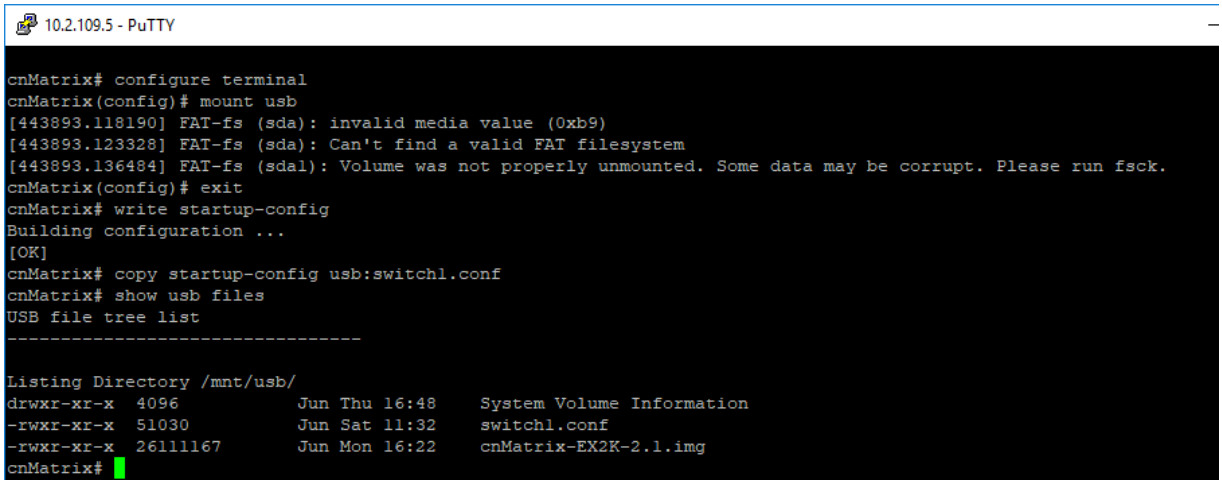
Limitations

- Only devices with format FAT32 are supported.
- USB3.0 speeds are not supported.
- You are able to write on the device only if the write protection option is disabled on the USB device.

Default Values

- No USB device is present by default.

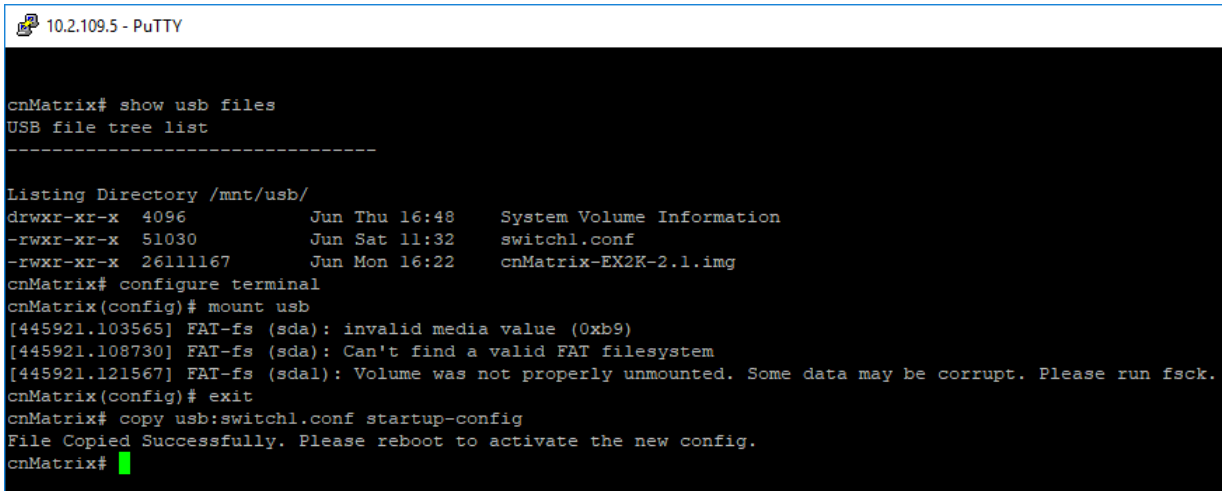
4.11.2 How to Copy Startup Config from Switch to USB (example)



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **mount usb** command into the terminal to mount a USB stick. Press the Enter key.
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **write startup-config** command into the terminal to save the switch configuration into a switch local file. Press the Enter key.
5. Type the **copy startup-config usb:switch1.conf** command into the terminal to copy the saved configuration file to USB . Press the Enter key.
6. Type the **show usb files** command into the terminal to display the files that are currently on the USB.

For more information, see USB Parameters and Commands.

4.11.3 How to Copy Startup Config from USB to Switch (example)

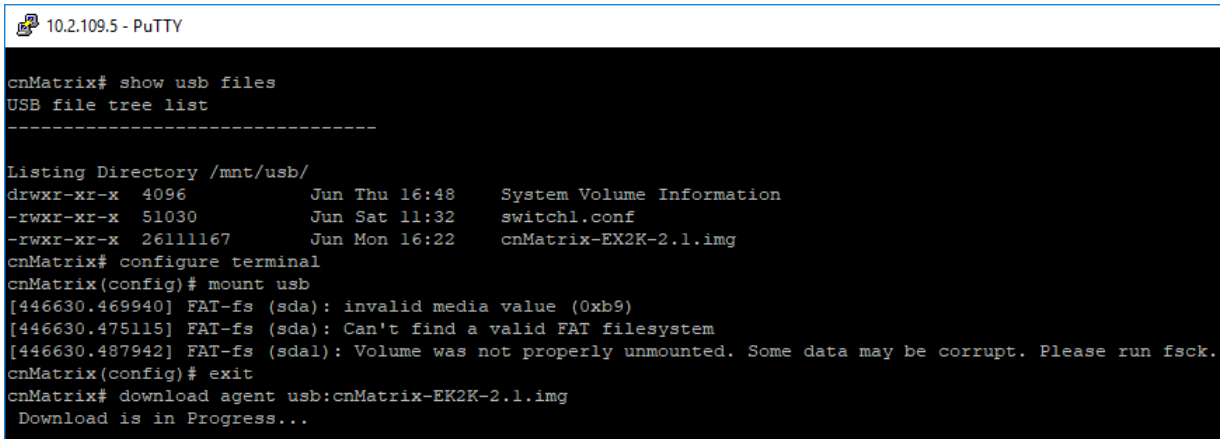


1. Type the **show usb files** command into the terminal to display the files that are currently on the USB. Press the Enter key.
2. Type the **configure terminal** command into the terminal. Press the Enter key.
3. Type the **mount usb** command into the terminal to mount a USB stick. Press the Enter key.
4. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **copy usb:switch1.conf startup-config** command into the terminal to copy an existing configuration file from the USB to your cnMatrix switch .

> Please reboot your switch to activate the new configuration.

For more information, see USB Parameters and Commands.

4.11.4 How to Upgrade your Software Using USB



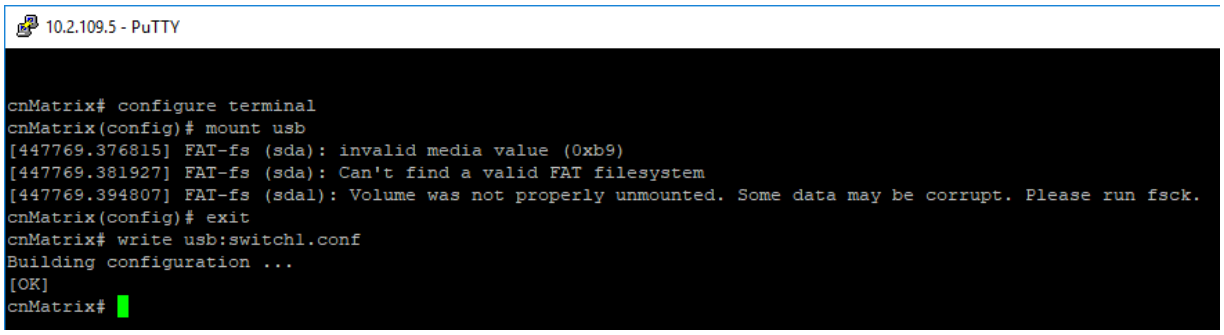
1. Type the **show usb files** command into the terminal to display the files that are currently on the USB. Press the Enter key.
2. Type the **configure terminal** command into the terminal. Press the Enter key.
3. Type the **mount usb** command into the terminal to mount a USB stick. Press the Enter key.

4. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the Enter key.

5. Type the **download agent usb:cnMatrix-EK2K-2.1.img** command into the terminal to download the new agent on your cnMatrix switch. Press the Enter key.

> Please reboot your switch to activate the new configuration.

4.11.5 How to Copy Running-Config to Switch



1. Type the **configure terminal** command into the terminal. Press the Enter key.

2. Type the **mount usb** command into the terminal to mount a USB stick. Press the Enter key.

3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

4. Type the **write usb:switch1.conf** command into the terminal to specify the destination path and to copy the switch current configuration on the USB device. Press the Enter key.

For more information, see USB Parameters and Commands.

4.11.6 Troubleshooting USB

Useful commands for troubleshooting:

- cnMatrix# show usb files
- cnMatrix# show usb tree
- cnMatrix# show usb info

5 Security Features

5.1 RADIUS

5.1.1 Managing RADIUS

5.1.1.1 Feature Description

Radius (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

The **cnMatrix Radius (IPv4/IPv6) client** is a security feature that offers the ability for cnMatrix to communicate with a Radius central server with the purpose of **authenticating** users and **authorizing**

their access to the system or a specific service. cnMatrix Radius (IPv4/IPv6) client is used with the login and PNAC features.

Standards

- cnMatrix Radius (IPv4/IPv6) client is RFC 2138, RFC 286, and RFC 2618 compliant.

Scaling Numbers

- cnMatrix Radius (IPv4/IPv6) is a client feature used for user authentication and authorization. Scalability falls on the server response capabilities.

Limitations

- cnMatrix Radius client (IPv4/IPv6) uses only the authentication and authorization subfeature of the Radius client feature. Accounting is not implemented.
- The number of Radius servers which can be programmed to be used by cnMatrix is limited to 5.
- Only one server is used in the authentication and authorization process. This one is called a primary server. If this server fails, only then another one will be used.

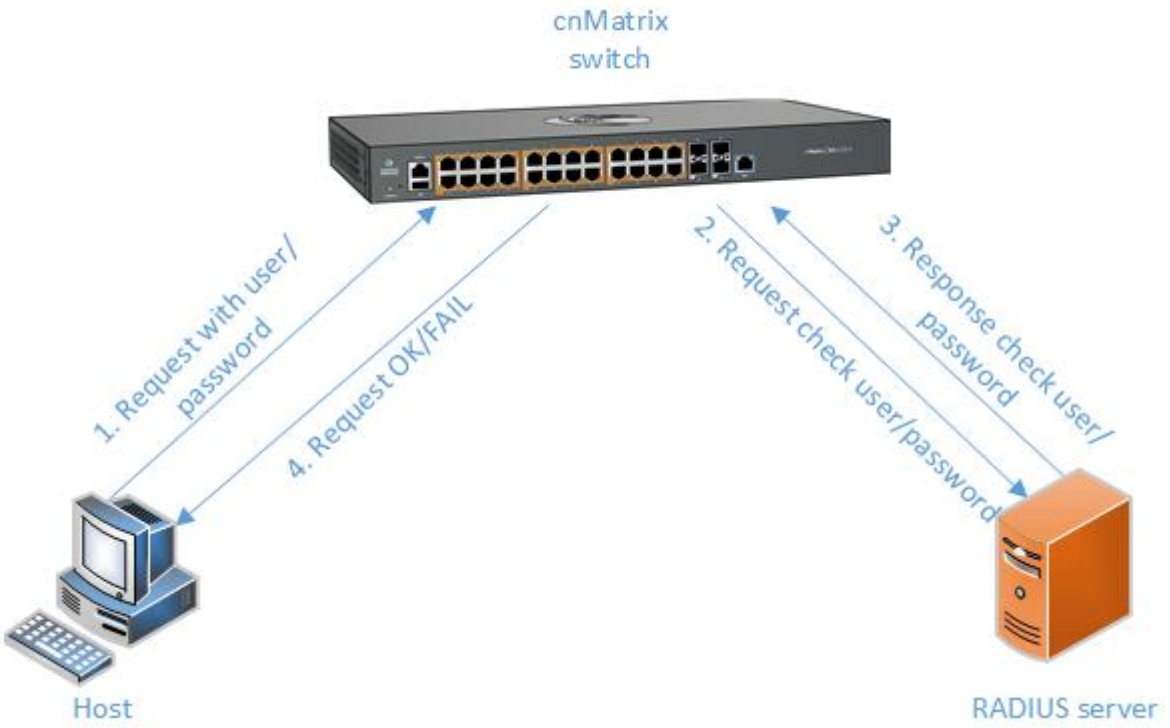
Default Values

- The default value for the time period in seconds for which a client waits for a response from the server before retransmitting the request: 10 seconds.
- The default value for the maximum number of attempts to be tried by a client to get response from the server for a request: 3 attempts.
- The default Authentication Port: 1812.
- The default Accounting Port: 1813.
- The debugging option is disabled by default.

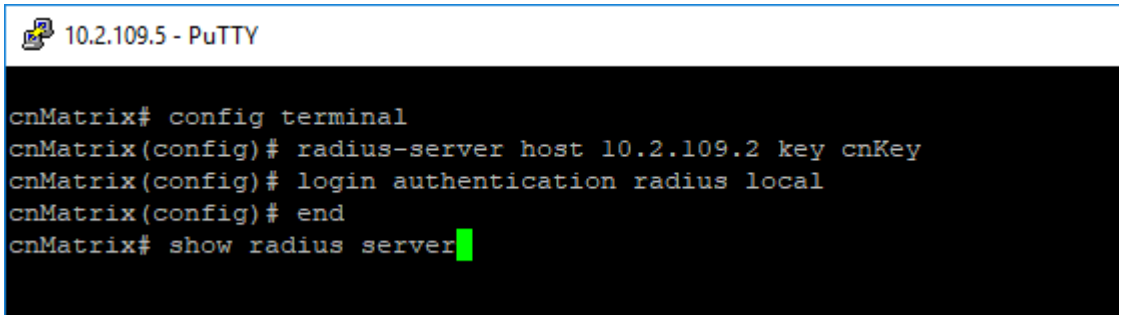
Prerequisites

N/A

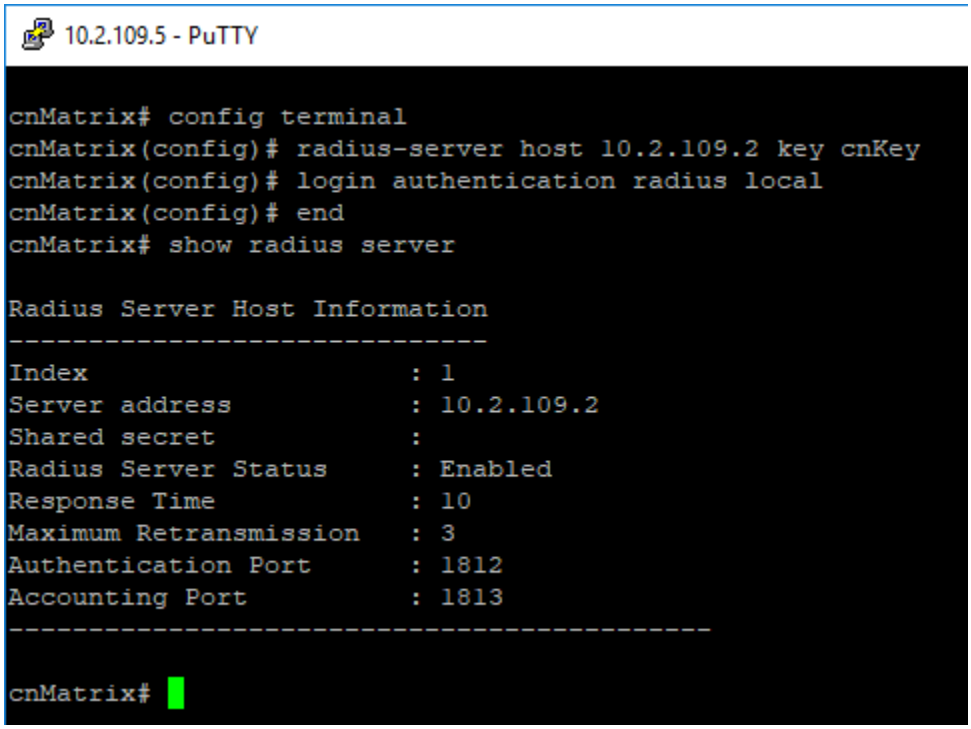
5.1.1.2 Network Diagram



5.1.2 How to Enable and Configure RADIUS in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **radius-server host 10.2.109.2 key cnKey** command into the terminal tp specify RADIUS parameters. Press the Enter key.
3. Type the **login authentication radius local** command into the terminal to set the authentication method for user logins. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show radius server** command into the terminal to display RADIUS server configurations. Press the Enter key.



For more information, see RADIUS Parameters and Commands.

5.1.3 Troubleshooting RADIUS

Useful commands for troubleshooting:

cnMatrix# show radius server

cnMatrix# show radius statistics

cnMatrix# debug radius all

5.2 TACACS

5.2.1 Managing TACACS

5.2.1.1 Feature Description

TACACS (Terminal Access Controller Access-Control System) is a protocol used in handling remote authentication and other related services for network access control through a centralized server. For a reliable delivery, TACACS uses the TCP transport protocol.

cnMatrix TACACS+ client(IPv4/IPv6) is a security feature that offers the switch the ability to communicate with a TACACS+ central server with the purpose of **authenticating** users. Therefore, TACACS works closely with the login feature.

Standards

- cnMatrix TACACS+ client (IPv4/IPv6) is in accordance with draft-grant-tacacs-02.

Scaling Numbers

- cnMatrix TACACS is a client feature used for user authentication at login. Scalability falls on the server response capabilities.

Limitations

- cnMatrix TACACS+ client (IPv4/IPv6) uses only the authentication subfeature of the TAC-

ACS+ client feature.

- cnMatrix TACACS+ client (IPv4/IPv6) uses only PAP(password authentication protocol) for the user authentication.
- The number of TACACS server which can be programmed to be used in the authentication process is limited to 5.
- Only one server is used in the authentication process. This one is called a primary server. If this server fails, only then another one will be used.

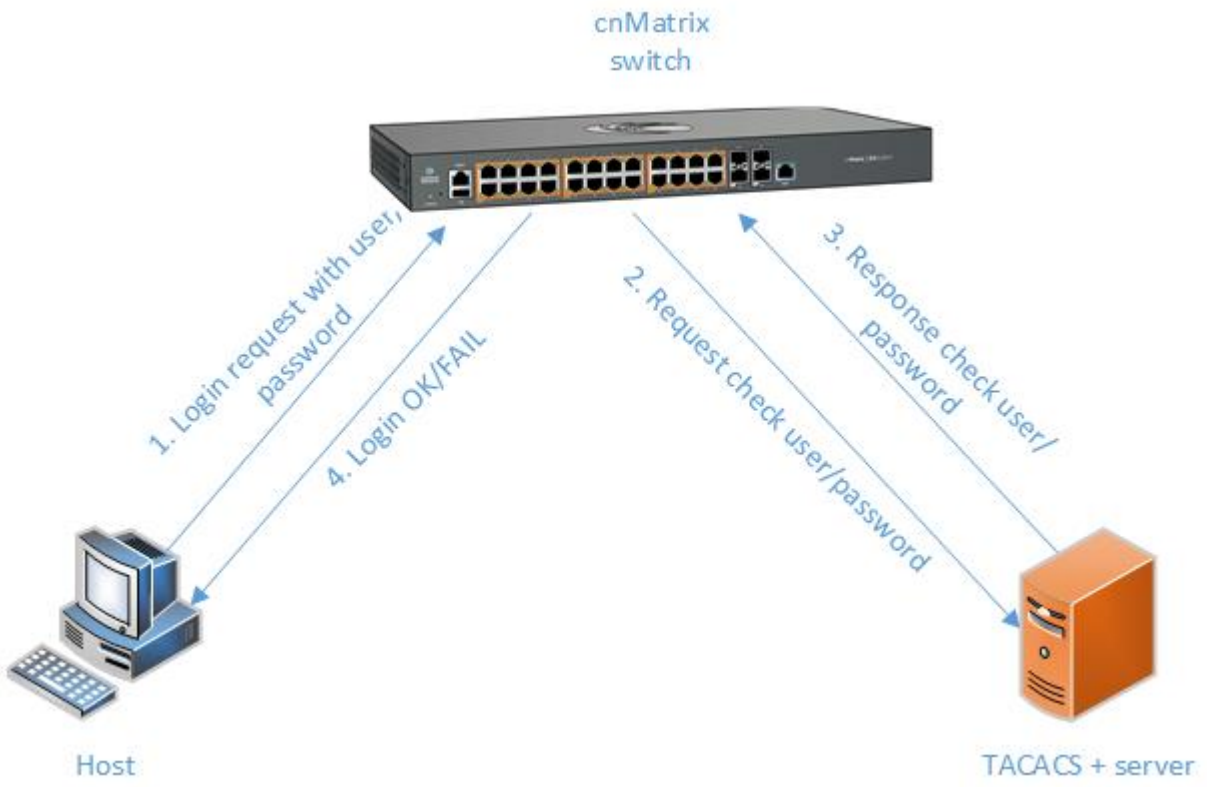
Default Values

- The default TCP port number: 49.
- The default timeout: 5 seconds.
- The default retransmit time: 2.
- The debugging option is disabled by default.
- The single-connection parameter is set to no by default.

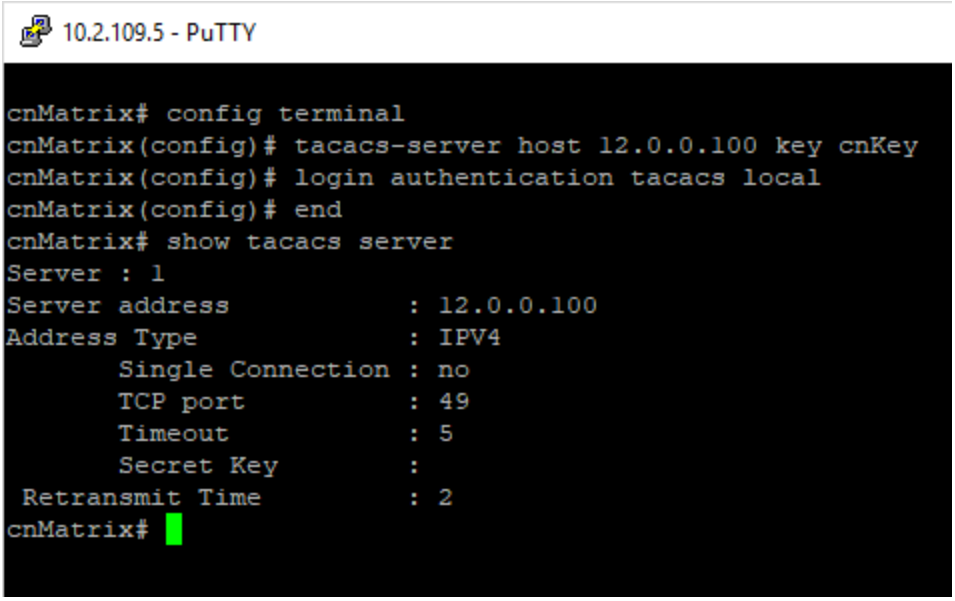
Prerequisites

N/A

5.2.1.2 Network Diagram



5.2.2 How to Enable and Configure TACACS in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **tacacs-server host 12.0.0.100 key cnKey** command into the terminal to configure the TACACS server address. Press the Enter key.
3. Type the **login authentication tacacs local** command into the terminal to set the authentication method for user logins. Press the Enter key.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show tacacs server** command into the terminal to display the configurations for the TACACS server. Press the Enter key.

For more information, see TACACS Parameters and Commands.

5.2.3 Troubleshooting TACACS

Useful commands for troubleshooting:

cnMatrix# debug tacacs

cnMatrix# show tacacs server

cnMatrix# show tacacs statistics

5.3 IGMP Snooping

5.3.1 Managing IGMP Snooping

5.3.1.1 Feature Description

The **IGMP Snooping** feature enables the cnMatrix switch to transmit multicast traffic to one or more ports in a broadcast domain.

IGMP Snooping allows a switch to snoop or capture information from IGMP packets (being sent back and forth between hosts and a router). Based on this information, the switch adds/deletes the multicast addresses from its address table, thereby enabling/disabling multicast traffic from flowing

to individual host ports.

Standards

- N/A

Scaling Numbers

- N/A

Limitations

- A maximum of 256 IGMP groups are supported.

Default Values

- The IGMP Snooping feature is globally disabled.
- The fast leave processing is disabled by default.
- The debugging functionality is disabled by default.

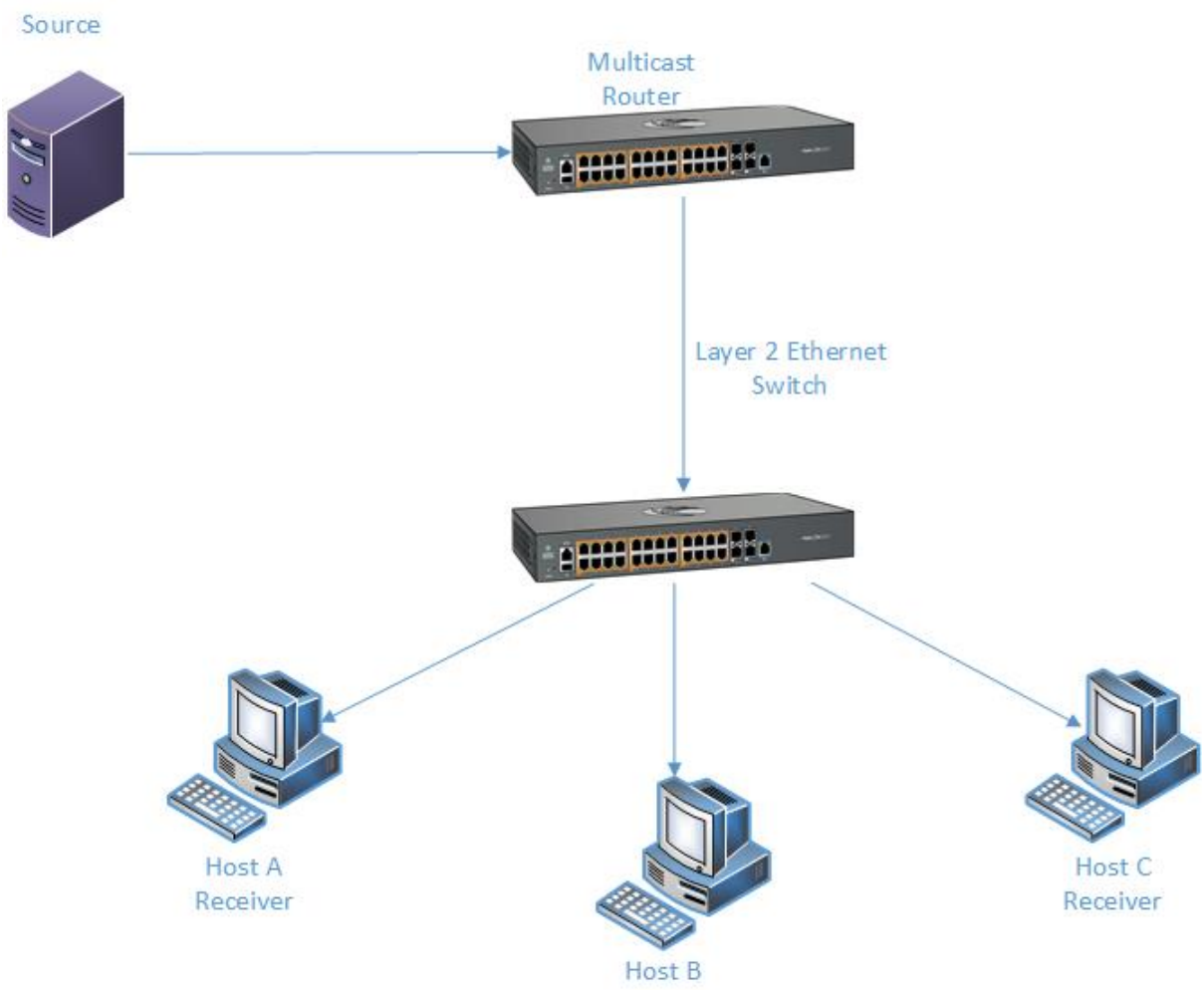
Prerequisites

- N/A

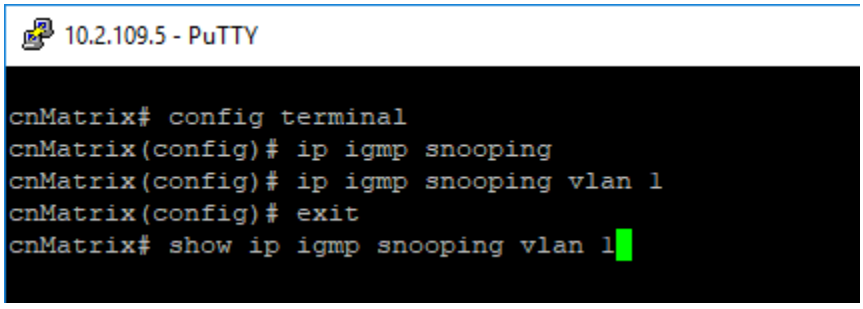
SNMP

- The IGMP Snooping feature can be configured using the SNMP tool.

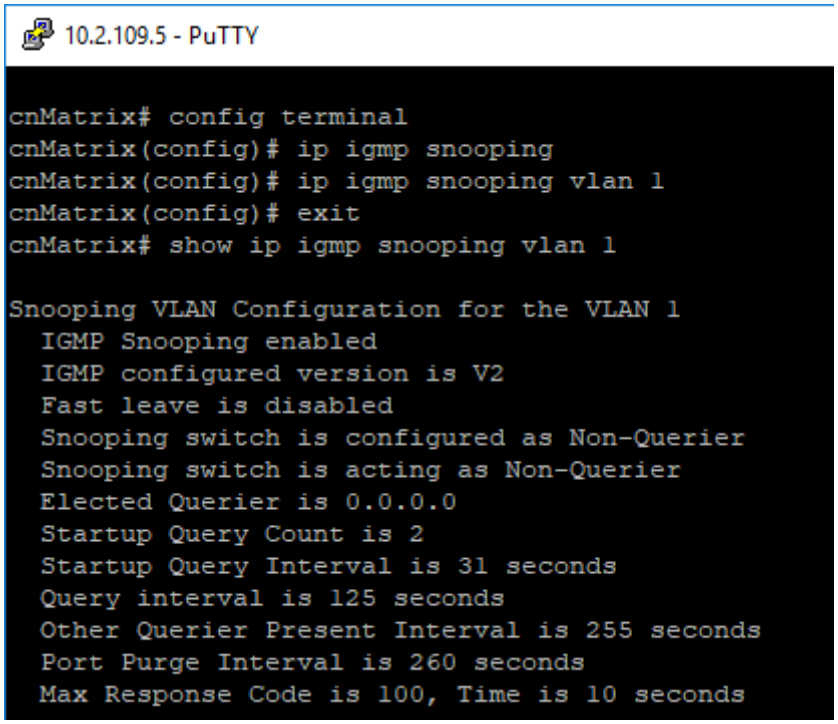
5.3.1.2 Network Diagram



5.3.2 How to Enable IGMP Snooping in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **ip igmp snooping** command into the terminal to enable IGMP Snooping. Press the Enter key.
3. Type the **ip igmp snooping vlan 1** command into the terminal to enable IGMP Snooping on a VLAN. Press the Enter key.
4. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. If you want to verify the IGMP Snooping information for VLAN 1, type the **show ip igmp snooping vlan 1** command into the terminal. Press the Enter key.



For more information, see IGMP Snooping Parameters and Commands.

5.3.3 Troubleshooting IGMP Snooping

Useful commands for troubleshooting:

```
cnMatrix# show ip igmp snooping

cnMatrix#show ip igmp snooping globals

cnMatrix#show ip igmp snooping statistics
```

5.4 IGMP Snooping Filtering

5.4.1 Managing IGMP Snooping Filtering

The **IGMP Snooping Filtering** feature enables you to filter multicast addresses. You have the option to create and IGMP profile, which contains certain multicast groups and specifies if the IGMP packets for that groups are processed or not.

IGMP Snooping Filtering has no relationship with the function that directs the forwarding of multicast traffic.

Standards

Scaling Numbers

Limitations

Default Values

- No IGMP profile is defined by default.
- Default number of IGMP groups that can be learned: 256.
- No IGMP filter is applied by default.

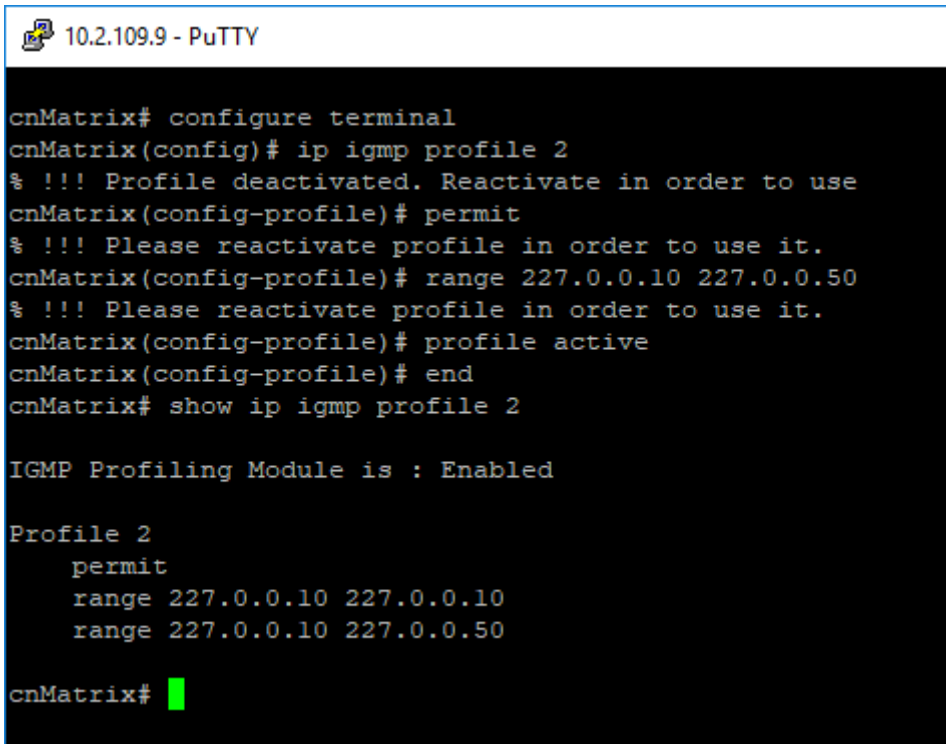
Prerequisites

- Enable the IGMP Snooping feature:

```
cnMatrix# configure terminal

cnMatrix(config)# ip igmp snooping
```

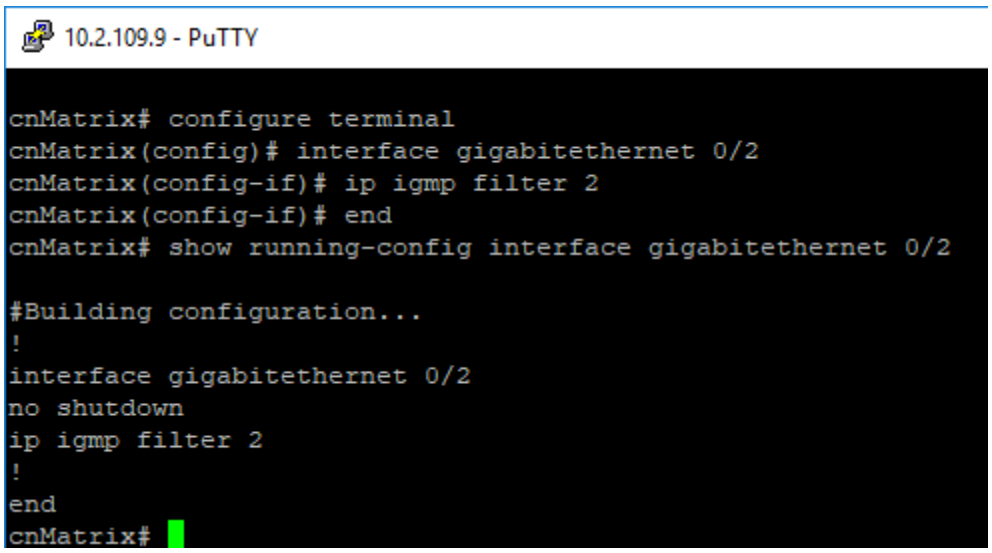
5.4.2 How to Enable, Configure and Apply IGMP Profiles in CLI Interface

5.4.2.1 Configuring IGMP Profile



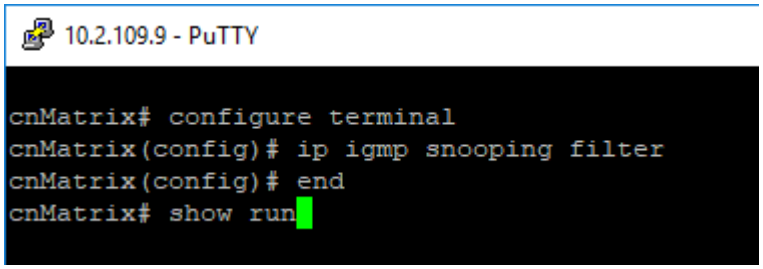
1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **ip igmp profile 2** command into the terminal. Press the Enter key to assign a number to the profile you are configuring.
3. Type the **permit** command into the terminal. Press the Enter key to permit access to the IP multicast address.
4. Type the **range 227.0.0.10 227.0.0.50** command into the terminal. Press the Enter key.
5. Type the **profile active** command into the terminal to activate profile 2. Press the Enter key.
6. Type the **end** command into the terminal. Press the Enter key.
7. Type the **show ip igmp profile 2** command into the terminal to display the status of the IGMP profiling module and the configuration performed on the selected igmp profile. Press the Enter key.

5.4.2.2 Applying IGMP Profiles



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/2** command into the terminal. Press the Enter key.
3. Type the **ip igmp filter 2** command into the terminal. Press the Enter key to apply the specified IGMP profile to the interface.
4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show running-config interface gigabitethernet 0/2** command into the terminal. Press the Enter key.

5.4.2.3 Enabling IGMP Snooping Filter

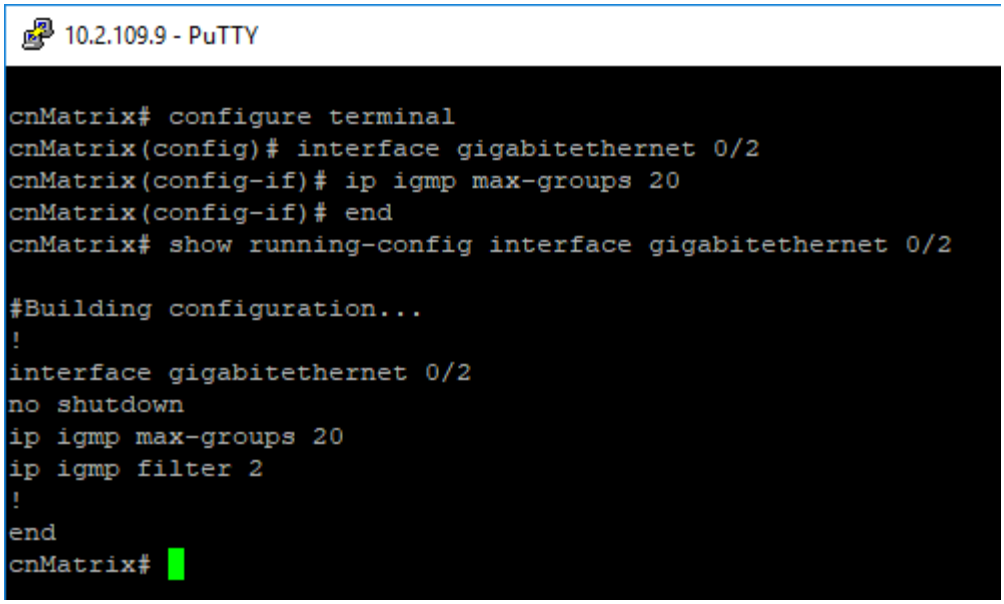


1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **ip igmp snooping filter** command into the terminal to enable the IGMP Snooping filter. Press the Enter key.
3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show run** command into the terminal to display the currently operating configuration in the system for multiple instances. Press the Enter key.

17 Press the Space key.

For more information, see IGMP Snooping Parameters and Commands.

5.4.3Setting the Maximum Number of IGMP Groups



1. Type the **configure terminal** command into the terminal. Press the Enter key.
2. Type the **interface gigabitethernet 0/2** command into the terminal to select an interface to be configured. Press the Enter key.
3. Type the **ip igmp max-groups 20** command into the terminal. Press the Enter key to set the maximum number of IGMP groups that the interface can join.

> No maximum value is set by default.

4. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
5. Type the **show running-config interface gigabitethernet 0/2** command into the terminal to display the operating configuration in the system for a certain interface.

For more information, see IGMP Snooping Parameters and Commands.

5.5 DHCP Snooping

5.5.1 Managing DHCP Snooping

5.5.1.1 Feature Description

The **DHCP Snooping** feature intercepts all DHCP packets from untrusted ports and after inserting the port specific information (option 82), forwards the DHCP client side packets on trusted ports. This option 82 will be used to redirect the DHCP responses from a server to the appropriate untrusted port. DHCP snooping binding table will be updated when a valid IP address is allocated for a host.

DHCP Snooping is a feature who filters untrusted DHCP messages and builds a binding database table. It acts as a firewall between untrusted hosts and DHCP servers. These untrusted messages are sent from devices outside a network and are usually sources of traffic attacks.

Standards

- The DHCP Snooping feature has been built in accordance with RFC7513.

Scaling Numbers

- N/A

Limitations

- DHCP Snooping is limited by the internal binding table. There is a maximum of 254 binding table entries. Beyond this number, the table will not be updated anymore, but the DHCP offers will be forwarded to the clients.

Default Values

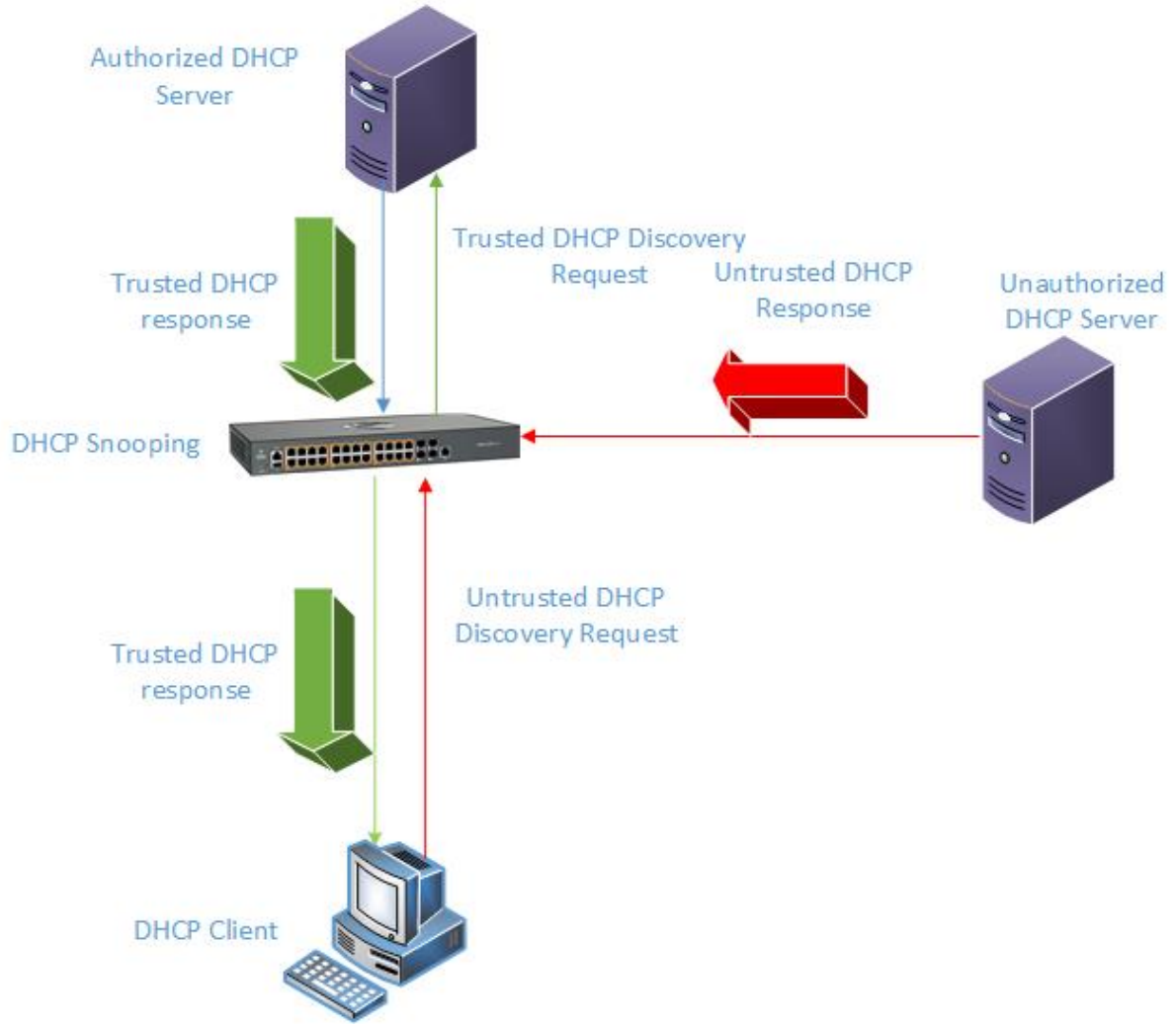
- The DHCP Snooping feature is inactive by default on all VLANs.
- The DHCP MAC address verification is inactive by default.
- All ports are considered as untrusted by default.

Prerequisites

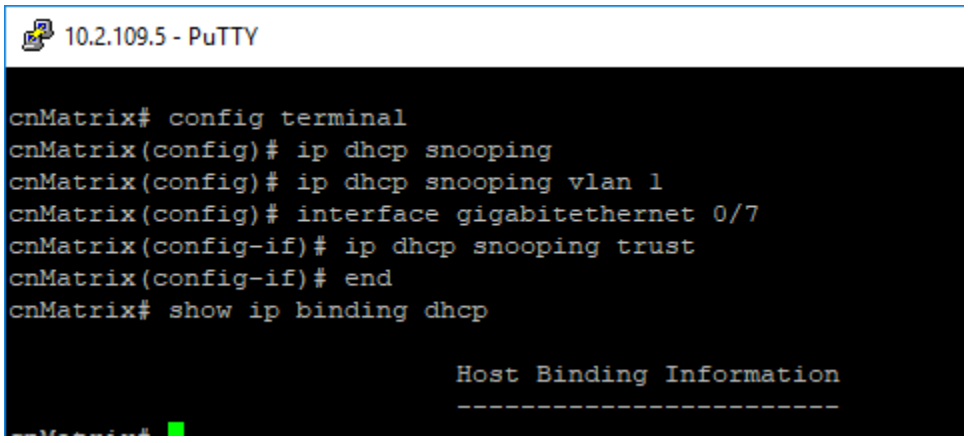
- N/A

The DHCP Snooping feature is not supported if the DHCP Relay feature is enabled.

5.5.1.2 Network Diagram



5.5.2 How to Enable and Configure DHCP Snooping in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **ip dhcp snooping** command into the terminal to enable globally the L2 DHCP Snooping feature in the system. Press the Enter key.
3. Type the **ip dhcp snooping vlan 1** command into the terminal to enable L2 DHCP Snooping on the VLAN Interface. Press the Enter key.

4 Type the **interface gigabitethernet 0/7** command into the terminal to select the interface to be configured. Press the Enter key.

5 Type the **ip dhcp snooping trust** command into the terminal to configure the interface as a trusted port. Press the Enter key.

6 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

7 Type the **show ip binding dhcp** command into the terminal to display the host binding information. Press the Enter key.

For more information, see DHCP Snooping Parameters and Commands.

5.5.3 Troubleshooting DHCP Snooping

Useful commands for troubleshooting:

- For information regarding packet statistics :

```
cnMatrix#show ip dhcp snooping vlan vlan-id
```

- For information regarding port trust/untrust status:

```
cnMatrix# show ip dhcp snooping port-security-state
```

- For dhcp snooping status:

```
cnMatrix# show ip dhcp snooping globals
```

- For feature debugging:

```
cnMatrix# debug ip dhcp snooping all
```

5.6 ACL

5.6.1 Managing ACL

The **ACL** feature provides the means for the user to create rules to match specific traffic based on the information in the packets. The packets matched by the rules can then be dropped, allowed or redirected, or they can be fed to the QoS engine to have them policed. Matched packets can be mirrored to a specific interface in order for them to be analyzed by a network administrator.

An ACL consists of three parts:

- **Rule** – a set of fields from the packet, and a set of values that the selected fields have to match.
- **Action** – what to do with the packets that match the rule (permit, deny, redirect).
- **Interface** - where the rule is applied (on ingress or egress direction).

There are three types of ACLs:

- **IP ACLs** – the rule can consist of the source IP and the destination IP
- **MAC ACLs** – the rule can consist of the source and destination MAC addresses, Ethernet type and the VLAN information

- **IP extended ACLs** – the rule can consist of the source IP and the destination IP, as well as Layer-4 information for protocols such as UDP (source/destination ports), TCP (ports, TCP flags), ICMP (message code, message type) or any IP type, specified by the IP protocol number, as defined by the Internet Assigned Numbers Authority (IANA).

There are two modes of configuring the ACL feature:

Consolidated	User configures the entire set of rules, then he commits them to the hardware.
Immediate	User configures the rules, and they are committed to hardware one-by-one, as the user inputs them. In the immediate mode, the priorities assigned by the users are ignored by the switch and are assigned in the order in which they are configured. This mode is not recommended for scenarios with complex rules, in which priorities are relevant.

Standards

N/A

Scaling Numbers

- The maximum number of ACLs that can be configured on a system: 145 extended and 128 standard. Also, take into consideration that when one ACL is applied to multiple ports, the available number of ACLs is reduced with the number of ports on which the rule is applied.

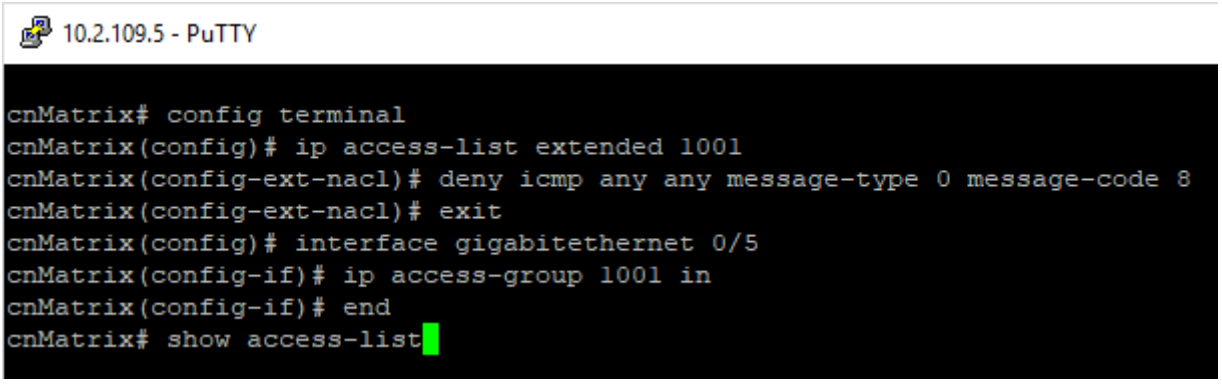
Limitations

- IPV6 access list only work when they are applied to the *ingress* of a port.
- If it is necessary to configure multiple ACL types on the same port, note that their priorities will not be respected in this case. Priorities only assign higher or lower precedence of rules of the same type.
- On *egress*, only one type of ACLs is supported at one time: either IP or MAC ACLs. This type can be set globally via the egress access-list mode command.

Default Values

- The default provisioning mode: immediate.
- No ACLs are preconfigured on the switch.
- Default egress access-list mode: ip.

5.6.2 Configuring ACL in CLI Interface - Immediate mode



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **ip access-list extended 1001** command into the terminal to create an IP access list. Press the Enter key.
3. Type the **deny icmp any any message-type 0 message-code 8** command into the terminal to specify the ICMP packets to be rejected based on IP address and associated parameters. Press the

Enter key.

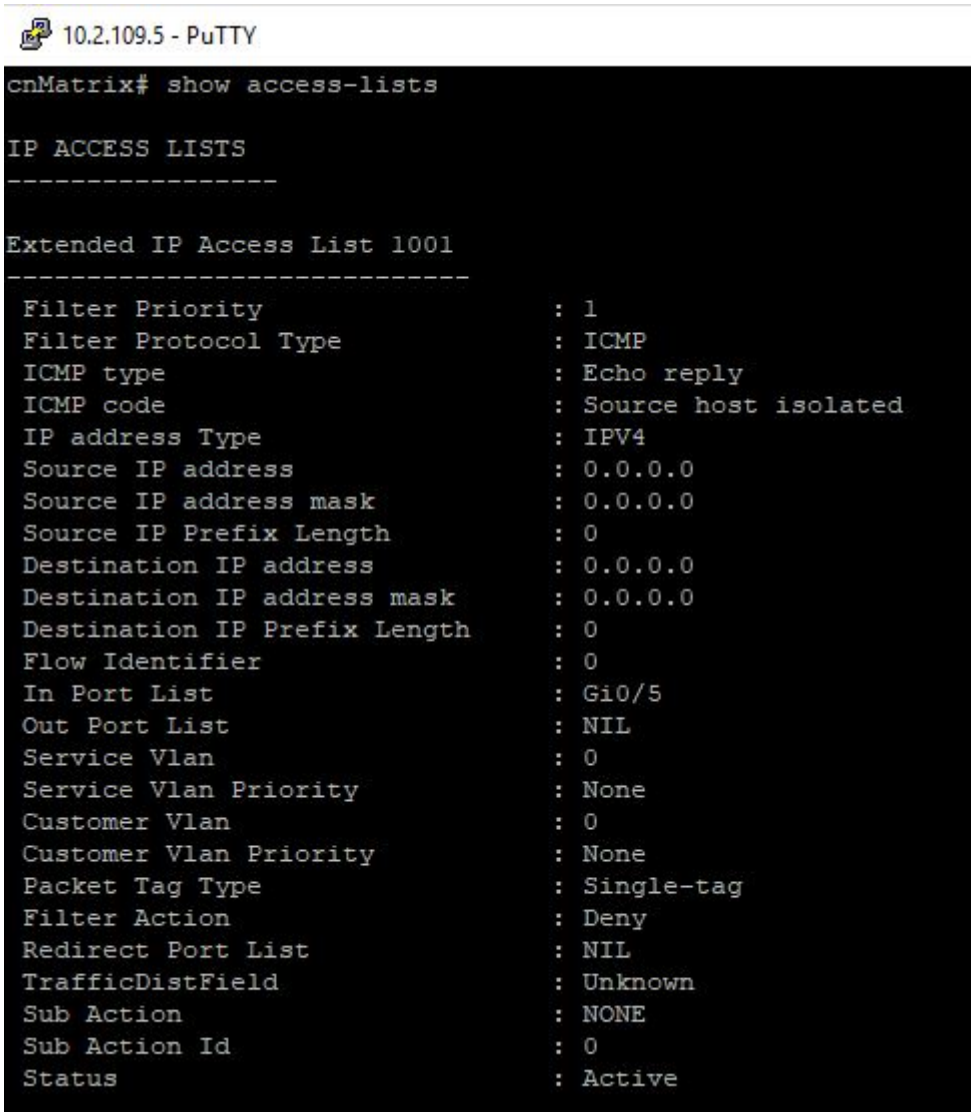
4. Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.

5. Type the **interface gigabitethernet 0/5** command into the terminal to select the interface to be configured and to go to the interface configuration mode. Press the Enter key.

6. Type the **ip access-group 1001 in** command into the terminal to enable access control for packets on the interface. Press the Enter key.

7. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

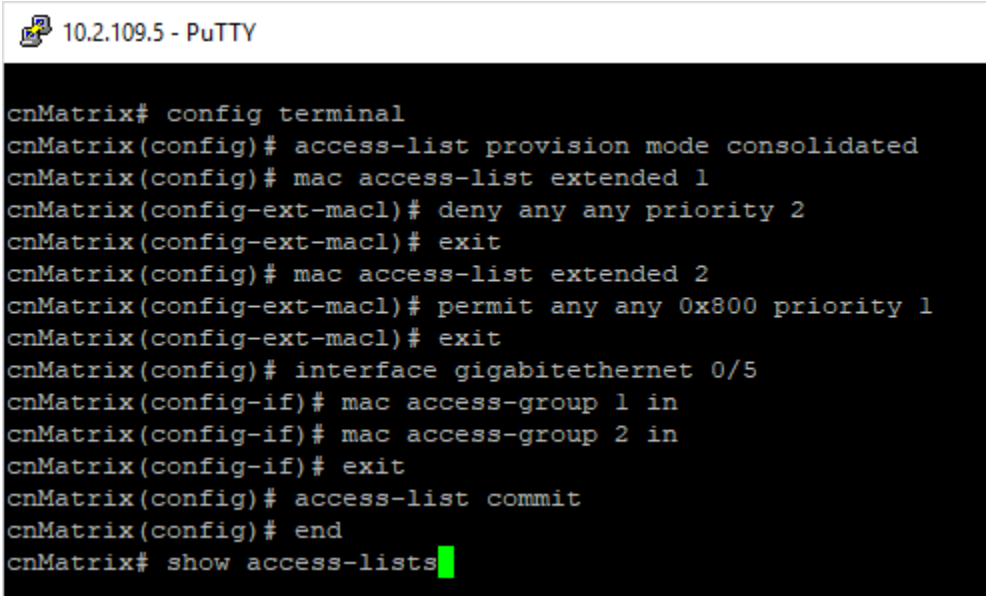
8. Type the **show access-list** command into the terminal to display the IP access lists. Press the Enter key.



9.

For more information, see ACL Parameters and Commands. **Starting with version 2.1**, see ACL Parameters and Commands version 2.1.

5.6.3 Configuring ACL in CLI Interface- Consolidated mode

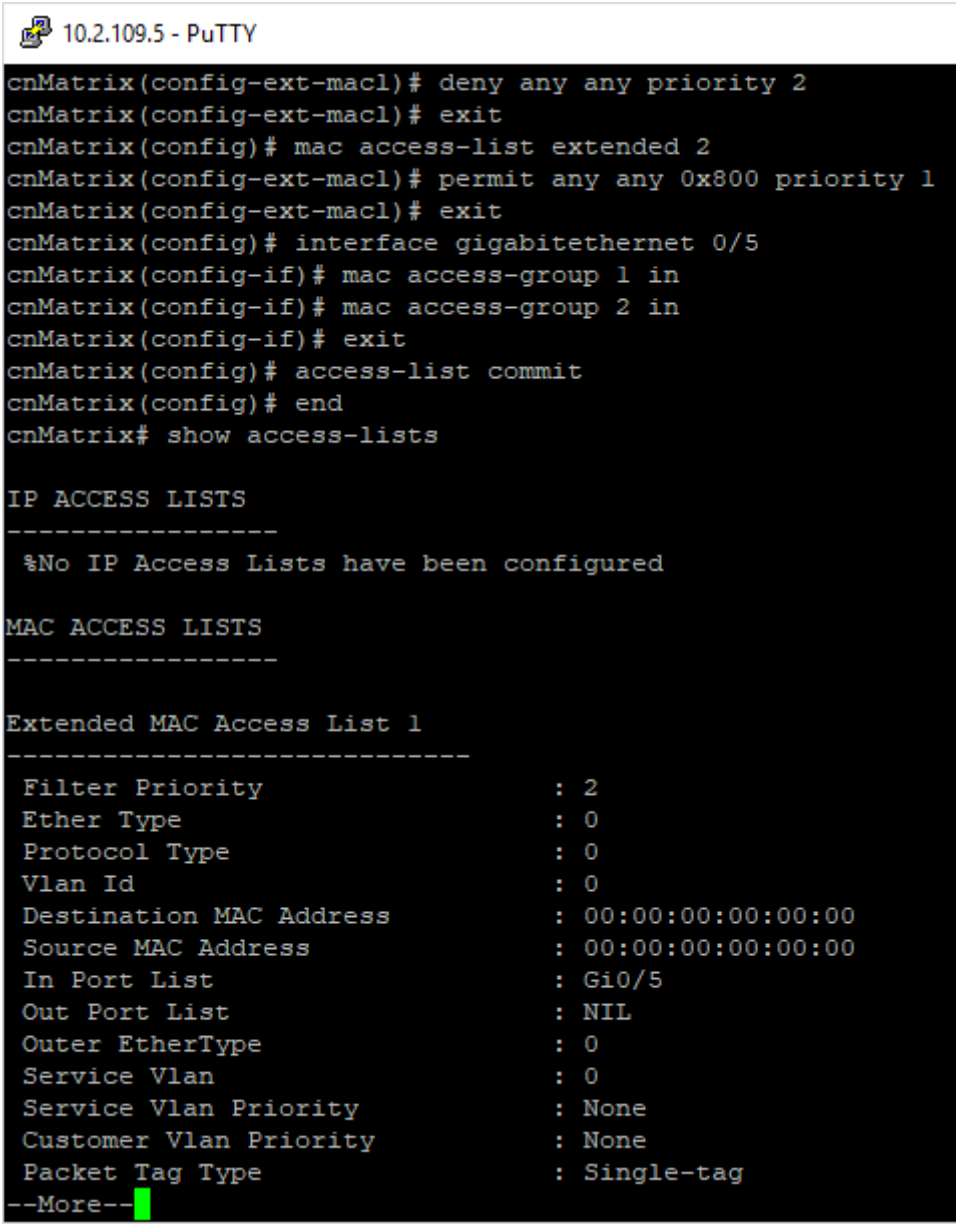


1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **access-list provision mode consolidated** command into the terminal to configure access-list provision mode as consolidated. Press the Enter key.
3. Type the **mac access-list extended 1** command into the terminal to create MAC access list. Press the Enter key.
4. Type the **deny any any priority 2** command into the field to specify the packets to be re-jected based on MAC address and the associated parameters. Press the Enter key.
5. Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
6. Type the **mac access-list extended 2** command into the terminal to create MAC access list. Press the Enter key.
7. Type the **permit any any 0x800 priority 1** command into the terminal to specify the packets to be forwarded based on MAC address and associated parameters. Press the Enter key.
8. Type the **exit** command into the terminal to go back to the configuration mode . Press the Enter key.
9. Type the **interface gigabitethernet 0/5** command into the terminal to select an interface to be configured. Press the Enter key.
10. Type the **mac access-group 1 in** command into the terminal to enable access control list 1 for inbound traffic on port . Press the Enter key.
11. Type the **mac access-group 2 in** command into the terminal to enable access control list 2 for inbound traffic on port. Press the Enter key.
12. Type the **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
13. Type the **access-list commit** command into the terminal. Press the Enter key.

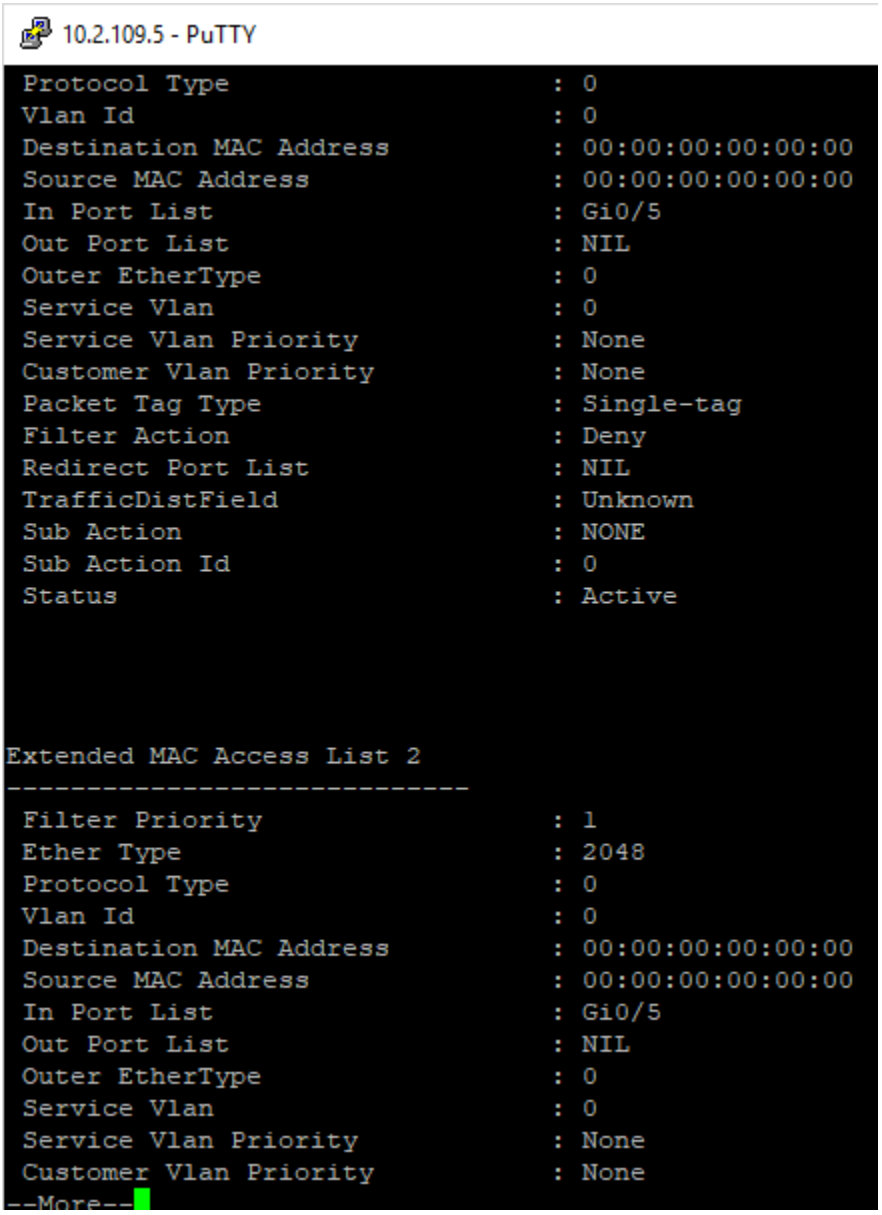
Note: This command is applicable only when the provision mode is consolidated.

14 Type the **end** into the terminal to go to the Privileged EXEC mode. Press the Enter key.

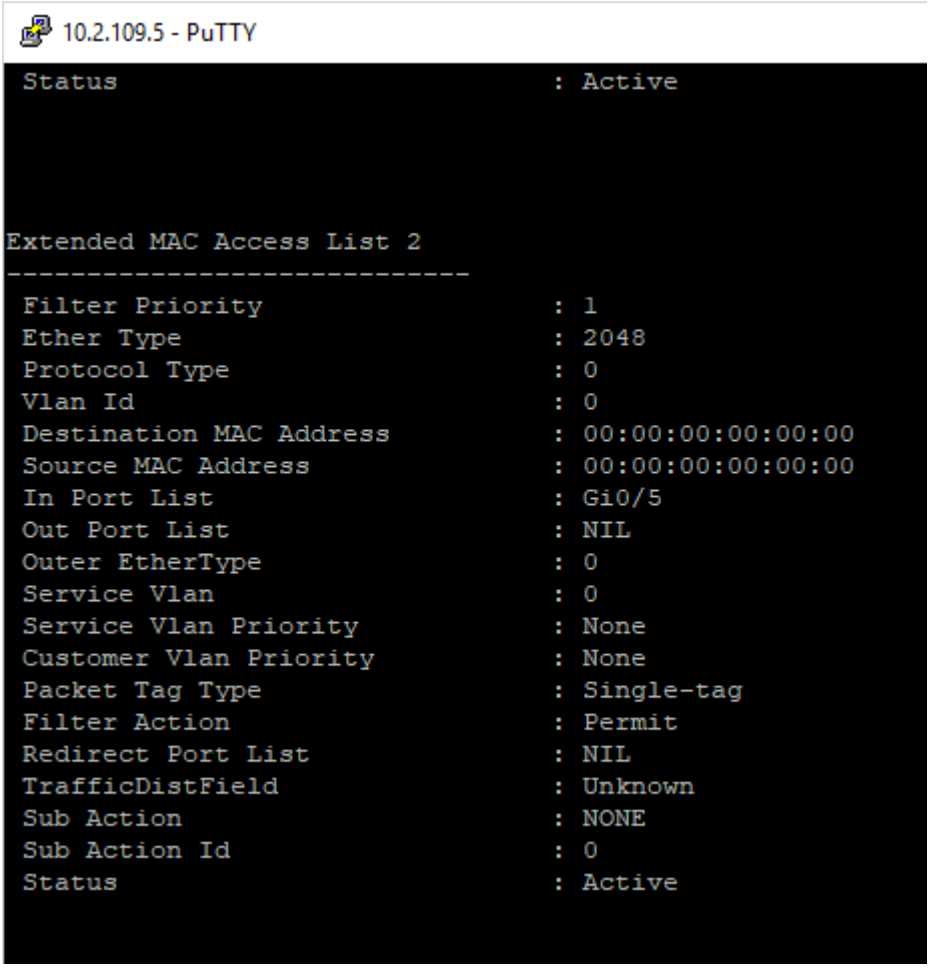
15 Type the **show access-lists** command into the terminal to display IP access lists. Press the Enter key.



16 Press the Space key.



17 Press the Space key.



For more information, see ACL Parameters and Commands. Starting with version 2.1, see ACL Parameters and Commands version 2.1.

5.7 Static MAC

5.7.1 Managing Static MAC

The switch allows the user to configure a **static MAC** address and assign it to a specific VLAN ID and to a specific port. The MAC addresses configured in this manner are immune to automatic MAC address aging and migration.

Normally, with a dynamically learned MAC address, traffic that enters the switch through a different port than the one currently present in the mac-address-table will be forwarded, and the entry's port will be migrated to the new value.

Traffic that enters the switch through a port and has a source MAC address that is statically configured to a different port will be dropped, and its source address will not be migrated.

Standards

- IEEE 802.1q.

Scaling Numbers

- 256 static MAC addresses can be configured on the switch.

Limitations

- Only unicastMAC addresses can be configured using this switch.
- A valid entry in the mac-address-table is a MAC/VLAN id pair, and assigning the same pair to more than one port will cause the switch to retain only the value configured last.

Default Values

- The status of the static unicast entry is set to permanent by default.

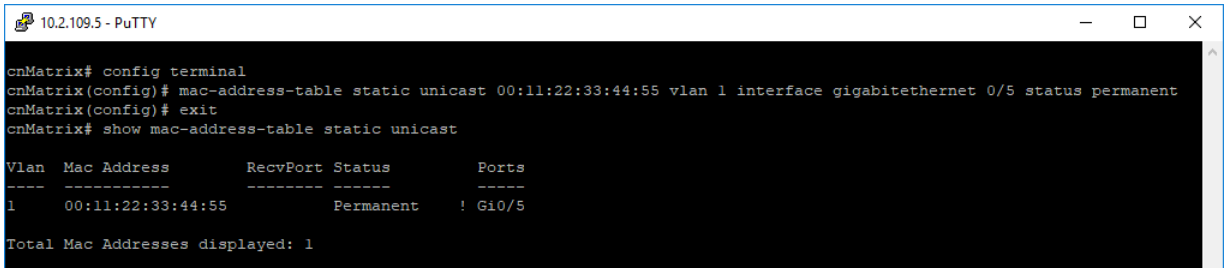
Prerequisites

- The VLAN to which the MAC address is assigned must be already created at the time the static MAC is configured, or an error message will be displayed.

SNMP

- SNMP support is available via dot1qStaticUnicastEntry in Q-BRIDGE-MIB.

5.7.2 Configuring Static MAC in CLI Interface



1 Type the **config terminal** command into the terminal. Press the Enter key.

2 Type the **mac-address-table static unicast 00:11:22:33:44:55 vlan 1 interface gigabitethernet 0/5 status permanent** command into the terminal to configure a static unicast MAC address. Press the Enter key.

3 Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

4 Type the **show mac-address-table static unicast** command into the terminal to display the static unicast MAC address table. Press the Enter key.

For more information, see Static MAC Parameters and Commands.

5.7.3 Troubleshooting Static MAC

Useful commands for troubleshooting:

```
cnMatrix# show mac-address-table static unicast
cnMatrix# show mac-address-table static unicast vlan # show mac-address-table stat-
ic unicast address
cnMatrix# show mac-address-table static unicast interface
cnMatrix# show mac-address-table count
```

5.8 Locally Managed Username and Password

5.8.1 Managing Locally Managed Username and Password

The CLI or Web interfaces can be accessed using locally configured user/password pair. By default, the switch has two users created with read-only and read-write rights.

Password complexity can be configured by setting the minimum number of lowercase, uppercase, numeric and symbols which are accepted.

Standards

- N/A

Scaling Numbers

- A maximum of 15 users are supported.

Limitations

- Only the **admin** user can create new users using this command.
- The **admin** user cannot be deleted.

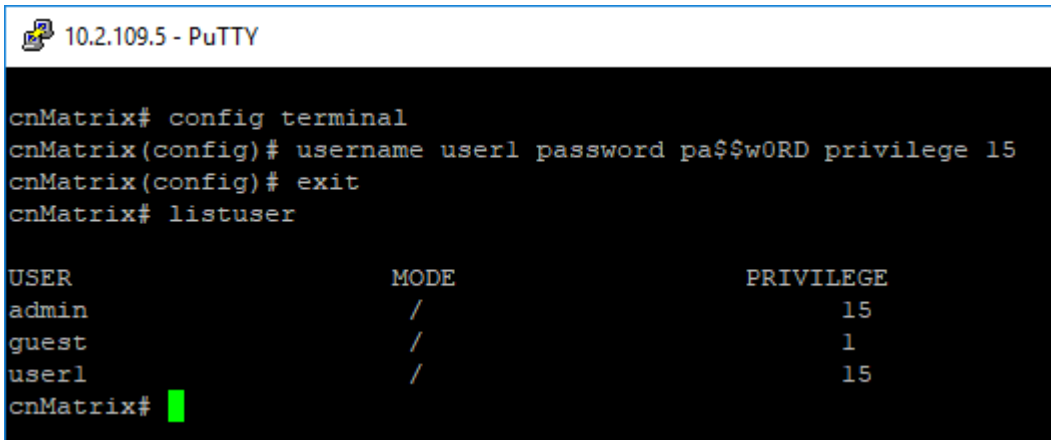
Default Values

- Two users are active by default: **admin** and **guest.**
- **admin** has root privileges (15) and can access configuration commands.
- **guest** user has lower privileges (1), which grant access only to **'clear', 'debug', 'ping'** and **'show'** commands.
- Password expiration: by default the max-life-time value is set to 0, which indicates that the password will not expire.

Prerequisites

- N/A

5.8.2 How to Create Username and Password in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **username user1 password pa$$w0RD privilege 15** command into the terminal to create a user with username, passowrd and privilege level (applies restrictions to user for access to the CLI commands). Press the Enter key.
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **listuser** command into the terminal to list all valid users, their permissible mode and their privilege level. Press the Enter key.

For more information, see Local Management User Name Password Parameters and Commands.

5.9 HTTPS

5.9.1 Managing HTTPS

5.9.1.1 Feature Description

The **cnMatrix HTTP** server works in such a way that it can be reached securely using TLS, or normally using the standard transport layer. A configuration option specifies whether HTTP or HTTPS is active.

SSL (Secure Sockets Layer), is a protocol developed for transmitting private information through an Internet connection. It works by using a public-private key mechanism to encrypt/decrypt data that is transferred over the SSL connection.

HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP for secure communication over an encrypted SSL/TLS connection.

Standards

- The cnMatrix SSL/TLS(IPv4/IPv6) feature is RFC 2246 compliant.

Scaling Numbers

- The maximum number of simultaneous HTTPS WebUI sessions is 4.
- The maximum number of HTTPS sessions supported is 10.

Limitations

- The SSL/TLS server is not compatible with Microsoft Edge and IE 10 browsers.
  - **Starting with version 2.1**, the SSL server is compatible with IE 11 and with Microsoft Edge version 41.16299.1004.0 on Windows 10.
- The crypto key pair that can be generated is either of 512 or of 1024 bits.
  - **Starting with version 2.1**, the default crypto pair that can be generated is of 2048 bits.

Default Values

- The SSL feature is enabled by default and uses a self-signed certificate.
- The default cipherssuite are: rsa-des-sha:rsa-3des-sha:rsa-exp1024-des-sha.
  - **Starting with version 2.1**, the default chipersuites are: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256.

Prerequisites

N/A

The cnMatrix SSL/TLS(IPv4/IPv6) feature provides Transport Layer Security as specified in RFC 2246 and is based on the SSL protocol specification supporting SSL 3.1, TLS v1.0 and starting with version 2.1, TLSv1.0, TLSv1.1 and TLSv1.2.

The TLS protocol is composed of two layers: a TLS Record Protocol and a TLS Handshake protocol The SSL server and the SSL client authenticate each other and negotiate encryption algorithm and cryptographic keys before the application transmits or receives data.

cnMatrix offers the capability of using a cnMatrix self-signed certificate or an external certificate given by the user. The external certificate has to be obtained from a certificate request generated on the cnMatrix switch.

The SSL/TLS server interoperates with SSL clients found in the following HTTP browsers:

- IE5 on Win98 and Win2000.
- IE6 on WinXP.
- Netscape7.0 on Win98.
- Netscape6.0 on RedHat-Linux 7.1.
- Google chrome version 70 on Win10.
- Mozilla Firefox version 52.7.2 on CentOS Linux release 7.4.

The TLS server supports the following:

- Algorithms :
  - Encryption Algorithms DES/3DES
  - Hash MD5/SHA
  - Key Negotiation can be done using RSA or Diffie-Hellman.
- Cipher suites:
  - TLS_RSA_WITH_NULL_MD5
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Port – the standard port used is 443.
- Fragmentation of information blocks into records carrying data in chunks of 2^14 or less.

The TLS server implementation does not support the following configuration:

- The optional compression capability of TLS Record Protocol is not supported due to the fact that the primary application of TLS for cnMatrix is for securing web based configuration in which the data transferred is relatively less.

Starting with version 2.1, the TLS server supports the following:

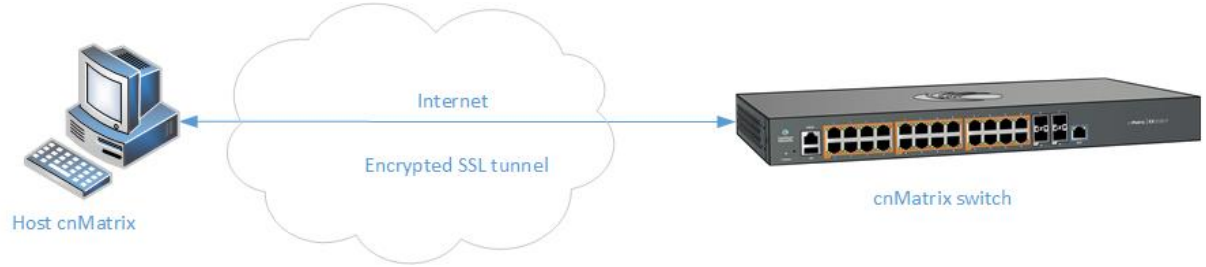
- Algorithms :
  - The key encryption algorithm : ECDHE.
  - The authentication algorithm: RSA.
  - The bulk encryption algorithms :AES128/256 either with or without the GCM mode, and CHACHA20 partnered with poly1350 mac algorithm.
  - The MAC algorithms: SHA256/384 or POLY1350 partnered with chacha20 encryption.
- Cipher suites:
  - TLS1_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS1_ECDHE_RSA_WITH_AES_128_SHA256
  - TLS1_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS1_ECDHE_RSA_WITH_AES_256_SHA384
  - TLS1_ECDHE_RSA_WITH_CHACHA20_POLY1305

The SSL functionality in cnMatrix is implemented using the open source software from

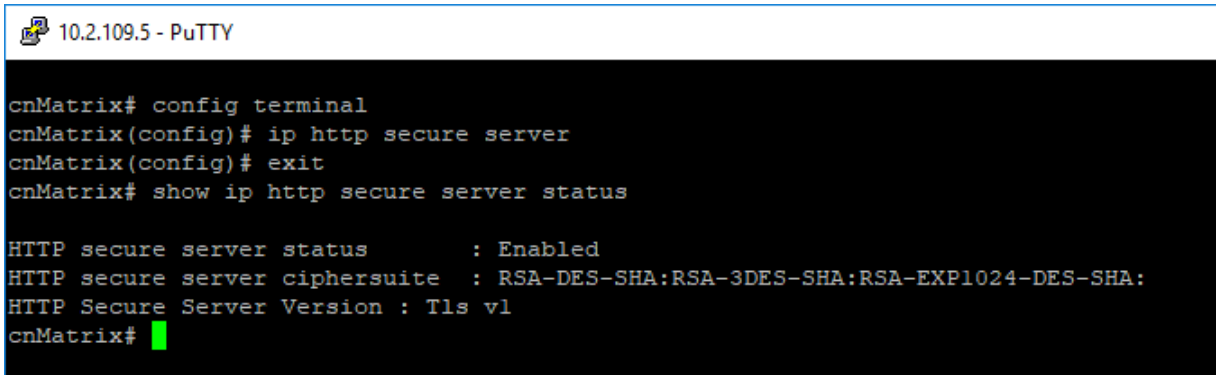
http://www.openssl.org, which include software written by Eric A. Young and Tim J. Hudson. All copyrights listed at http://www.openssl.org/ apply. With respect to licensing terms, the same web-site explains the following: "The OpenSSL toolkit is licensed under an Apache-style license, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions." A copy of the license file is available at: http://www.openssl.org/source/license.html.

Starting with version 2.1:

5.9.1.2 Network Diagram



5.9.2 How to Enable HTTPS in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **ip http secure server** command into the terminal to enable the SSL server on the device and to configure ciphersuites and crypto keys. Press the Enter key.
3. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show ip http secure server status** command into the terminal to display the SSL status (verify if the status is Enabled) and the configuration. Press the Enter key.

For more information, see HTTPS Parameters and Commands.

5.9.3 Troubleshooting HTTPS

Useful commands for troubleshooting:

```
cnMatrix#show ip http secure server status

cnMatrix#debug ssl all

cnMatrix#show ssl server-cert
```

5.10 HTTP

5.10.1 Managing HTTP

5.10.1.1 FeatureDescription

The **Hypertext Transfer Protocol** (HTTP) is an application protocol used in the implementation of the cnMatrix WEB user interface.

The cnMatrix switch includes an implementation of the HTTP server that implements the HTTP protocol version 1.1. This implementation is a subset of the HTTP 1.1 specification optimized for embedded systems, and is not a complete implementation of the full HTTP 1.1 specification.

The HTTP server in the software maintains persistent connections with clients over both Ipv4 and Ipv6 addresses, over TCP and over SSL. After the server processes a request from the client, the server immediately closes the socket connection unless the client had sent a KEEP_ALIVE header or indicated the content-type as MULTIPART in its request, if the version of the client is less than 1.1. If the version of the client is 1.1 or greater the server does not close the socket connection immediately. This allows the same socket connection to be reused for serving all the requests from the client. Thus, resulting in better WebUI management performance. The connection is closed if the server receives a close connection token in the request, or if there is no activity on the connection for more than 5 minutes, or if any network or client failure is suspected. In the last case, the server also sends a message with the connection header containing a close connection token.

The HTTP server allows further requests to come from the same client, while processing one request from the client.

The server buffers the requests and dispatches the requests to other internal managed modules in the same order in which the requests arrived.

The server collects the status of the requests and sends responses to the client in the same order in which the requests arrived.

A browser that supports pipelining can take advantage of this capability to reduce the latency associated with multiple requests. The server implements the expiration model and the validation model to allow clients to cache web pages.

All the WebUI management pages implemented for managing features in the cnMatrix, are statically compiled into the cnMatrix image. This allows the client to specify an absolute URL (for example, GET http://www.host.com/path.file.html). The server accepts this and looks for such a file on the file system in the switch. If present, the file is then returned.

The server parses the requests from the clients to find out the character set used in the requests. If the server does not support the requested character set, the server returns an error message to the client. The server also parses the Transfer Encoding header field in the requests from the clients. If the Transfer Encoding is chunked, the server extracts data from the request message depending upon the size of the chunk. A 501 (Unimplemented) error code is returned and the connection is closed, if it receives an entity body with the Transfer Encoding that it does not understand. The response headers are composed of the following:

- HTTP version – 1.1;
- Date header including current time in the form of Greenwich Mean Time;
- Delta seconds (the number of seconds elapsed after receiving the request message from the client);
- Character sets supported – Accept-charset:iso-8859-1;
- Content coding – Used to support compression.
- Connection field – Indicates whether a connection is persistent or will be closed.
- Content length

- Entity tag – Provided for all separate entities send in the response messages.
- Internet Media Types in the Content-Type and Accept header fields.
- Language tags
- Access Authentication field
- Authorization field

The server provides the following response codes:100 (Continue); 200 (OK) ; 202(Accepted);304(Not Modified) ;405(Method Not Allowed); 406(Not Acceptable); 414 (Request-URI Too Long);413(Request Entity Too Large) ;411 (Length Required); 415(Unsupported Media Type; 505(HTTP Version Not Supported).

The HTTP server implementation supports an Authentication Framework that provides three authentication mechanisms:

- DEFAULT - This is a Form-Based proprietary authentication scheme used by the software to authenticate the HTTP clients. In it the client trying to access the Web UI will be presented a Login Page where the user has to enter the Credentials and Submit. The user is allowed access to the Web UI upon successful authentication of the credentials. This is the default authentication scheme used by the software.
- BASIC - This is an HTTP Authentication scheme where the client must authenticate itself with a user-ID and a password for a realm. The HTTP server provides a single protection space called the cnMatrix protection space and a single realm namely “cnMatrix” which corresponds to the software’s protection space. The protection space contains all the web pages of the cnMatrix server. The HTTP server will service the request only if it can validate the user-ID and password for the cnMatrix protection space.
- DIGESTS - This is an HTTP Authentication scheme where the HTTP server challenges the HTTP client using a WWWAuthenticate header containing a nonce value. A valid Authorization request from the client contains a checksum (the MD5 checksum) of the username, the password, the given nonce value, the HTTP method and the requested URI. In response to the Authorization request, the server sends an Authentication-Info header to communicate the status of the authentication attempt. The Authentication framework of the software provides two parameters:
  - Operational Authentication Scheme - governs the scheme to be used to authenticate all the HTTP sessions. This is a READ-ONLY parameter which is initialized at software startup time.
  - Configurable Authentication scheme contains the scheme which can be modified at runtime through the CLI or the Web UI. The modified value is applied only after the restart of the software.

Standards

- The HTTP server is RFC 1945 RFC 2068 (HTTP 1.1 – partial), and 2617 compliable.

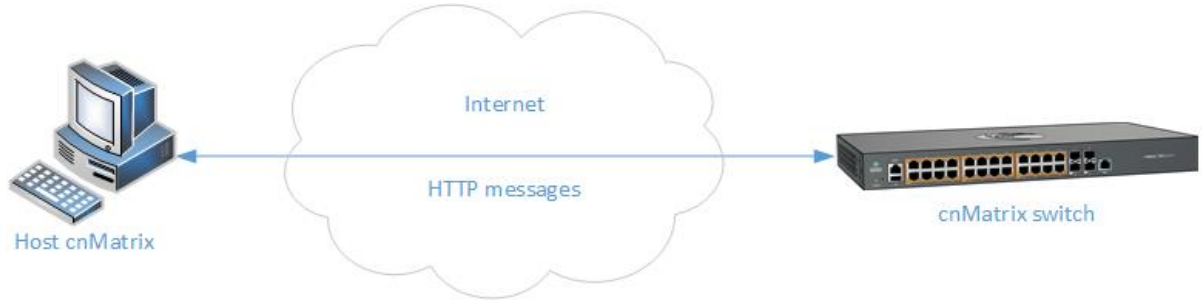
Scaling Numbers

- The HTTP server supports maximum 4 HTTP WEB UI sessions opened simultaneously.

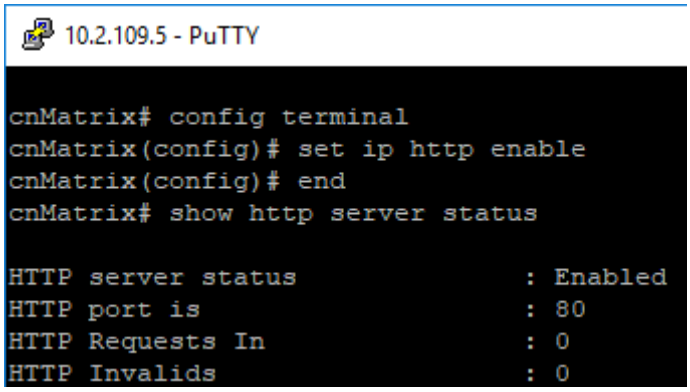
Default Values

- The default authentication scheme: default.
- The HTTP redirection option is disabled by default.
- The default HTTP port: 80.
- HTTP is disabled by default in the switch.

5.10.1.2 Network Diagram



5.10.2 How to Enable HTTP in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **set ip http enable** command into the terminal to enable HTTP. Press the Enter key.
3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.
4. Type the **show http server status** command into the terminal to display the HTTP server status (verify if the HTTP server status is Enabled). Press the Enter key.

For more information, see HTTP Parameters and Commands.

5.10.3 Troubleshooting HTTP

Useful commands for troubleshooting:

```
cnMatrix# show http server status
```

5.11802.1x Authentication

5.11.1Managing 802.1x Authentication

The **802.1X** feature enables network devices authentication on the switch and prevents unauthorized devices from accessing the services provided by the Switch and LAN.

The cnMatrix switch controls physical access to the network based on the authorization status of Client devices. It requests the credentials (Identity and Password) of the Client and submits it to the Authentication Server (RADIUS). In addition, the cnMatrix switch acts as a RADIUS client and is responsible for encapsulating and decapsulating the EAP frames to interact with the RADIUS server.

The following host modes are available:

- single-host
- multi-host

> The switch has a local authentication server in order to support local authentication without the RADIUS server.

Standards

- IEEE 802.1X
- RFC 2865

Scaling Numbers

- N/A

Limitations

- N/A

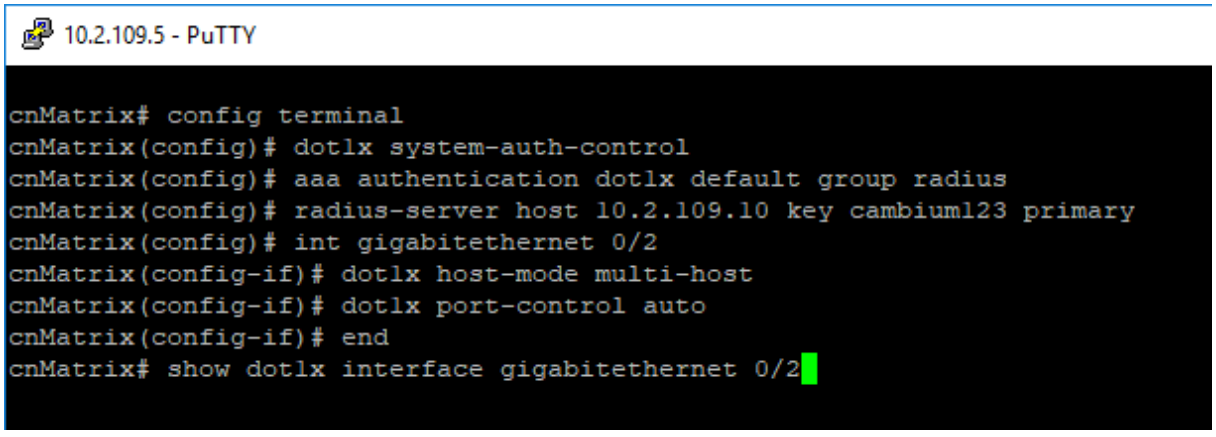
Default Values

- 802.1X is disabled by default.
- 802.1X per port Authentication Mode is set to Multi-Host by default.

Prerequisites

- N/A

5.11.2 How to Enable and Configure Authentication in CLI Interface



1. Type the **config terminal** command into the terminal. Press the Enter key.
2. Type the **dot1x system-auth-control** command into the terminal to enable the 802.1X authentication feature . Press the Enter key.
3. Type the **aaa authentication dot1x default group radius** command into the terminal to set the RADIUS server as the remote authentication method for all ports. Press the Enter key.
4. Type the **radius-server host 10.2.109.10 key cambium123 primary** command into the terminal to specify the RADIUS query parameters. Press the Enter key.
5. Type the **int gigabitethernet 0/2** command into the terminal to select the interface to be

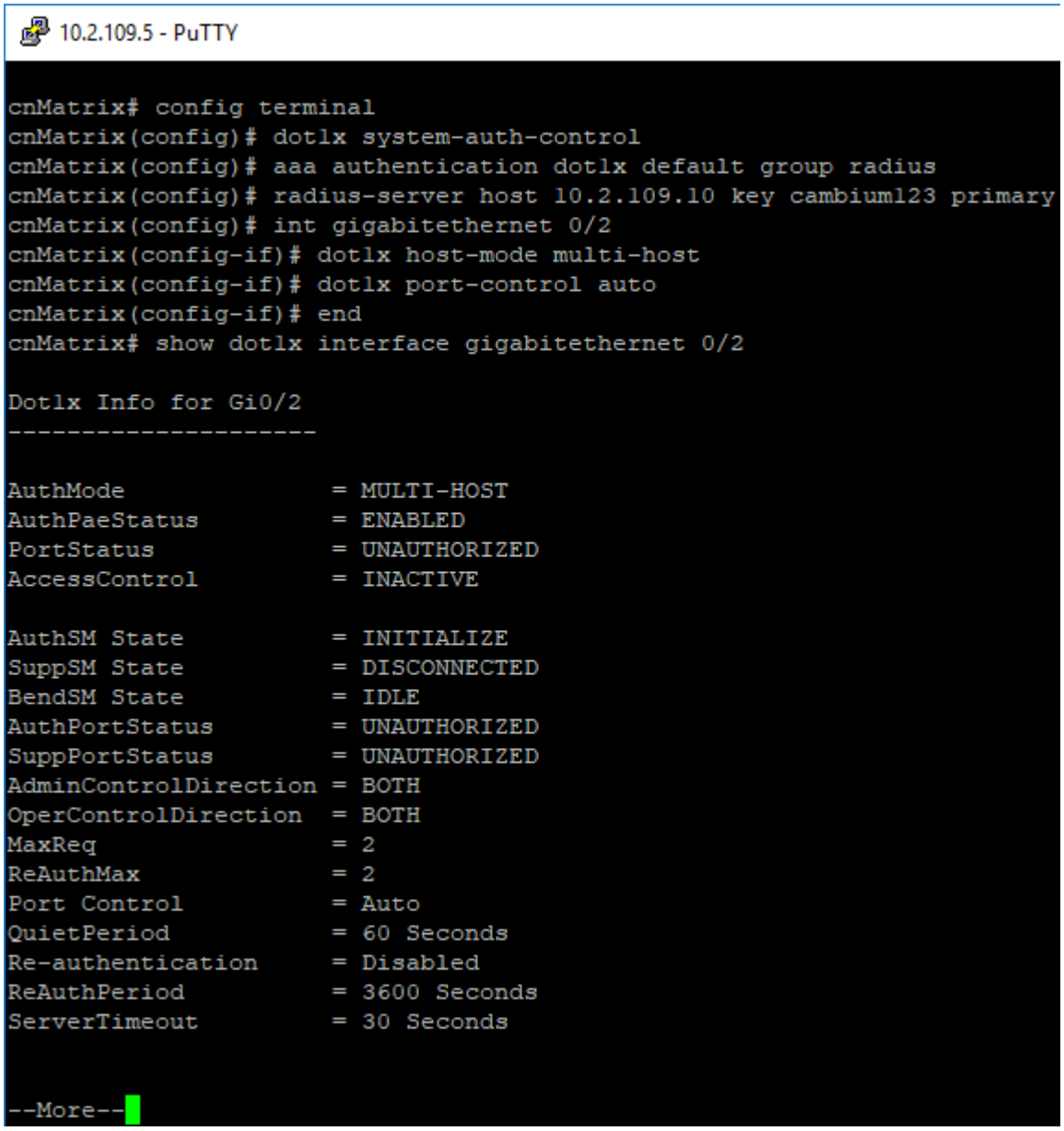
configured. Press the Enter key.

6 Type the **dot1x host-mode multi-host** command into the terminal to configure port authentication mode. Press the Enter key.

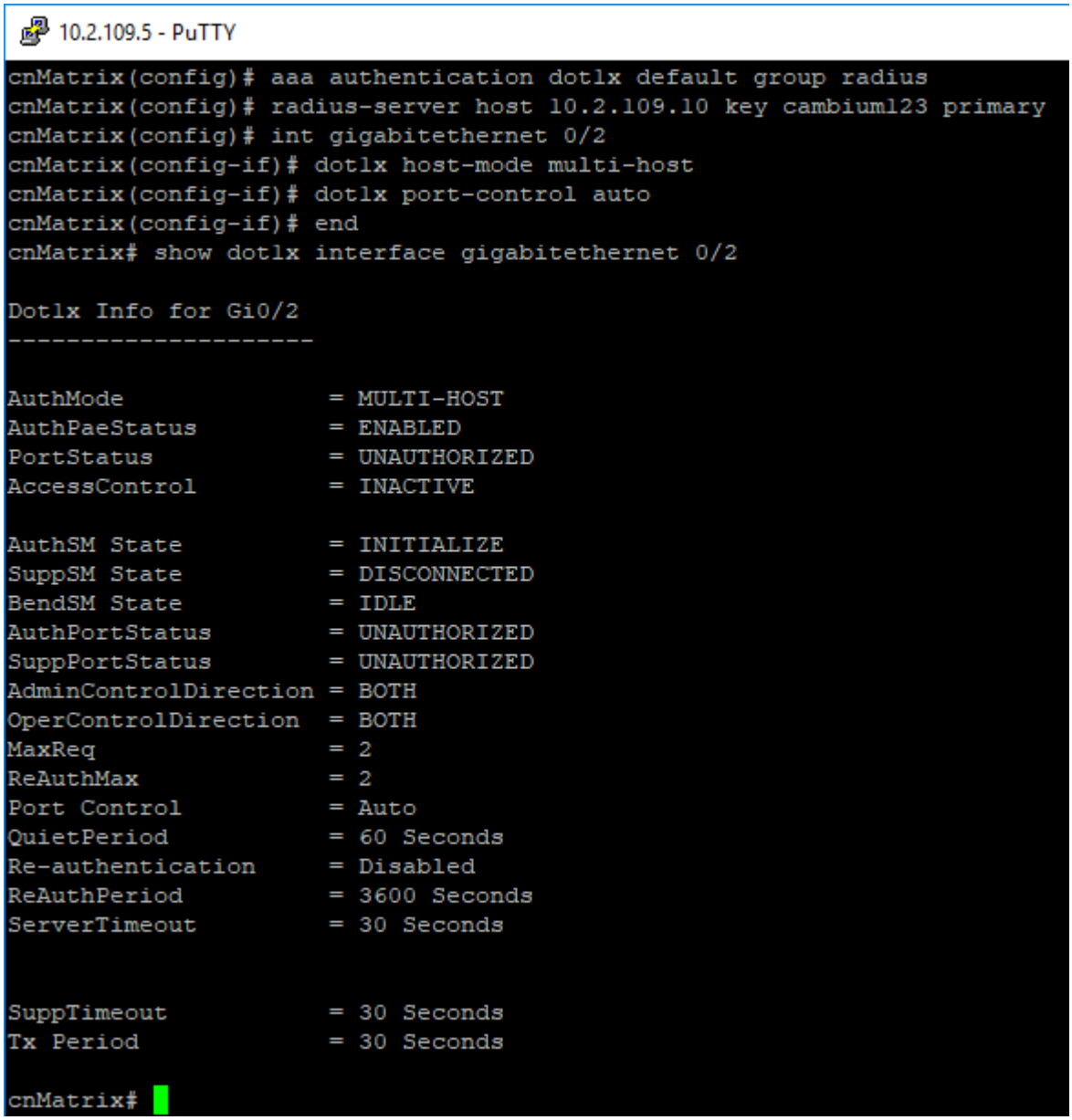
7 Type the **dot1x port-control auto** command into the terminal to configure the authentication port control. Press the Enter key.

8 Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the Enter key.

9 Type the **show dot1x interface gigabitethernet 0/2** command into the terminal to display the information of the 802.1X authentication for the gi0/2 interface. Press the Enter key.



10 Press the Space key.



For more information, see 802.1x Authentication Parameters and Commands.

6 Regulatory and Compliance

6.1 Legal and Regulatory Information

6.1.1 Legal and Reference Information

6.1.1.1 Introduction

This chapter provides legal notices including software license agreements.

Attention

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

The following topics are described in this chapter:

- Open Source Components incorporated in the Hardware and associated notices
- Hardware Warranty
- Limitation of Liability
- Compliance with Safety Standards

6.1.2 Cambium Networks End User License Agreement

6.1.2.1 Introduction

ACCEPTANCE OF THIS AGREEMENT

In connection with Cambium Networks' delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium Networks is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement ("Agreement"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT ORINSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCTTO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUTNOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

DEFINITIONS

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Cambium Networks' fixed wireless broadband devices for which the Software and Documentation is licensed for use.

GRANT OF LICENSE

Cambium Networks Limited ("Cambium") grants you ("Licensee" or "you") a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in "Conditions of use" and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

CONDITIONS OF USE

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.
2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.
3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.
4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for backup purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium Networks copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including

machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

TITLE AND RESTRICTIONS

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium Networks and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this

Agreement will result in automatic termination of this license.

CONFIDENTIALITY

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will

result in irreparable harm to Cambium Networks for which monetary damages would be inadequate and for which Cambium Networks will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the

confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care. You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium Networks prior to such disclosure and provide Cambium Networks with a reasonable opportunity to respond.

RIGHT TO USE CAMBIUM'S NAME

Except as required in "Conditions of use", you will not, during the term of this Agreement or thereafter, use any trademark of Cambium Networks, or any word or symbol likely to be confused with any Cambium Networks trademark, either alone or in any combination with another word or words.

TRANSFER

The Software and Documentation may not be transferred to another party without the express written consent of Cambium Networks, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

UPDATES

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An "Update" means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium Networks makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

MAINTENANCE

Except as provided above, Cambium Networks is not responsible for maintenance or field service

of the Software under this Agreement.

DISCLAIMER

CAMBIUM NETWORKS DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM NETWORKS SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS." CAMBIUM NETWORKS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM NETWORKS MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

LIMITATION OF LIABILITY

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING,

WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of

incidental or consequential damages, so the above exclusion or limitation may not apply to you.)

IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

U.S. GOVERNMENT

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or

disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

TERM OF LICENSE

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium Networks in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium

Networks, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

GOVERNING LAW

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

ASSIGNMENT

This agreement may not be assigned by you without Cambium's prior written consent.

SURVIVAL OF PROVISIONS

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

ENTIRE AGREEMENT

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium Networks may modify this Agreement as necessary to comply with applicable laws.

THIRD PARTY SOFTWARE

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

6.1.3 Source Code

6.1.3.1 Source Code

OpenSSL 1.1.0	OpenSSL License ========== Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE

	USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ========== This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). Original SSLeay License ---------- Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED

	OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Libwebsockets v1.3-chrome37-firefox30	Copyright (C) 2010-2014 Andy Green andy@warmcat.com Libwebsockets and included programs are provided under the terms of the GNU Library General Public License (LGPL) 2.1 (available in Appendix A), with the following exceptions: 1) Static linking of programs with the libwebsockets library does not constitute a derivative work and does not require the author to provide source code for the program, use the shared libwebsockets libraries, or link their program against a user-supplied version of libwebsockets. If you link the program to a modified version of libwebsockets, then the changes to libwebsockets must be provided under the terms of the LGPL in sections 1, 2, and 4. 2) You do not have to provide a copy of the libwebsockets license with programs that are linked to the libwebsockets library, nor do you have to identify the libwebsockets license in your program or documentation as required by section 6 of the LGPL. However, programs must still identify their use of libwebsockets. The following example statement can be included in user documentation to satisfy this requirement: "[program] is based in part on the work of the libwebsockets project (http://libwebsockets.org)"

Jansson 2.11	Copyright (c) 2009-2016 Petri Lehtinen <petri@digip.org> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Zlib 1.2.11	(C) 1995-2017 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any dam-

	ages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code. If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes. Please read the FAQ for more information on the distribution of modified source versions.

OpenSSL 0.9.8i	OpenSSL 0.9.8i Copyright (c) 1998-2008 The OpenSSL Project Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson All rights reserved. OpenSSL License ========== Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the

OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
7. "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

	Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: - "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" - The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related. 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: 5. "This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.

Open SSH 5.1	1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name oth-

er than "ssh" or "Secure Shell".

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto";.

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORREC-

	TION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license. Cryptographic attack detector for ssh - source code Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE. Ariel Futoransky <futo@core-sdi.com> <"">http://www.core-sdi.com>; 3) ssh-keyscan was contributed by David Mazieres under a BSD-style license. Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact. 4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license: @version 3.0 (December 2000) Optimised ANSI C code for the Rijndael cipher (now AES) @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)
One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)
Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjölä
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUD-

ING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42):

<phk@login.dknet.dk> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995
This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOW-

	EVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Some code is licensed under an ISC-style license, to the following copyright holders: Internet Software Consortium. Todd C. Miller Reyk Floeter Chad Mynhier Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Some code is licensed under a MIT-style license to the following copyright holders: Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Appendix A	GNU Lesser General Public Library version 2.1 GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.
We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be

affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work

that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".) "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.
   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) The modified work must itself be a software library.
   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.
This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent

access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.
However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.
If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.
You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:
- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly

	with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. • c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. • d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. • e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute. 7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: • a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. • b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work. 8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance. 9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it. 10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.
NO WARRANTY
15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PRO-

VIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.
one line to give the library's name and an idea of what it does.
Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990
Ty Coon, President of Vice

	That's all there is to it!

6.1.4 Hardware Warranty

Hardware Warranty

cnMatrix™ switch family ("Covered Product") hardware is covered with a 5 - year Limited Lifetime Warranty. "Lifetime" is defined as the period beginning on the date of original purchase by the first end user of the Product and ending five (5) years thereafter. Under this Limited Lifetime Warranty, Cambium warrants to its end users for the Lifetime (as defined) that the Covered Product purchased by such end user, when used under normal conditions and consistent with applicable Covered Product documentation supplied with the Covered Product, will be free from defects in material and workmanship, and will perform in accordance with the documentation supplied for such Covered Product.

Except as otherwise prescribed by applicable law, in the event of a breach of this Hardware Limited Lifetime Warranty, the sole and exclusive remedy, and Cambium's sole and exclusive liability, will be for Cambium to use commercially reasonable efforts to repair or replace the Covered Product that caused the breach of this warranty. If Cambium cannot, or determines that it is not practical to, repair or replace the Covered Product, then the sole and exclusive remedy and the limit of Cambium's obligation will be to refund the amount received by Cambium for purchase of such Covered Product. The Hardware Limited Lifetime Warranty is provided to the original end user only and is not transferrable.

6.1.5 LIMITATION OF LIABILITY

LIMITATION OF LIABILITY

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.)

IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT

6.1.6 Compliance with Safety Standards

Intended Use: The Cambium Networks cnMatrix next-generation switching platform offers a cloud-managed, high-performance, feature-rich enterprise-grade ethernet switching solution. This equipment is intended for professional applications for fixed indoor installations only.

Installation and Operation: Installation and operation of this product are complex and Cambium Networks therefore recommends professional installation and management of the system. Please follow the instructions in this leaflet. Further guidance on cnMatrix installation and operation is available in the accompanying *Quick Start Guide*, which can also be found online at the link below

The installer must have sufficient skills, knowledge, and experience to perform the installation task and is responsible for:

- Familiarity with current applicable national regulations, including electrical installation and surge protection
- Installation in accordance with Cambium Networks' instructions

Product Safety Information:

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product *User Guide, web link*

below, for more details. Please observe the following safety rules:

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e., touch grounded bare metal) before touching the product. Ensure that the product is properly grounded.

Ensure that the equipment is not powered during installation. Always disconnect equipment from its power source before servicing.

Always use a qualified electrician to install cabling.

Use outdoor-rated cables for connections that will be exposed to the outdoor environment.

Operation in the EU – Restrictions:

- This equipment is for indoor use only.
- CE EMI Class A Warning: This equipment is compliant with Class A of CISPR32. In a residential environment, this equipment may cause radio interference.

Waste Electrical and Electronic Equipment (WEEE) Directive:

Please do not dispose of electronic and electric equipment or electronic and electric accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. If you reside in European Union countries, please contact your local equipment supplier representative or the Cambium Networks Support Center for information about the waste collection system in your country

Useful Web Links:

- User Guide: https://www.cambiumnetworks.com/guides
- Technical Training: https://learning.cambiumnetworks.com
- Cambium Support Center: https://support.cambiumnetworks.com/
- EU Declaration of Conformity: http://www.cambiumnetworks.com/eu_dofc

Equipment Manufacturer:

Cambium Networks Ltd, Unit B2 Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP, United Kingdom