Cambium Networks™

USER GUIDE

cnMatrix

Release 6.1

Reservation of Rights

Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium recommends reviewing the Cambium Networks website for the latest changes and updates to products. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

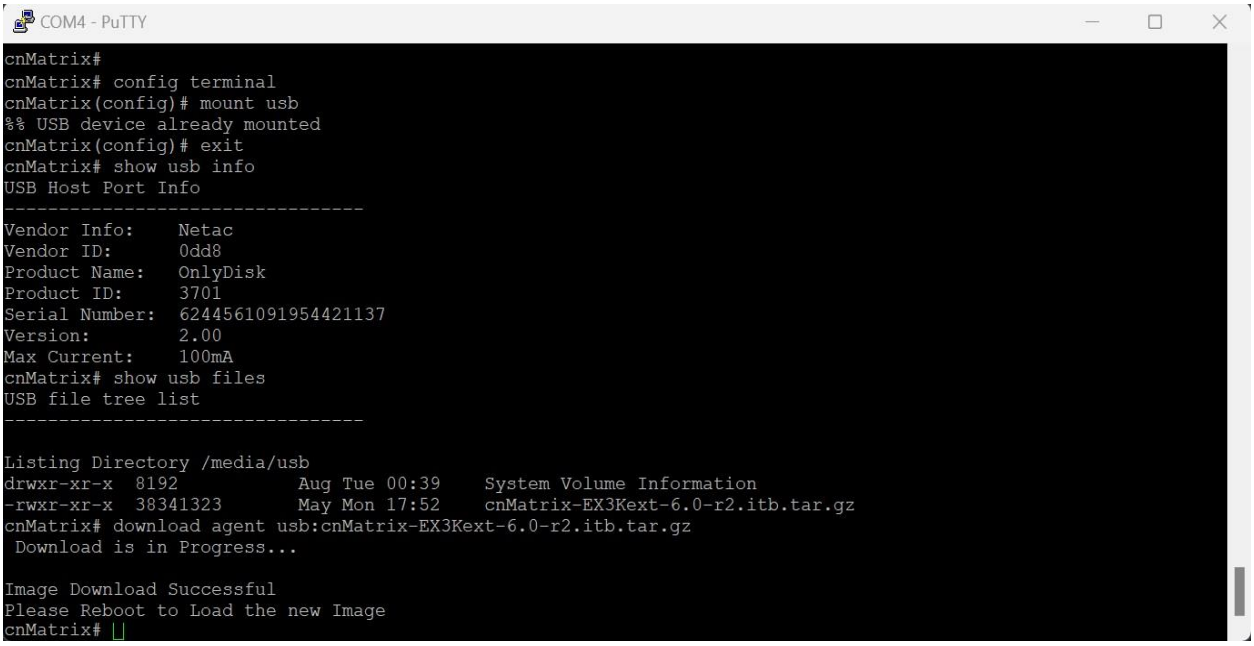
High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”).

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

January 2025

Contents



Getting Started

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 visibility. 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 the emerging needs of business and residential customers.

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

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.

Tip

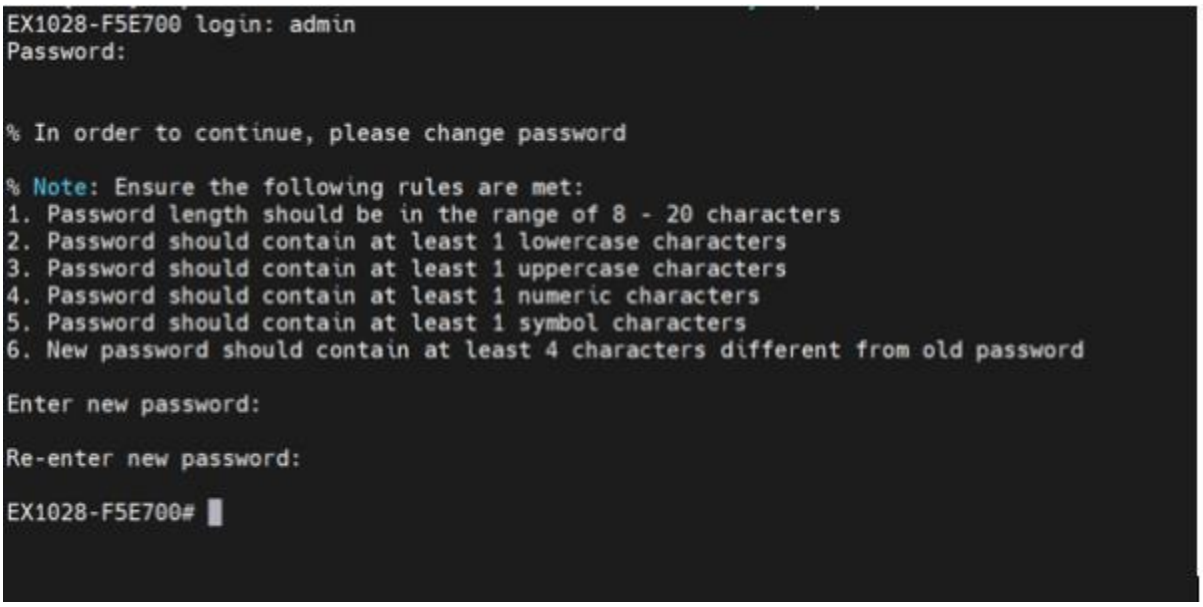
The default user name and password is **admin**. After logging in as an admin user, you can create a new user or delete an existing user and modify your password or the ones created for the new users.

First login

For security reasons, at first login you are asked to change default password **admin**.

The new password should comply the following rules:

1. Password length should be in the range of 8 - 20 characters.
2. Password should contain at least one lowercase character.
3. Password should contain at least one uppercase character.
4. Password should contain at least one numeric character.
5. Password should contain at least one symbol character.
6. New password should contain at least four characters different from old password.



In the above figure you can see that if the password is introduced follow the rules, it is asked to reintroduce the password. If you succeed in changing the default password, you can use the switch further, otherwise you will not until change the password.

Note:

By default, if the user fails to authenticate three times, the user will be locked for 10 minutes. For more information see:_User_authentication_retries.

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 Privileged 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>	cnMatrix#	To logout from Privileged EXEC mode, the **exit** command is used.
Global Configuration	In the Privileged EXEC mode, type the **configure terminal** command to enter the Global Configuration mode.		

Command Mode	Access Method	Prompt	Exit Command
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-BandInterface Mode	In the Global Configuration mode, type the **interface mgmt0** command to enter the Out-Of-Bandmode.	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 Configuration mode, type the **ip dhcp pool <id>** command to enter the DHCP Pool Configuration Mode.	cnMatrix(dhcp-config)#	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.
SNTP Configuration Mode	In the Global Configuration Mode, type the **sntp** command to enter the SNTP Configuration mode.		To exit to the Global Configuration mode the

Command Mode	Access Method	Prompt	Exit Command
		cnMatrix(config-sntp)#	**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.

Basic Switch Configuration in CLI Interface

Configuring CLI and cnMaestro

Accessing CLI Interface (examples)

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.**

Accessing CLI Interface Using Serial Port

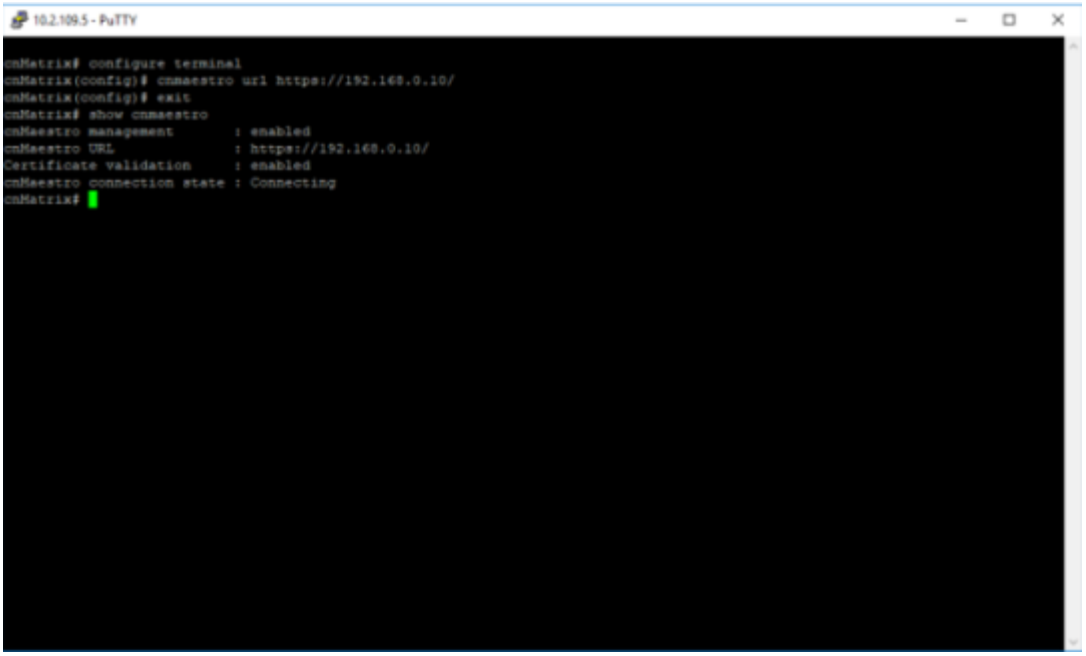
1. Connect the console cable to PC and to console port on the switch.
2. Open **PuTTY** application.
3. In the **PuTTY Configuration** window, select **Serial** in the **Connection type** section.
4. In the **Serial line** section, enter the name of the serial connection.
5. In the **Speed** section,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

   username: **admin**

   password: **admin**

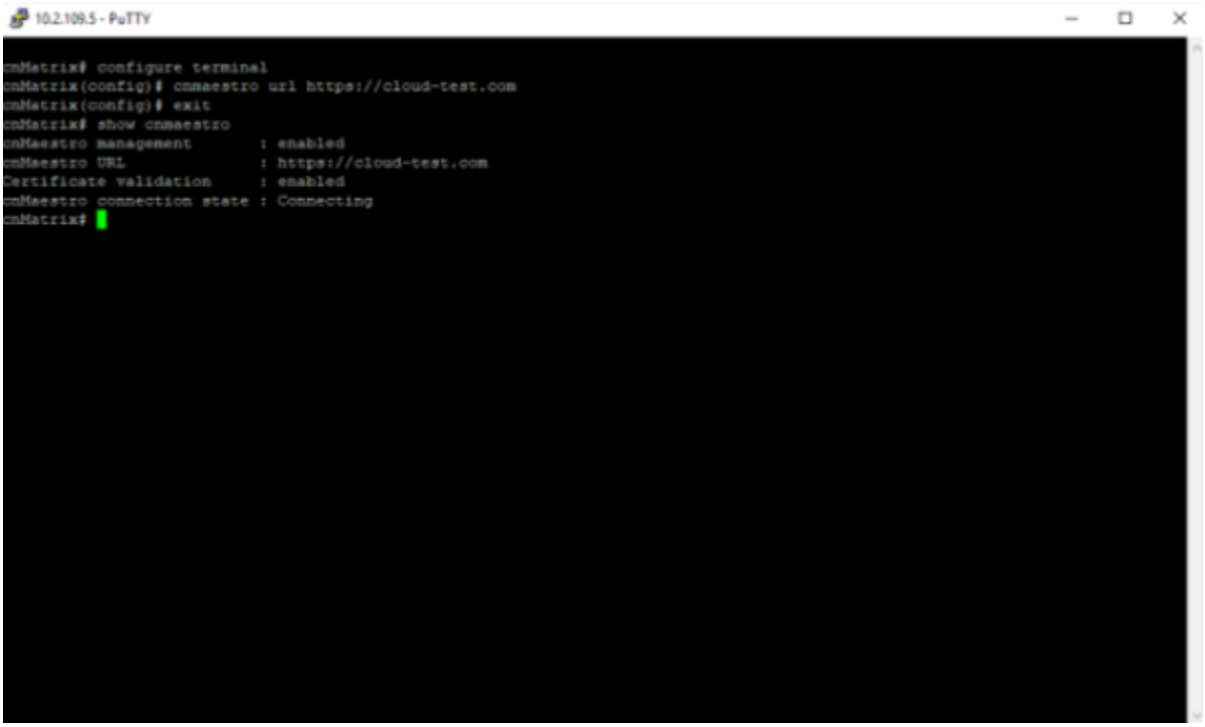
Configuring cnMaestro Using CLI

cnMaestro URL Configuration as IP



1. Type the **config 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 the cnMaestro URL as IP. 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 **Enter** key.

cnMaestro URL Configuration as String



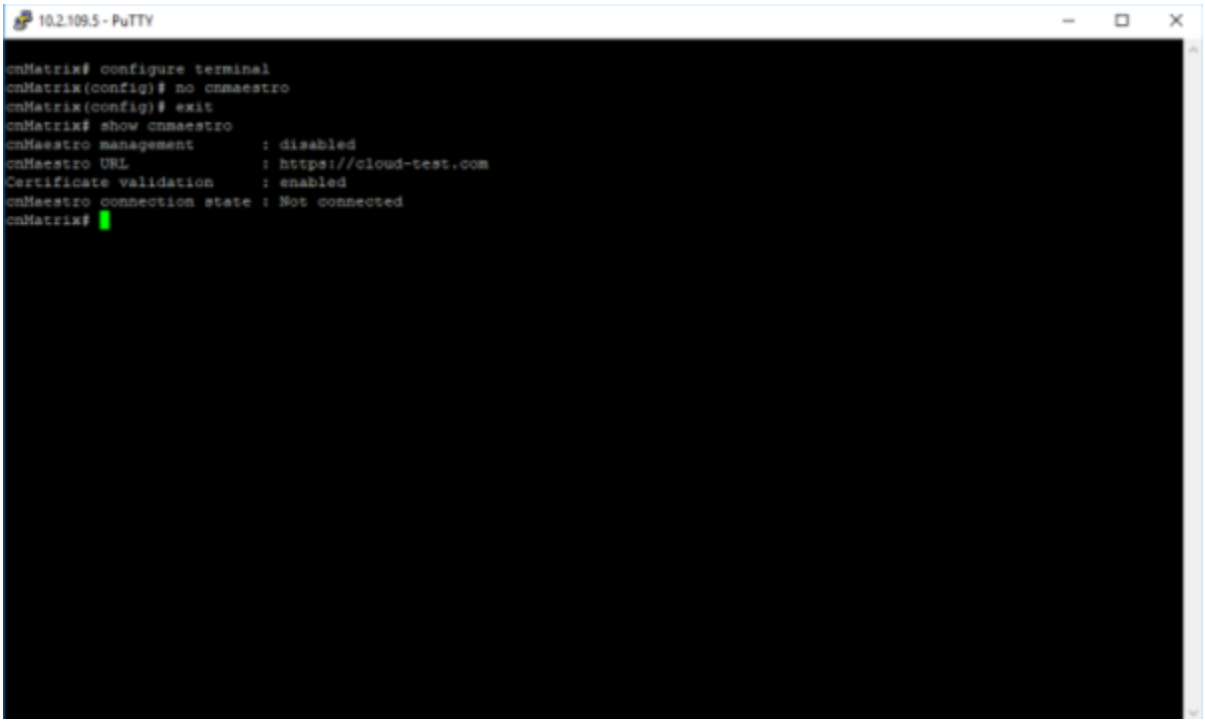
1. Type the **config terminal** command into the terminal. Press **Enter** key.
2. Type **cnmaestro url <cnMaestro on premise URL>** command into the terminal. On-Premise cnMaestro URL should be https://hostanme.domainname.
3. Type the **exit** command into the terminal. Press **Enter** key.
4. Type the **show cnmaestro** command into the terminal to display cnMaestro information. Press the key. Press **Enter** key.
5. Make sure that a DNS service is working properly in your network.

Note

The default cnMaestro url: .

By default, the switch will acquire dynamic IP, default gateway, and DNS configuration and it will automatically attempt connection to cnMaestro Cloud.

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 the 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.

How to Disable cnMaestro Server Certificate Validation

Caution

Disabling Server Certificate Validation is not recommended as it exposes the switch to man-in-the-middle attacks.

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

How to Enable cnMaestro On-Premises Server Certificate Validation

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **cnmaestro validate-cert** full command into the terminal to enable certificate validation for cnMaestro On-Premises. Press the **Enter** key.
3. Type the **end** 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.

Troubleshooting cnMaestro

Useful commands:

- cnMatrix# debug cnmaestro all

Display management interfaces information

Starting with release 3.2-r4 new commands are available for displaying aggregate information for cnMaestro and XMS-Cloud Management, SSH, HTTPS, HTTP, and Telnet.

```
# show management
Remote Management
  Config                          : Enabled
  Status                          : Connected to cloud.cambiumnetworks.com (xms)
  Certificate Validation          : Cloud-Only
  Last Action                     : Connected
  Last Sync                       : Never
GUI
  HTTP                  : Enabled
  HTTPS                 : Enabled
Command Line
  Telnet                : Disabled
  SSH                   : Enabled
```

The remote cnMaestro Cloud or XMS-Cloud management can be configured with the **management cambium-remote** command. The functionality is similar to **cnmaestro** command.

```
(config)# management cambium-remote ?

<CR>                              Enables the remote management interface
url                               Specify static remote management interface
                                  URL
validate-cert                     Enable cloud certificate validation
```

Save/Restore/Erase/Download Configurations in CLI

Feature Overview

Configuration changes performed on the cnMatrix switch after a system reset must 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 the system startup. 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 default settings.

Caution

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

Note

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

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

Default Values

- Auto-save 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 configuration feature either works 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.

Boot Partial Default

The **boot partial default** feature enables you to delete all configurations, 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 **boot partial default** command.

Copy Switch Configuration from the remote server

How to Copy Switch Configuration from a TFTP server

```
# write startup-config
# copy startup-config tftp://10.2.109.2/my_config.conf

# copy tftp://10.2.109.2/my_config.conf startup-config
  ...Completed: 10 %...
  ...Completed: 20 %...
  ...Completed: 30 %...
  ...Completed: 40 %...
  ...Completed: 50 %...
  ...Completed: 60 %...
  ...Completed: 70 %...
  ...Completed: 80 %...
  ...Completed: 90 %...
File Copied Successfully. Please reboot to activate the new config.
```

Note

1. Make sure to first save your configuration to Flash before copying it to the TFTP server.
2. Some TFTP servers could require to have the configuration file created and with RW rights before the upload process starts.
3. The configuration file should have a **.config** extension.

How to Copy Switch Configuration from an SFTP server

```
# write startup-config
# copy startup-config sftp://username:password@10.2.109.2/my_config.conf

# copy sftp://username:password@10.2.109.2/my_config.conf startup-config

File Copied Successfully. Please reboot to activate the new config.
```

Note

1. Make sure to first save your configuration to Flash before copying it to the SFTP server make sure to first save your configuration to Flash before copying it to the SFTP server.
2. **username** and **password** are the SFTP login credentials.
3. The configuration file should have a **.config** extension.

How to Copy Switch Running-Config to a TFTP server

copy running-config tftp://<server IP address>/<filename>

How to Copy Switch Running-Config from a TFTP server

copy tftp://<server IP address>/<filename> running-config

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.

Attention

Starting with version 2.1, the default host name is generated using the last 6 digits of the base MAC address (e.g: EX2010P-FEB430).

Note

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

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

cnMatrix Features

cnMatrix feature availability varies between hardware platforms and cloud managers. Consult the feature availability from the following table:

cnMatrix Feature	cnMaestro Configurable (5.1)	EX1K EX2K EX3K Legacy	EX3024F
Industry-standard Command Line Interface (CLI)	Yes	Yes	Yes
Web Management	Yes	Yes	Yes
cnMaestro Cloud-based Management	Yes	Yes	Yes
Zero-touch Remote Provisioning	Yes	Yes	Yes
SNMPv1/v2c/v3	Yes	Yes	Yes
Telnet Client/Server	Server	Yes	Yes
Out-Of-Band Ethernet Management	No	Except TX1K TX2K and EX1K	Yes
SSH/SSH v2	No	Yes	Yes
DHCP Client	Yes	Yes	Yes
DHCP Server	No	Yes	Yes
Local/Remote Syslog	No	Yes	Yes
System Resource Monitoring	Yes	Yes	Yes
802.1Q VLAN and Trunking Support	Yes	Yes	Yes
QinQ 802.1ad	cnMaestroX	Except EX1K	No
802.1d STP, 802.1w RSTP	Yes	Yes	Yes
802.1s MSTP	Yes	Yes	Yes
PVRST (Per VLAN RSTP)	Yes	Yes	Yes
802.1p Quality of Service	No	Yes	Yes
ACL QoS: Mapping/Marking ToS/DSCP, 802.1p, Priority Queue	Partially	Yes	Yes
Inbound Traffic Policing, and Outbound Traffic Shaping	No	Yes	Yes
Storm Control	Yes	Yes	Yes
Flow Control Per Port	No	Yes	NO**

802.1ab Link Layer Discovery Protocol (LLDP)	No	Yes	Yes
802.3ad Link Aggregation	Yes	Yes	Yes
IGMP Snooping v1/v2	Yes	Yes	Yes
IGMP Snooping Proxy	No	Yes	Yes
Private VLAN Edge	Yes	Yes	Yes
Port Mirroring: Port-based, ACL-based	Yes (port-based only)	Yes	Yes
SNTP	Yes	Yes	Yes
Port Statistics	Yes	Yes	Yes
RMON	No	Yes	Yes
Routing Between Directly Connected Subnets	No	Yes	Yes
Routed Interfaces	No	Yes	Yes
IPv4 static route	Yes	Yes	Yes
IPv6 static route	No	No	No
Host routes	No	Yes	Yes
DHCP Relay	No	Yes	Yes
802.1x Authentication	Yes	Yes	NO**
Radius Change Of Authorization	Yes	Yes	NO**
Radius/TACACS+	Radius	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
Static MAC	No	Yes	Yes
IGMP Filtering	No	Yes	Yes
Locally Managed Username and Password	Yes	Yes	Yes
cnMaestro on-premise	Yes	Yes	Yes
RIPv1/v2	No	Except EX1K and TX1K	Yes
OSPFv2	No	Except EX1K and TX1K	Yes
USB support	No	Except TX1K	Yes
Reset button	Yes	Except TX1K	Yes
Dynamic ARP Inspection	Yes	Yes	Yes
LLDP-MED	No	Yes	Yes
CLI ‘do’ command	No	Yes	Yes
cnMaestro Configuration	Yes	Yes	Yes
XMS-Cloud Configuration	N/A	Except TX1K and TX2K	NO
Cambium Sync	Yes	Only TX2K	No

802.3 af/at/bt	Yes	• EX1K • EX3K up to 30W • EX2K up to 30W • EX2016-P up to 60W • TX1K TX2K up to 90W	No
PoE autodetect cnMedusa	Yes	TX1K and TX2K, some ports only	No
PoE autodetect cnWave	Yes	TX1K and TX2K, some ports only	No
PoE high temperature mode	No	TX2K	No
PoE hybrid mode	Yes	Yes	No
PoE Budget	N/A	Full/Reduced on EX1K	No
PoE+ (30W)	N/A	Yes	No
24V Passive PoE	Yes	TX1K and TX2K, some ports only	No
54V Passive PoE	Yes	TX1K and TX2K	No
PoE on 4 Pairs (90W)	N/A	EX2016M-P TX1K TX2K on some ports only	No
PoE on 4 Pairs (60W)	N/A	EX3052R-P: ports 24-48 (60W) EX3028R-P: ports 12-24 (60W)	No
Transceiver ports	N/A	SFP+/SFP on EX2010 and EX1K	SFP+
Cable Diagnostics	cnMaestroX	On copper 10/1001000 ports	No
Removeable Power Supplies	No	• EX3K • EX2052R-P • TX2K	No
Dual Redundant Power Supplies	No	Only on: • EX3K • TX2020R-P	Yes
PBA	Yes (cnMaestroX on EX1K)	Yes	Yes
PBA Localization	cnMaestroX	Yes	Yes
PBA MAC List	cnMaestroX	Yes	Yes
Auto recovery of connected devices	cnMaestroX	Yes	Yes
HTTP(S) Client Proxy	No	Yes	Yes

Automated Voice VLAN	Yes	Yes	Yes
Ethernet Ring Protection Service (ERPS – G.8032)	No (requires cnMaestroX in future)	Except EX1K	NO
PIM-SM	No (requires cnMaestroX in future)	No	Yes

L2 Features

VLAN

Managing VLAN

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 an 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.

Note

The port can be set as an access port, only if the following three 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. The acceptable frame type is automatically set as **untagged And Priority Tagged** if the first two conditions are met.

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

Note

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

Note

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 conjunction with the Acceptable Frame Type:

- If the **Acceptable Frame Type** is set to **All**, the hybrid 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 **untagged and PriorityTagged**, the hybrid port will accept and send the untagged and priority tagged traffic.

Attention

Be aware that when the **Acceptable Frame Type** is set to **All** or **Tagged**, you have to configure the PVID value in conjunction with the Acceptable Frame Type 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 4094 VLANs can be created.

Limitations

- A maximum of 64 VLANs can be configured in PVRST mode.

Default Values

- VLAN functionality 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 is hybrid.

Note

The static MAC addresses configured on a specific VLAN will be removed after deleting the VLAN.

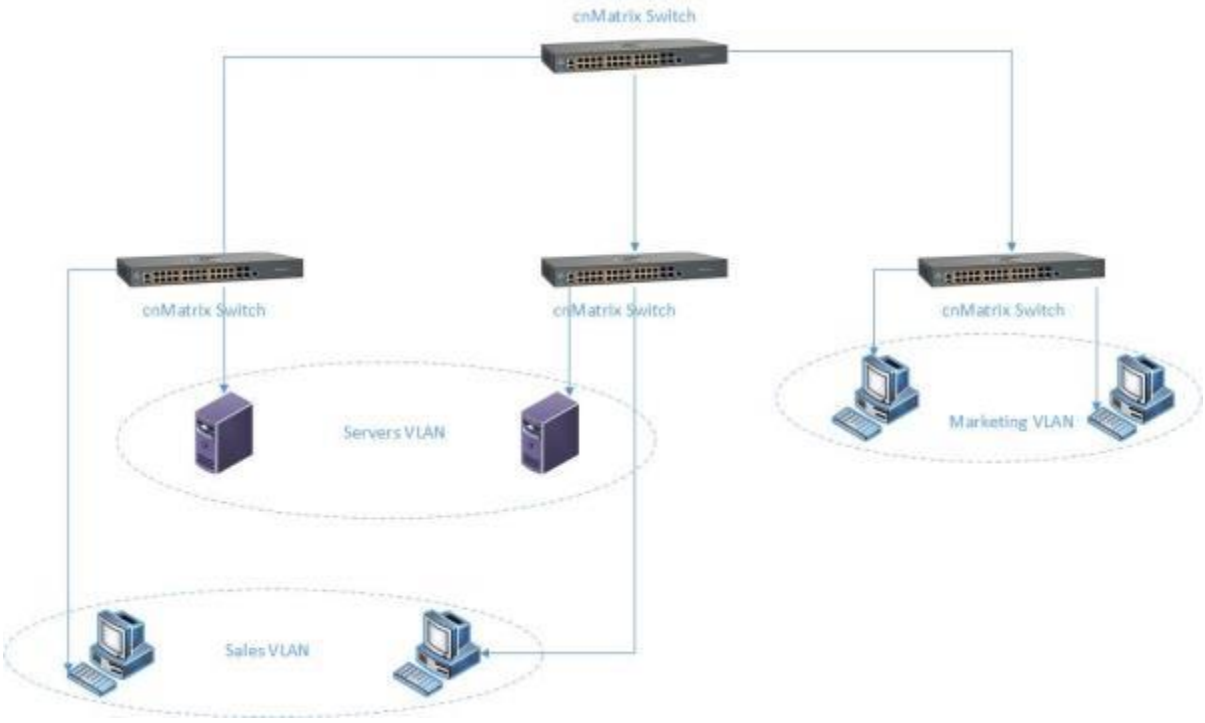
Note

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

Attention

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

Network Diagram



How to Create a VLAN in CLI Interface

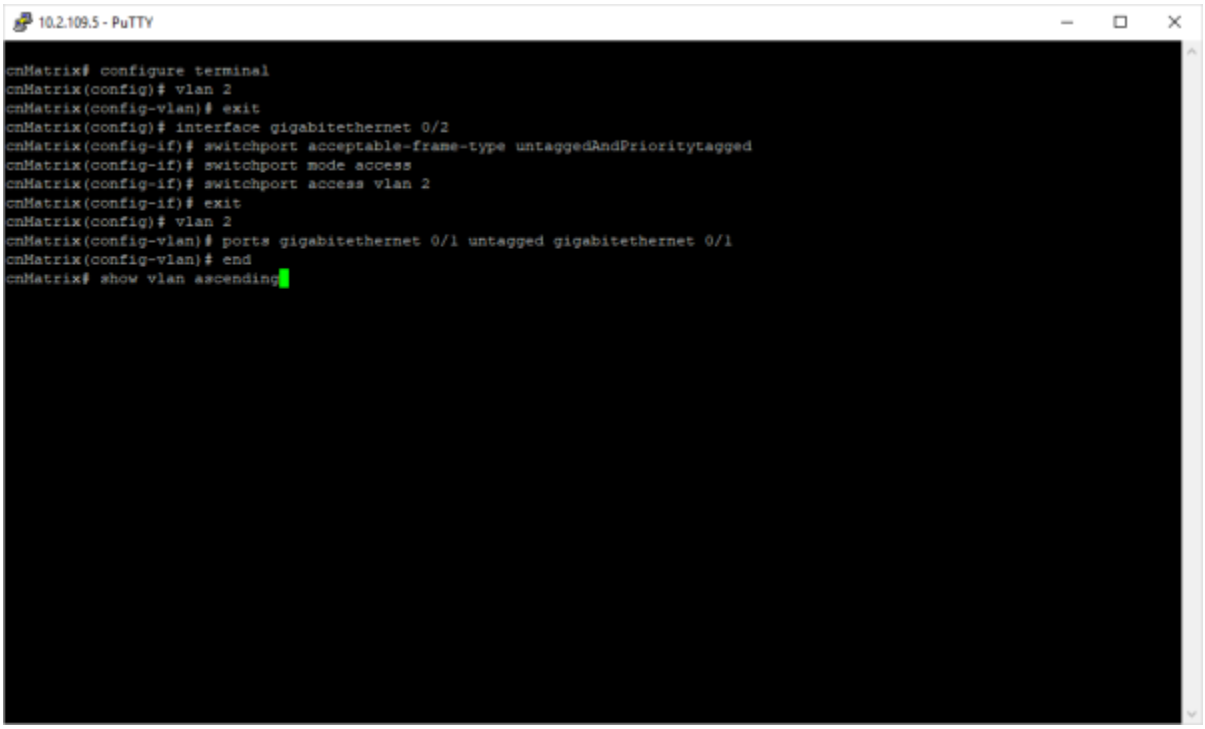
```
10.140.134.12 - PuTTY
cnMatrix(config)# vlan 50
cnMatrix(config-vlan)# ports add gigabitethernet 0/3 untagged gigabitethernet 0/
3
cnMatrix(config-vlan)# end
cnMatrix# show vlan id 50

VLAN Database
-------------
VLAN ID             : 50
Member Ports        : Gi0/3
Untagged Ports      : Gi0/3
PBA Ports           : None
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 Mode                          : Hybrid
 Port-and-Protocol Based Support    : Enabled
 Default Priority                   : 0
 Port Protected Status              : Disabled
 ------------------------------------------------------

cnMatrix#
```

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

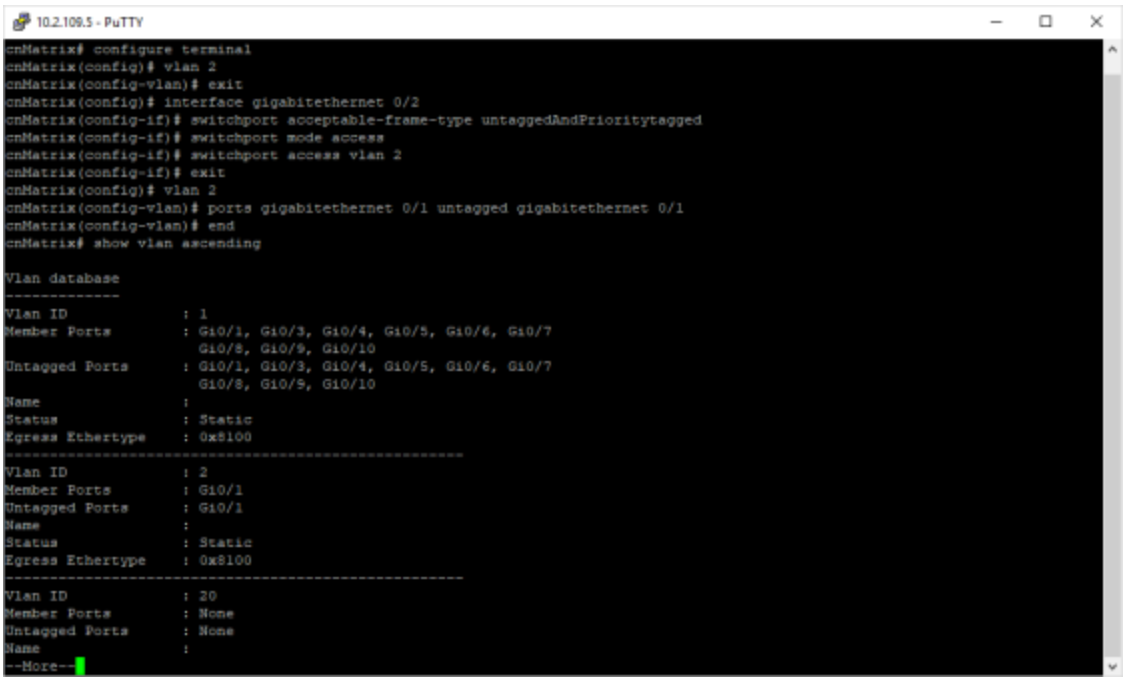
1. Type the **vlan 50** command into the terminal to configure a VLAN. Press the **Enter** key.
2. Type the **ports add gigabitethernet 0/3 untagged gigabitethernet 0/3** command into the terminal to configure port list for a VLAN. Press the **Enter** key.
3. Type the **end** command into the terminal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

For more information, see VLAN Parameters and Commands.

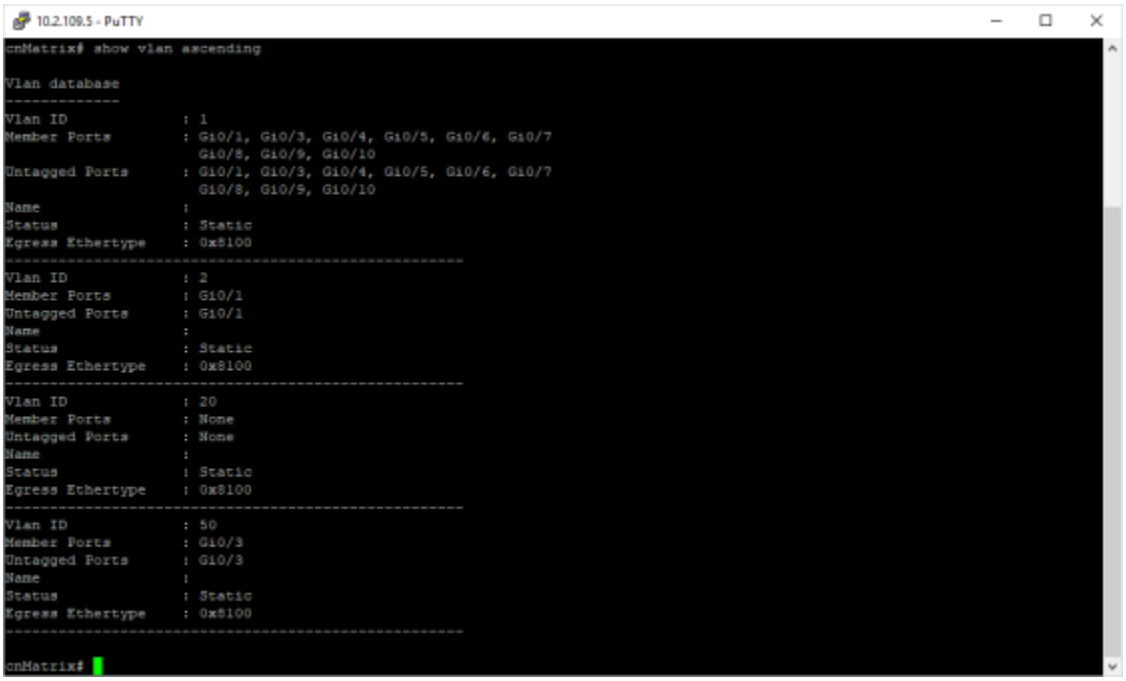
Configuring Port-Based VLAN (Example)



1. Type the **configure 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 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. Press the **Enter** key.
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.

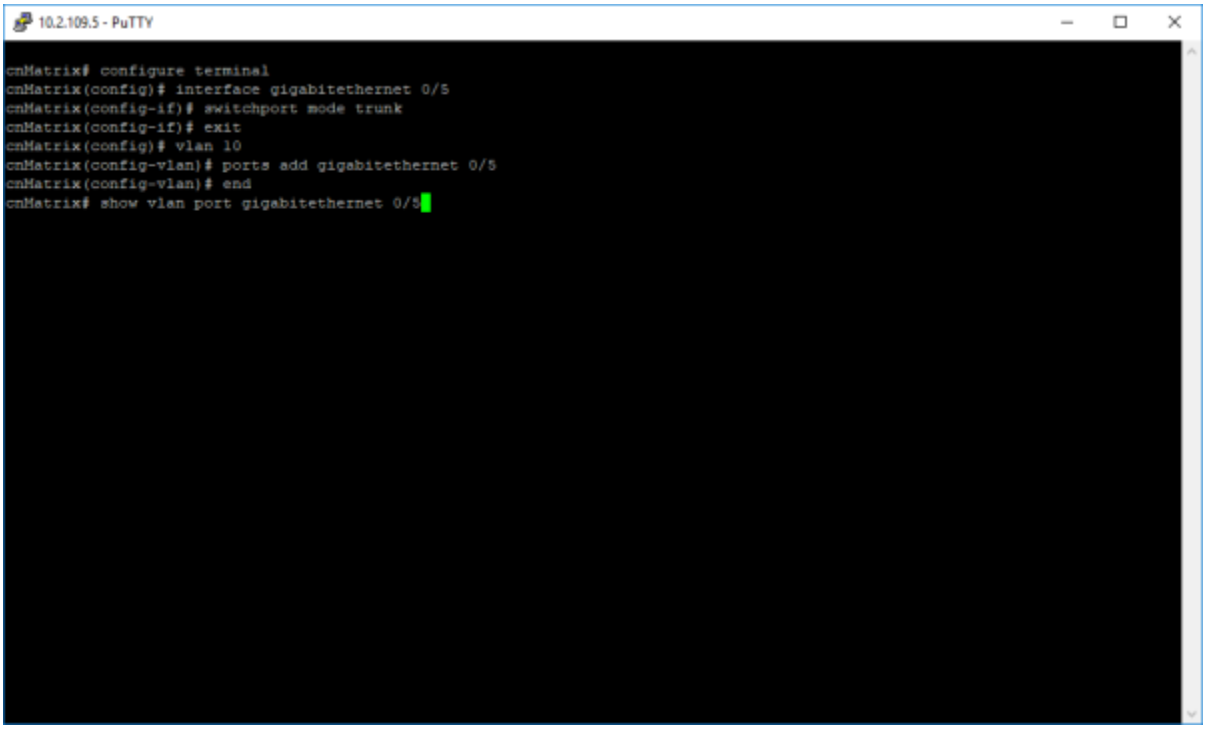


13. Press **Enter** key.

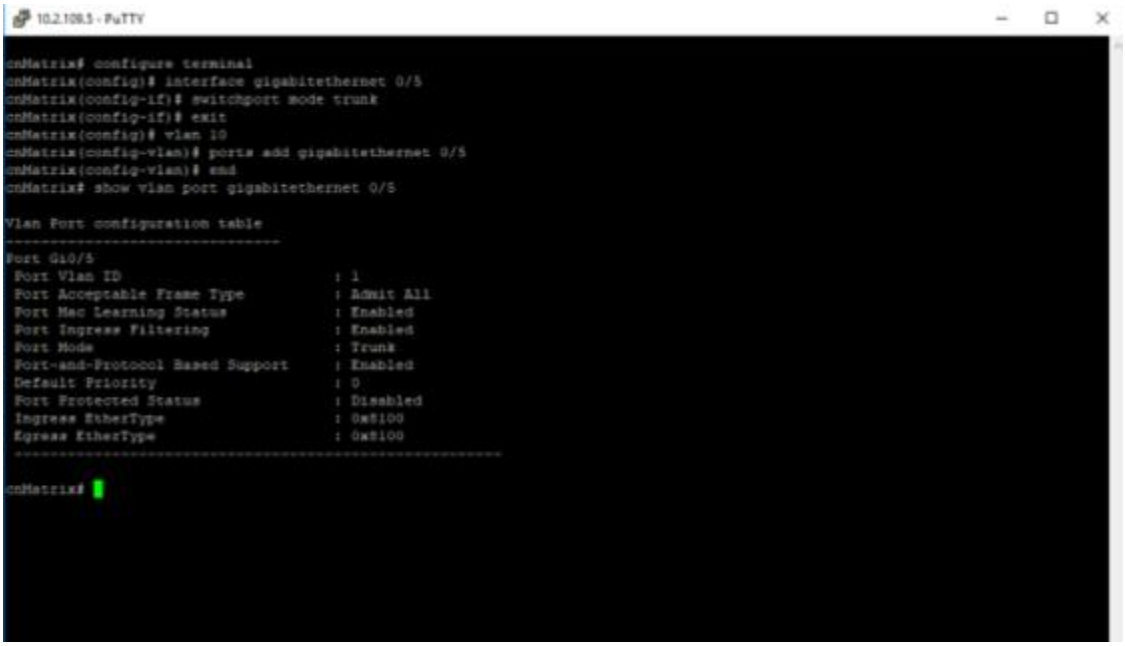


For more information, see VLAN Parameters and Commands.

Configuring 802.1Q Tagging VLAN



1. Type the **configure terminal** command into the terminal. Press **Enter** key.
2. Type the **interface gigabitethernet 0/5** command into the terminal to select the interface to be configured. Press **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** command into the terminal to go back to the global configuration mode. Press **Enter** key.
5. Type the **vlan 10** command into the terminal to enter the configuration vlan mode, and to select the VLAN to be configured. Press **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 **Enter** key.
8. Type the **show vlan port gigabitethernet 0/5** command into the terminal to display information about the configured interface. Press **Enter** key.



For more information, see VLAN Parameters and Commands.

Create a range of VLANs

Starting with cnMatrix 3.0.1 release you can create a group of VLANs using vlan range command.

- Create a VLAN range

EX2052-123460(config)# vlan range 10-20

- Add ports to a VLAN range

EX2052-123460(config-vlan-range)# ports add gigabitethernet 0/3,0/4

- Remove ports from a VLAN range

EX2052-123460(config-vlan-range)# no ports gigabitethernet 0/3,0/4

Troubleshooting VLAN

Useful commands for VLAN 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>]

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 32 PVRST instances can be configured in PVRST mode.
- A maximum of 32 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 that supports legacy STP feature.

Default Values

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

Prerequisites

N/A

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

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

RSTP has three port states:

- Discarding
- Learning
- Forwarding

RSTP ports can have the following roles:

- Alternate
- back-up
- Root
- Designated

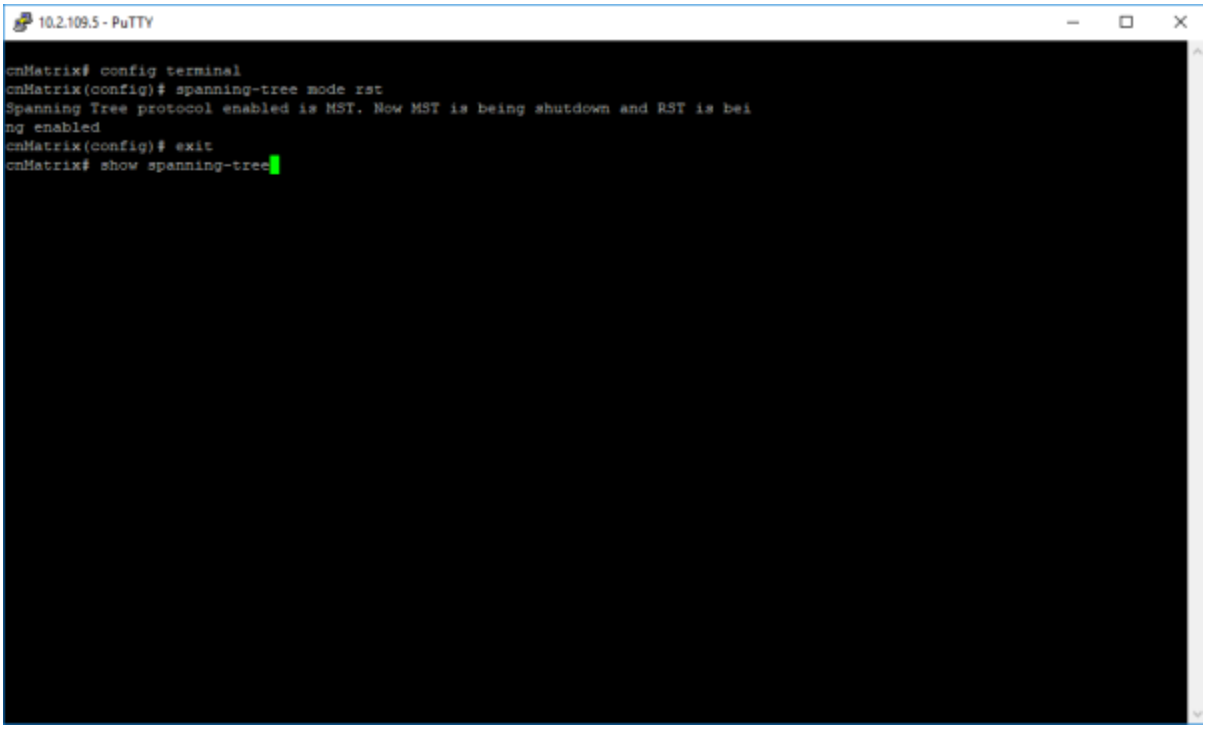
Standards

- 802.1w

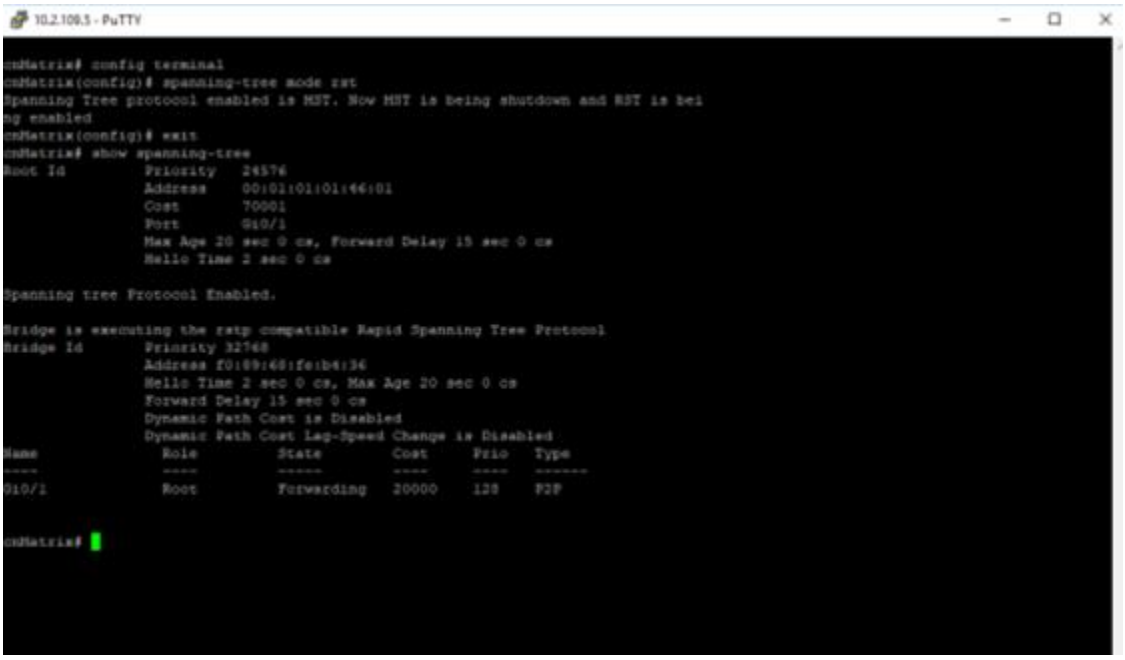
Default Values

- Hello time - 2 seconds.

How to Enable RSTP in CLI Interface

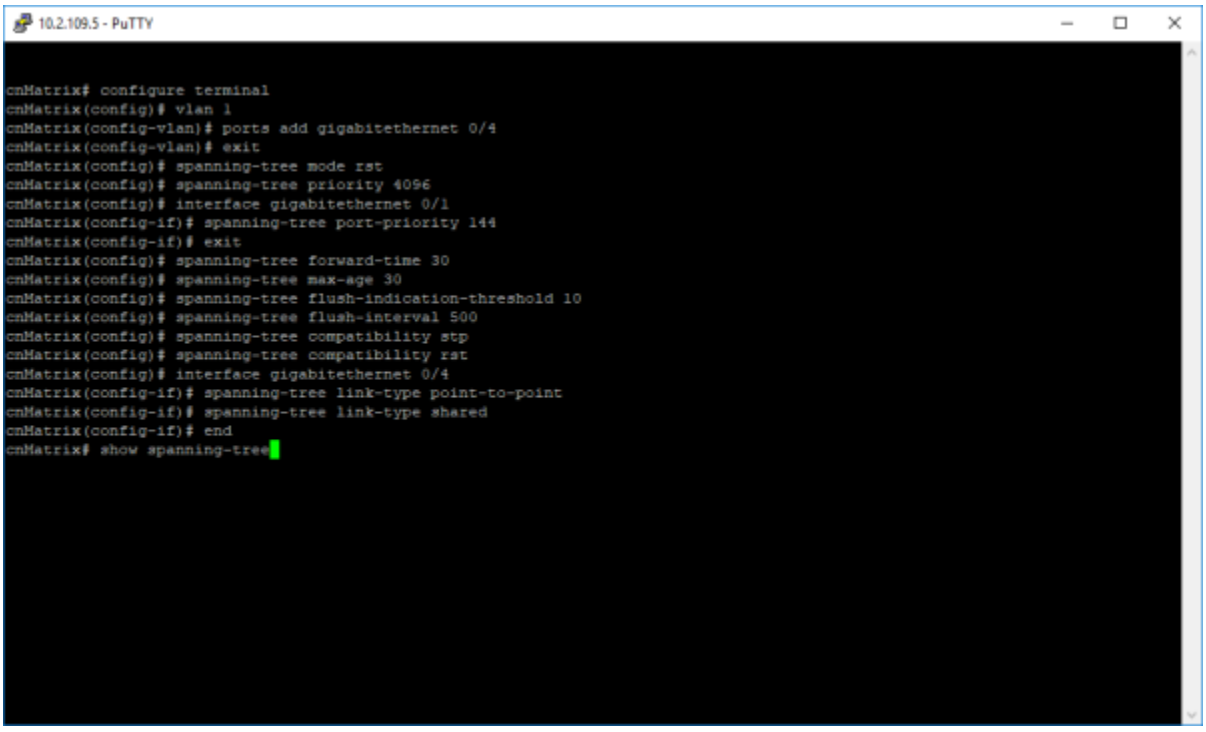


1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree mode rst** command into the terminal to set the spanning-tree operating mode. Press the **Enter** key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode.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



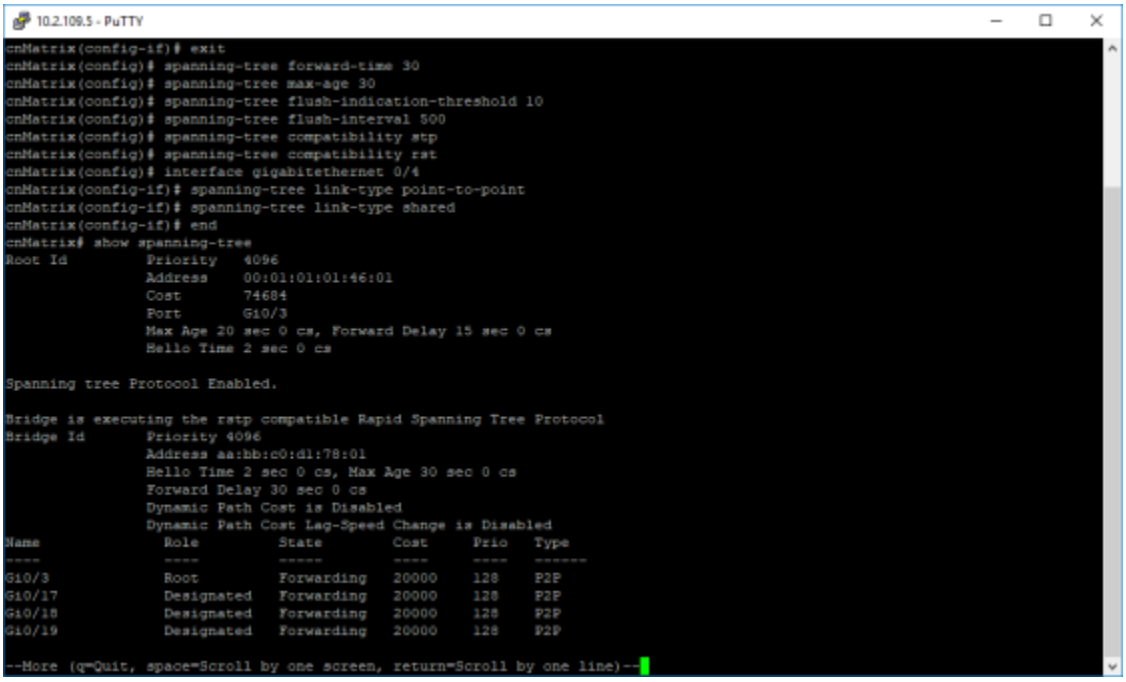
For more information, see RSTP Parameters and Commands.

Configuring RSTP in CLI Interface (Example)

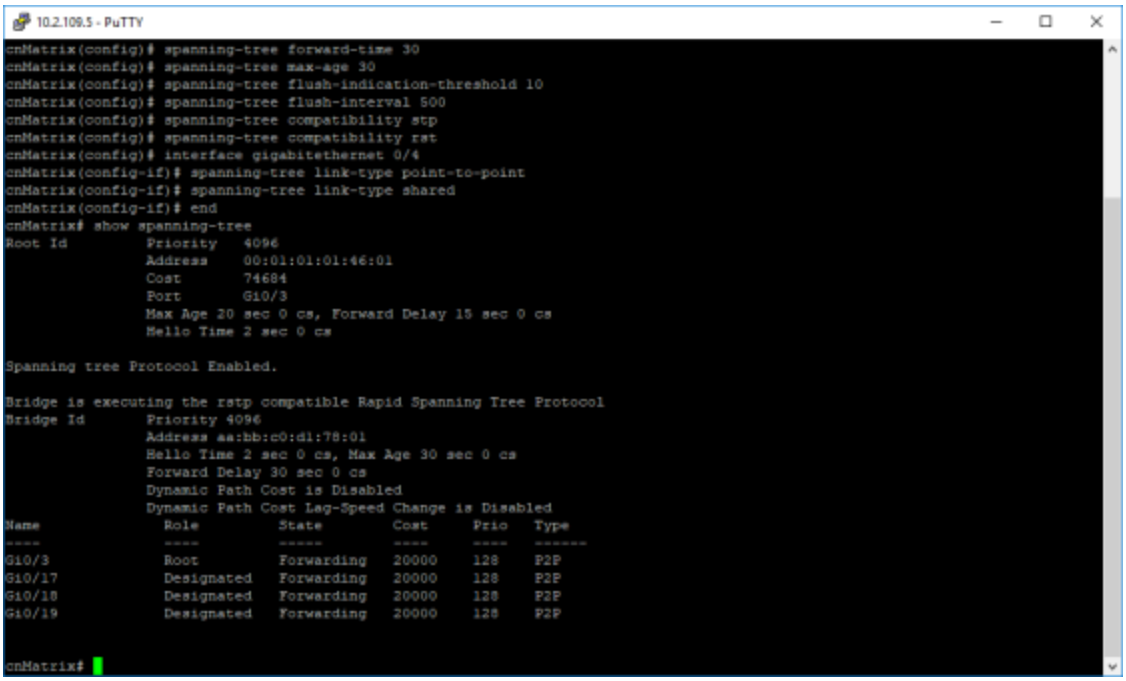


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **vlan 1** command into the terminal to configure a VLAN. Press the **Enter** key.
3. Type the **ports add gigabitethernet 0/4** command into the terminal to configure the port list for the selected VLAN. 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 **Enter** key.



For more information, see RSTP Parameters and Commands.

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 corresponding 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

Managing MSTP

Feature Description

Caution:

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. The Instance ID can be configured from 1 to 31.

Limitations

N/A

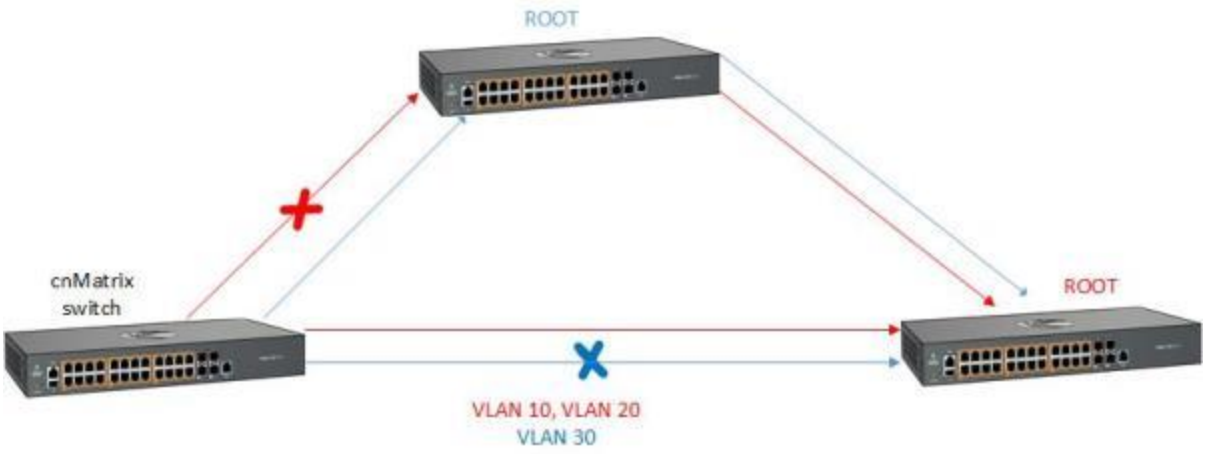
Default Values

- 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.

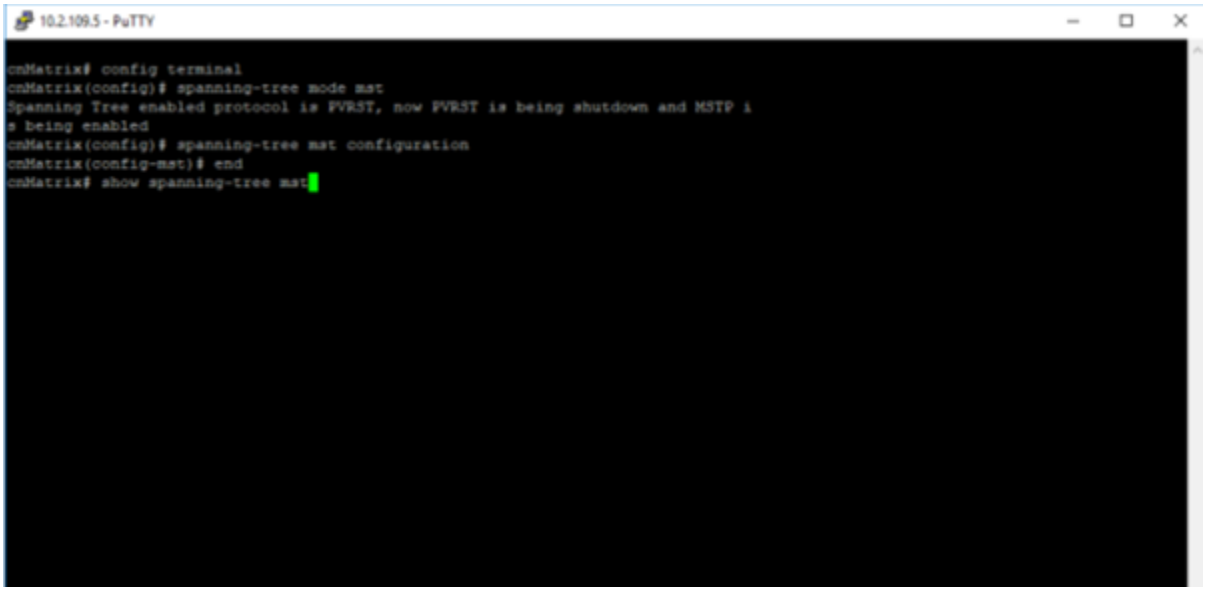
Prerequisites

- N/A

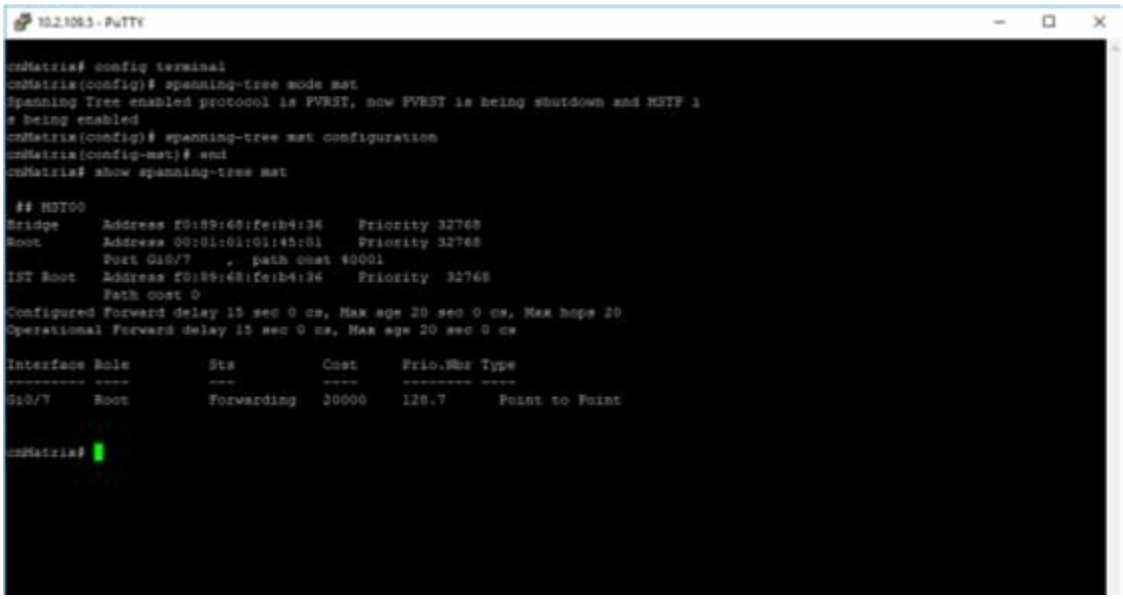
Network Diagram



How to Enable MSTP in CLI Interface

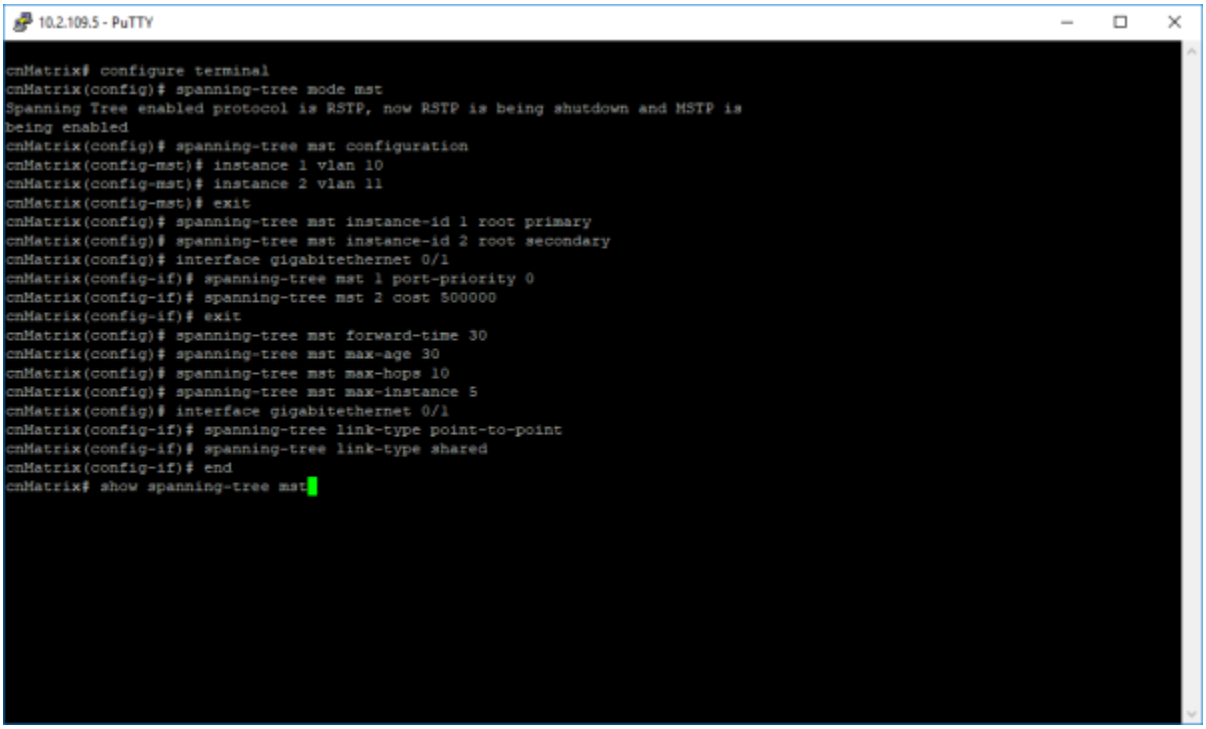


1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree mode mst** command into the terminal to set the spanning-tree operating mode. Press the **Enter** key.
3. Type the **spanning-tree mst configuration** command into the terminal to enter MST 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.



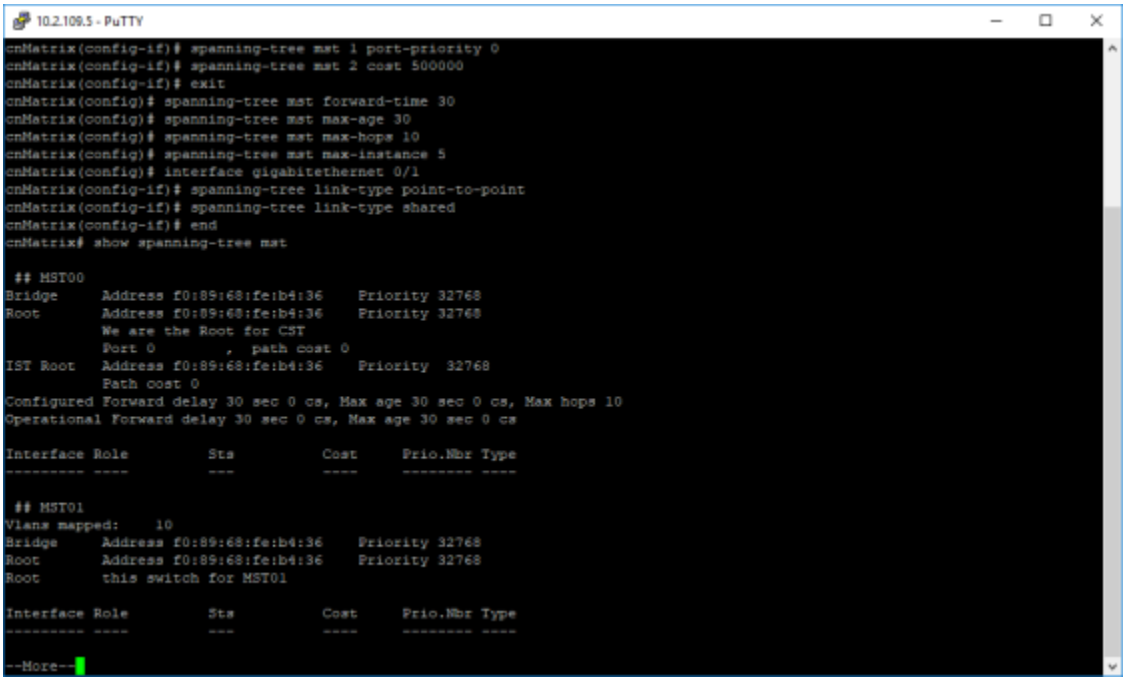
For more information, see MSTP Parameters and Commands.

Configuring MSTP in CLI Interface (Example)

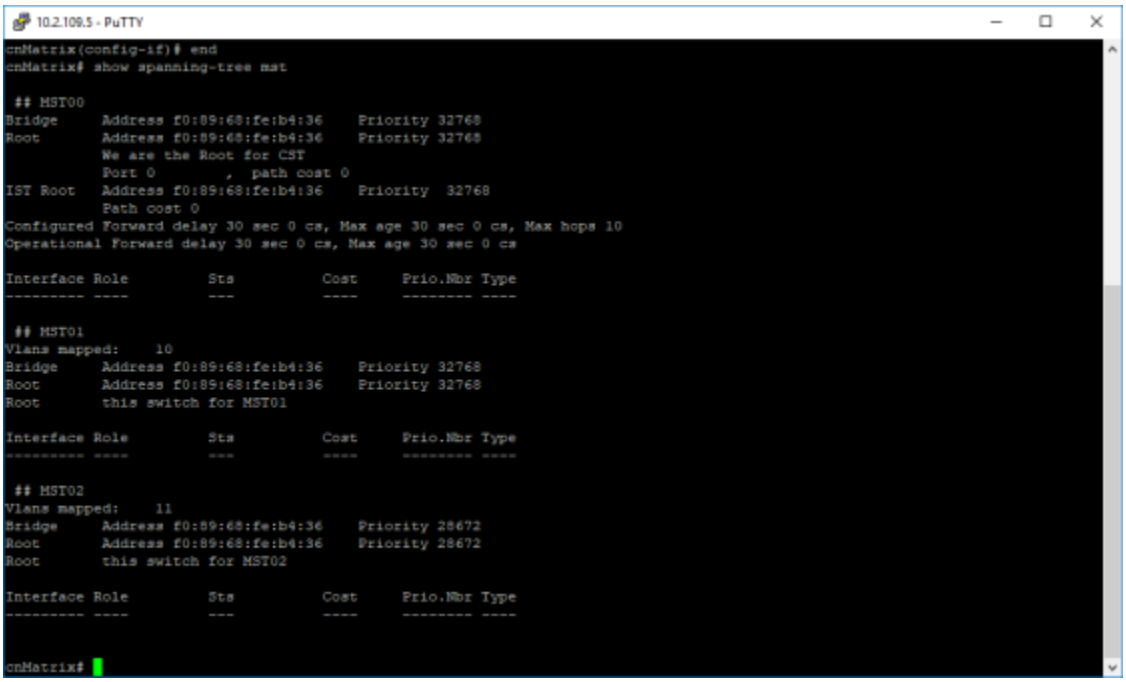


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree mode mst** command into the terminal to enable the MSTP feature. Press the **Enter** key.
3. Type the **spanning-tree mst configuration** command into the terminal to enter the MSTP mode. 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 terminal. Press the **Enter** key.
10. Enter **spanning-tree mst 1 port-priority 0** into the field to configure the 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 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 **Enter** key.



For more information, see MSTP Parameters and Commands.

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

Managing PVRST

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 to provide better control traffic in the network.

Standards

- 802.1w

Scaling Numbers

- Up to 64 PVRST instances.

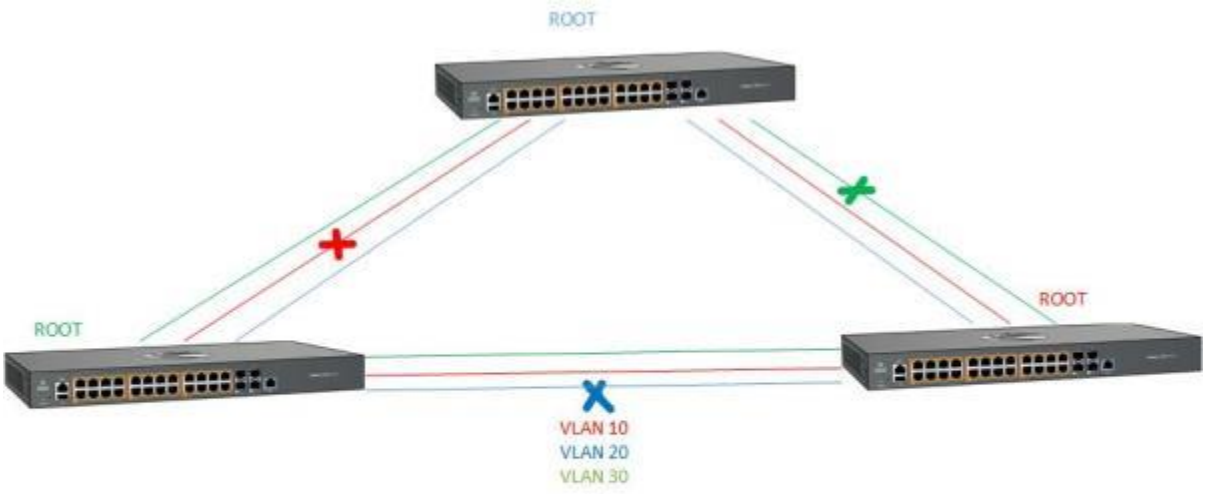
Default Values

- 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.

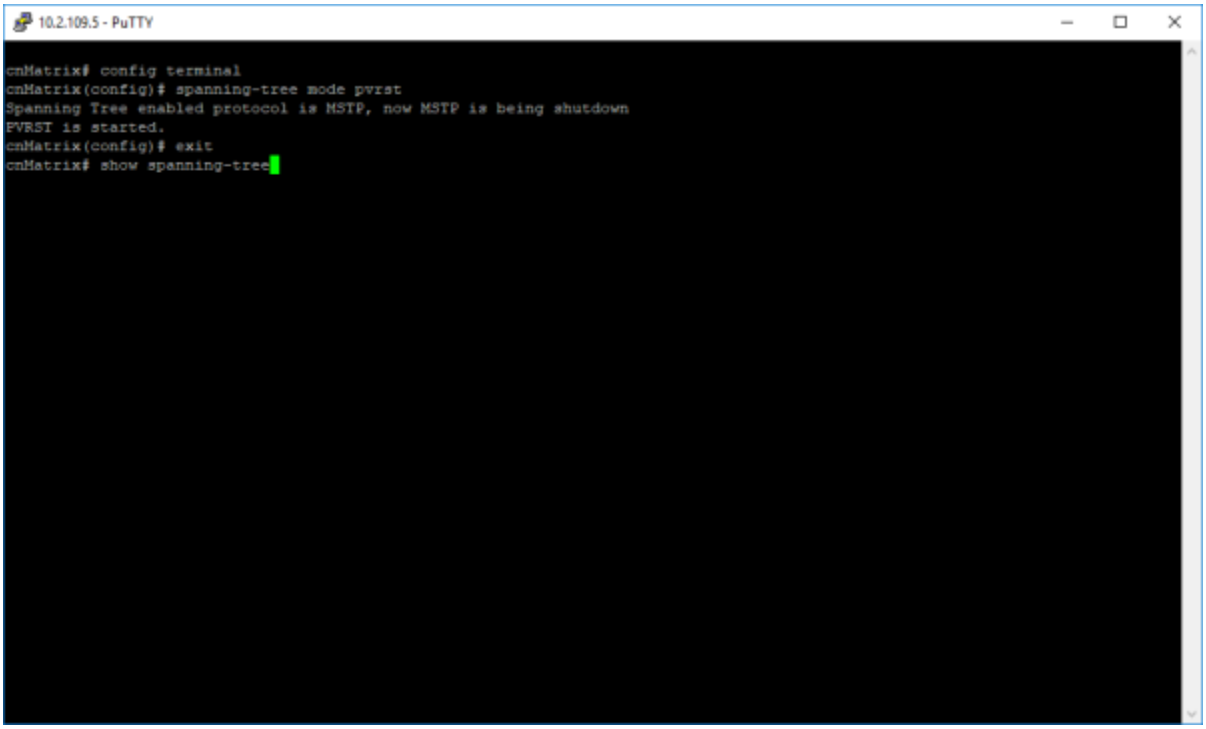
Prerequisites

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

Network Diagram

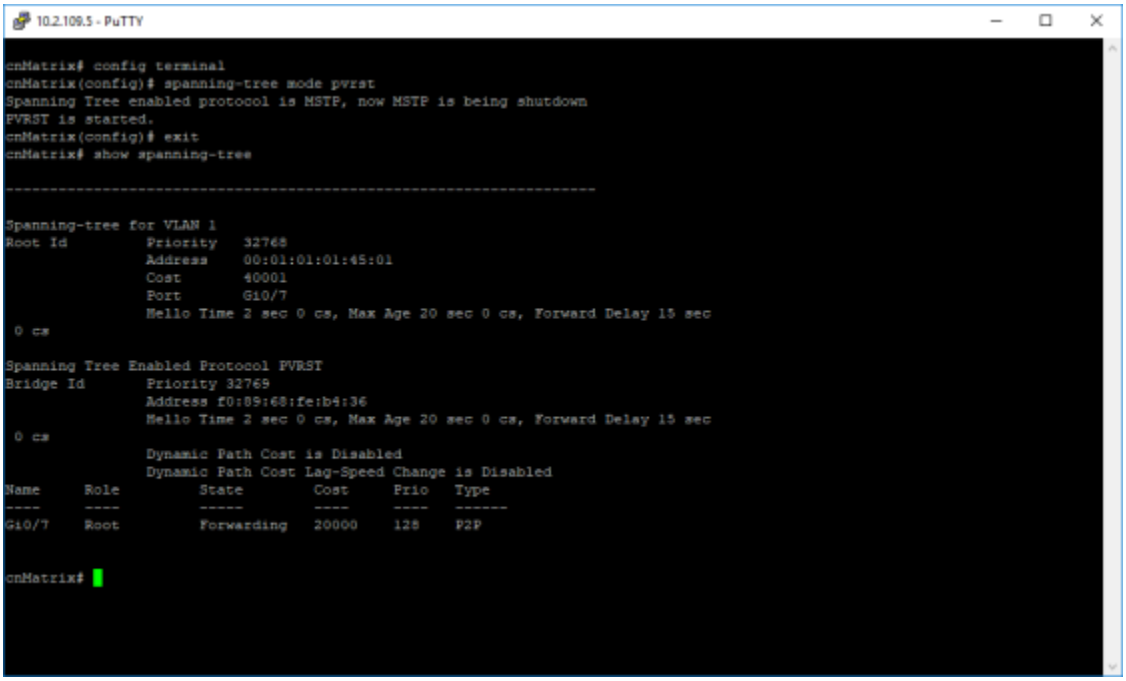


How to Enable PVRST in CLI Interface



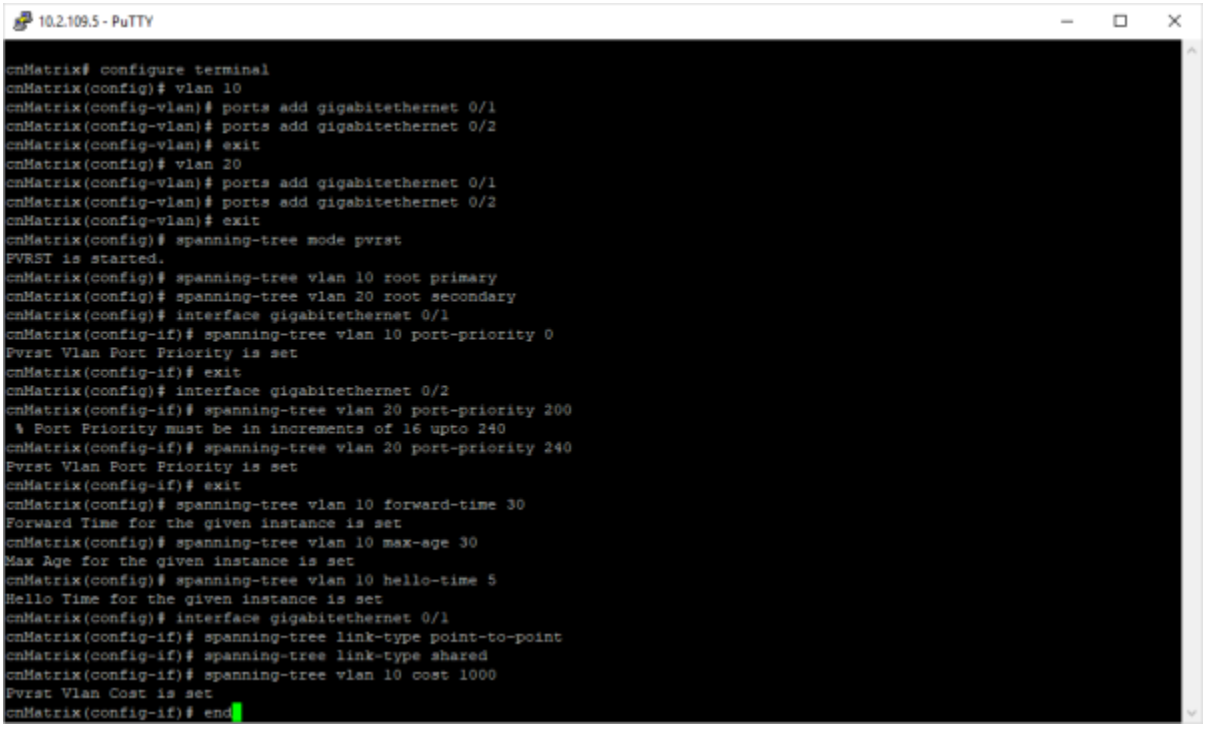
1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree mode pvrst** command into the terminal to set the spanning-tree operating mode. Press the **Enter** key.

3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the **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 PVRST Parameters and Commands.

Configuring PVRST in CLI Interface (Example)



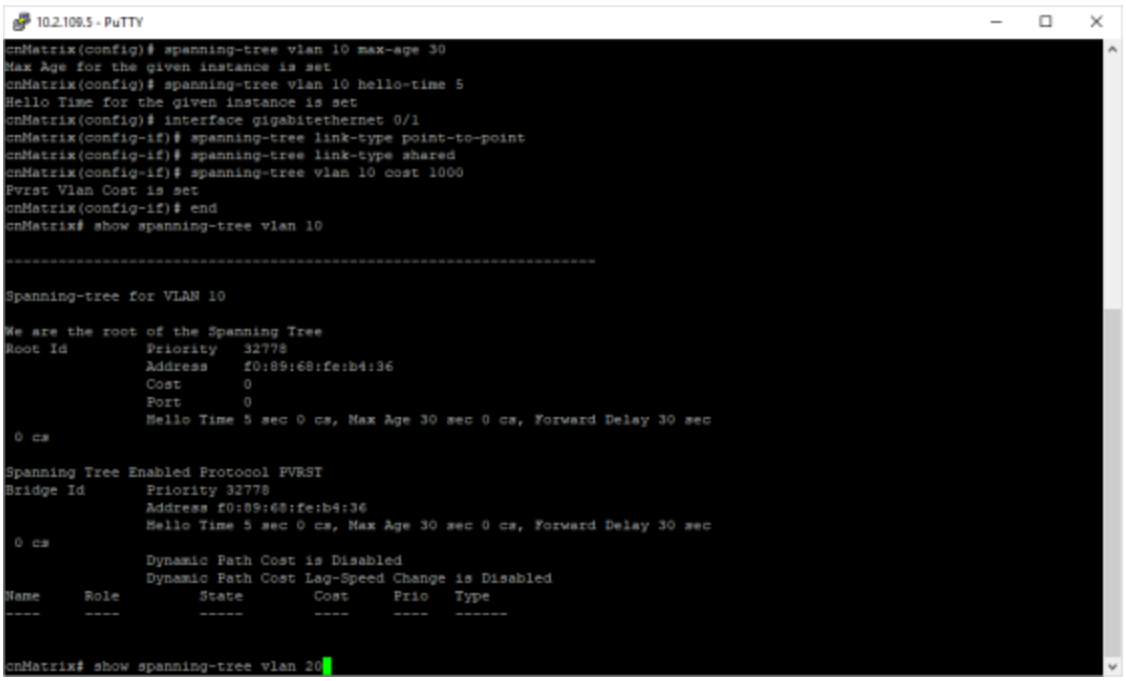
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.

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 **interface gigabitethernet 0/1** command into 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 240** command into the terminal to configure port priority for VLAN 20. Press the **Enter** key.

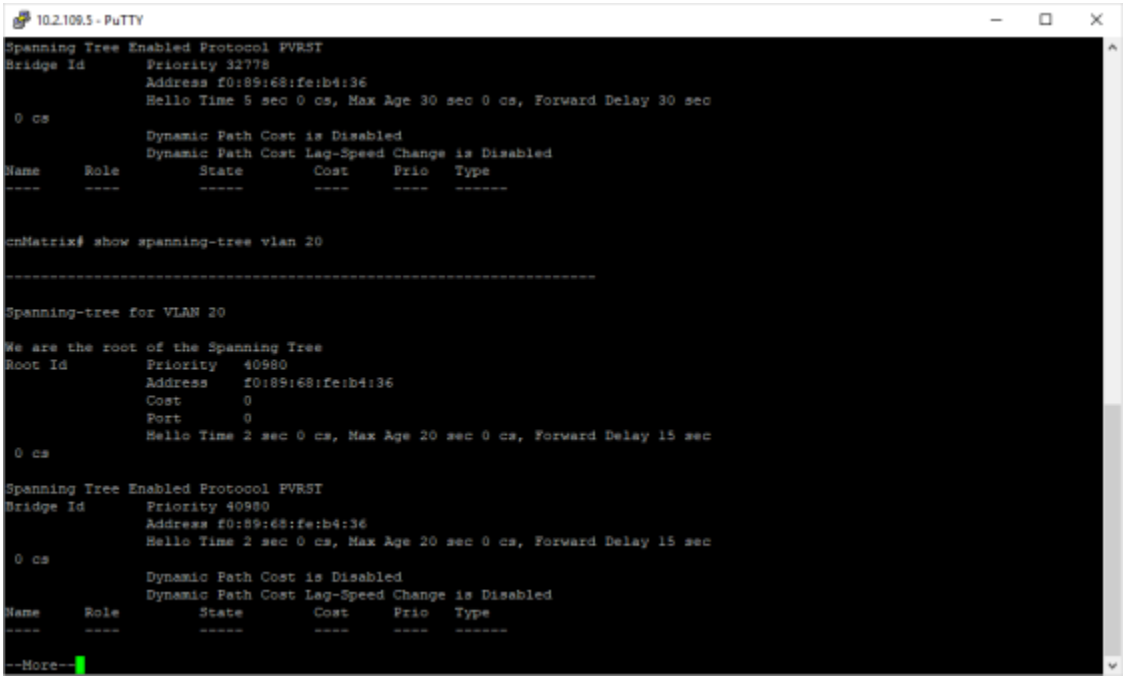
Caution

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

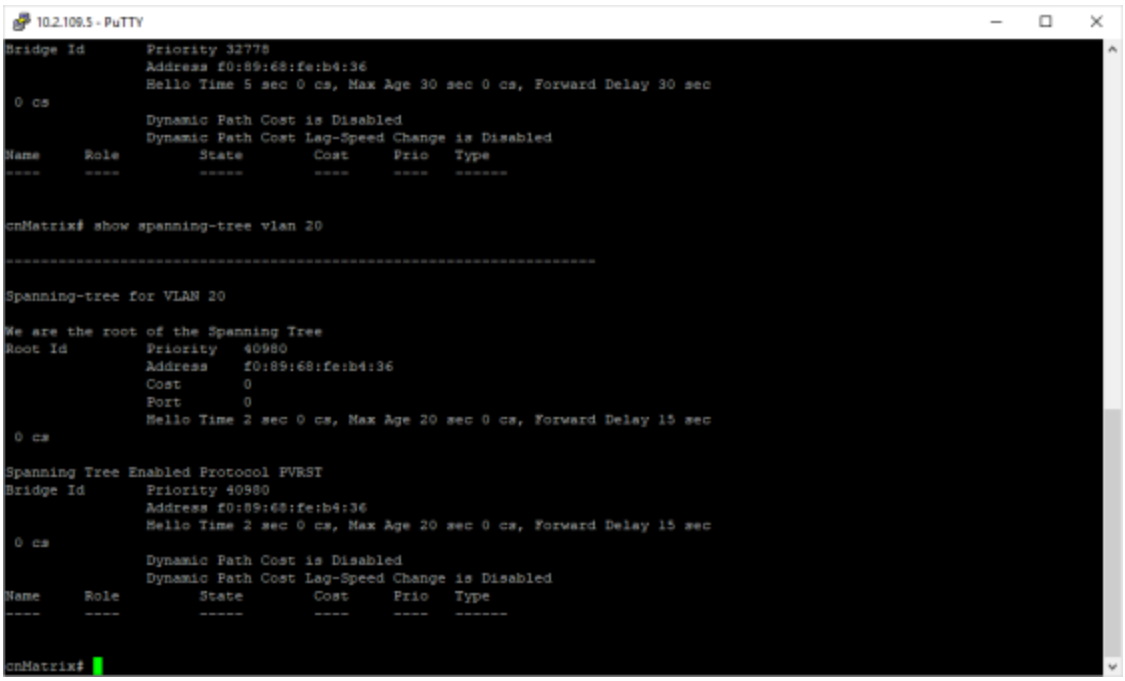
18. Type the **spanning-tree vlan 20 port-priority 240** command into the terminal. Press the **Enter** key.
19. Type the **exit** command into the terminal to go back to the global configuration mode. Press the **Enter** key
20. Type the **spanning-tree vlan 10 forward-time 30** command into the terminal 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. Type the **show spanning-tree vlan 20** command into the terminal to display the PVRST configurations and status. Press the **Enter** key.



30. Press the **Enter** key.



For more information, see PVRST Parameters and Commands.

Troubleshooting PVRST

Useful commands for troubleshooting:

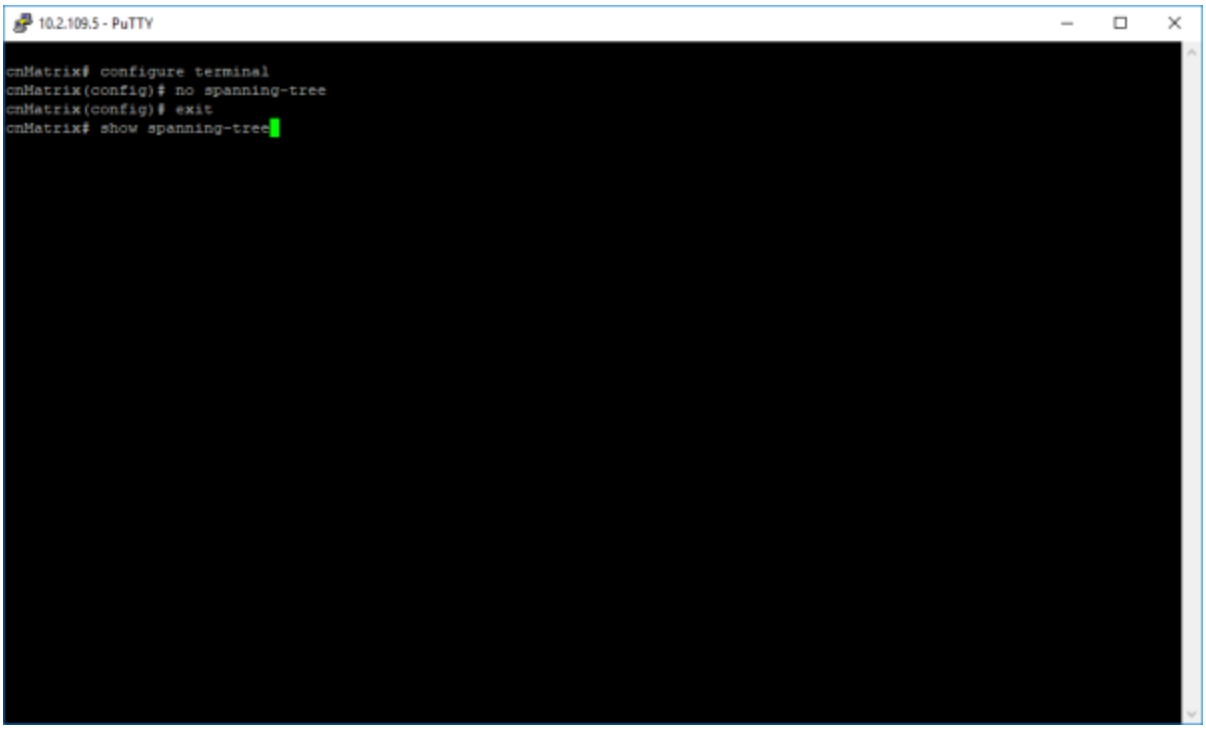
- cnMatrix#show spanning-tree vlan

How to Enable/Disable Spanning Tree

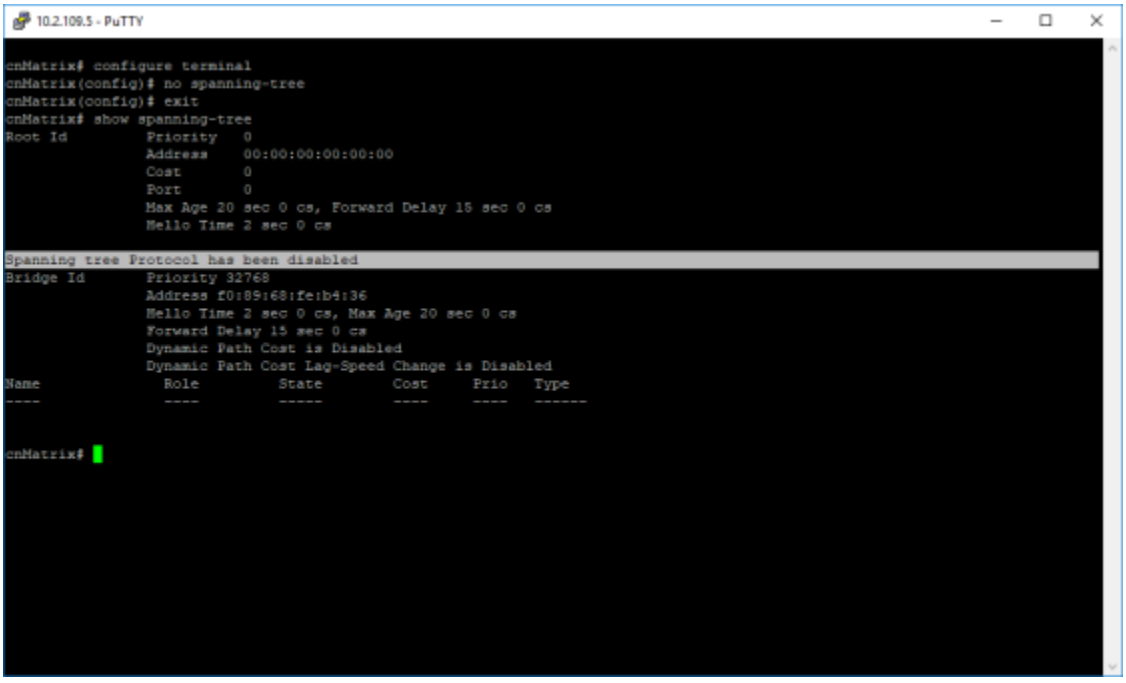
How to Disable Spanning Tree Globally

Note

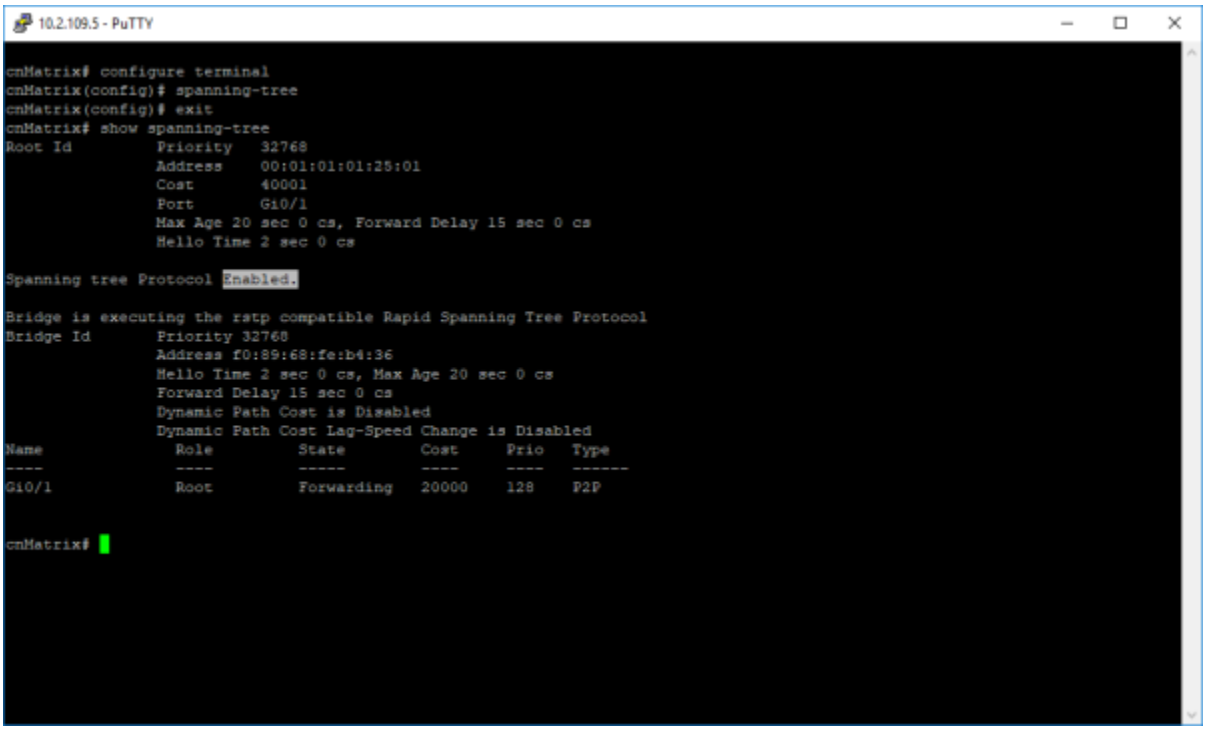
Spanning Tree is enabled by default.



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 information. Press the **Enter** key.



How to Enable Spanning Tree Globally

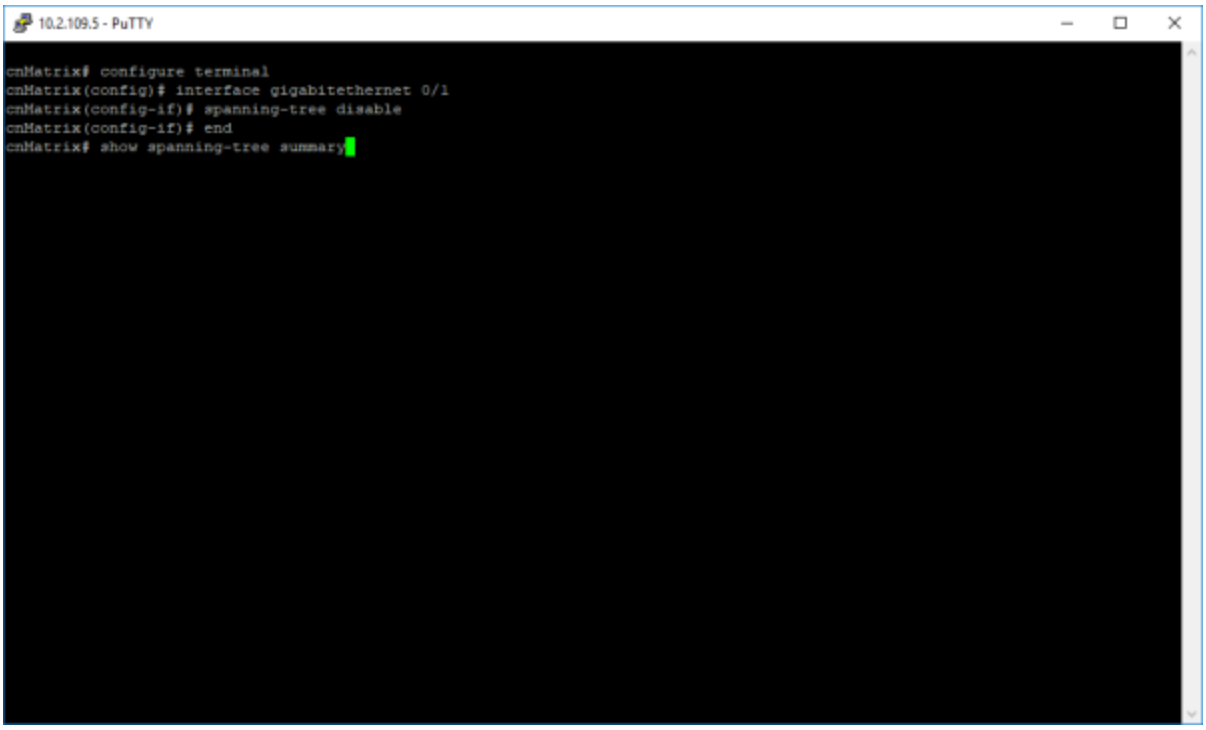


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree** command into the terminal to enable Spanning Tree globally. Press the **Enter** key.
3. Type the **exit** command into the terminal to go back to the Privileged EXEC mode. Press the **Enter**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

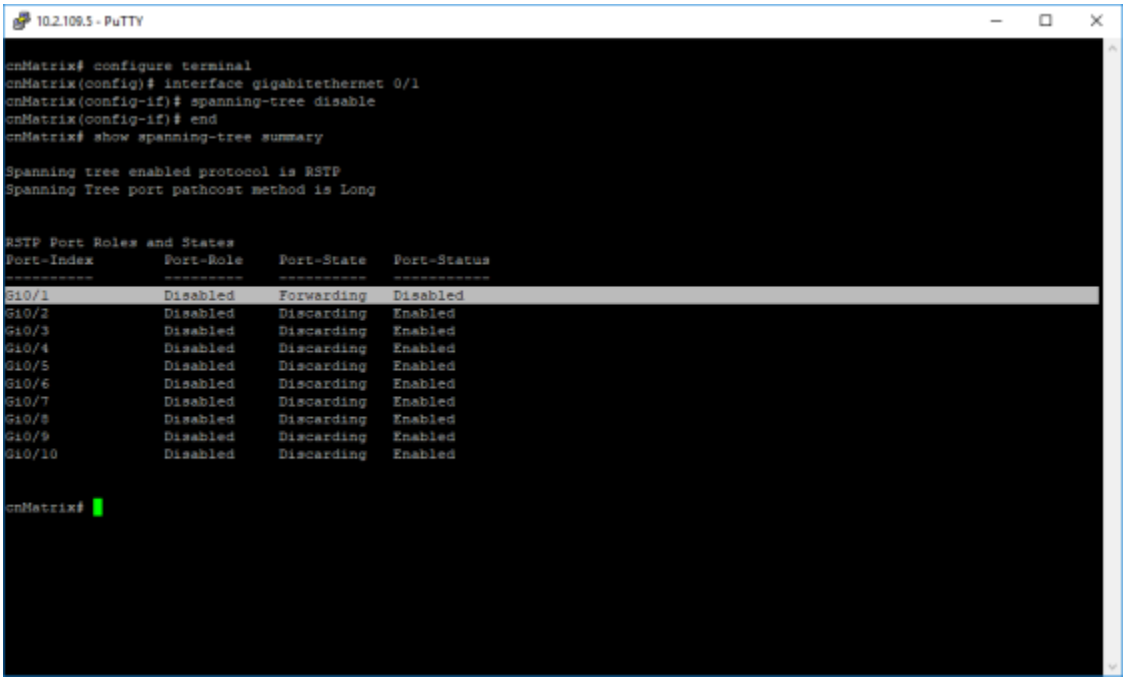
How to Disable Spanning Tree per Interface

Note

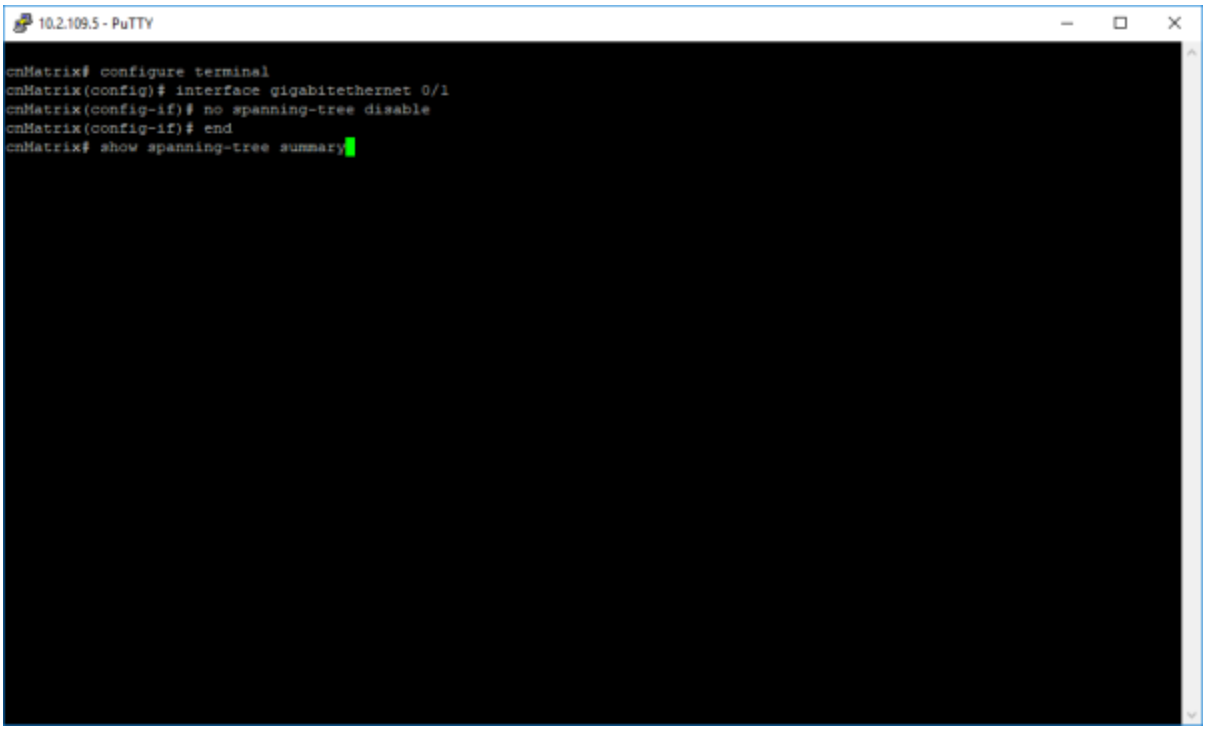
Spanning Tree is enabled by default per interface.



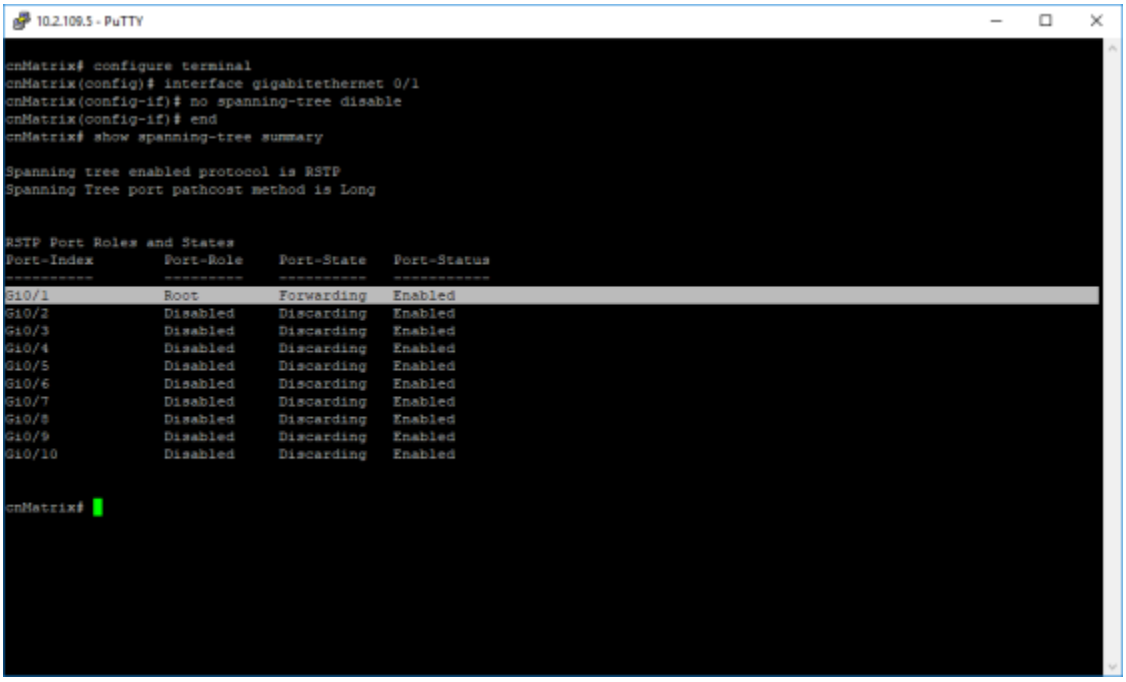
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/1** command into the terminal. Press the **Enter** key.
3. Type the **spanning-tree disable** command into the terminal. Press the **Enter** key.
4. Type the **end** command 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.



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

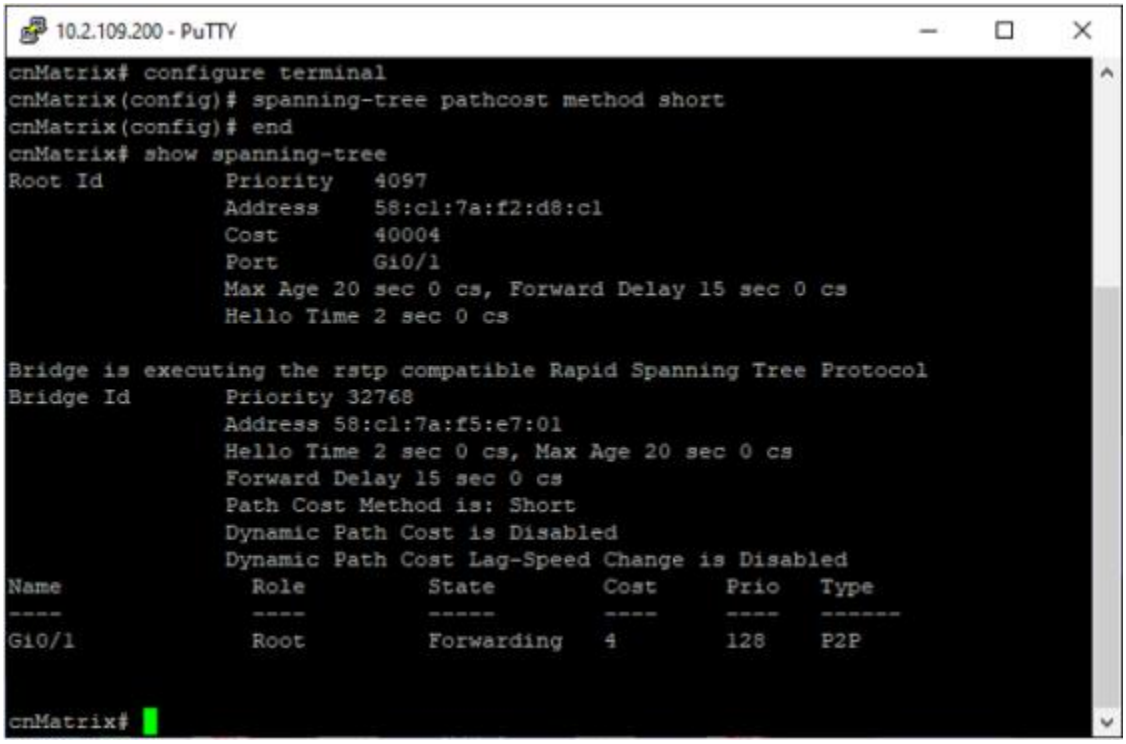
Changing the STP path cost method

The switch allows the user to select between the IEEE 802.1D-1998 (short) and the IEEE802.1T (long) default STP path cost values. This is a per-switch (global) STP configuration and can be set in each STP operating mode (RSTP, PVRST, and MSTP). The default method is **long**.

Path cost values will be immediately modified on the operational ports, and the STP trees will be recalculated accordingly. Ports on which the cost is set manually will not be affected by this global setting.

The command is available for all STP modes.

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **spanning-tree path cost method short** command into the terminal. Press the **Enter** key.
3. To verify the new configuration, type the **show spanning-tree** command into the terminal. Press the **Enter** key.



LLDP

Managing LLDP

Feature Overview

The LLDP feature enables you to discover network devices that support the LLDP protocol. 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 can be learned.

Limitations

- LLDP-MED is not supported in this release.

Default Values

- The default transmission interval: 30 seconds.
- The default value for hold time-multiplier: 4.
- The default value for reinitialization delay time: 2.
- Transmission/reception of LLDPU is 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.

Enhancements

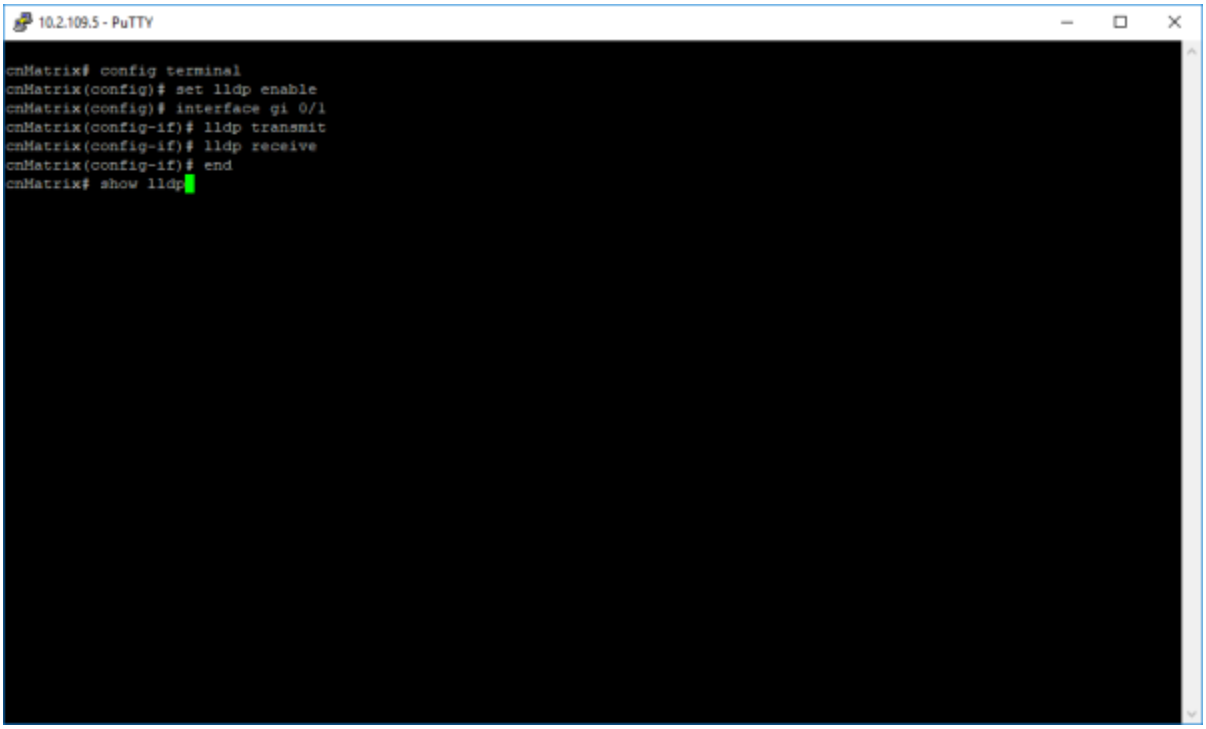
- Starting with Release 4.0, standard LLDP data supports an automated mechanism to **reset** non-responding remote (connected) devices:
    - Remote devices are **reset** by toggling the PoE power status on the device port (power inline disable or power inline enable). The reset ability does not apply to non-PoE switches.
    - Remote devices are considered non-responsive after they are initially learned and the TTL (advertised mandatory Time to Live TLV) expires. TTL expiration (and the associated reset action) does NOT occur for link-down and forced remote device deletion (remote device advertising a TTL = 0) events.
    - A new CLI command is defined to enable or disable the support on a per-port basis:

      (config-if)# **[no] lldp expiration-reset**

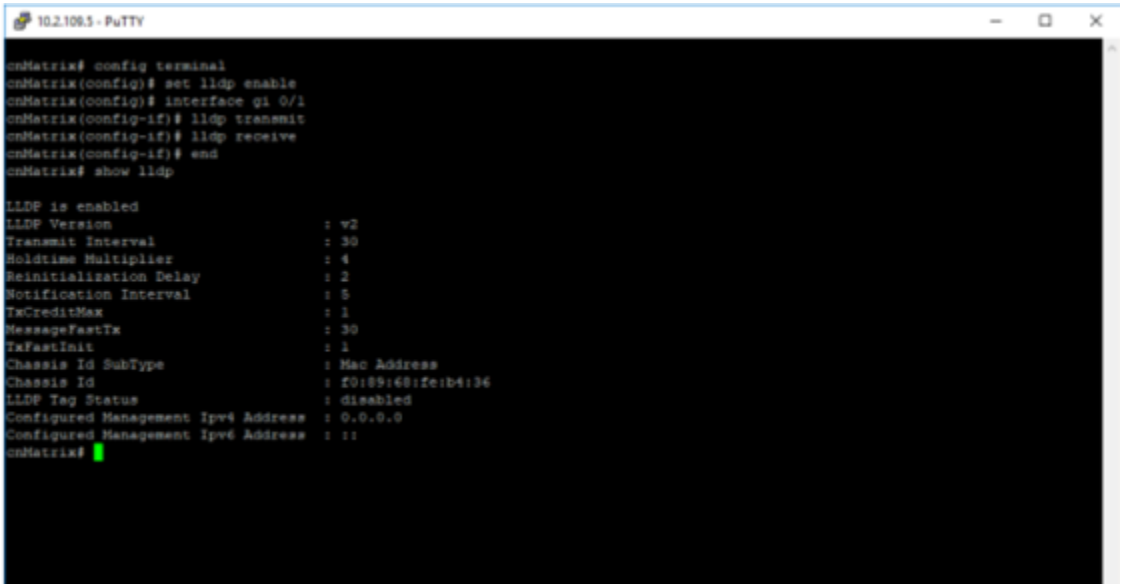
      # **show lldp interface** CLI command displays the current setting.

    - A new LLDP port setting that accessible via the Web interface is available:
        - **Layer 2 Management** > **LLDP** > **Interface Settings**.
    - The user only needs to enable the support on the appropriate ports (support is disabled by default).
    - The user does not need to establish expiration or reset intervals per-device. The LLDP standard TTL value serves this purpose. This value is already configured to an appropriate value on the remote device.
    - Remote device expirations are already tracked on a per-port basis (Total Entries Aged). A reset counter is defined and reported using the same mechanism used to display current LLDP local port settings (show lldp interface CLI command).

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 terminal. Press the **Enter** key.



Note

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

For more information, see LLDP Parameters and Commands.

Managing LLDP-MED (Starting with version 2.1)

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 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

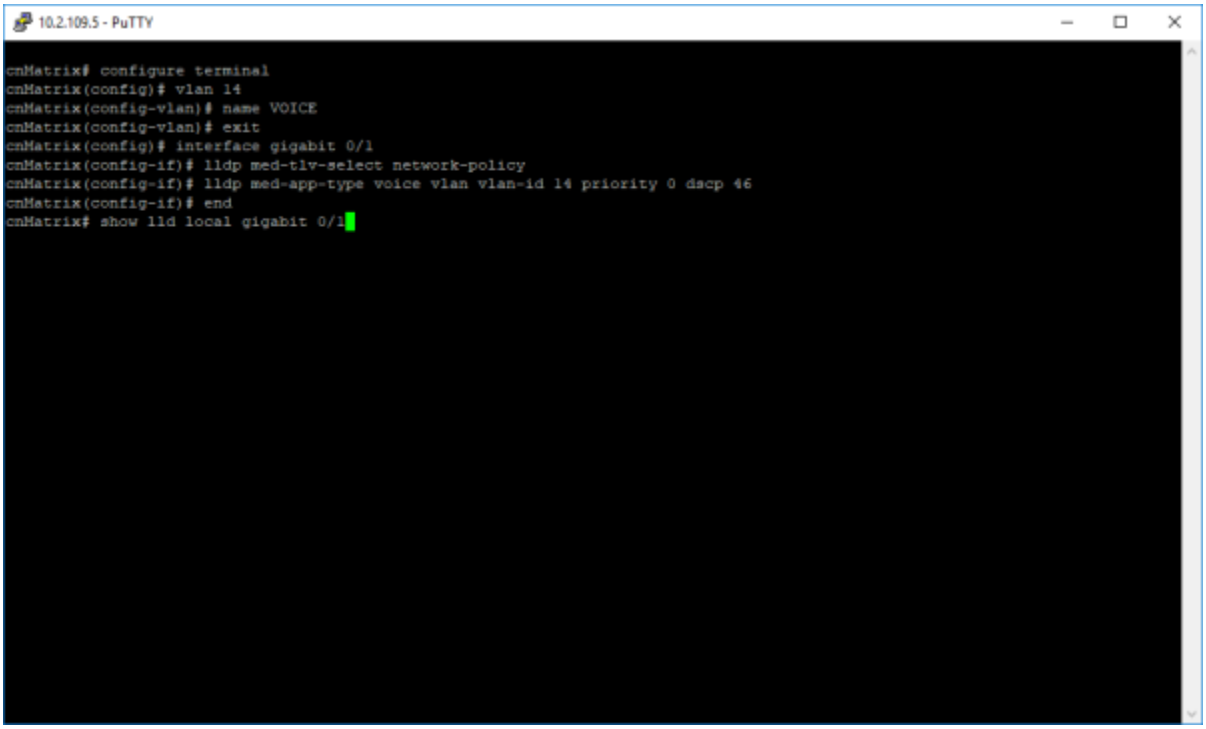
- By default, all ports send only MED Capability TLV.

Prerequisites

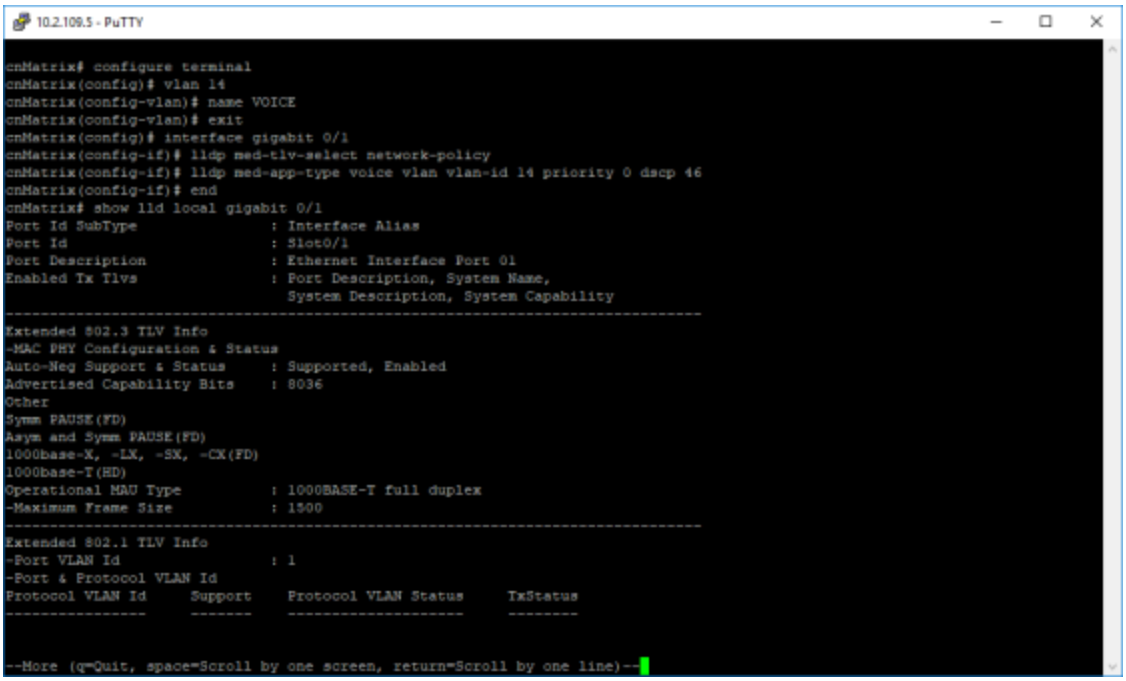
- To send and receive LLDP-MED TLVs, the TX/RX of LLDPDUs must be enabled on the port.

Network Diagram

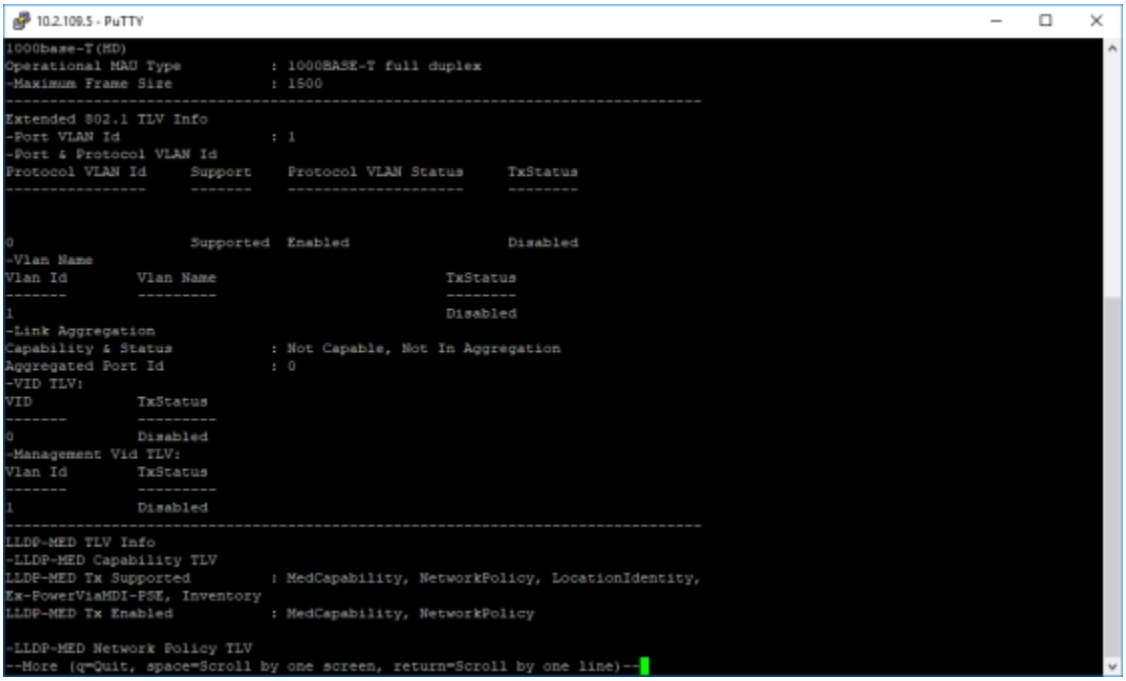
How to Configure Network Policy (Starting with version 2.1)



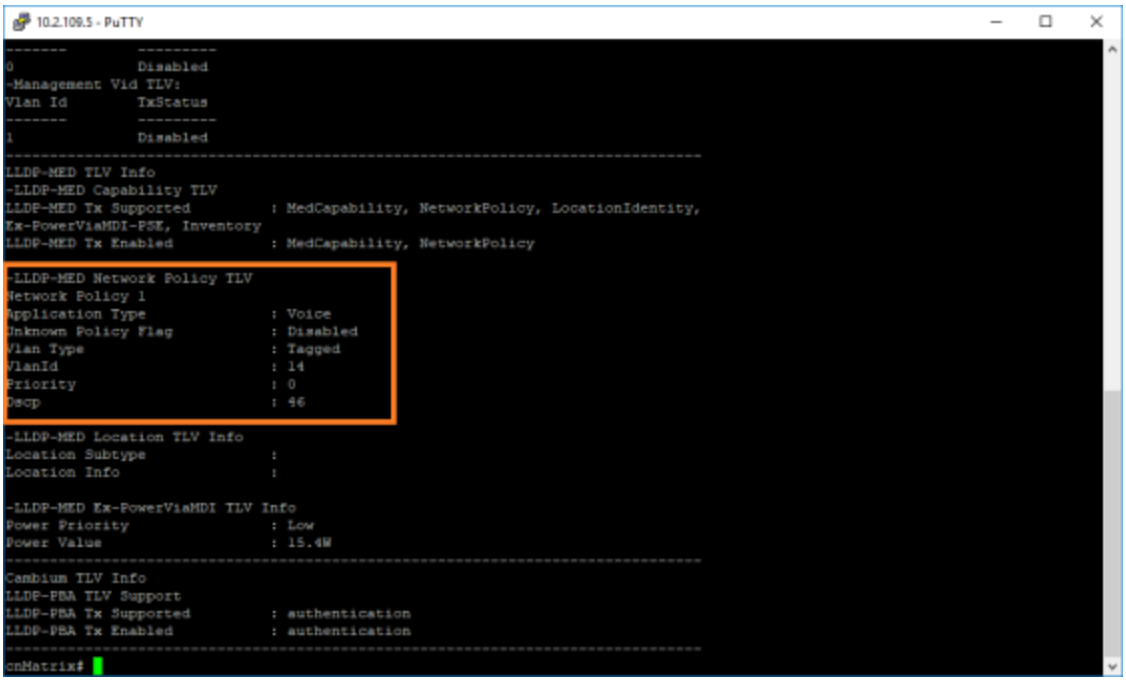
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **vlan 14** command into the terminal to configure a VLAN. Press the **Enter** key.
3. Type the **name VOICE** command into the terminal to configure a name for the VLAN. Press the **Enter** key.
4. Type 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 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 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 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 **Enter** key.

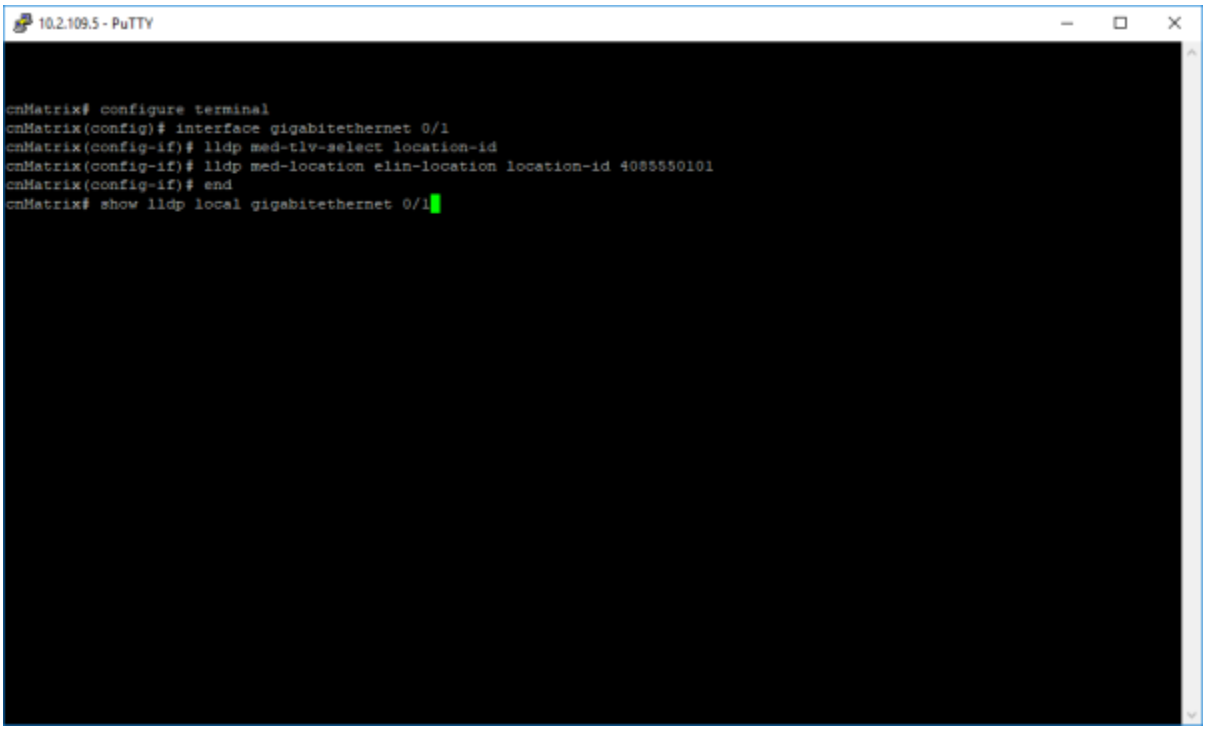


11. Press the **Enter** key.



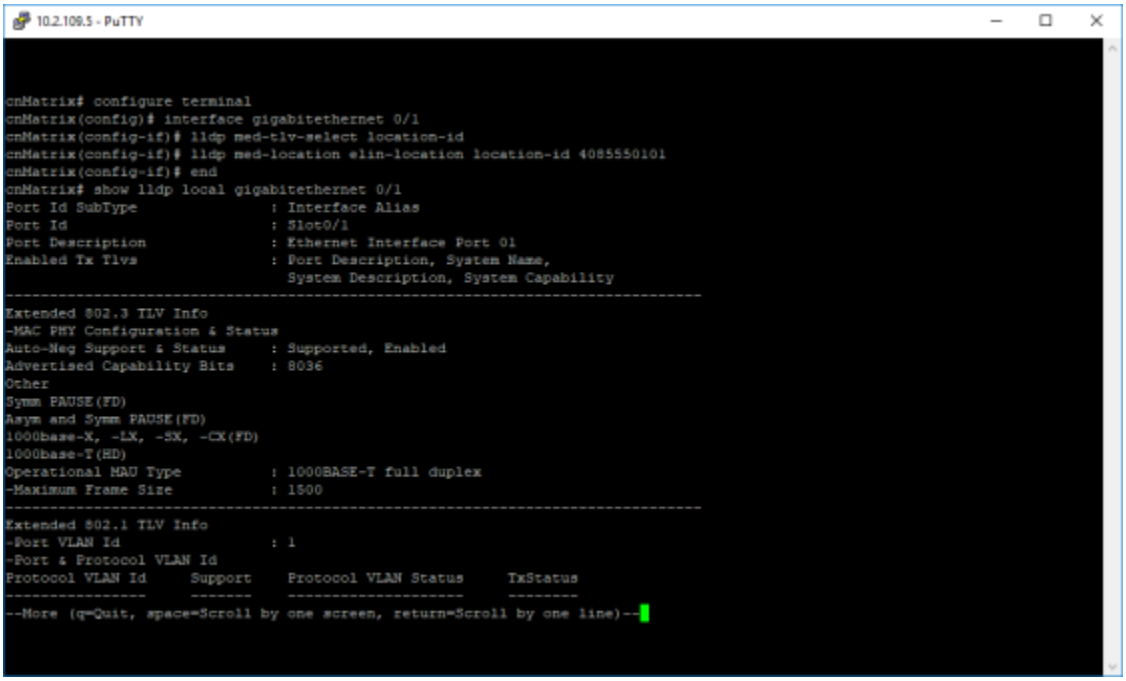
For more information, see LLDP-MED Parameters and Commands.

How to Enable Location ID (Starting with version 2.1)

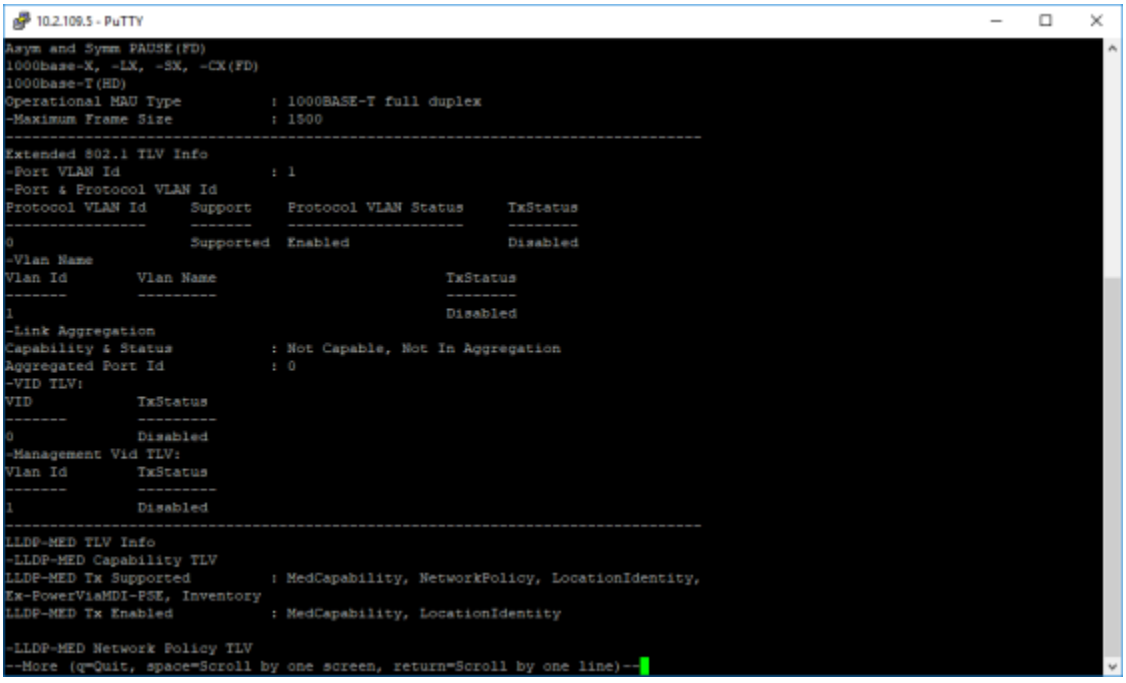


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the **Enter** key.
3. Type the **lldp med-tlv-select location-id** command into the terminal to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

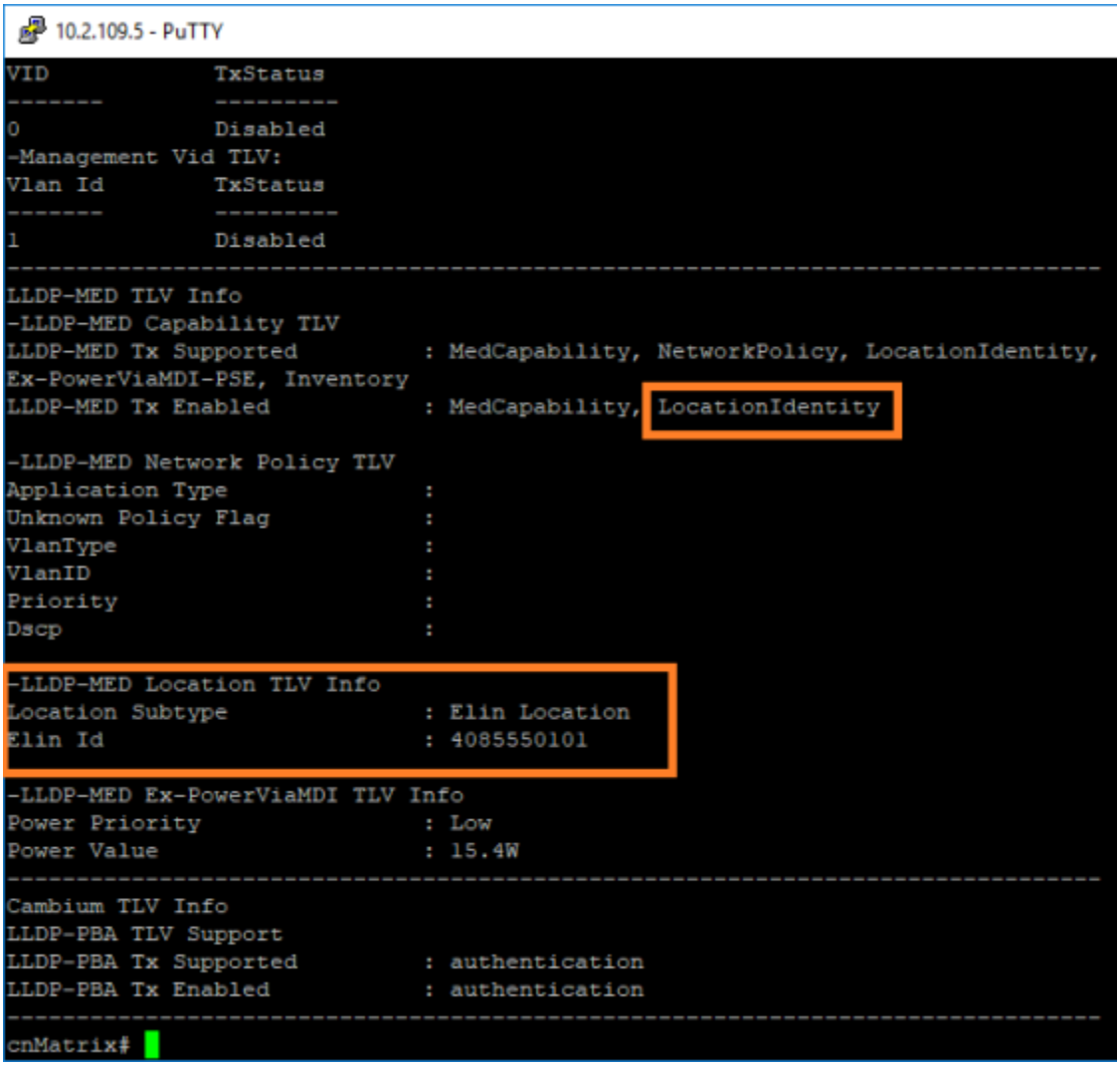
4. Type the **lldp med-location elin-location location-id 4085550101** command into the terminal to configure the Emergency Location Information Number (ELIN) location subtype information advertised by the endpoint. Press the **Enter** key.
5. Type the **end** command into the terminal to go back to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

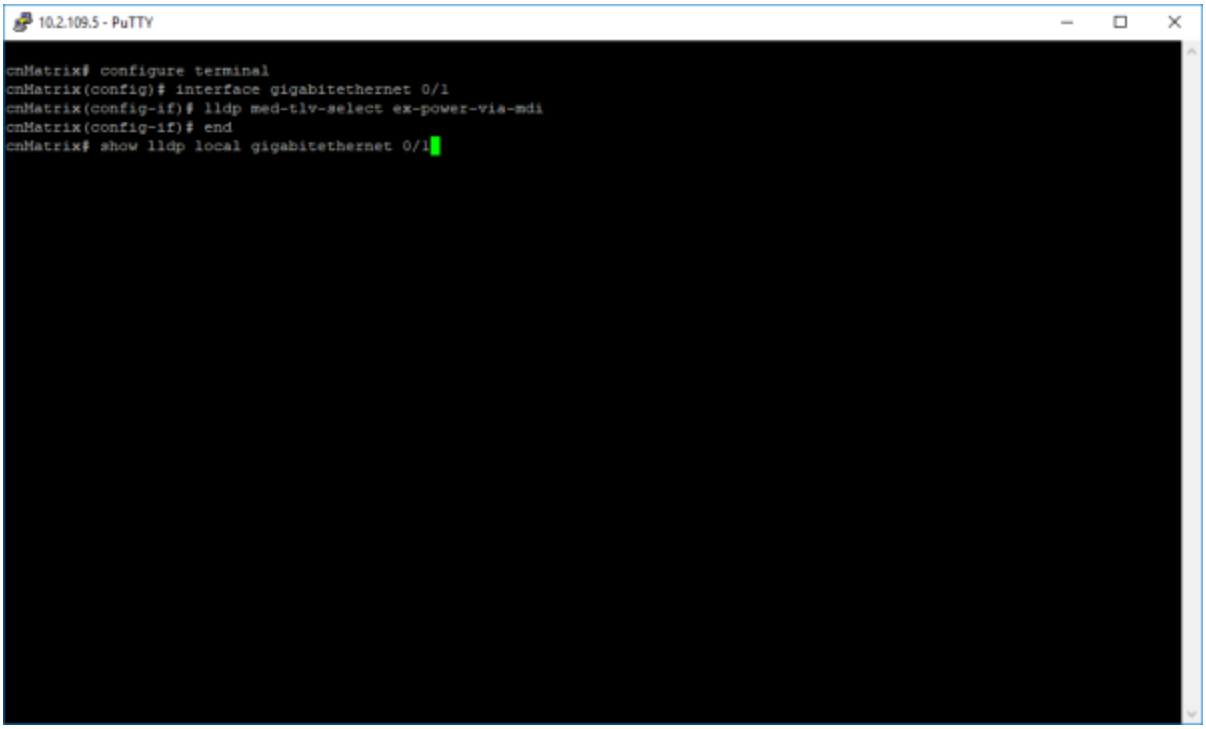


8. Press the **Enter** key.

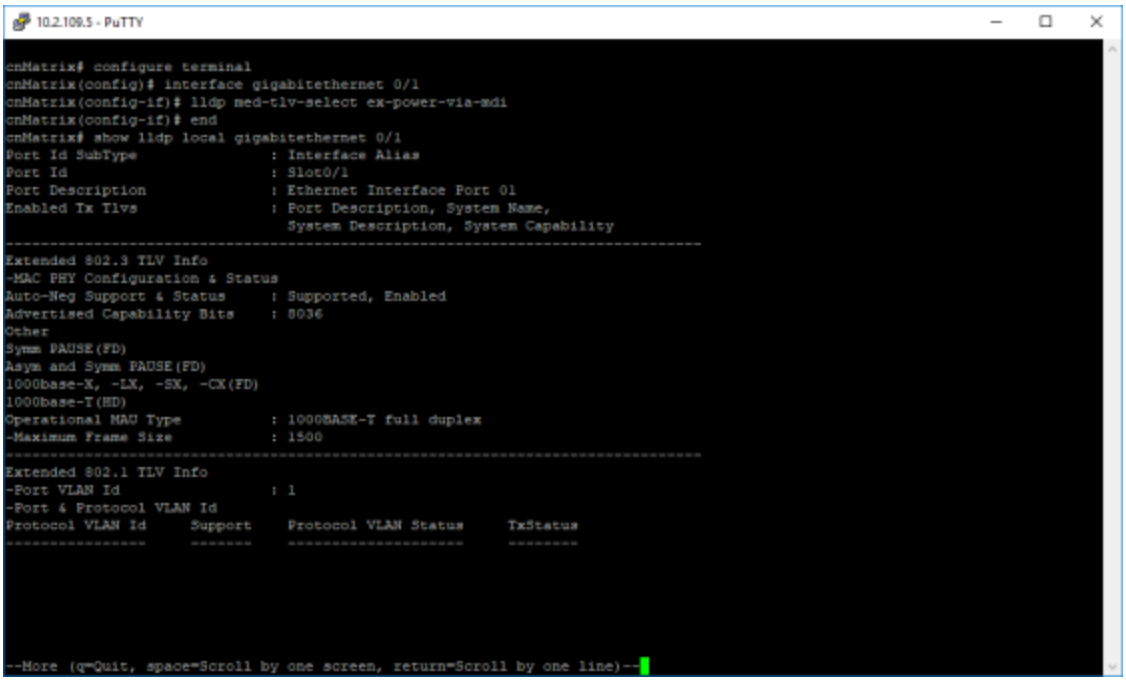


For more information, see LLDP-MED Parameters and Commands.

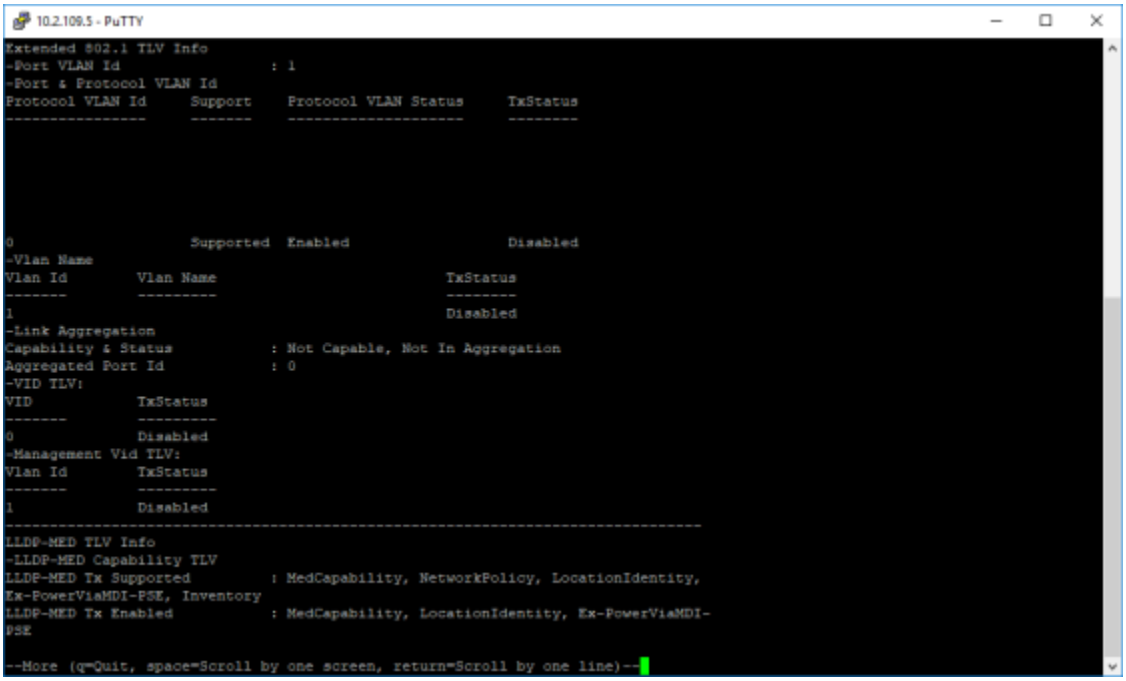
How to Enable Extended Power via MDI



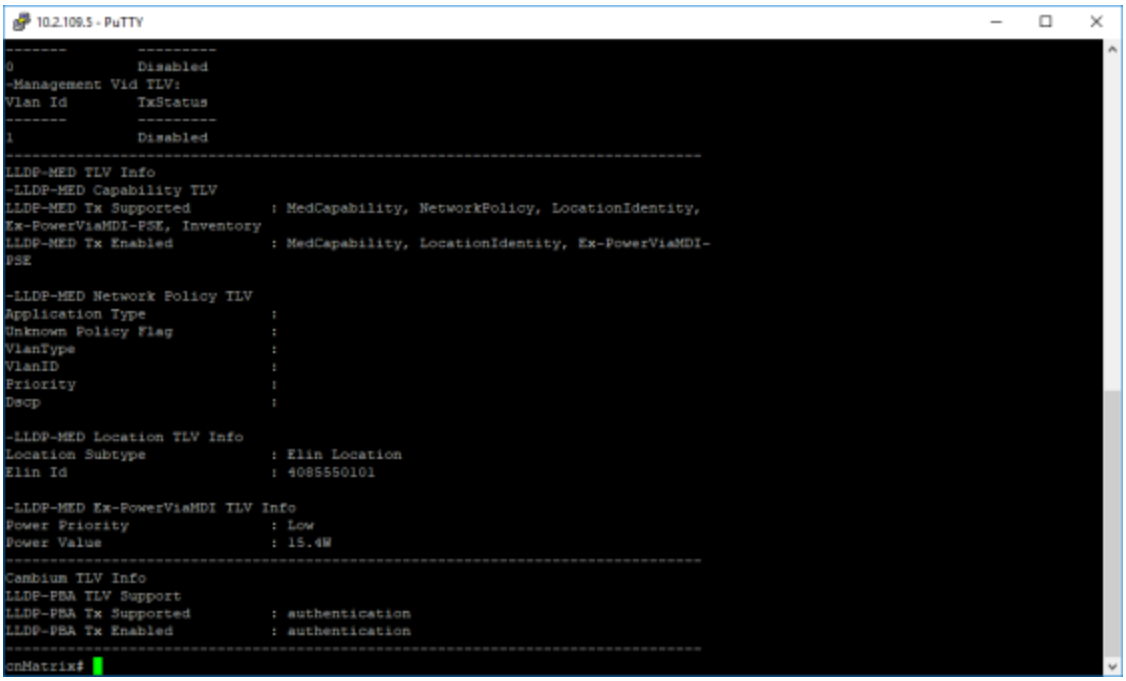
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/1** command into the terminal to select an interface to be configured. Press the **Enter** key.
3. Type the **lldp med-tlv-select ex-power-via-mdi** command into the terminal 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 **Enter** key.



7. Press the **Enter** key.



RMON

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.

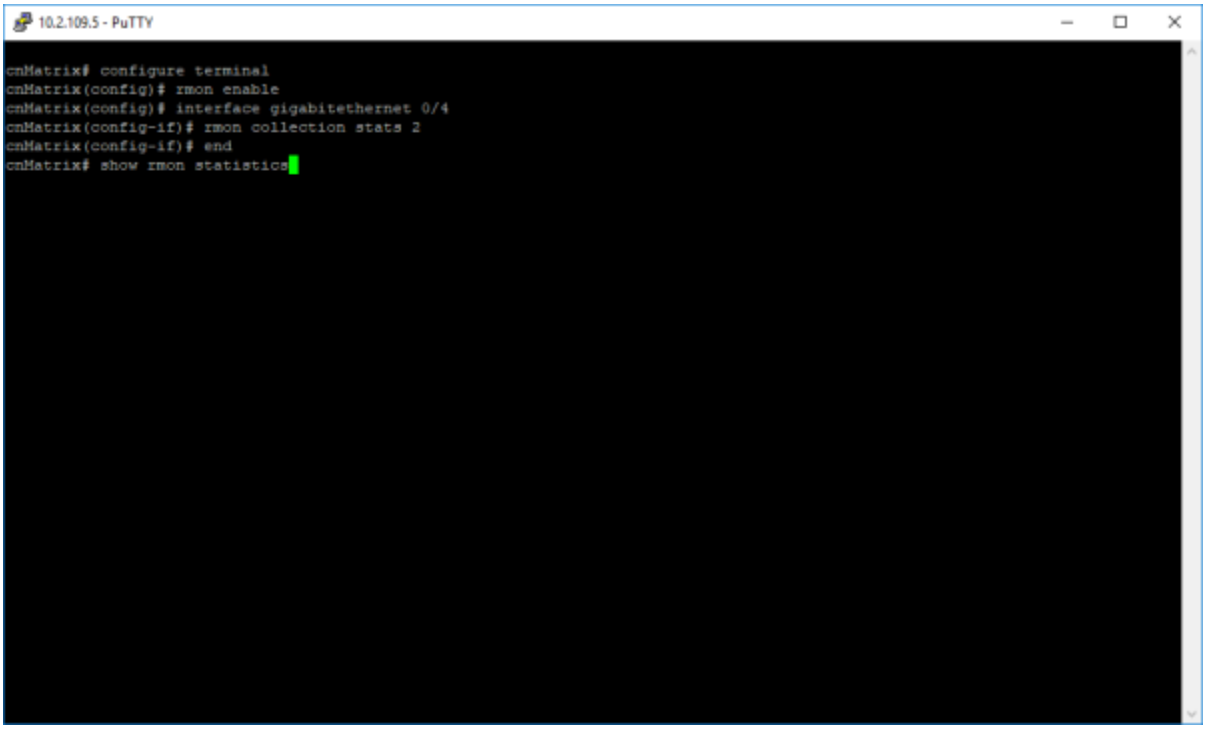
Limitations

- 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 the 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.

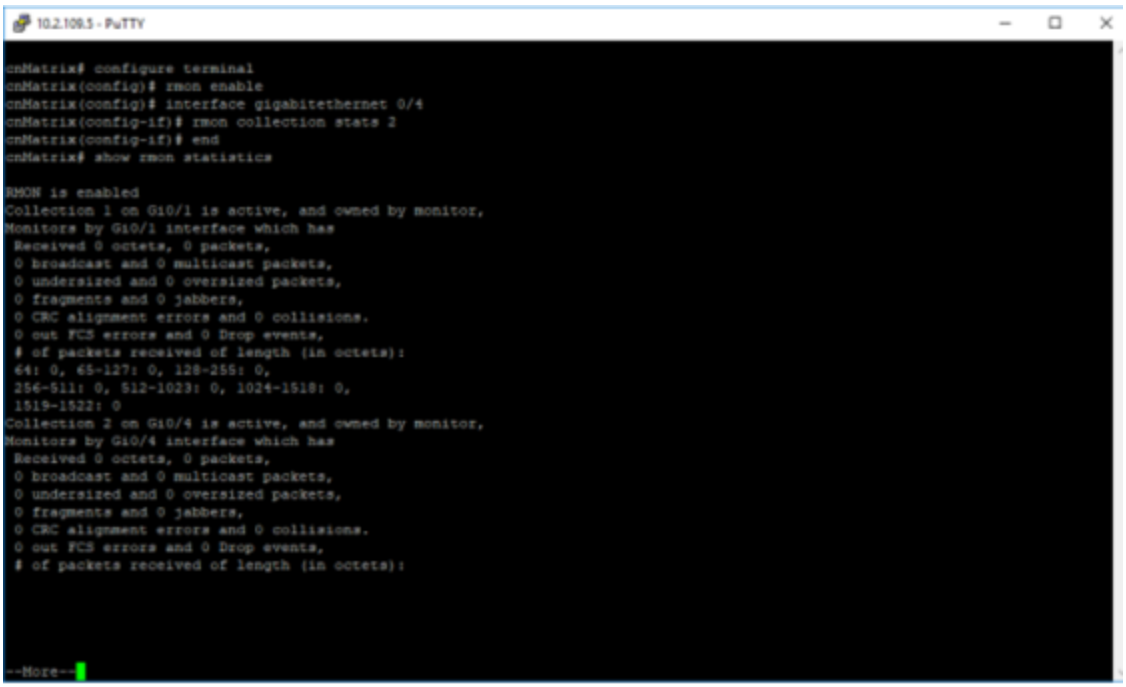
Default Values

- 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.

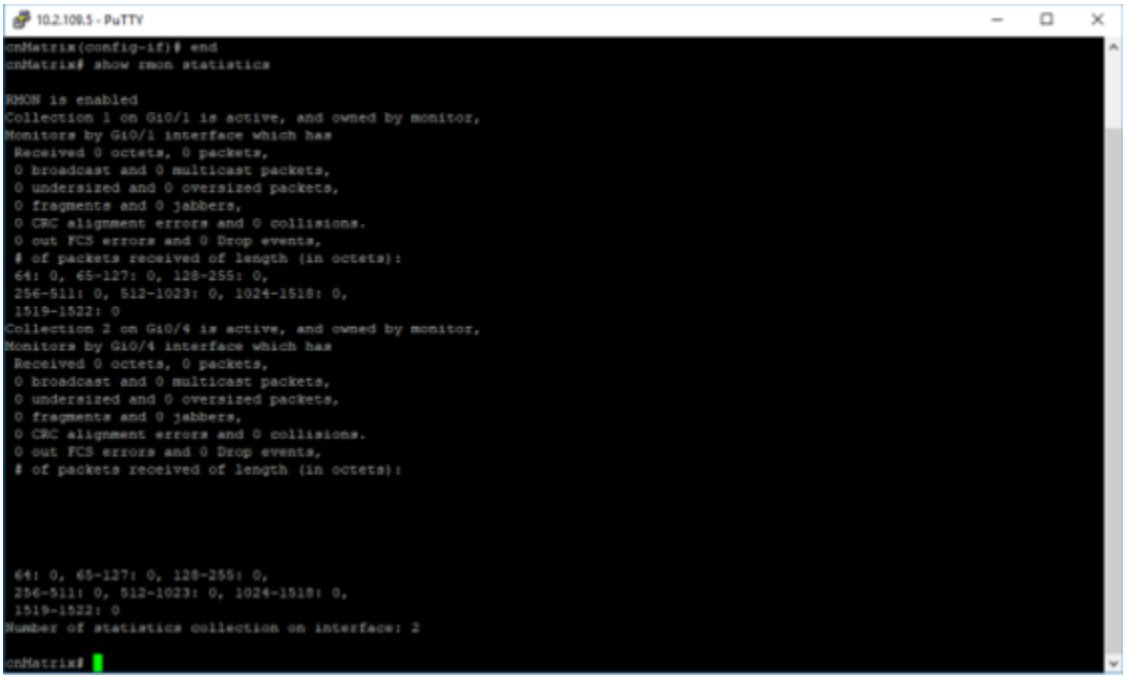
How to Enable and Configure RMON in CLI Interface (Interface Mode)



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 configured. 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.

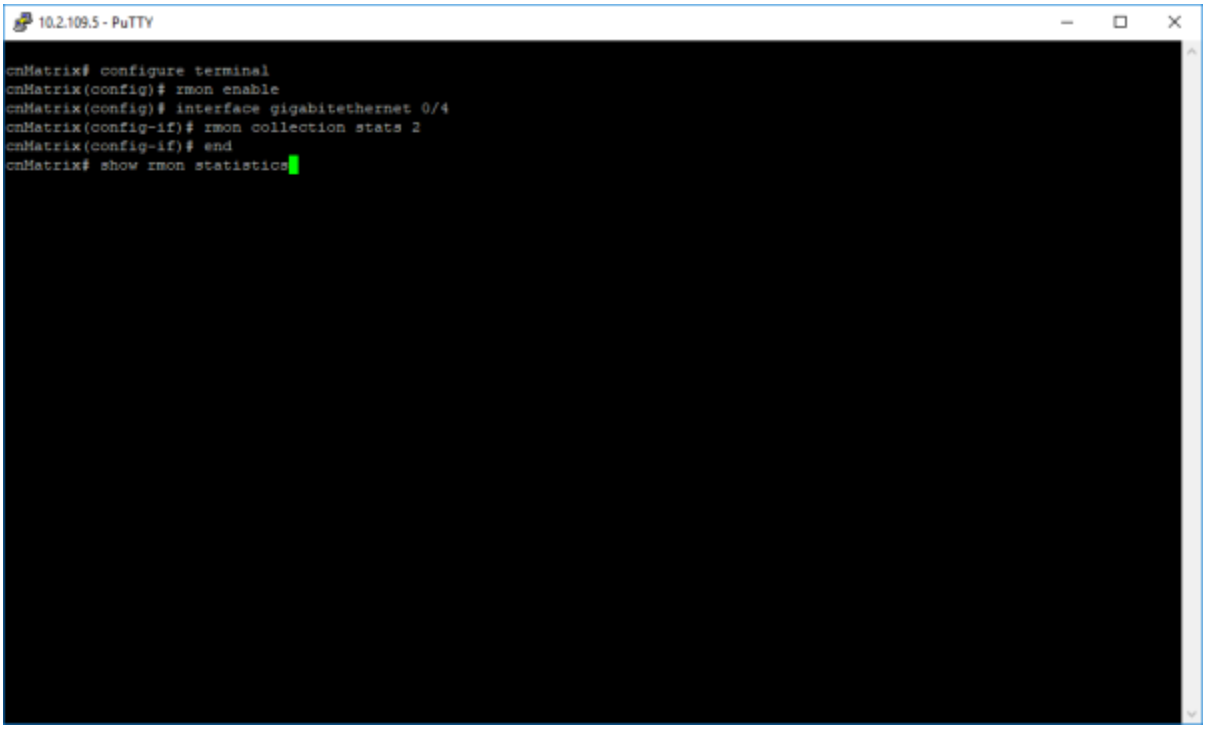


7. Press the **Enter** key.

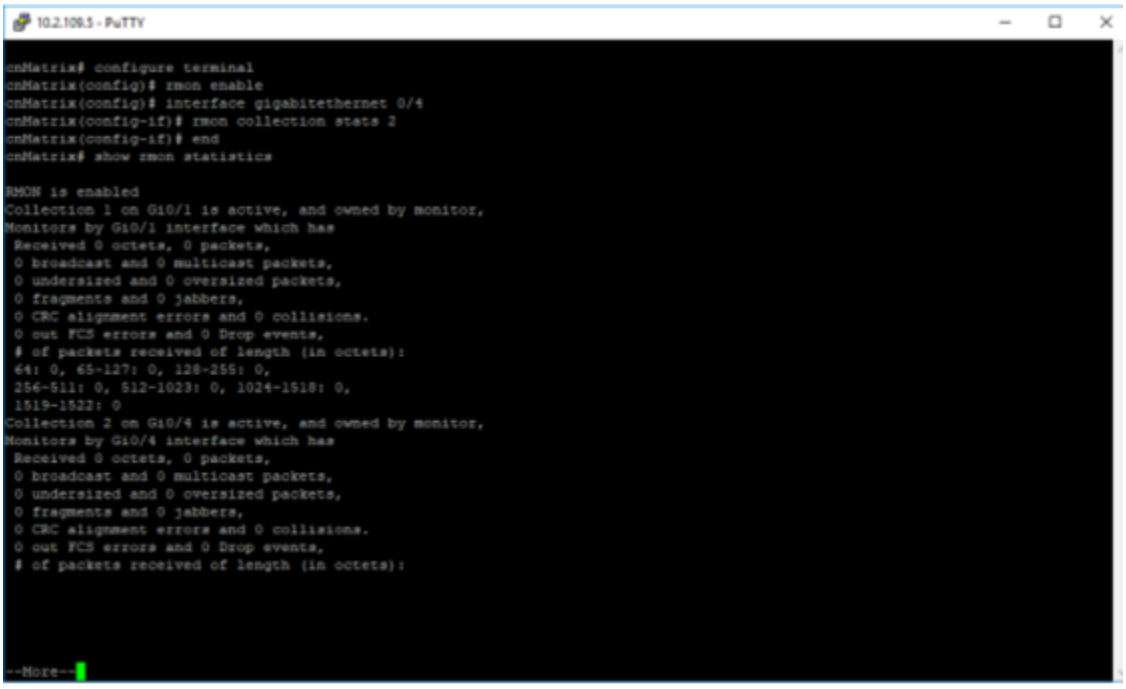


For more information, see RMON Parameters and Commands.

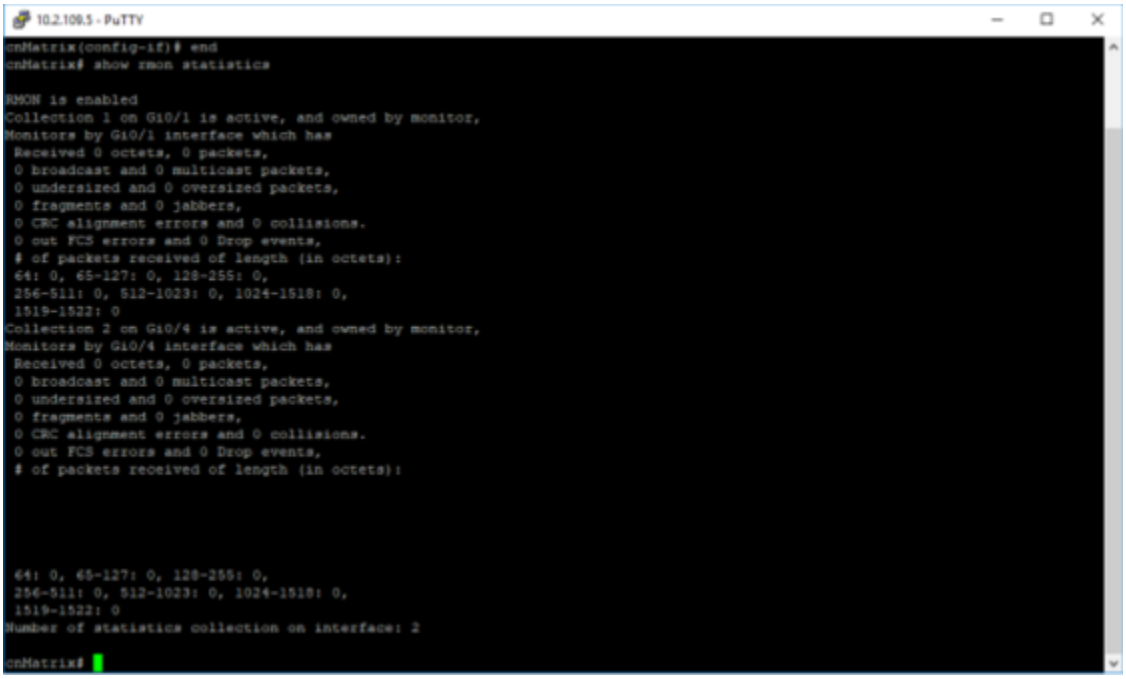
How to Enable and Configure RMON in CLI Interface (VLAN Mode)



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 **Enter** key.



For more information, see RMON Parameters and Commands.

Troubleshooting RMONs

Useful commands for troubleshooting:

- cnMatrix#show rmon statistics
- cnMatrix#show rmon alarms
- cnMatrix#show rmon history
- cnMatrix#show rmon events

SNTP

Managing SNTP

Feature Description

The **SNTP** client feature enables you to synchronize the time and date in cnMatrix with an SNTP Server and to determine the time, and roundtrip delay.

Standards

- cnMatrix SNTP client is RFC 4330 compliant.

Scaling Numbers

- cnMatrix SNTP is a client feature and depends only on the 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.
- cnMatrix SNTP client does not support SNTP symmetric mode.
    - When configured to function in Unicast addressing mode, the software delivers the functionality listed below:
        - Dynamically 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 a client request messages with less than 1-minute periodic interval.
        - Stops sending request packets to a particular server while receiving a reply with a 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 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 a 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 determining 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 the reply packet start the field set as zero.

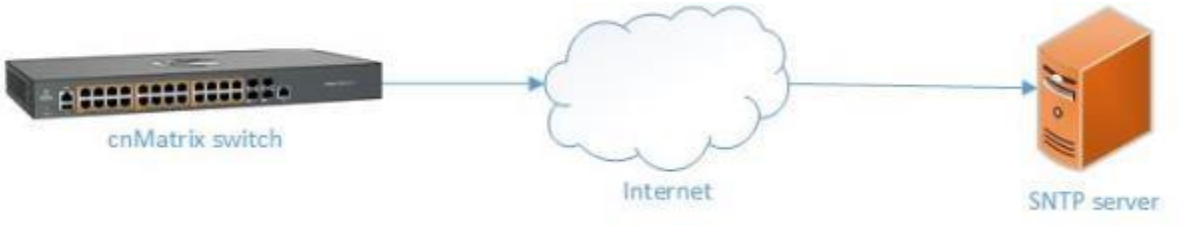
Default Values

- The default SNTP client version: v4.
- The default SNTP addressing mode is unicast.
- The SNTP to send status requests 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.

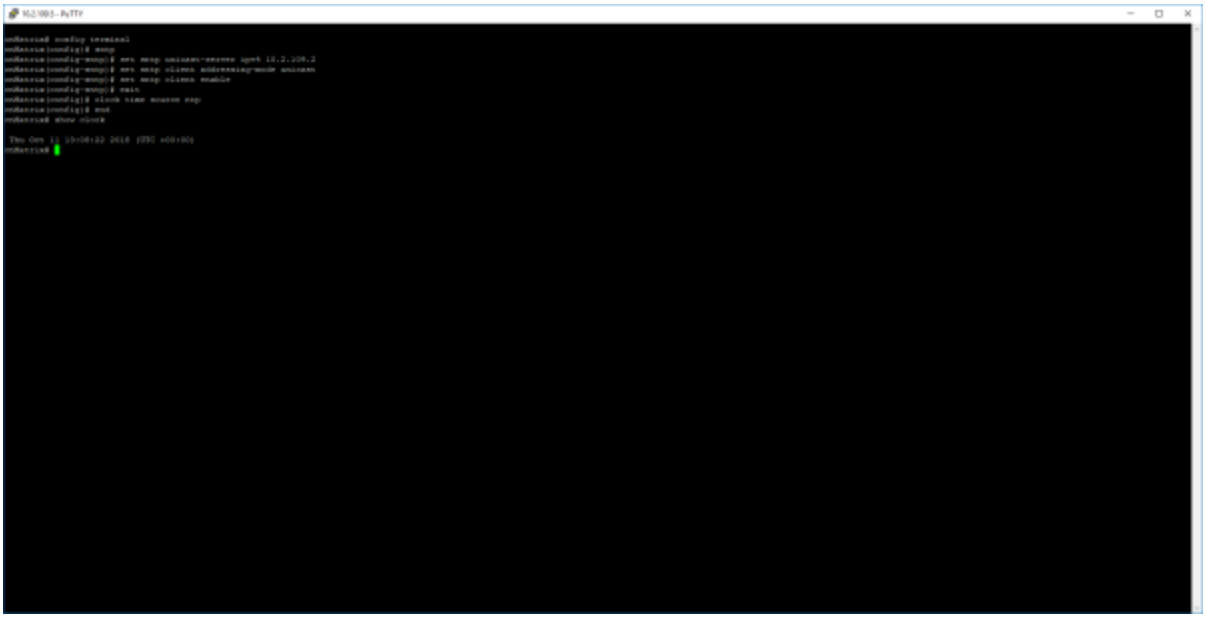
Prerequisites

- Network connectivity to an SNTP server.

Network Diagram



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 configuration 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 the 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.

Configure time-zone and day-light saving

1. Type the config terminal command into the terminal. Press the **Enter** key.
2. Type the **clock timezone PST -8** command into the terminal to configure the standard timezone. Press the **Enter** key.
3. Type the **clock summer-time PDT recurring 2 sunday march 02:00 first sunday november 02:00** 60 command into the terminal to configure the day-light saving time. 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 clock detail** command into the terminal to display the system clock. Press the **Enter** key.

Configure time-zone and day-light saving

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **clock timezone PST -8** command into the terminal to configure the standard timezone. Press the **Enter** key.
3. Type the **clock summer-time PDT recurring 2 sunday march 02:00 first sunday november 02:00 60** command into the terminal to configure the day-light saving time. 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 clock detail** command into the terminal to display the system clock. Press the **Enter** key.

Port Settings Feature

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.

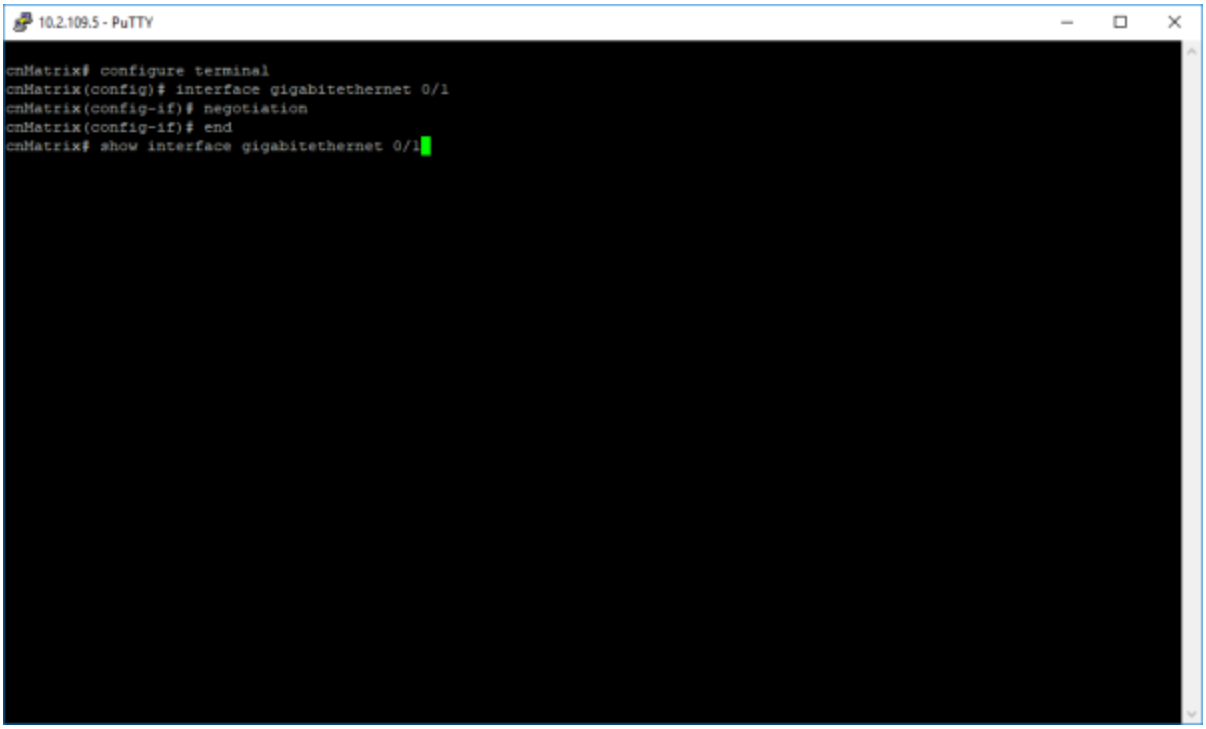
Prerequisites

- N/A

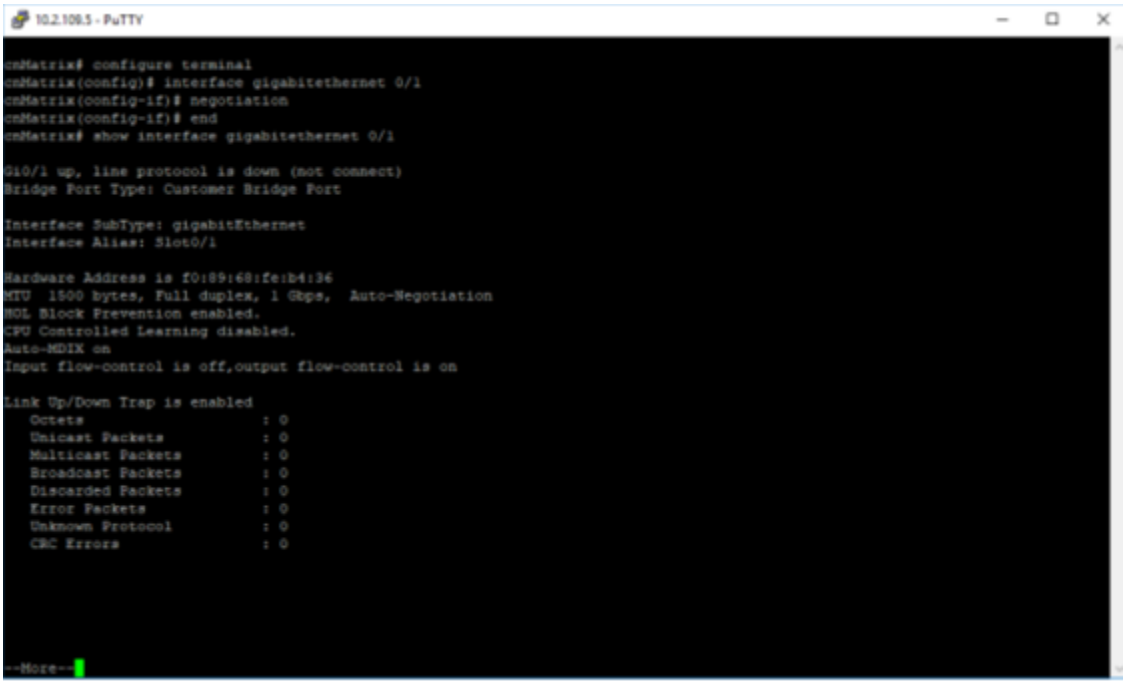
SNMP

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

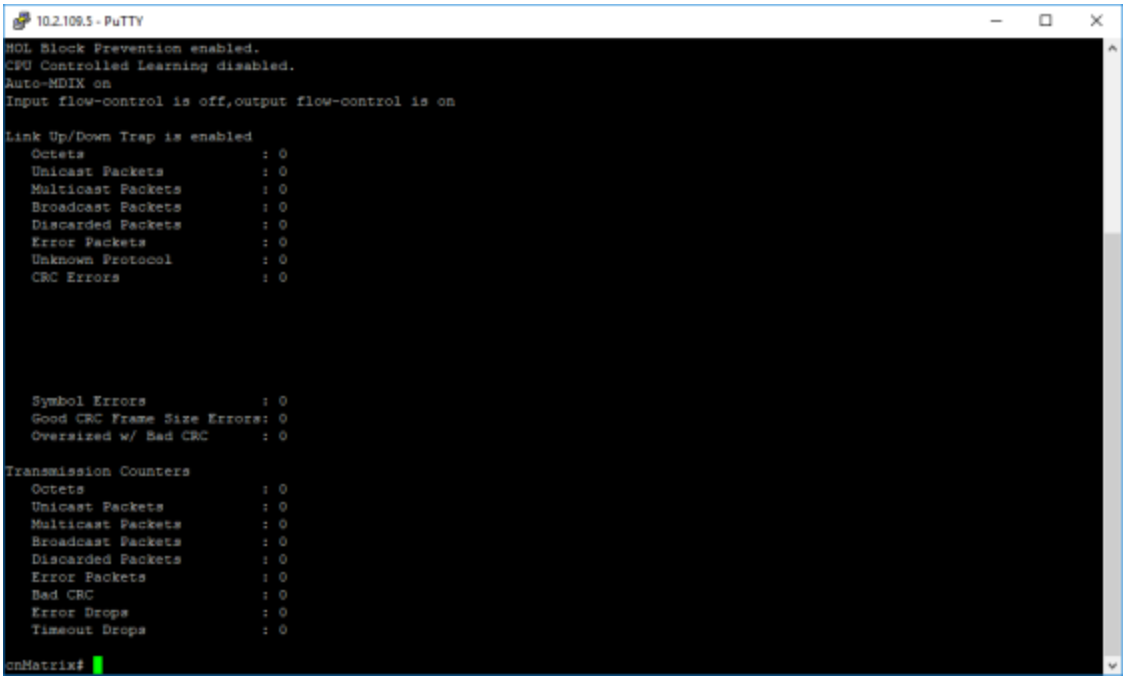
How to Enable and Configure Negotiation in CLI Interface



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).

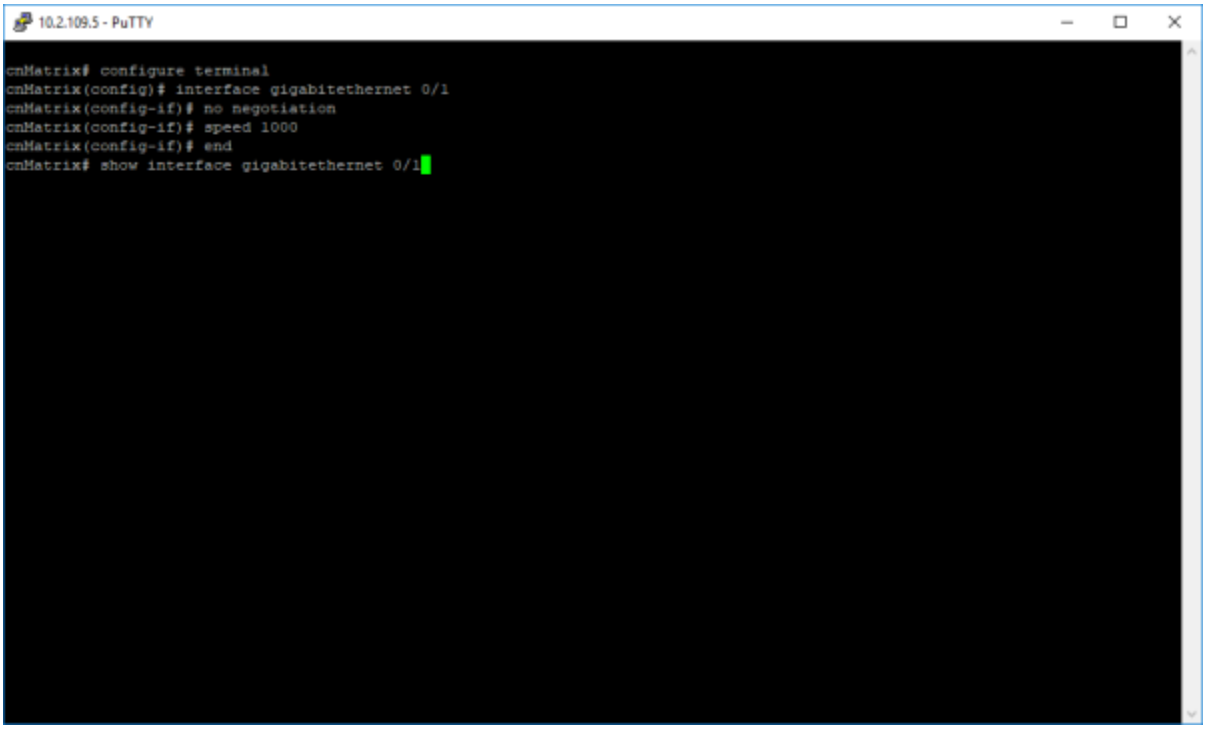


6. Press the **Enter** key.



For more information, see Port Settings Parameters and Commands.

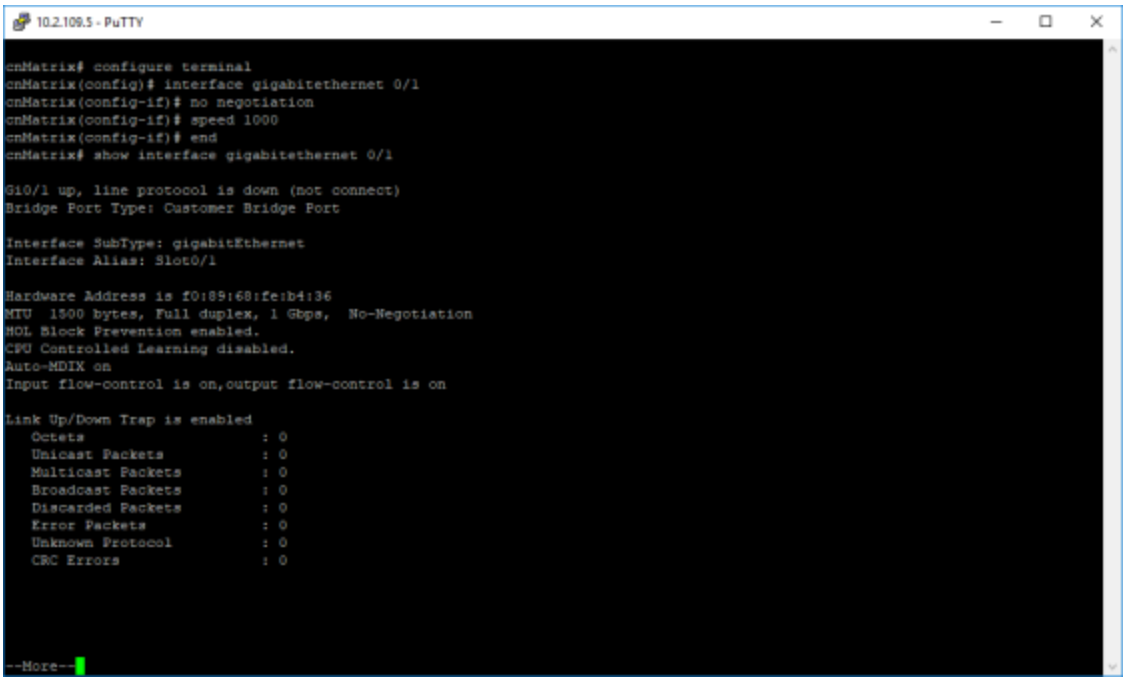
How to Enable and Configure Speed in CLI Interface



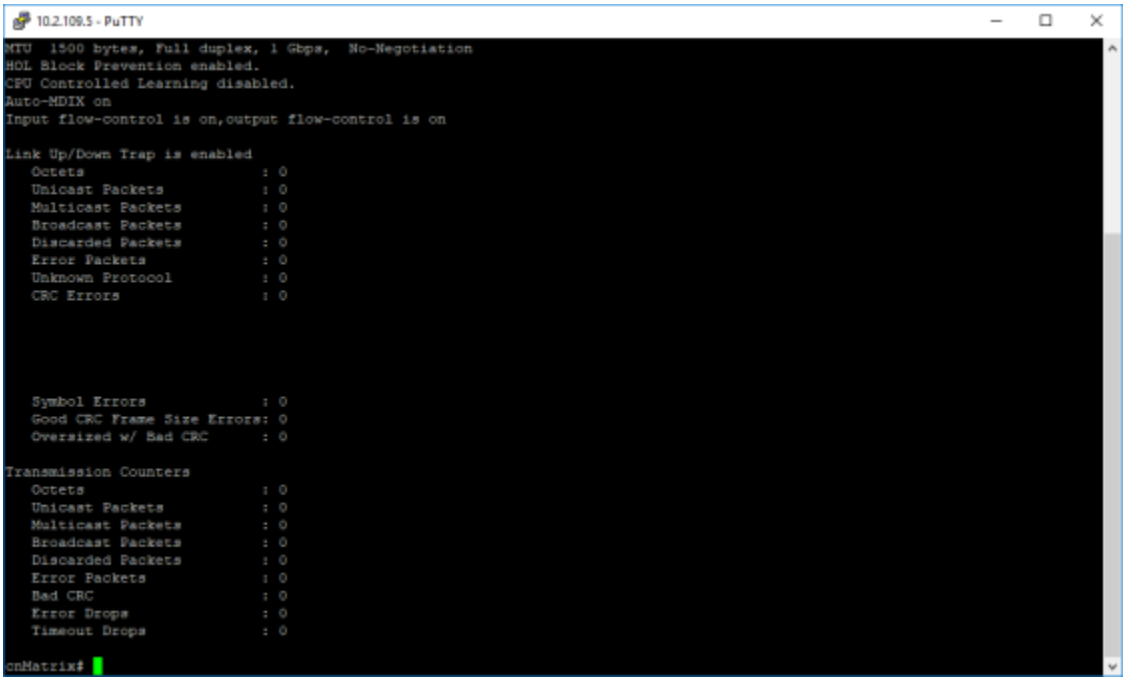
1. Enter **configure terminal** into the field. Press the **Enter** key.
2. Enter **interface gigabitethernet 0/1** into the field to select an interface to be configured. Press the **Enter** key.
3. Enter **no negotiation** into the field to disable auto-negotiation on the interface. Press the **Enter**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

> **Note**
>
> 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 **Enter** key.



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

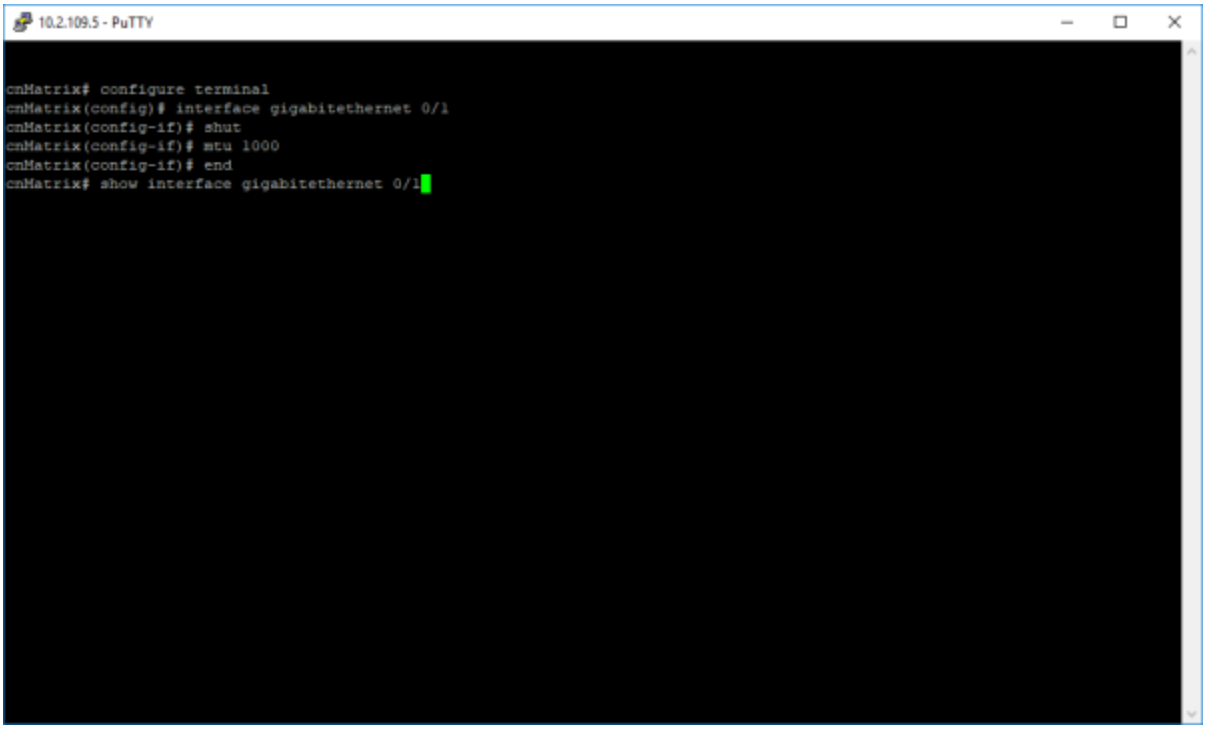
SNMP

The object is called Main MTU, and it is accompanied by an index that represents the port number. It is part of the main table.

Caution

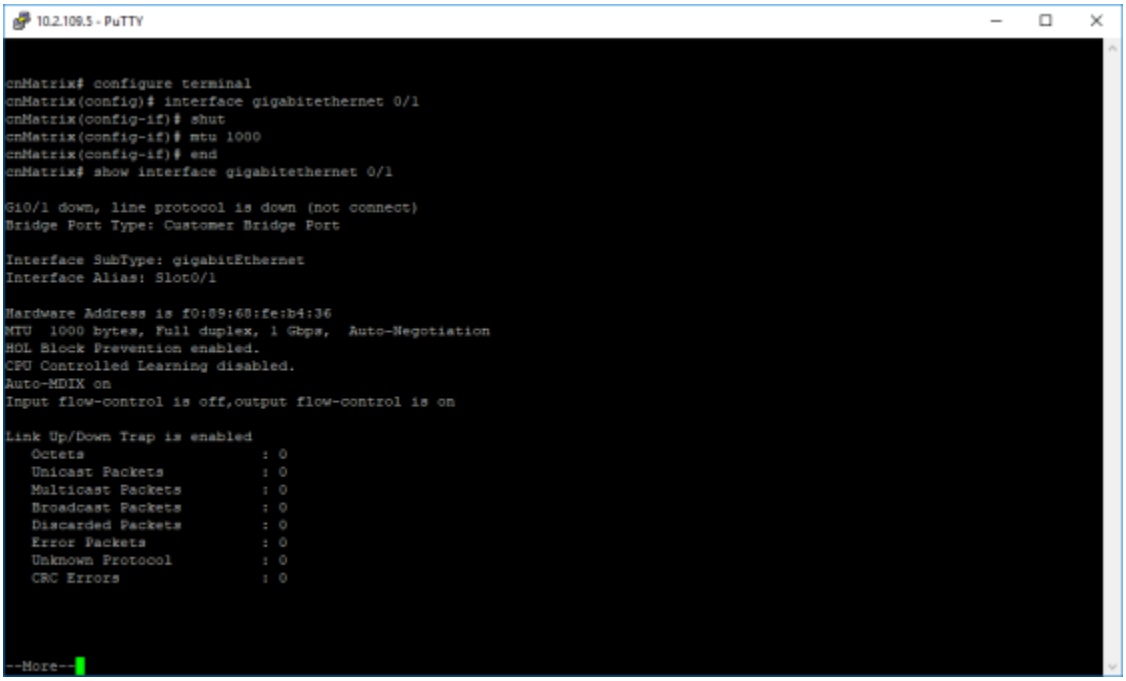
The MTU value can be changed only if the **Admin State** is set as **Down**.

How to Enable and Configure MTU in CLI Interface

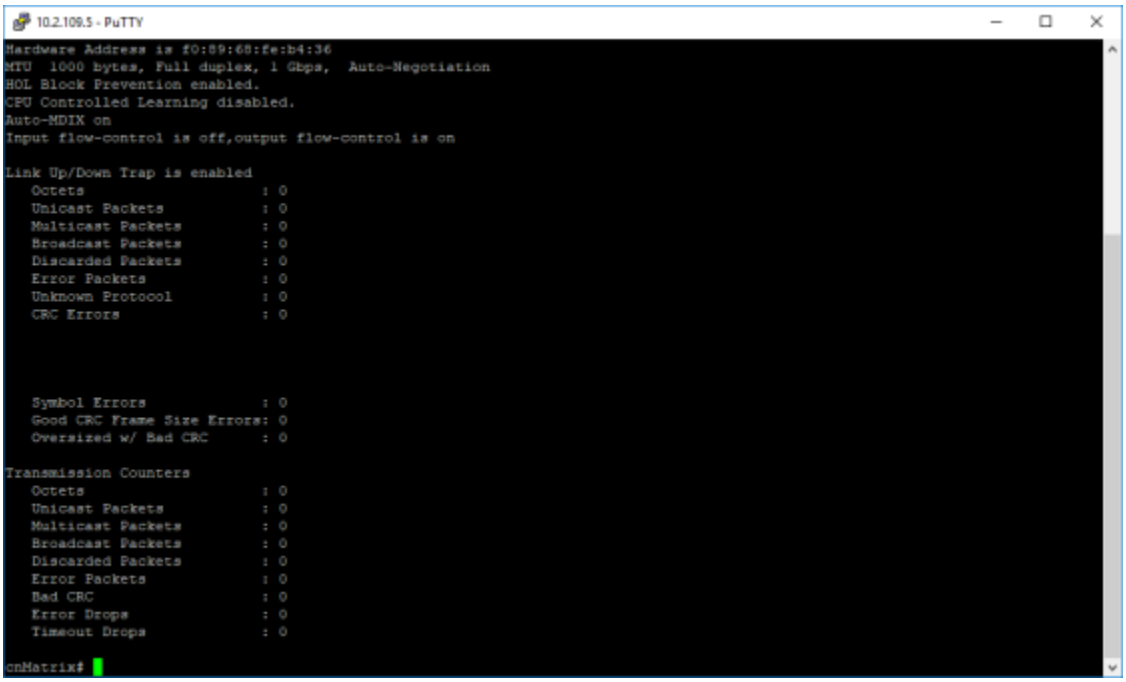


1. Enter **configure terminal** into the field. Press the **Enter** key.
2. Enter **interface gigabitethernet 0/1** into the field to select an interface to be configured. Press the **Enter** key.
3. Enter **shut** into the field to disable a physical interface. Press the **Enter** key.

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 **Enter** key.



For more information, see Port Settings Parameters and Commands.

Managing Duplex Setting

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.

Caution

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.

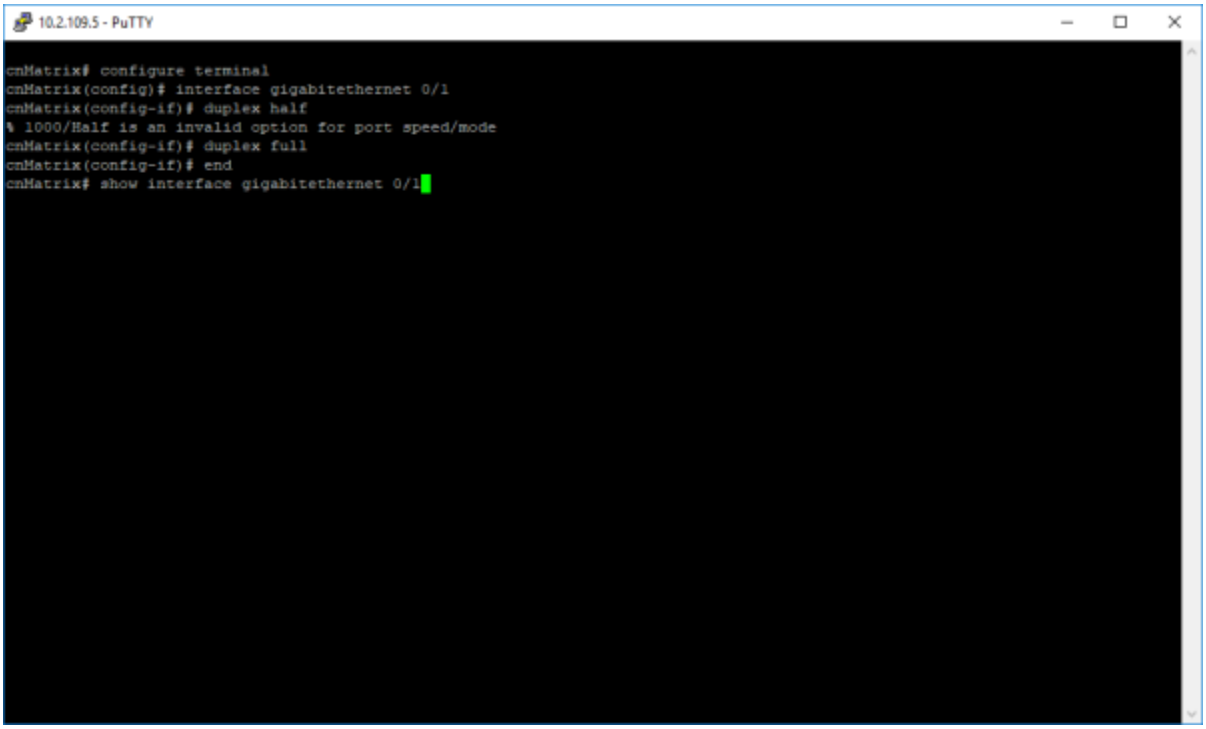
Prerequisites

- N/A

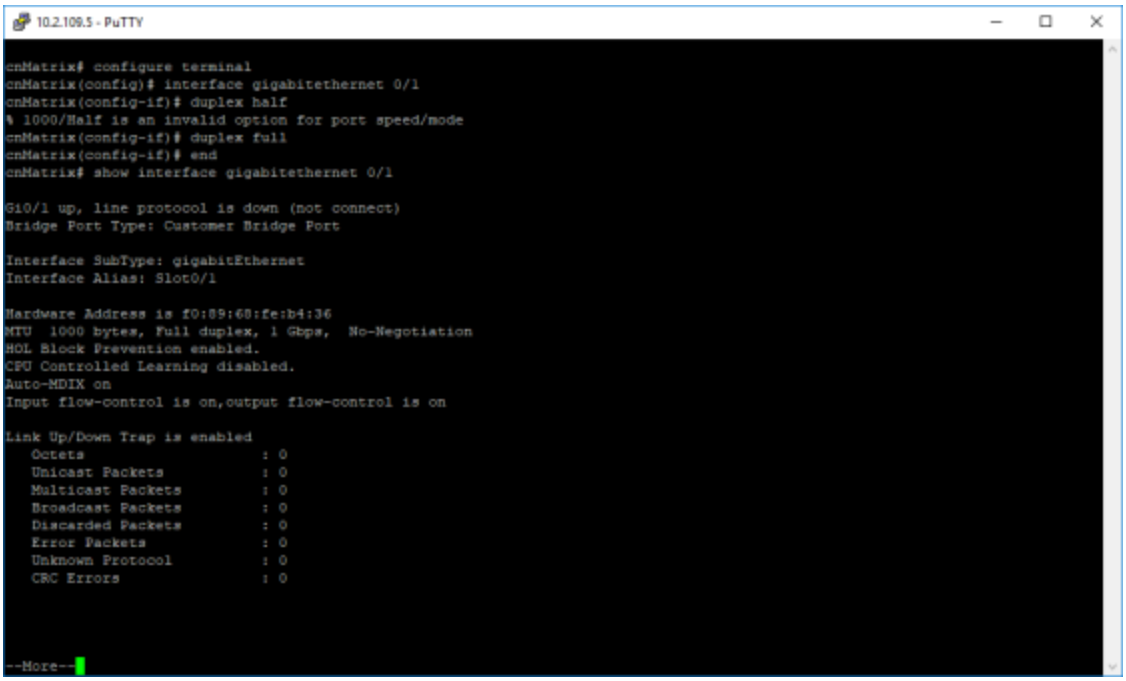
SNMP

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

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.

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

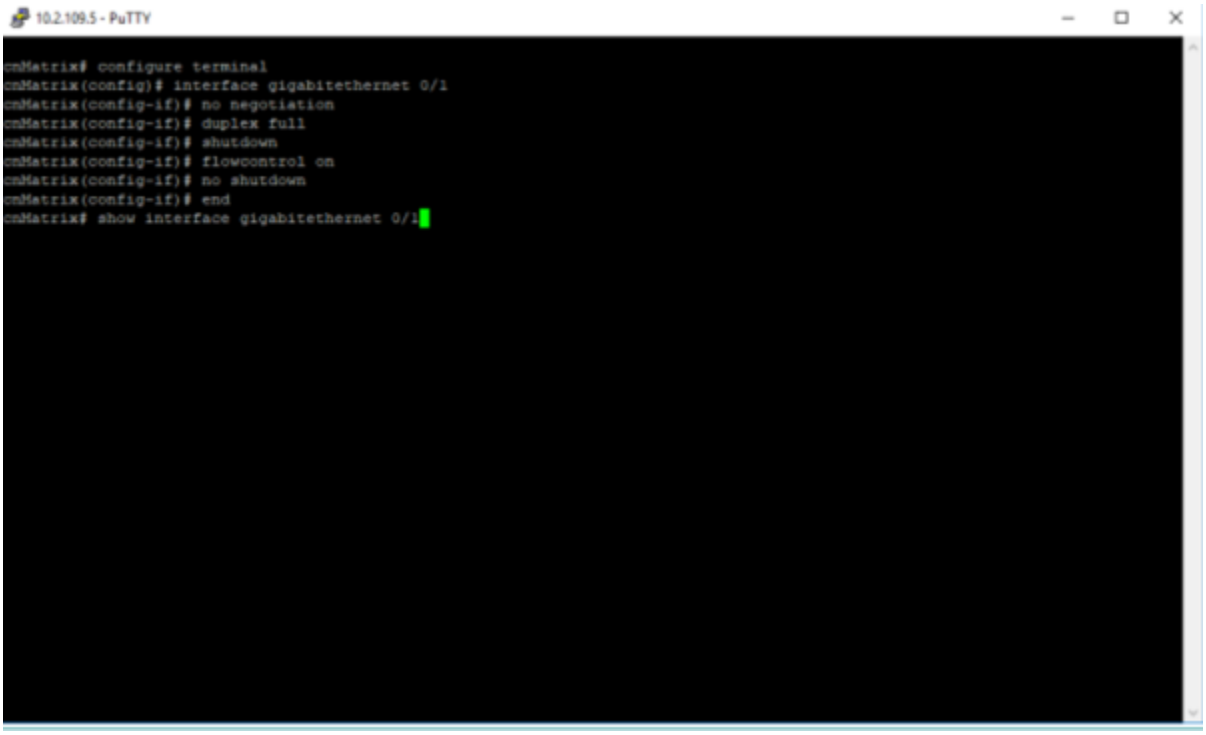
Limitations

- 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.

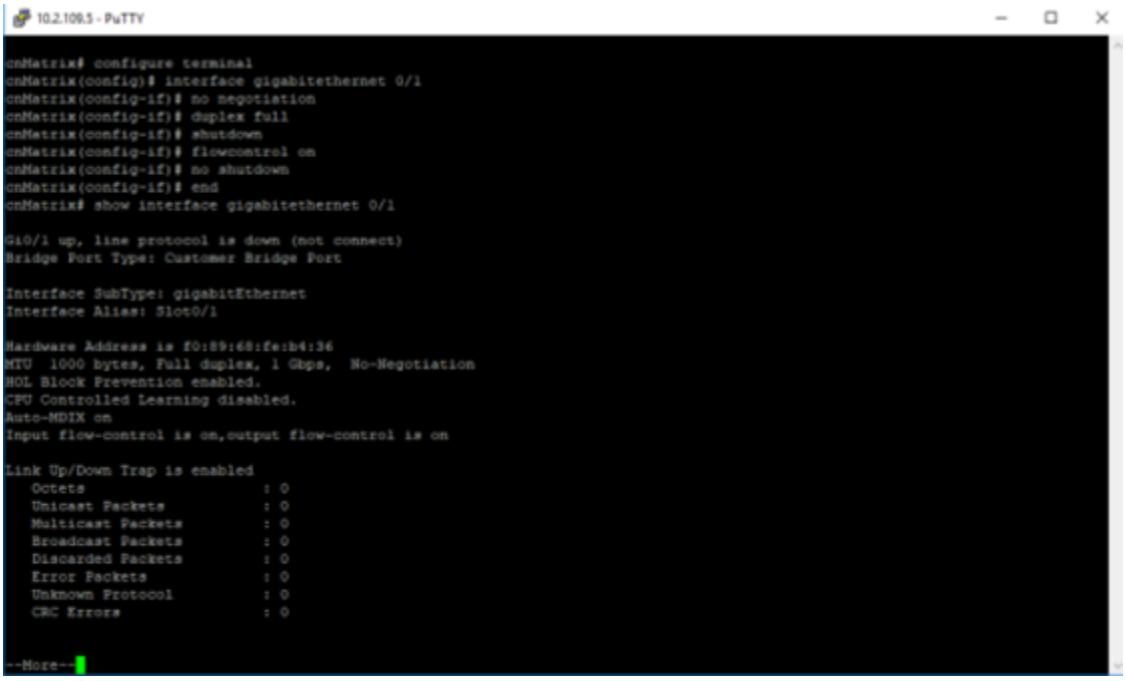
Default Values

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

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 duplicity 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.

How to Display Transceiver Information (Starting with version 2.1)

Feature Overview

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

  cnMatrix# show interfaces transceivers

- The ports do not need to have a link up 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+.
- The EX1028 and EX1028-P models only support SFP transceivers.
- The EX1010 and EX1010-P models only support SFP transceivers.

Prerequisites

- Insert a transceiver in your cnMatrix switch.

Link-Transitions Count

Managing Link-Transitions Count

Feature Overview

The Link-Transitions Count feature provides a way for the switch to count the number of link transition events per-port. The feature shows the number of link transition events on a per-port basis, for all ports available and the time stamp of the last transition.

Note

The **link-transitions counters** can be displayed via CLI, Web, and SNMP.

Attention

Link-Transitions Count feature is supported starting with cnMatrix release 4.0.1.

Standards

N/A

Limitations

Last transition date and time field have an error of +/- one second.

Default Values

- The feature is enabled by default.
- The counters sum up all the link Up and link Down transitions on each port, for all physical ports. The feature does not count link Up/Down events for VLAN interfaces or OOB port.
- The counters start from zero at boot time and reset to zero on each reboot.

How to show link-transitions counters

```
TX2020RP-EC4C40# show interfaces link-transitions

Interface  OpStatus  Link-Transitions  Last-Transition
---------  --------  ----------------  --------------------------
Gi0/1      Up              3           Fri Apr  9 15:15:14 UTC 2021
Gi0/2      Down            0
Gi0/3      Down            0
Gi0/4      Down            0
Gi0/5      Up              1           Fri Apr  9 15:15:13 UTC 2021
Gi0/6      Up              1           Fri Apr  9 15:15:13 UTC 2021
Gi0/7      Down            0
Gi0/8      Down            0
Gi0/9      Down            0
Gi0/10     Down            0
Gi0/11     Down            0
Gi0/12     Down            0
Gi0/13     Down            0
Gi0/14     Down            0
Gi0/15     Down            0
Gi0/16     Down            0
Ex0/1      Down            0
Ex0/2      Down            0
Ex0/3      Down            0
Ex0/4      Down            0
TX2020RP-EC4C40#
```

1. Type the **show interfaces link-transitions** command into the terminal to display link-transitions counters. Press the **Enter** key.

Note

The link transition counters are shown on a per-port basis or for all ports.

If a counter is greater than zero, the last transition date and time is also displayed.

To show a single interface (example):

```
TX2020RP-EC4C40# show interfaces link-transitions gig 0/1

Interface  OpStatus  Link-Transitions  Last-Transition
---------  --------  ----------------  --------------------------
Gi0/1      Up              3           Fri Apr  9 15:15:14 UTC 2021
TX2020RP-EC4C40# _
```

2. Type the show interfaces link-transitions gig 0/1 command into the terminal. Press the **Enter** key.

How to clear link-transitions counters

```
TX2020RP-EC4C40# clear link-transitions
```

1. Type the **clear link-transitions** command into the terminal. Press the **Enter** key.

To clear a single interface counter(example):

```
TX2020RP-EC4C40# clear link-transitions gig 0/1
```

2. Type the **clear link-transitions gig 0/1** command into the terminal. Press the **Enter** key.

Note

The link transition counters are cleared on a per-port basis or for all ports.

The link transition counters can be cleared in a similar manner from the config terminal.

```
TX2020RP-EC4C40(config)# clear link-transitions
```

3. Type the configure terminal command into the terminal. Press the **Enter** key.
4. Type the clear link-transitions command into the terminal. Press the **Enter** key.

Troubleshooting Link-Transitions Count

Useful commands for troubleshooting

- cnMatrix# show interfaces link-transitions

Front panel LEDs

LED	Color	Description
Copper Link LED (left)	Off	No link
	Green (solid)	1G link, without traffic
	Green (blinking)	1G link, with traffic
	Amber (solid)	2.5G link, without traffic
	Amber (blinking)	2.5G link, with traffic
SFP+ Link LED	Off	No link
	Green (solid)	1G link, without traffic
	Green (blinking)	1G link, with traffic
	Amber (solid)	10G link, without traffic
	Amber (blinking)`	10G link, with traffic
Copper PoE LED (right) Only PoE models	Off	No power output
	Amber	802.3 standard power output
	Green	Passive power output

Link Aggregation

Managing Link Aggregation

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

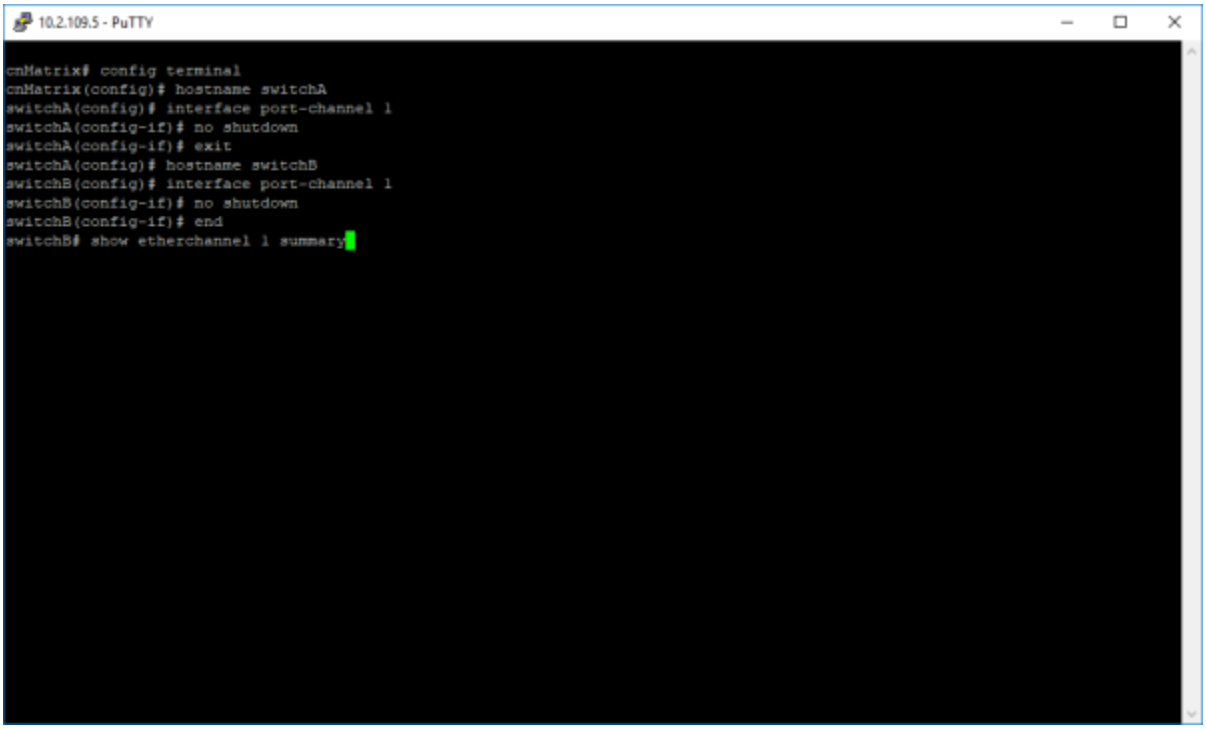
- The Link Aggregation feature is enabled by default.
- The admin status of the Link Aggregation Status in the switch is disabled by default.
- The default LACP wait-time: 2.
- The default LACP timeout period: long.
- The default LACP rate: normal.

Prerequisites

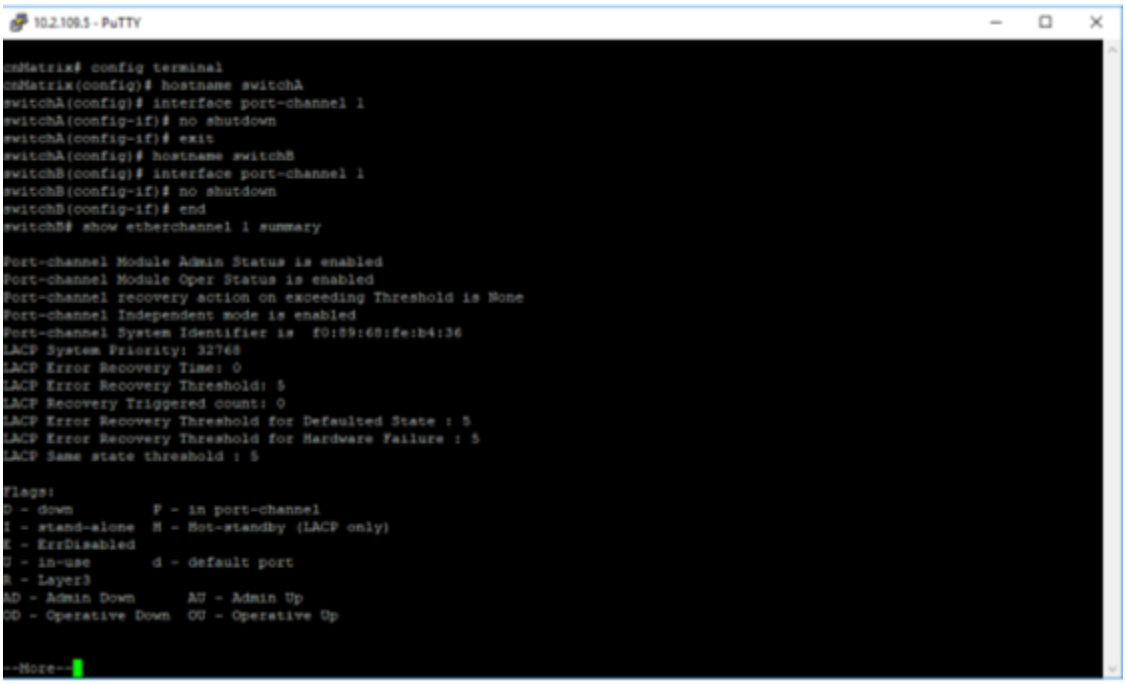
N/A

Network Diagram

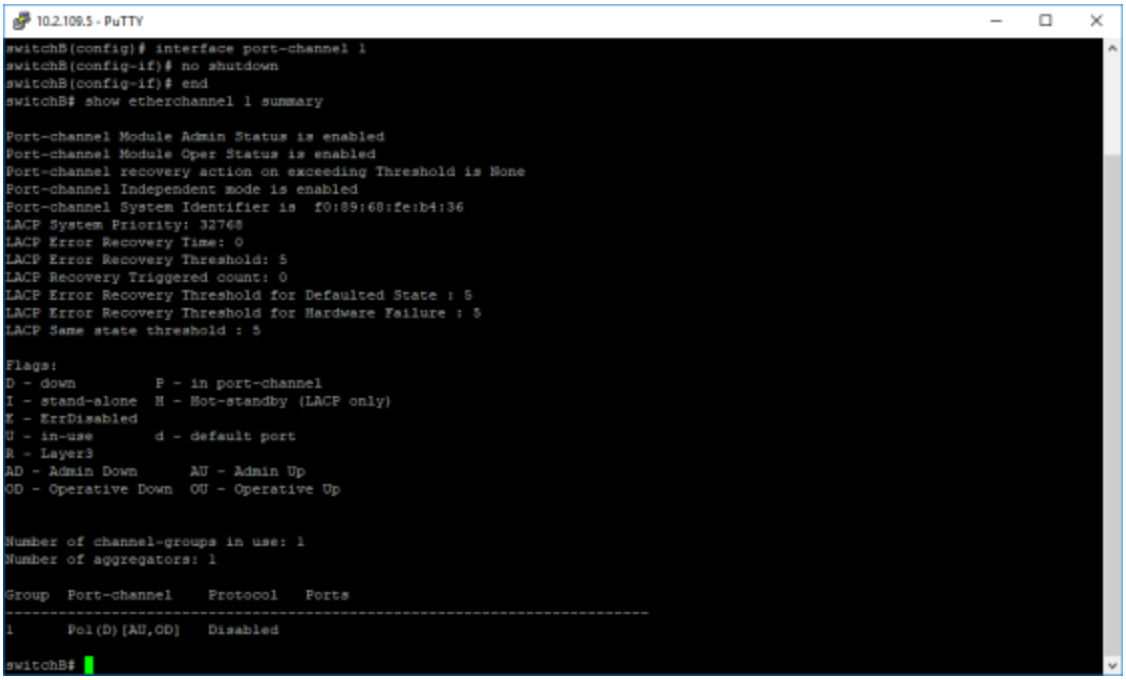
How to Enable and Configure Link Aggregation in CLI Interface



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 **Enter** key.



For more information, see Link Aggregation Parameters and Commands.

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

Private VLAN Edge

Managing Private VLAN Edge

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

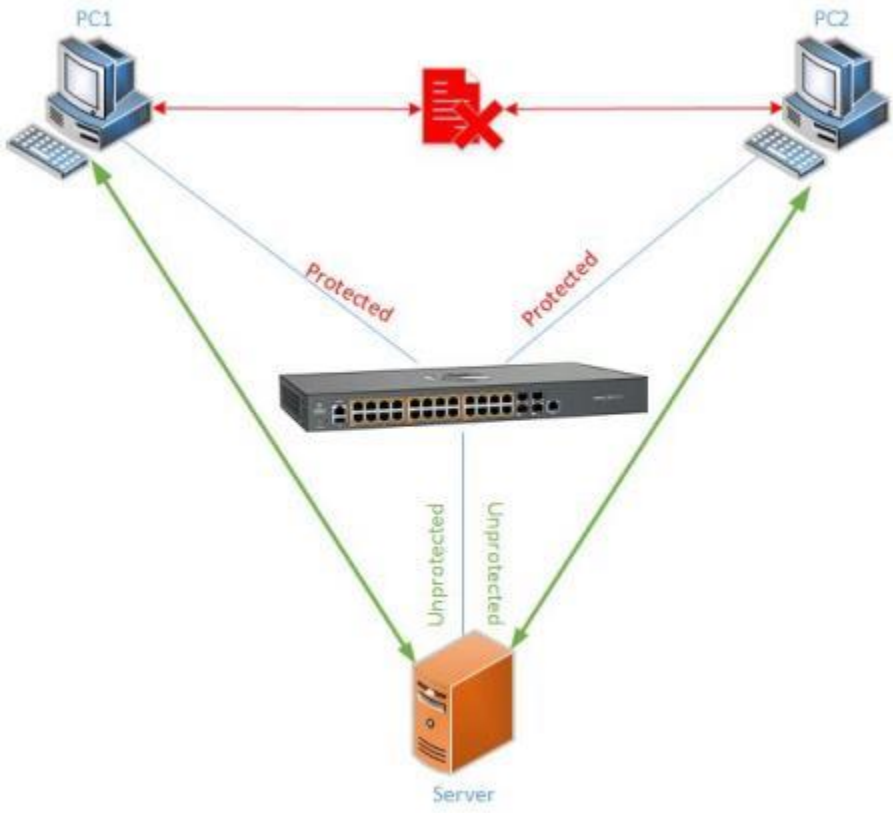
Default Values

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

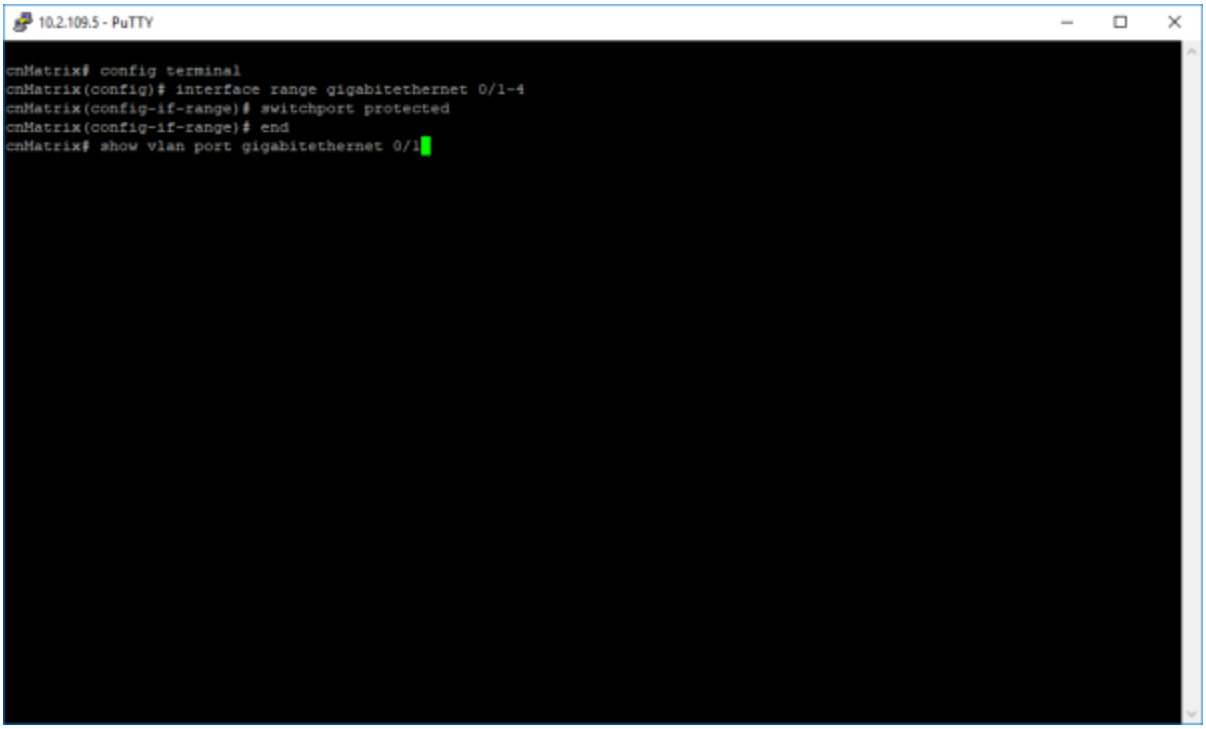
Prerequisites

- N/A

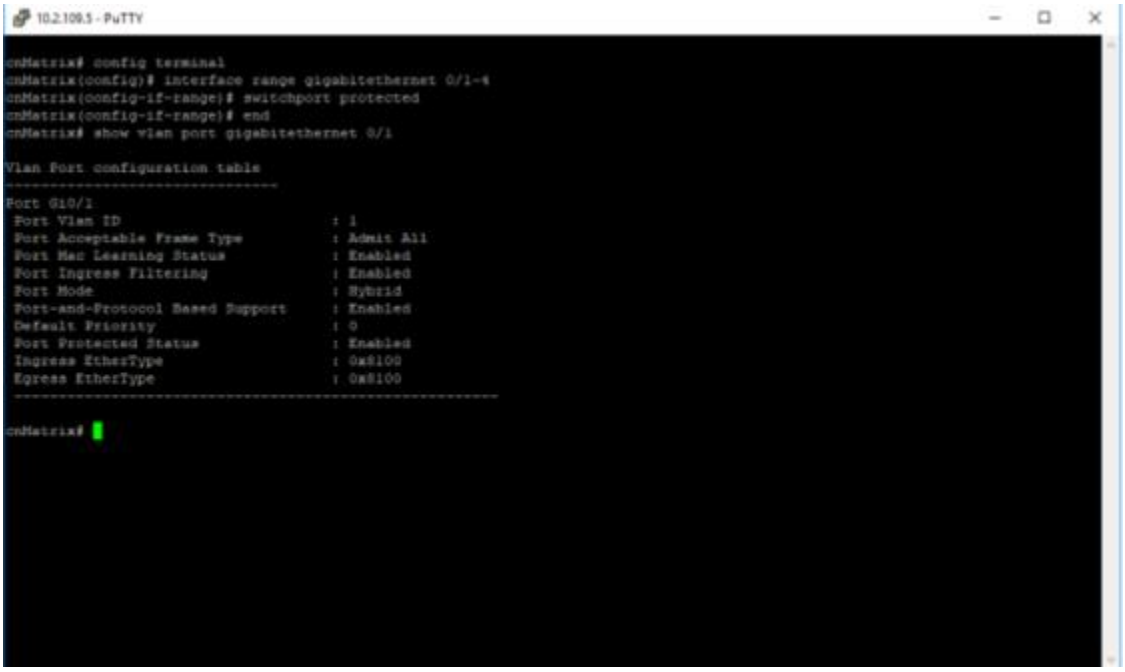
Feature Description



How to Enable Private VLAN Edge in CLI Interface



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.

Troubleshooting Private VLAN Edge

Useful commands for troubleshooting:

- cnMatrix# show vlan port gigabitethernet 0/1

Power over Ethernet

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. PoE technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network.

Attention

EX1028-P is supported starting with cnMatrix release 3.1. **EX1028-P** has a PoE budget of 200W.

EX1010-P is supported starting with cnMatrix release 3.2. **EX1010-P** has a PoE budget of 75W.

TX2020R-P and **TX2012R-P** are supported starting with cnMatrix release 4.0.

TX2028RF-P is supported starting with cnMatrix release 4.1.

Standards

- IEEE 802.3af
- IEEE802.3at
- IEEE802.3bt (only on EX2016M-P and TX2020R-P and TX2012R-P)

Scaling Numbers

N/A

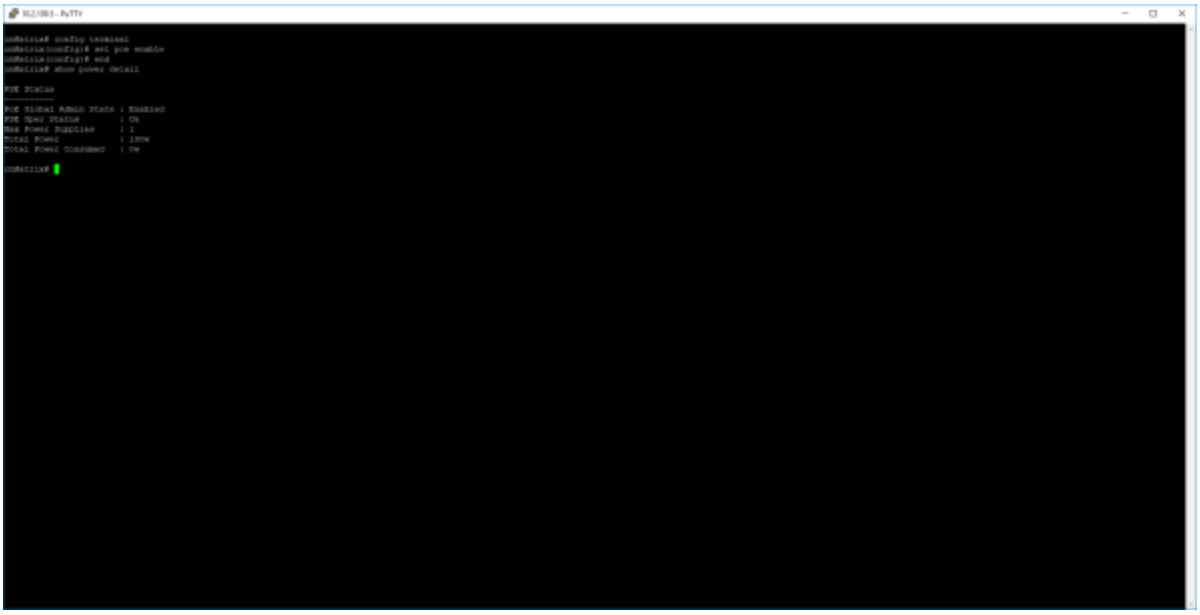
Limitations

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.

How to Enable PoE in CLI Interface



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 PoE 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 PoE power supply status. Press the **Enter** key.

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

Configuring PoE priority (example)

PoE priority can be configured on a per-port basis. Available options are: critical, high, and low.

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/3** command. Press the **Enter** key.
3. Type the **power inline priority critical** command into the terminal to configure the priority to critical on port gi0/3. 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 power inline** command into the terminal to display the per-port PoE information. Press the **Enter** key.

Port pruning

- When power budget is exceeded, ports will be pruned based on their priority (first low priority ports, then high priority ports and finally, critical priority ports).
- If the decision has to be made between ports with equal priority, the biggest port number will be pruned.
- If a higher priority device gets connected and there is no power budget for it, then the lowest priority port will get pruned based on the logic presented above.

Troubleshooting PoE

Useful commands for troubleshooting:

- cnMatrix# show power detail
- cnMatrix# show power inline
- cnMatrix# show power inline measurements

Note:

- Starting with Release 4.0, new PoE functionality has been added exclusively for the WISP switches.
- For more details check the PoE subsection of the WISP chapter.

Port Mirroring

Managing Port Mirroring

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.

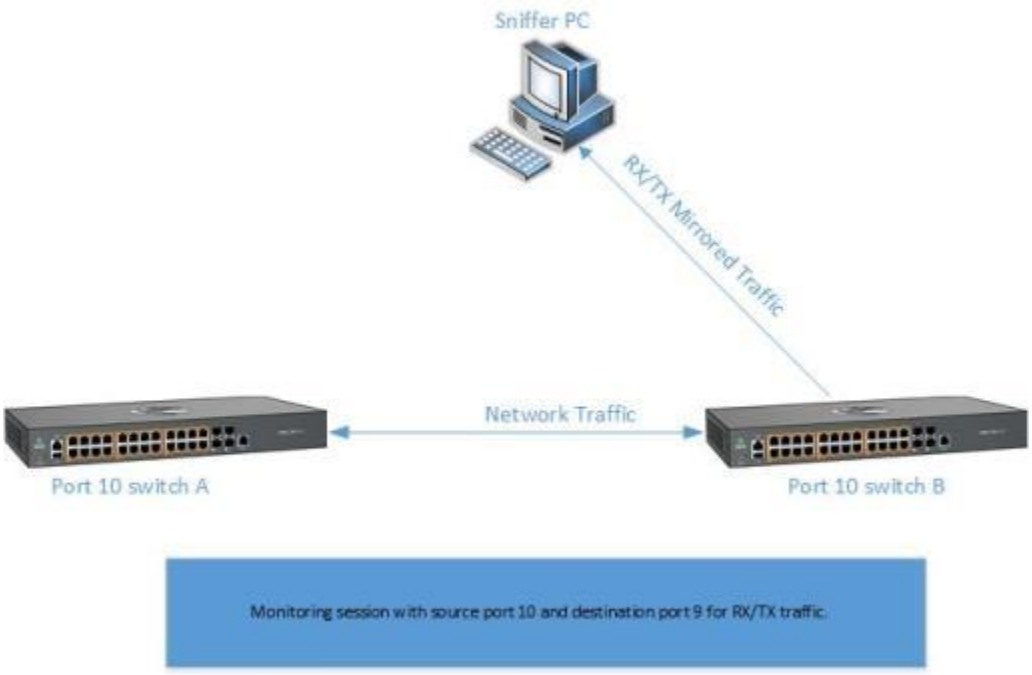
Default Values

- The Port Mirroring feature is not enabled by default.

Prerequisites

- N/A

Network Diagram



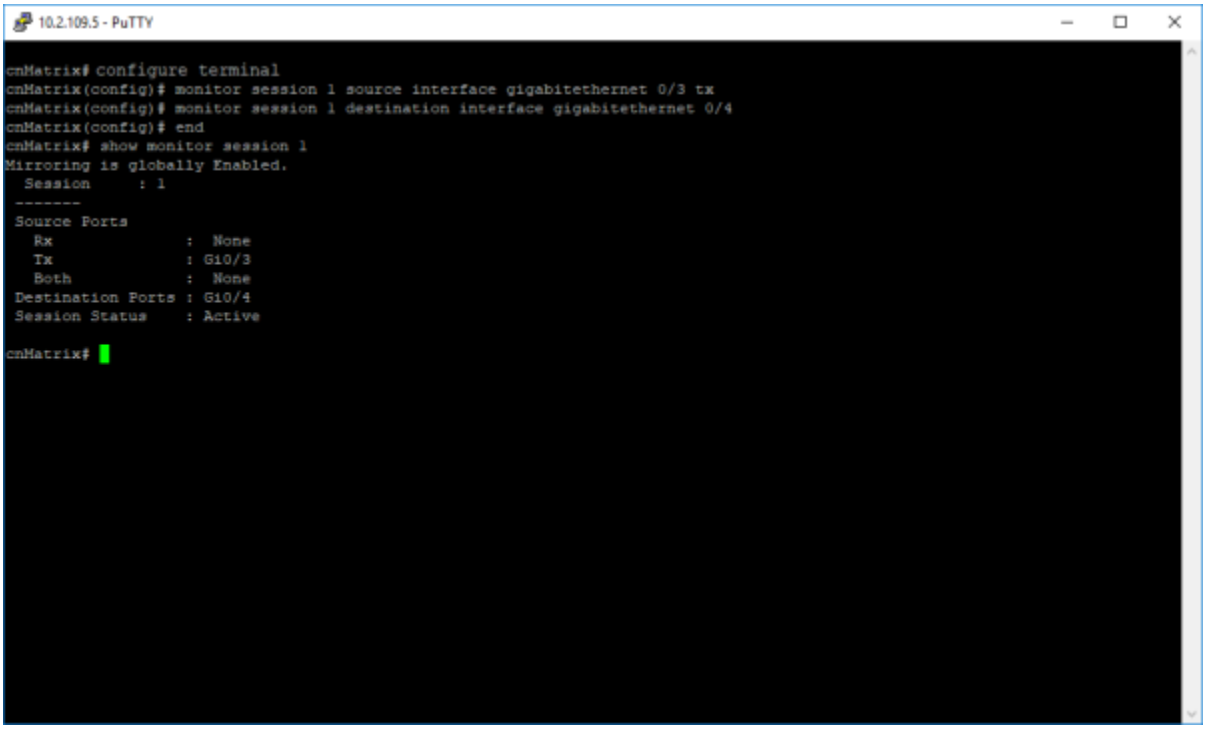
Destination port:

- Can be any Ethernet physical 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.

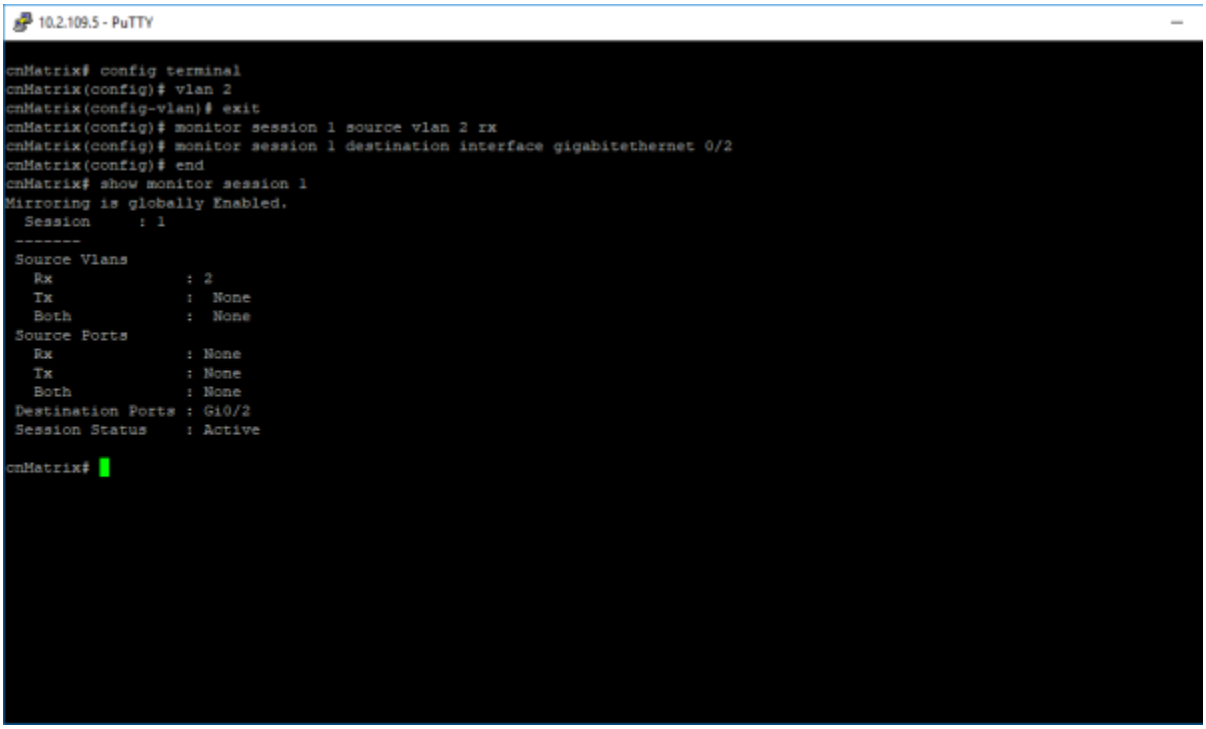
Configuring Port Mirroring - Port Based in CLI Interface (Example)



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.

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



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

1. Type the **vlan 2** command into the terminal to configure a VLAN. Press the **Enter** key.
2. Type the **exit** command into the terminal. Press the **Enter** key.
3. 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.
4. 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.
5. Type the **end** command into the terminal to back to the Privileged EXEC mode. Press the **Enter** key.
6. Type the **show monitor session 1** command into the terminal. Press the **Enter** key.

For more information, see Port Mirroring Parameters and Commands.

Troubleshooting Port Mirroring

Useful commands for troubleshooting:

- cnMatrix# show monitor session all

Cable Diagnostics

Managing Cable Diagnostics

Feature overview

The cable diagnostics feature offers the possibility to locate and characterize faults in ethernet cables by using time-domain reflectometry. A cable diagnostics test verifies the status of all the four twisted pairs of an ethernet cable and displays the results for each of them. The status for each pair can be one of the following: **OK**, **Pair Open**, **Same Pair**

Short, **Cross Pair Short**, **Pair Busy**, and **Test in Progress**. The cable diagnostics test also determines the distance in meters at which the fault occurs. A time stamp is also attached to each test to know when they were performed.

Note

The cable diagnostics feature can be configured via CLI, Web, and SNMP.

Attention

Cable diagnostics capable switch is supported starting with cnMatrix release 4.0.

A cable diagnostics test will cause a loss of link for several seconds on that interface.

If a cable diagnostics test is started on an interface that has no cable connected then the status on that interface will become **Test in Progress**. It will remain with that status until a cable is connected so the test can run its course. This does not affect the linking capabilities of that interface.

Standards

N/A.

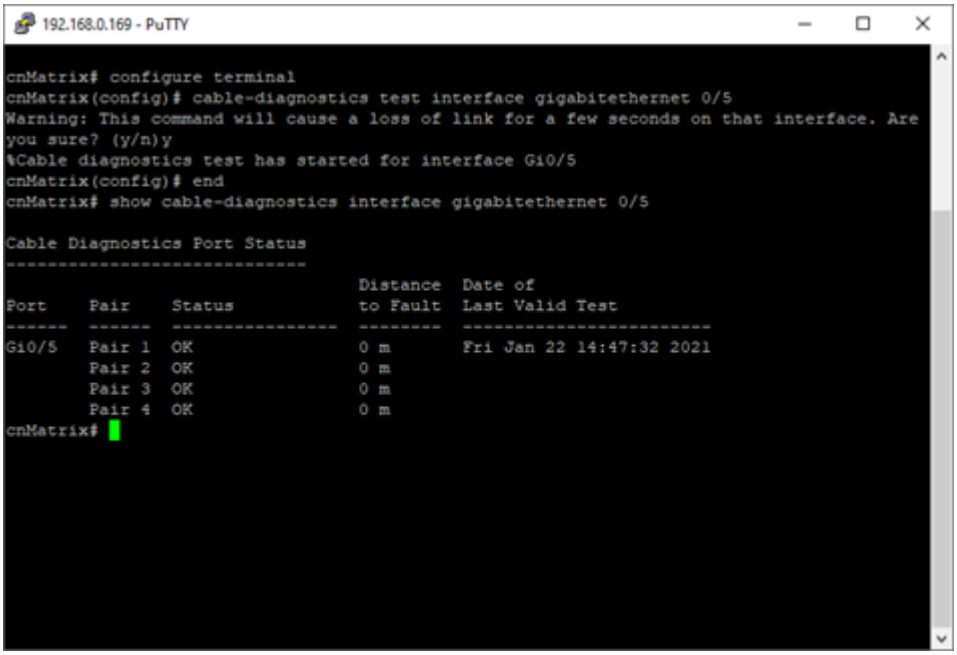
Limitations

- Cable diagnostics is supported only on copper-ports.
- For EX2016M-P cable diagnostics is not supported on the 2.5G ports (the last six copper-ports).
- Only one interface can be tested at one time.

Default Values

- All interfaces have status None.

How to start a Cable Diagnostics test



1. Connect the test cable to the cnMatrix interface 0/5. The other end of the test cable must also be connected to a network device.
2. Type the **configure terminal** command into the terminal. Press the **Enter** key.
3. Type the **cable-diagnostics test interface gigabitethernet 0/5** command into the terminal to start the test. Press the **Enter** key.
4. Read the **Warning** message. If you want to continue type **y**, **yes**, **Y** or **YES** into the terminal.
5. Type the **show cable-diagnostics interface gigabitethernet 0/5** command into the terminal to display cable diagnostics test results. Press the **Enter** key.

Note

The **Warning** message can be overridden by using the **force** parameter at the end of the command.

Example: **cnMatrix(config)# cable-diagnostics test interface gigabitethernet 0/5 force**.

Troubleshooting Cable Diagnostics

Useful command for troubleshooting:

- cnMatrix# **show cable-diagnostics**

Storm Control

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 broadcast, 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 100pkts/sec.

Default Values

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

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.

Quality of Service

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 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 is 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.

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 does not 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.

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 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.

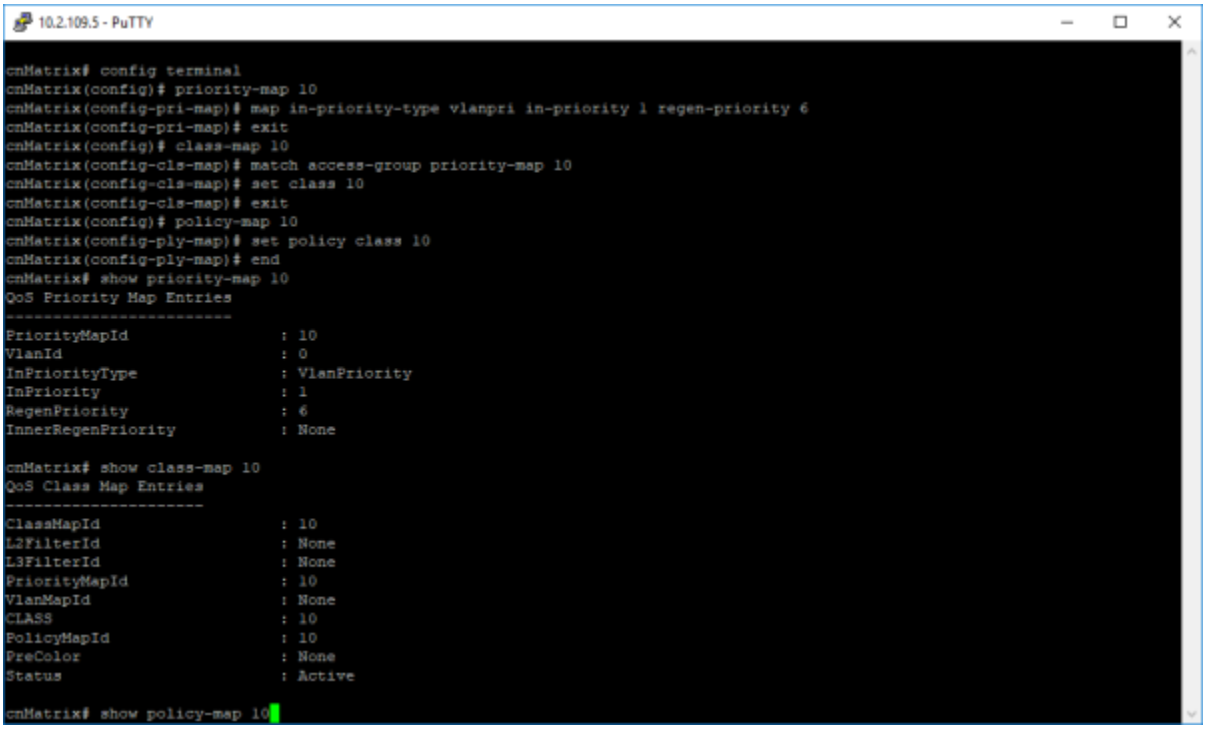
Limitations

- 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 the 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.

Remarking with Priority Maps (QoS)

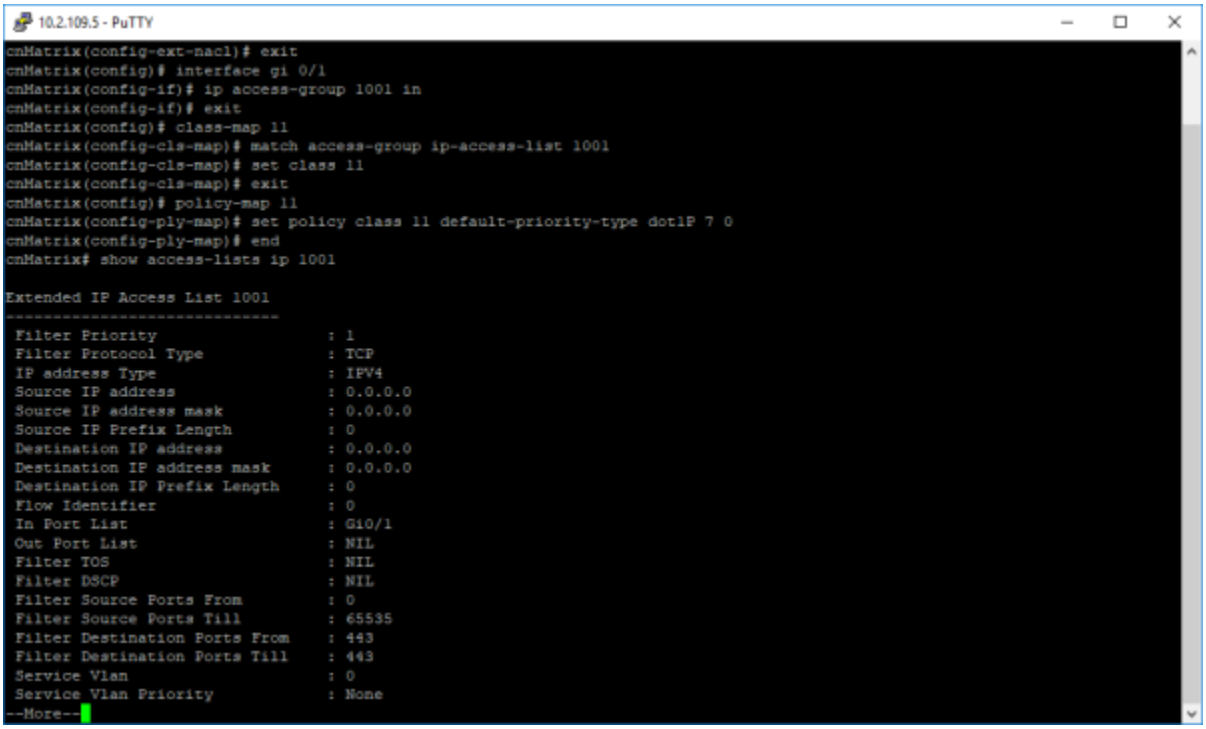


1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **priority-map 10** command into the terminal to add a priority map entry. Press the **Enter** key.
3. Type the **map in-priority-type vlanpri in-priority 1 regen-priority 6** command into the terminal (mapping 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.
13. Type the **config terminal** command into the terminal. Press the Enter key
14. Type **interface gi 0/1** command into the terminal to specify the interface to be configured. Press the Enter key.
15. Type **switchport mode trunk** command into the terminal to configure port as trunk. Press the Enter key.
16. Type **qos trust dot1p** command into the terminal to set qos trust mode as dot1p. Press the Enter key.
17. Type **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
18. Type **interface gi 0/2** command into the terminal to specify the interface to be configured. Press the Enter key.
19. Type **switch-port mode trunk** command into the terminal to configure port as trunk. Press the Enter key.
20. Type **exit** command into the terminal to go back to the configuration mode. Press the Enter key.
21. Traffic with dot1p 1 coming from port 1 will egress with dot1p 6.

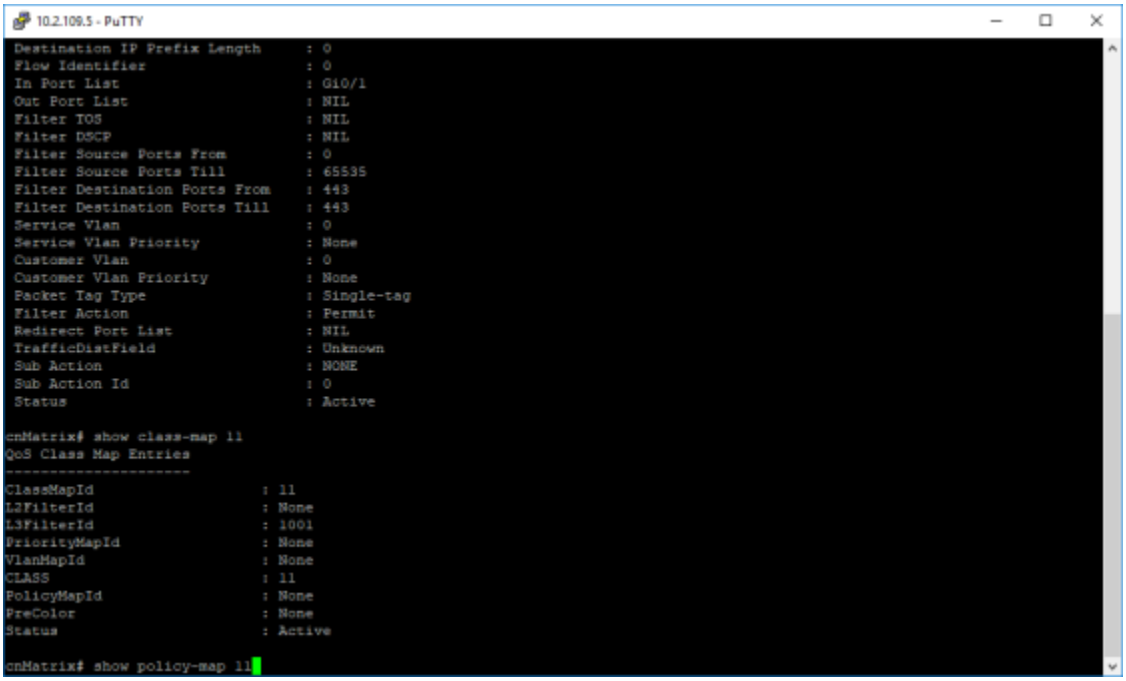
For more information, see QoS Parameters and Commands.

Remarking with ACL (QoS)



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 specify the interface to be configured. Press the **Enter** key.

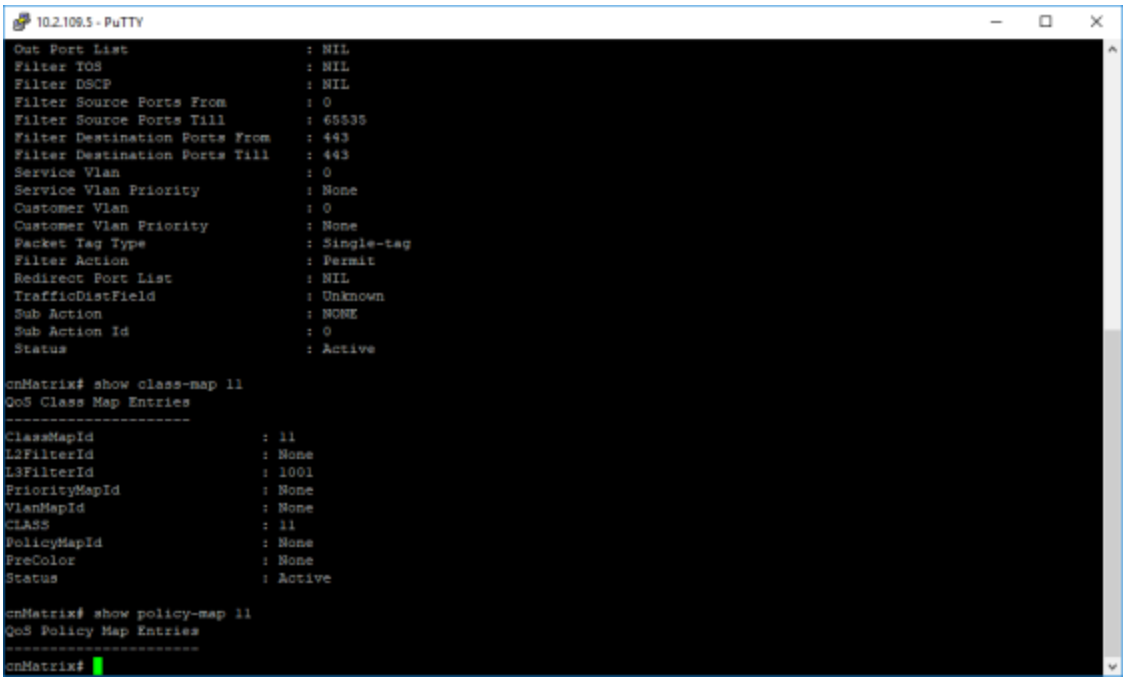
6. Type the **ip access-group 1001 in** command into the terminal to apply ACL on inbound packets. Press the **Enter** key.
7. Type the **exit** command into the terminal to go back to the configuration mode. Press the **Enter** key.
8. Type the **class-map 11** command into the terminal to add a class 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. Type the **show class-map 11** command into the terminal to display the QoS class map entries. Press the **Enter** key.
17. Type the **show policy-map 11** command into the terminal to display the QoS policy map entries. Press the **Enter** key.

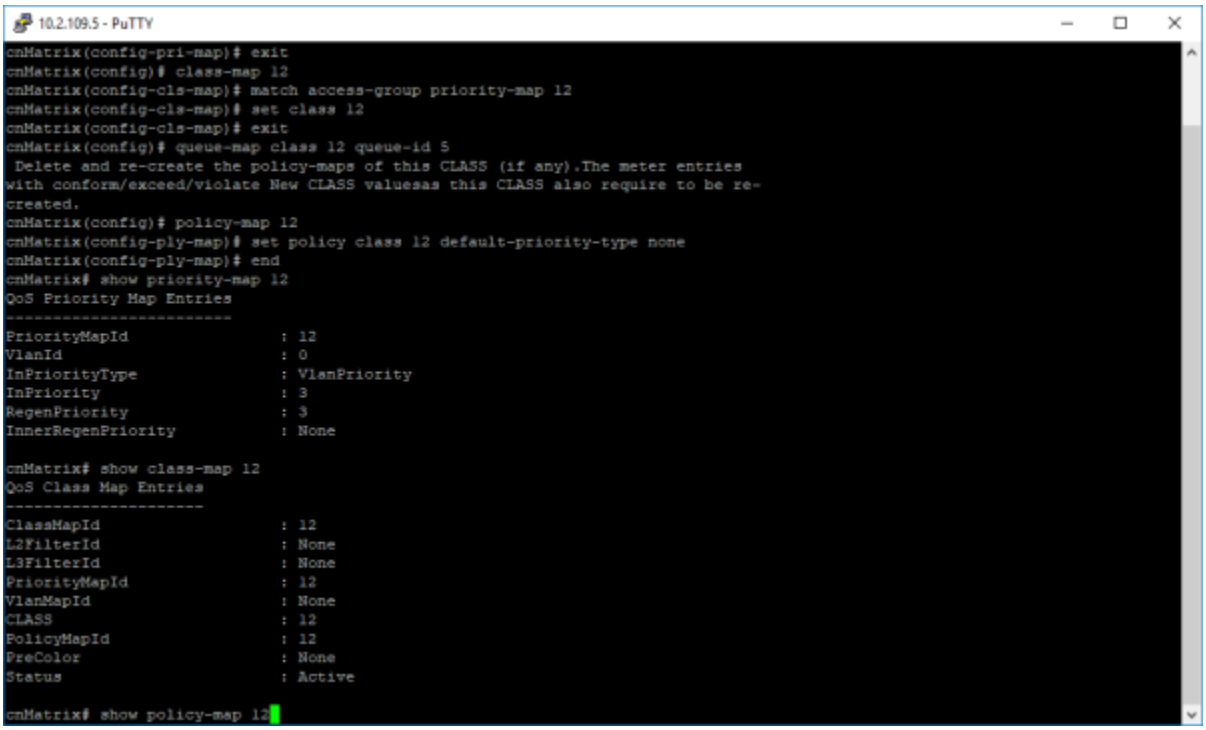
Note

In order for the traffic to show the modified dot1p value, the egress port has to be configured as trunk or hybrid, in order to keep the VLAN tag upon egressing the switch.



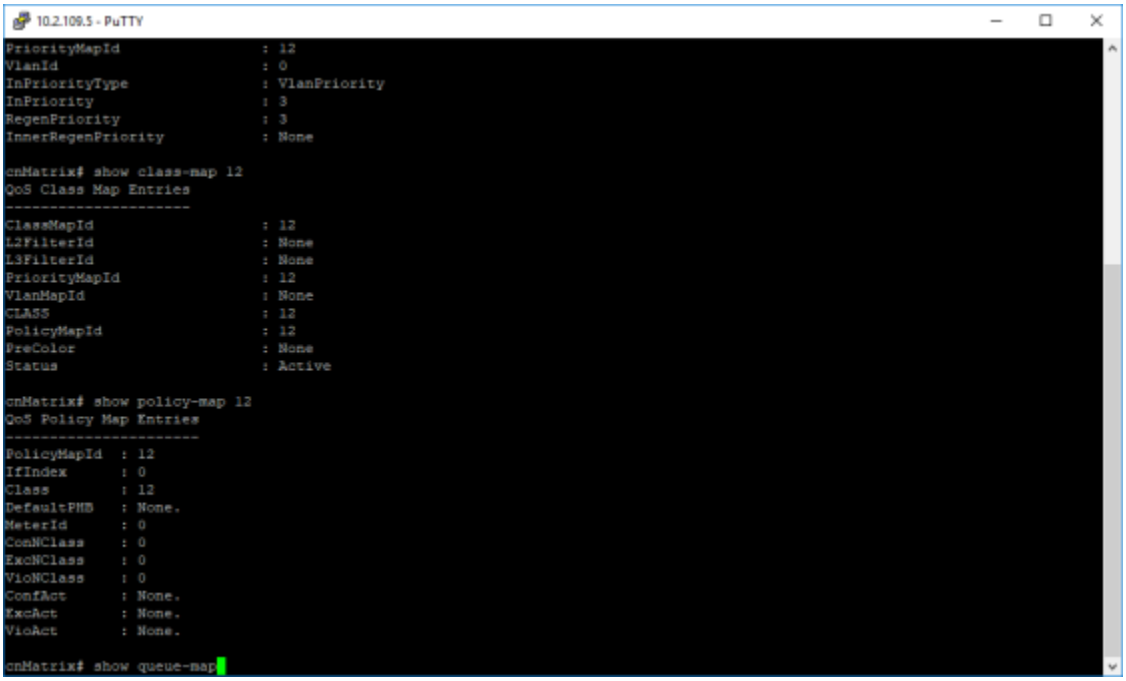
For more information, see QoS Parameters and Commands.

Queue Map(QoS)

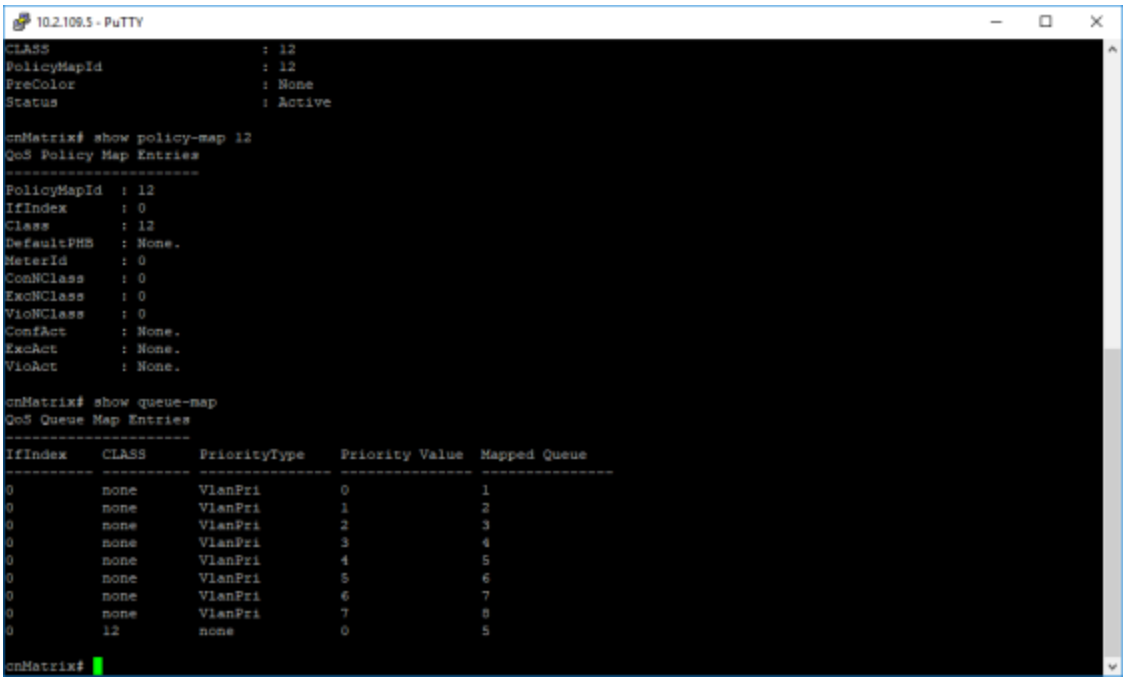


1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **priority-map 12** command into the terminal to add the priority map ID. Press the **Enter** key.
3. Type the **map in-priority-type vlanPri in-priority 3 regen-priority 3** command into the terminal to set 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 priority 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.

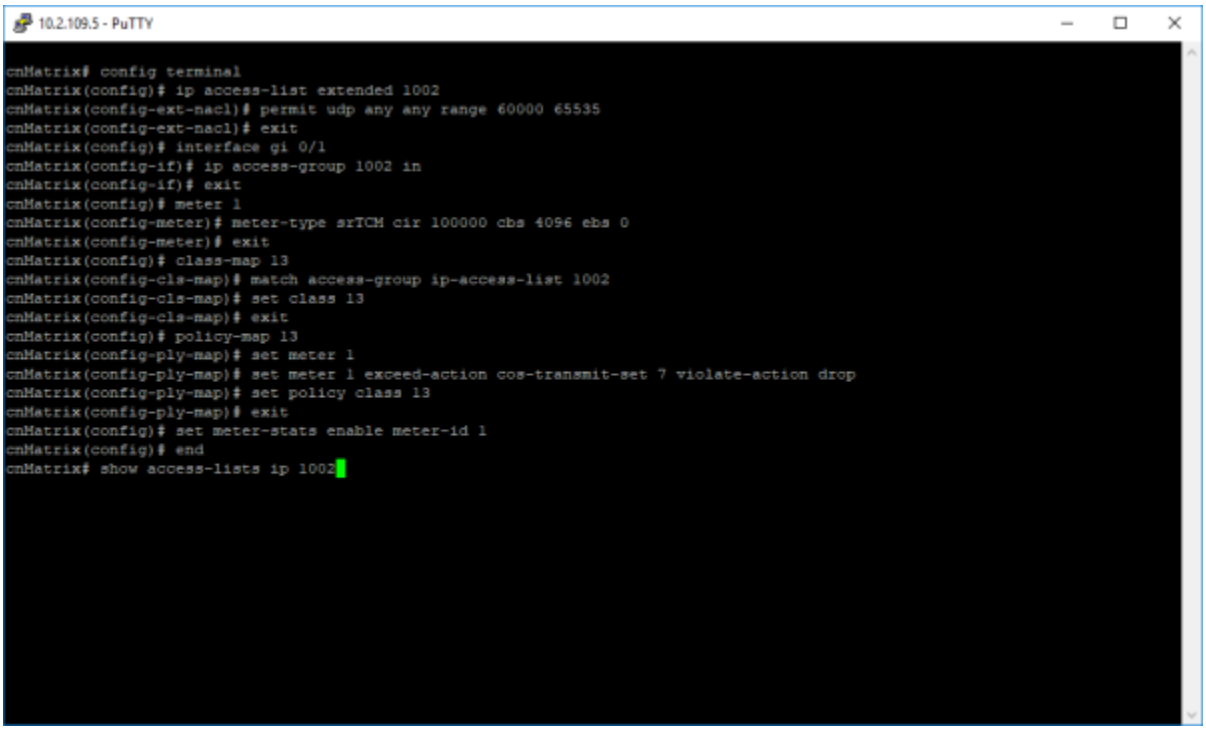


16. Type the **show queue-map** into the terminal to display the queue map entries. Press the **Enter** key.



For more information, see QoS Parameters and Commands.

Ingress Metering with ACL + Enable Metering(QoS)



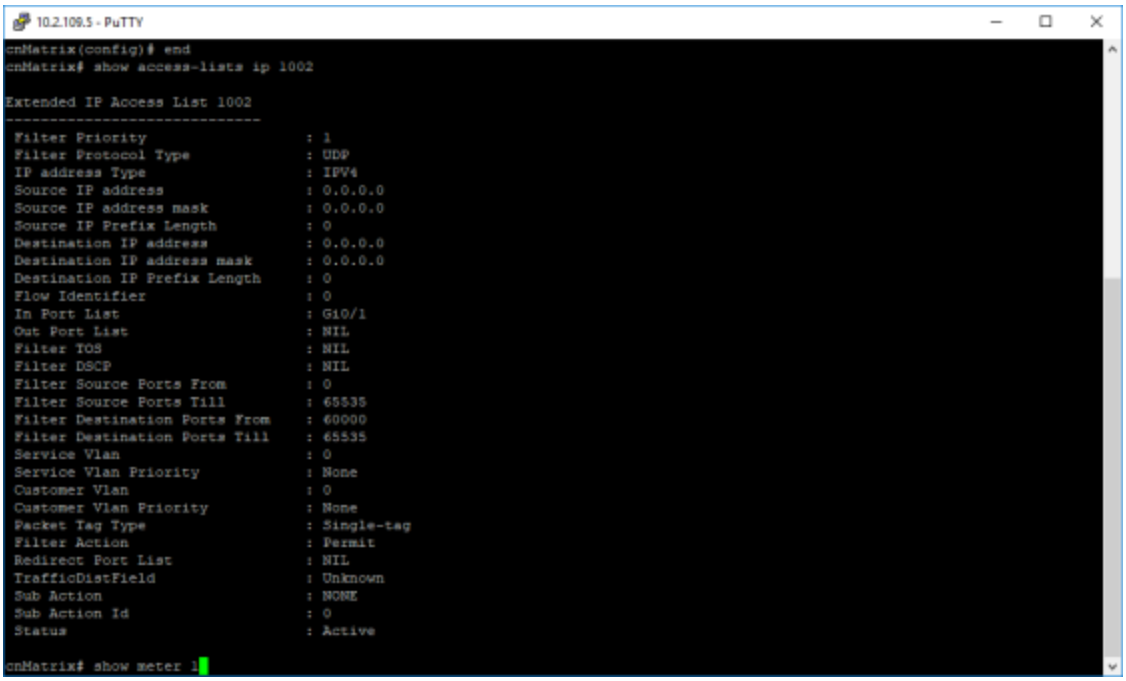
1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **ip access-list extended 1002** command into the terminal to create an IP access-list. Press the **Enter** key.
3. Type the **permit udp any any range 60000 65535** command into the terminal to specify the 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 ACL 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 ACL 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 outgoing 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.

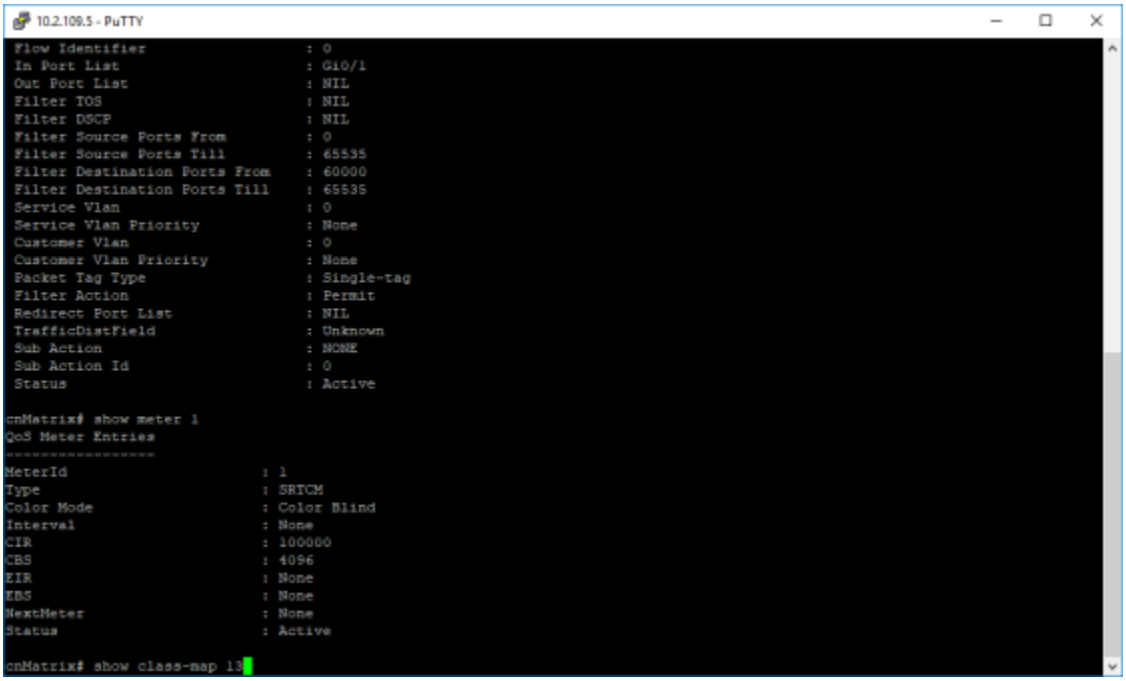
Note

Starting with version 2.1, this command has been removed. The meters stats are now enabled by default.

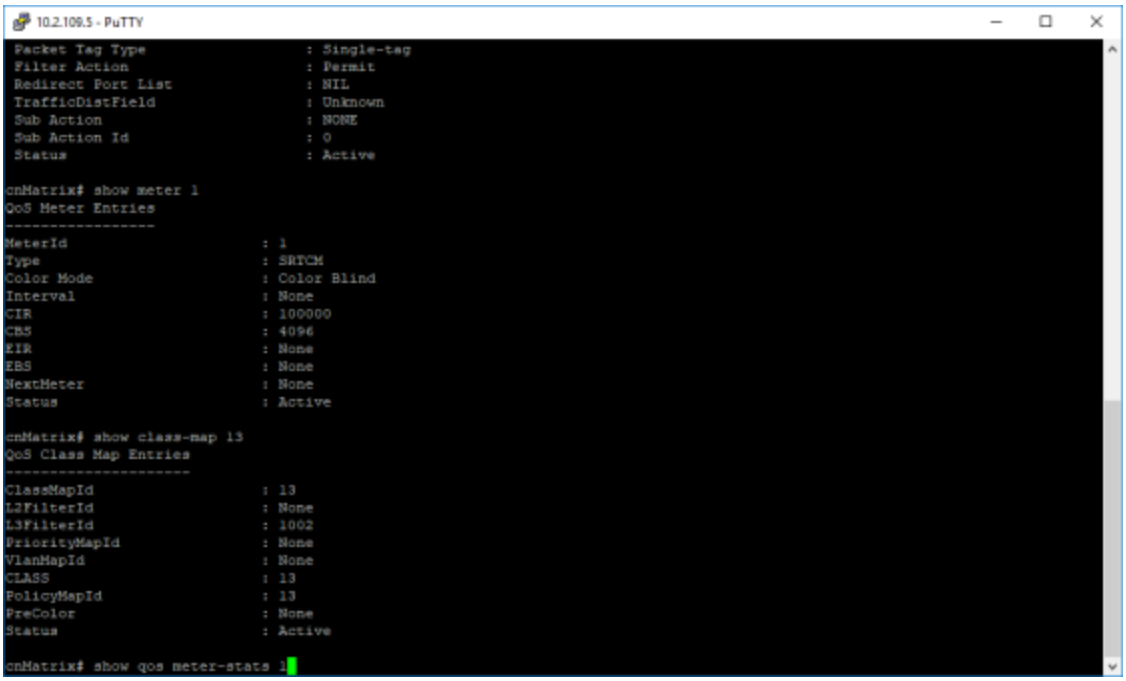
21. Type the **end** into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.
22. Type the **show access-lists ip 1002** command into the terminal to display the configured IP access list. Press the **Enter** key.



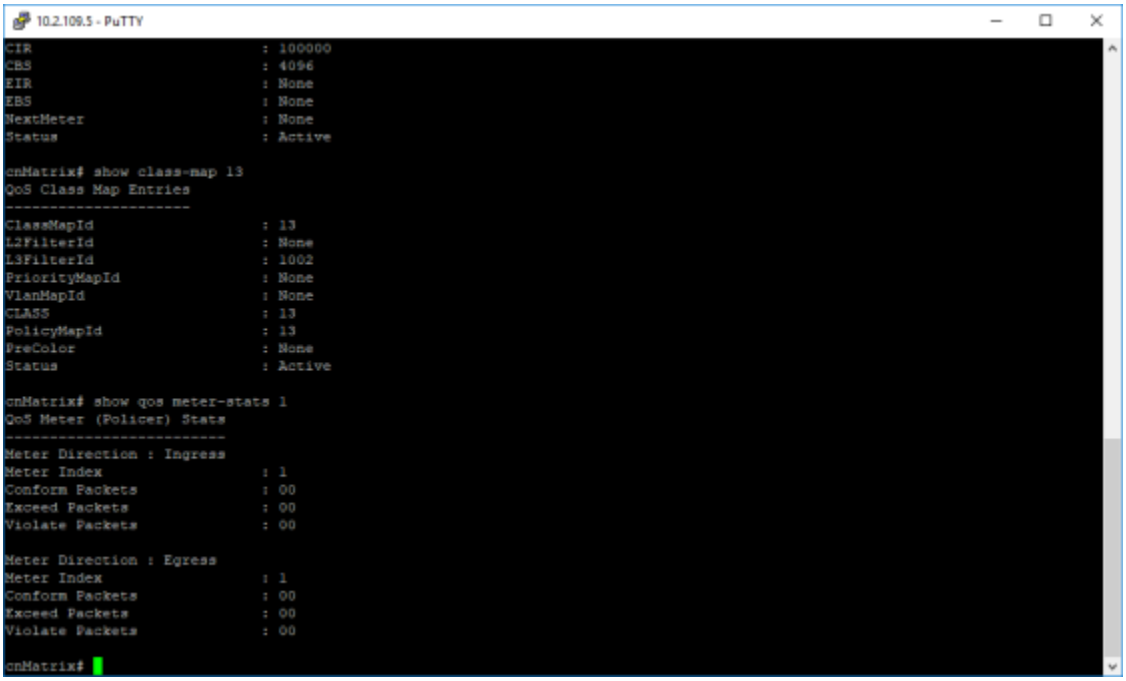
23. Press the **Enter** key.
24. Type the **show meter 1** command into the terminal to display the QoS meter entries. Press the **Enter** key.



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

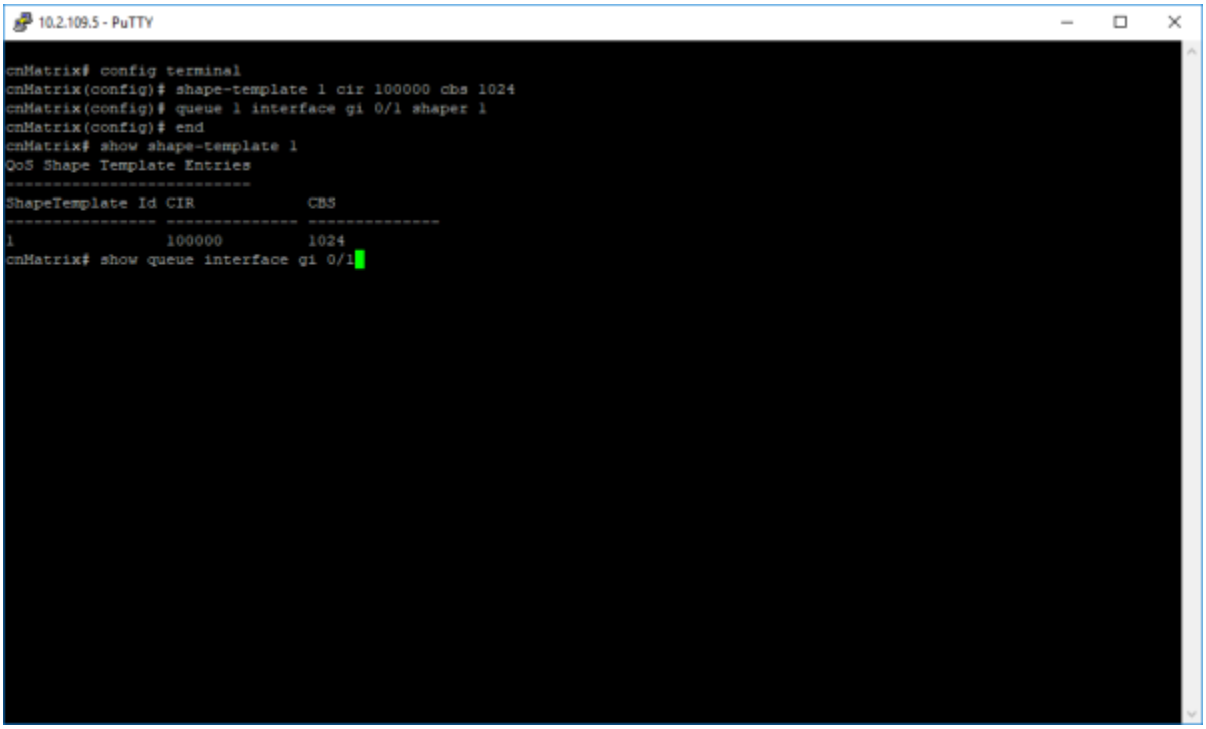


26. Type the **show qos meter-stats 1** command into the terminal to display the meter (policer) stats. Press the **Enter** key.



For more information, see QoS Parameters and Commands.

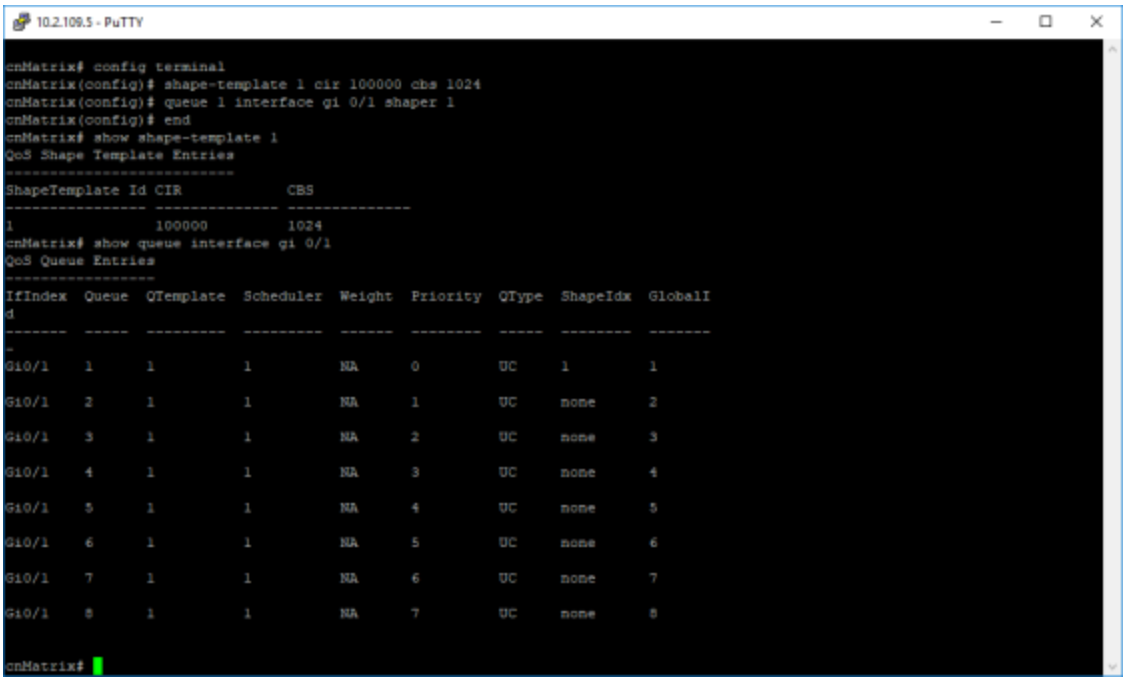
Queues + Shapers (QoS)



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

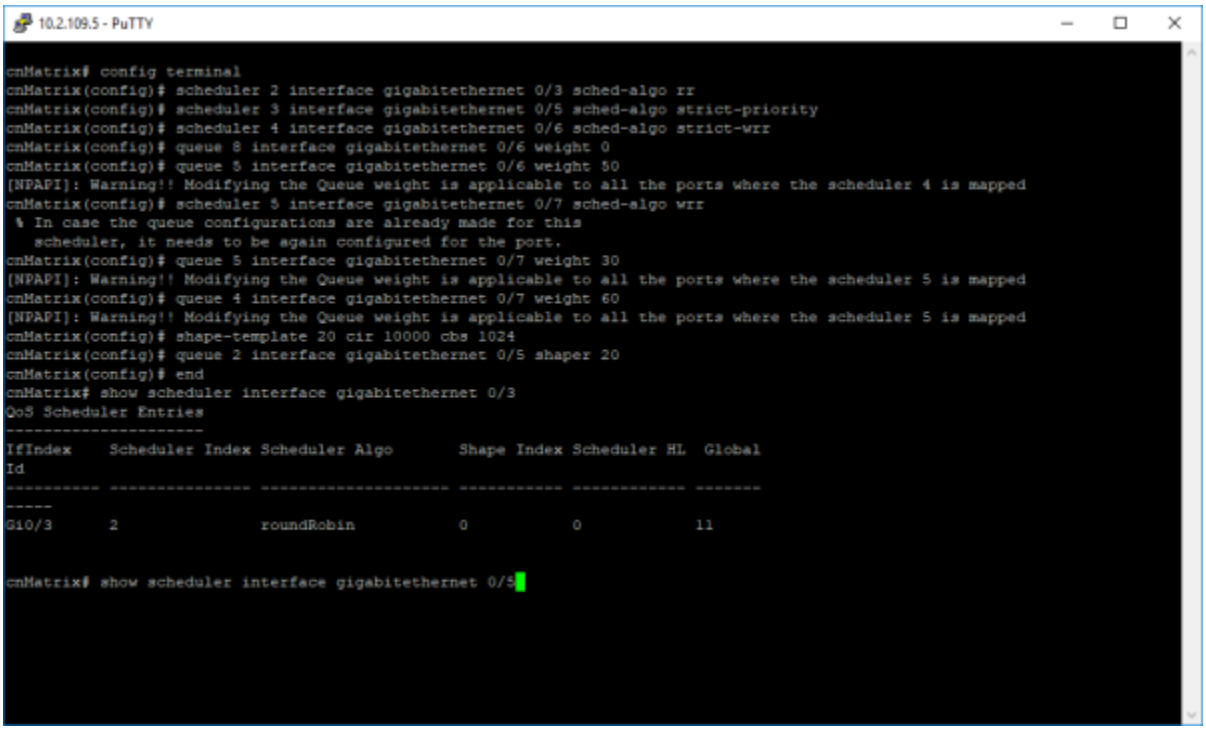
> Note
>
> On **EX3024F** units only, the max value for CBS is 1023, for other devices it is 4095.

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.

Configuring Schedulers (QoS)



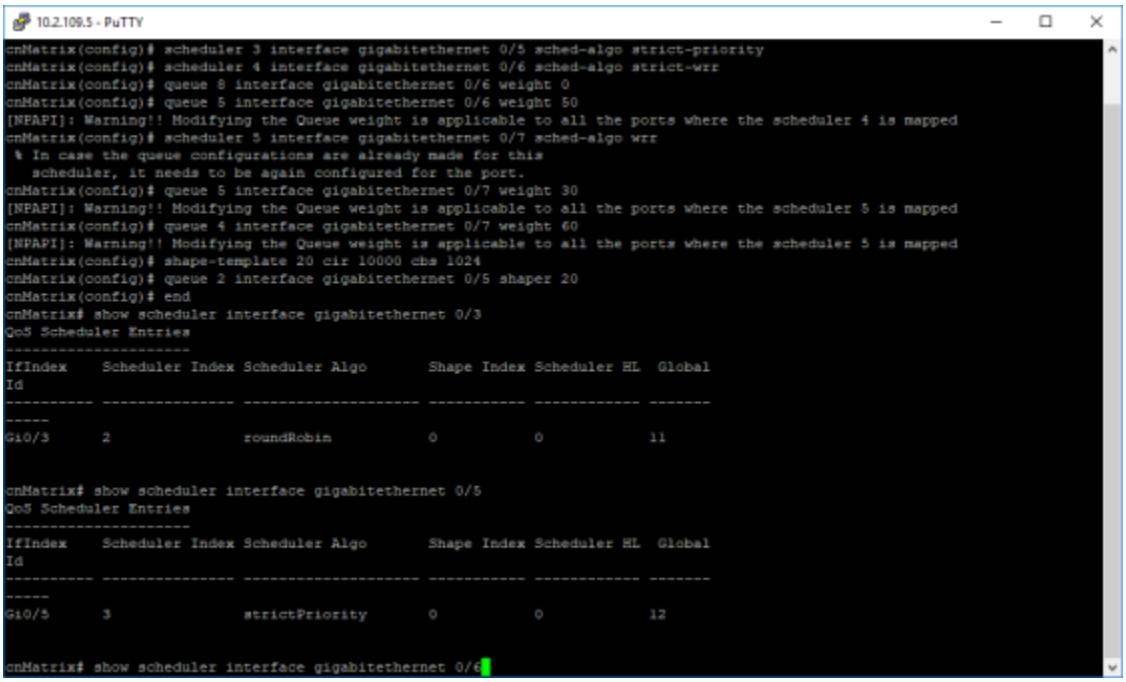
1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **scheduler 2 interface gigabitethernet 0/3 sched-algo rr** command into the terminal to create the scheduler 2 on a certain interface and to configure the packet scheduling algorithm as round robin. Press 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.

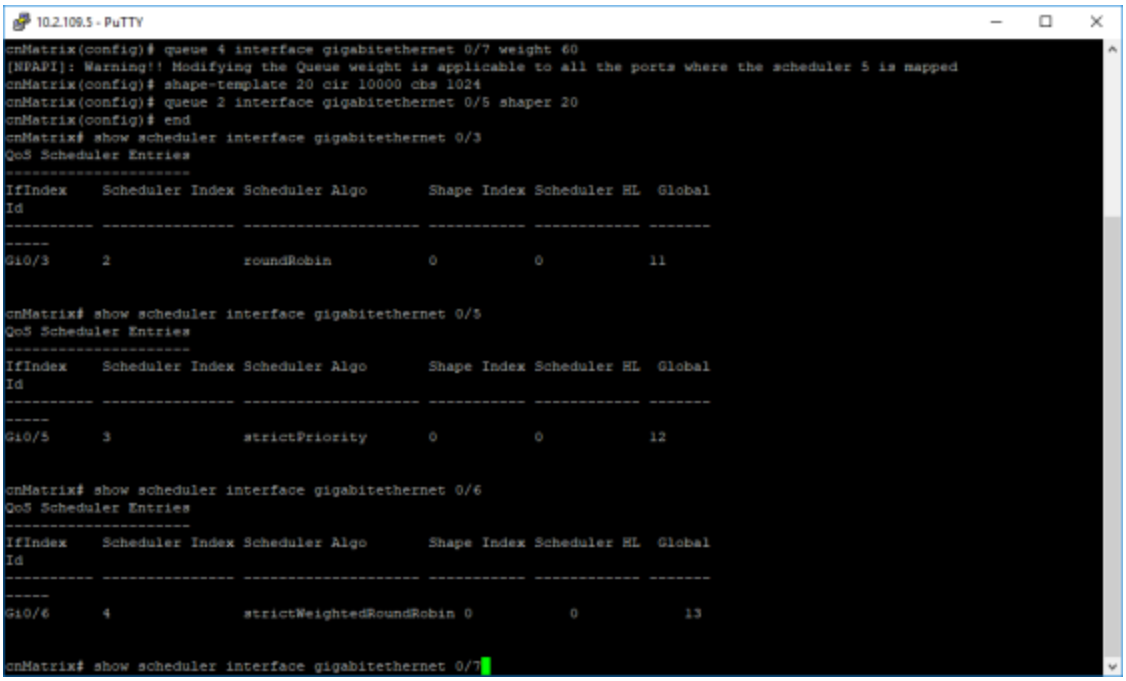
Note

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

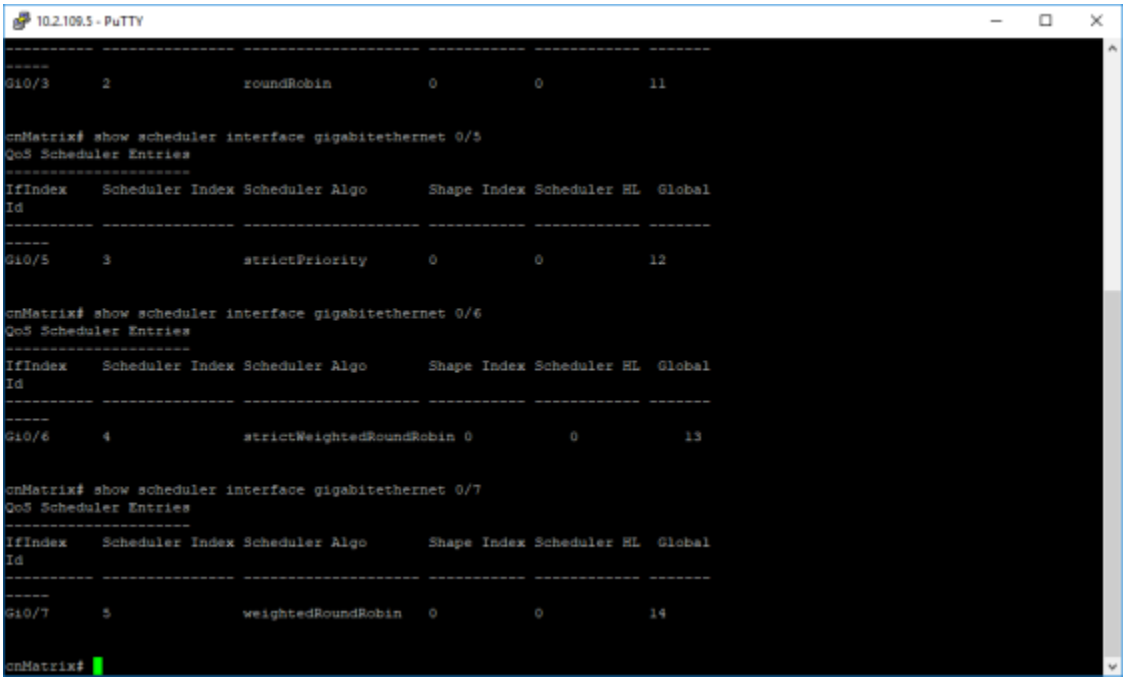
6. Type the **queue 5 interface gigabitethernet 0/6 weight 50** command into the terminal. Press the **Enter** key.
7. Type the **scheduler 5 interface gigabitethernet 0/7 sched-algo wrr** command into the terminal. Press the **Enter** key.
8. Type the **queue 5 interface gigabitethernet 0/7 weight 30** 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.

Rate-Limit-Output

Managing Rate-Limit-Output (Example)

The R**ate-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

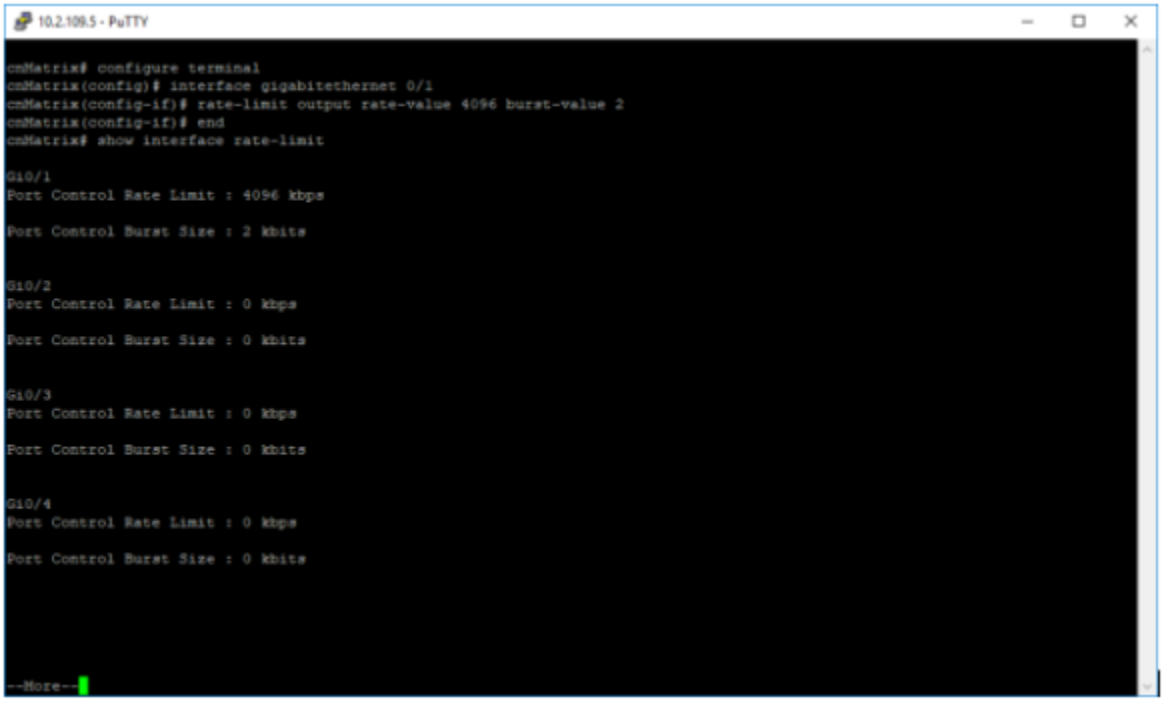
Limitations

N/A

Default Values

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

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 the rate-limit and burst size are displayed in the output with the previously configured values). Press the **Enter** key.

Rate-Limit-Input

Managing Rate-Limit-Input (Example)

The **Rate-Limit-Input** feature limits the ingress traffic of the switch on a port by using ACL's to capture any traffic that ingresses that port and a meter to limit the traffic based on the configured rate in kilobytes.

Standards

N/A

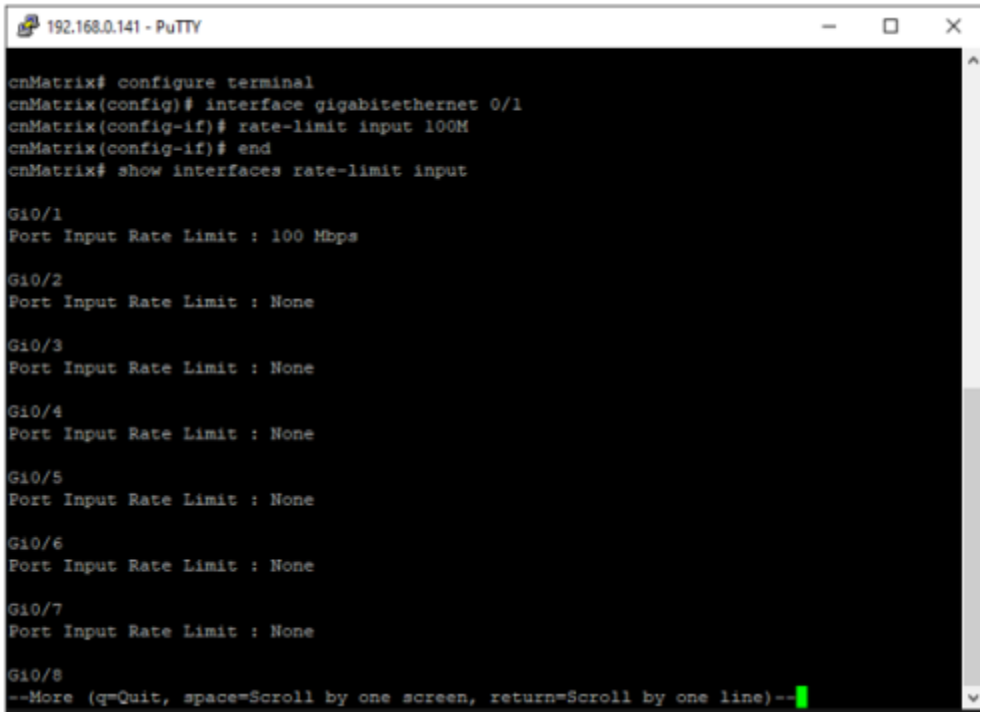
Scaling Numbers

N/A

Default Values

By default, Rate-Limit-Input is not configured

Configuring Rate-Limit-Input 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 input 100M** command into the terminal to configure the rate-limiting 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 input** into the terminal to display the interface status and configurations (verify if rate-limit is displayed in the output with the previously configured values). Press the **Enter** key.

cnMatrix Rate-Limit-Output Parameters and Commands

Commands	Description	CLI Mode
rate-limit output [<rate-value>] [<burst-value>] Available options: • rate-value - Configures the maximum rate (in kbps) at which packets can be sent out through the interface. • burst-value - Configures the burst size in kilobytes with which the rate is to be implemented.	Enables the rate-limiting and burst size rate limiting by configuring the egress packet rate of an interface.	Interface Configuration (Physical Interface)

Policy Based Automation with Dynamic Configuration

Managing Policy Based Automation Using Auto Attach

Feature Overview

The core goal of the Policy Based Automation (PBA) 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 the 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).

Policy Based Automation is intended to overcome the burden of constant manual reconfiguration. End-devices are automatically detected based on specific device criteria (e.g., MAC address, LLDP device identification data) and device-specific settings are automatically installed or updated based on predefined PBA/AA 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.
- Default port 802.1p user priority value.
- Default port QoS mode (Trusted/Untrusted).
- PoE port priority.
- Protected port status.
- Port speed and negotiation characteristics.

- Cambium-Sync status.
- Default uplink interfaces.
- Automatic Device Recovery (ADR) status.
- Automatic VoIP configuration.
- DHCP Snooping trust status.
- STP Portfast operation.
- Static VLAN exclusion.

When an end-device is detected on a port, PBA is passed to the device data (e.g., MAC address, LLDP-based device data) and the ingress port. If the end-device data matches device identification criteria in a configured PBA policy, the associated PBA 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, MAC aging) or when the switch reboots.

PBA/AA 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
- PBA Monitoring/Configuration
    - CLI
    - SNMP

PBA/AA Release 2.1.0 Capabilities

- Device Identification
- LLDP Core TLVs (user-specified string matching of TLV data)
    - Management Address (TLV Type 8)
- MAC address match
    - Single MAC (exact MAC address match)
    - MAC address range (searching for MAC address in a configured range)
    - MAC-OUI
- Dynamic Actions
    - Switch port mode (Access/Hybrid/Trunk) update
    - Default port QoS mode (Trusted/Untrusted) update
    - Default port 802.1 user priority update
    - VLAN membership update for uplink ports
    - Establish port PoE priority
    - Automatic interface description updates
- PBA Monitoring/Configuration
    - Web GUI

PBA/AA Release 3.0.1 Capabilities

- Device Identification

        - Dynamic policy reordering based on PBA policy precedence
        - Customizable MAC address match restrictions
            - Restricted MAC address matching
            - MAC address match lockdown
- PBA Monitoring/Configuration
    - cnMaestro Cloud and on-premise support

PBA/AA Release 3.1 Capabilities

- Auto-VLAN support
    - Introduction of Cambium proprietary PBA LLDP TLVs supporting automatic VLAN configuration by connected Cambium devices.

PBA/AA Release 3.2 Capabilities

- Device Identification
    - Default PBA rule/policy support
- Dynamic Actions
    - Interface bounce following a Native VLAN update
    - Action modification support
    - Protected port status update
    - Global (default) uplink definition
- PBA Monitoring/Configuration
    - XMS-Cloud support

PBA/AA Release 4.0 Capabilities

- Device Identification
    - Rule combination support
- Dynamic Actions
    - Cambium-Sync status update
    - Port speed and negotiation characteristics update
- • Global Auto-VLAN status update

PBA/AA Release 4.1 Capabilities

- Dynamic Actions
    - Automatic Device Recovery (ADR)

PBA/AA Release 4.2 Capabilities

- Dynamic Actions
    - Automated VoIP support
- Dynamic-to-static PBA settings update support

PBA/AA Release 4.4 Capabilities

- Device Identification
    - Rule modification support
    - LLDP-ANY match criteria update (search all PBA-supported LLDP string-based TLVs)
- PBA Policy Enhancements
    - Port-specific policy definition
    - Policy modification support

PBA/AA Release 4.5 Capabilities

- Device Identification
  - MAC address list support
- Dynamic Actions
  - Support for localized actions
- PBA Policy Enhancements
  - Dynamic action selection based on the device localization setting
- Switch localization configuration
- PBA MAC list file support

PBA/AA Release 5.0 Capabilities

- Dynamic Actions
  - VLAN range support
  - Increased VLAN count (maximum increased to 200)
- PBA Policy Enhancements
  - VLAN range support
- PBA MAC list file support for MAC OUIs
- Per-port restricted MAC match control

PBA/AA Release 6.1 Capabilities

- Dynamic Actions
  - DHCP Snooping trust state
  - STP Portfast status
  - Static VLAN exclusion
- PBA Policy Enhancements
  - Time-of-Day policy control (enable/disable)
  - Extended history
- Time-of-Day (ToD) capabilities
- Auto-VLAN extensions

Feature Overview

- **Release 2.0.1**
  - Device Identification
    - Core LLDP TLVs are supported for device discovery (standard required LLDP TLVs Chassis ID, Port ID, and standard optional LLDP TLVs Port Description, System Name, System Description, System Capabilities).
    - MAC-based device detection is not supported.
    - Active PBA policies are only cleared when they are no longer applicable (the precedence of other applicable PBA policies are not taken into account following initial policy installation).
  - Dynamic Actions
    - VLAN creation, VLAN port memberships, and native VLAN (PVID) update.
    - Switch port mode updates are limited to hybrid and updates are static if data is saved by the user while dynamic updates are present.
  - Limitations
    - 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.
    - CLI and SNMP PBA support is available. No support for PBA when using the Web GUI.
    - cnMaestro template support is available. No GUI support is available.
    - Auto Attach agent cannot run while Spanning Tree mode PVRST is enabled.
- **Release 3.0.0**

- Device Identification
    - LLDP core (standard optional) Management Address TLV is supported.
    - MAC address matching options are supported for device detection.
        - Single MAC (exact MAC address match).
        - MAC address range (match MAC addresses that fall within a configured range).
        - MAC-OUI (match MAC addresses with a specific OUI value).
    - A defined PBA policy can be enabled or disabled by the administrator. A policy is enabled by default. Disabling a policy that is active immediately clears dynamic updates that were initiated when the policy was applied. Disabled policies are ignored during policy evaluation.
- Dynamic Actions
    - 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 is required. 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 cannot 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.
    - Automatic interface description updates can (optionally) be initiated when a PBA policy is applied to a port. The user may select the information used to update the port description.
- Limitations
    - 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 cannot 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.

- **Release 3.0.1**
    - Device Identification
    - Deletion of active PBA policies is supported. Previously, a referenced (active) policy could only be deleted when it was no longer applied to a port. This potentially required the user to take the port down, disable PBA on the port or disable PBA for the switch overall. The requirement has been eliminated.
    - Dynamic policy reordering based on PBA policy precedence is available. This configurable option (enabled/disabled) allows PBA policies with higher precedence to replace currently active PBA policies with lower evaluation precedence when both are applicable to the discovered device. Active policy reordering is enabled by default.
    - MAC address matching support can be customized for the environment to prevent matching devices that are not directly connected. cnMatrix Release 2.1.0 MAC address-based policy matching will match MAC addresses that are not directly connected. In a bridged network with address flooding, this can result in PBA policies being applied on potentially unexpected ports.

The updated support allows the user to select whether the current PBA MAC address-based policy operation is suitable for their environment or if restricted MAC matching (targeting MACs of directly connected devices only) is required.

- A user configurable PBA setting is defined to control whether restricted MAC matching is enabled or disabled (restricted MAC matching is enabled by default).
- New rules are enforced when evaluating whether PBA MAC-based policies should be applied based on FDB events (enforced when restricted MAC matching is enabled):
  1. Do not apply MAC-based policies on switchport mode 'trunks'.
  2. Ports with only one learnt MAC address are permitted to have policies that match the MAC data be applied.
  3. Ports with more than one learnt MAC are only allowed to have a policy applied that matches the MAC address data that is the source MAC of the LLDPDU received on the port. If no LLDP data is present, matches are not allowed.

- MAC address-based policy lockdown is available. MAC-based policies are permitted to remain active after the associated MAC address has been aged from the FDB. The goal is to support devices that go to sleep or do not send traffic frequently and get removed from the FDB. Continual removal and reinstallation of policies for these types of devices is non-optimal because this results in a certain amount of traffic loss each time. The user can determine the behavior they prefer (i.e., clear policies based on MAC address aging or leave the policies temporarily applied) based on the devices they connect.
  - Default behavior will be to NOT age MAC-based policies.
  - MAC-based policies that are not aged will be removed upon a link-down or for any other PBA event just as they are in prior releases (e.g., PBA disable, PBA port disable, policy delete/disable).
  - A new configurable option allows the user to age or not age MAC-based policies so that the behavior can be customized to the user's connected devices.
- **Release 3.1**
  - Auto-VLAN support
    - New Cambium vendor-specific LLDP TLVs are introduced to support automatic VLAN configuration on cnMatrix for directly connected Cambium devices (e.g., cnPilot). The new PBA TLVs are implemented as an extension to the LLDP standard, using its flexible extension mechanism. They are implemented as vendor-specific (Cambium OUI: 58-C1-7A) TLVs using TLV type 127 as described in the 802.1ab (LLDP) standard. Two new TLVs have been defined:
      - PBA Authentication TLV – used by cnMatrix to export current authentication-related data and settings for use by attached Cambium devices.
      - PBA Device Settings TLV – used by Cambium devices leveraging PBA to export required PBA device settings (i.e., to push policies) to cnMatrix.

      From a functional perspective, cnMatrix, acting as the upstream device, includes the PBA Authentication TLV in the regularly generated LLDPDUs for a port. The PBA port operational status (enabled/disabled), the LLDP PBA Authentication TLV Tx status (enabled/disabled) and the state of the PBA application overall (enabled/disabled) impacts whether the TLV is included in LLDPDUs on a port. The downstream device (e.g., cnPilot) receives the PBA Authentication TLV and, if policy data is present to be pushed to cnMatrix, a PBA Device Settings TLV is constructed and added to the LLDPDU for the port.

      When received by cnMatrix, the PBA Device Setting TLV is authenticated (if necessary), decoded and the action components (VLAN list, native VLAN, state flags) are used to create a dynamic rule, action and policy that is applied to the port through which the TLV was received. The policy remains in effect until the LLDP port status changes (e.g., downstream neighbor LLDP data expires, PBA disabled on the port, link-down event), the policy data being pushed by the downstream neighbor changes (e.g., the VLAN list is updated) or a higher precedence PBA policy is determined to be applicable to the port.

      The Auto-VLAN support can be controlled on a per-port basis by enabling/disabling generation of the PBA LLDP TLVs using the port-based LLDP TLV selection support.

- **Release 3.2**

- Device Identification
    - Default policy support allows the user to define a policy that is automatically applied to a port on which one or more MAC addresses are learned, if no other PBA policies apply to the port (based on standard device detection capabilities such as LLDP data matching and MAC address matching). In essence, a default policy is assigned a precedence that is lower than any the user can specify. All user-defined policies therefore take precedence over the default policy when policy-matching device characteristics are present.
        - A single default policy can be defined by the user. A policy is designated as the "default" policy when the associated rule has the rule type 'default'.
        - Only one rule with the rule type 'default' can be defined.
        - Device detection data associated with the default rule is ignored.
        - Rule applicability is determined solely by the presence of learned MAC address data.
        - Restricted MAC matching rules do not apply to the default policy.
        - Precedence data associated with the "default" policy is ignored.
- Dynamic Actions
    - The ability to bounce (shutdown/no shutdown) a port on which a native VLAN (PVID) is updated when a PBA policy is applied to the port is available. This support is configurable on a per-action basis (using the 'reset-link' action modifier) and is disabled by default.
    - Both inactive and active (referenced by a PBA policy that is applied to a port) PBA action modifications are available. Modification of an active action causes the associated PBA policy to be bounced allowing the updated action criteria to be applied.
    - The VLAN 'protected' setting for a port (i.e., the protected port status) can be updated based on device discovery. The protected port status setting is restored to the previous statically configured value during the device cleanup phase.
    - The VLAN membership update for uplink ports action, introduced in the 2.1 release, allows the user to identify uplinks on a per-action basis. This support is also required for policies that are created dynamically, such as Auto-VLAN policies, and for those that include embedded action criteria.
        - The global uplink definition setting has the same semantics as the per-action uplink setting. 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 slot/port naming convention (e.g., 'Gi0/5,Ex0/1'). Uplink data is only processed if the associated policy includes VLAN data for port membership updates. Otherwise it is silently ignored.
        - Per-action uplink data takes precedence over global (default) uplink data. When a PBA policy is installed, if action uplink data isn't defined and global uplink data is defined, the global data is used to identify uplinks for dynamic VLAN membership. If both per-action and global uplink data is specified, the per-action uplink data is used.
        - Global uplink data is defined using the top-level 'auto-attach uplink' CLI command and through the Web Auto-Attach Basic Settings page.
- PBA Monitoring/Configuration
    - XMS-Cloud support is available for PBA monitoring and configuration starting with the XMS 10.3 release.

- **Release 4.0**
    - Device Identification
        - PBA Rule Combination support allows multiple distinct rules to be treated as a single unit during PBA policy evaluation. If a policy references a rule combination name (versus using rule criteria embedded in the policy itself) and not an individual rule name, the device matching criteria from all of the rule combination members is used when determining if the policy should be applied.
            - When defining a PBA rule, a rule combination name can be specified as well. The rule combination name is optional and no rule combination name (empty string) is the default value (i.e., no change from current operation). Rules that

have the same rule combination name are considered members of the same rule combination.
- Rule combination membership can be modified at any time, even if the rule combination criteria is being used by an active policy (i.e., a policy that is currently applied to a port). During evaluation of rules in a rule combination, the different match criteria is processed as a logical 'and'. All individual rules must match for the overall rule combination to be considered a match.
- Many PBA rule types (all LLDP TLV string-based options) can be included in the rule combination multiple times to support matching different data in a single LLDP TLV. For example, several non-contiguous strings in a device's System Description can be matched to support specialized device identification. Certain types of rules are naturally limited when it comes to rule combination membership:
  - No more than one instance of certain PBA LLDP rule types can be present in a rule combination (capabilities, IPv4 management address).
  - Only one MAC-based rule (MAC rule types oui, full, range) can be present in a rule combination.
  - The default rule cannot be present in a rule combination.
- Rule combination changes (rule additions/deletion) made to combinations that are currently referenced by an active PBA policy cause the policy to be bounced to allow the updated rule combination criteria to be applied appropriately. Note that the last member of a rule combination referenced by the policy definition cannot be deleted until the policy is deleted.

- Dynamic Actions
  - Cambium-Sync signal generation can be enabled/disabled on a per-port basis (on applicable devices) based on device discovery. The Cambium-Sync setting is restored to the previous statically configured value during the device cleanup phase. The Cambium-Sync setting is ignored for PBA actions that are applied to devices that do not support this signal generation capability.
  - The Port Speed action setting allows multiple port speed-related settings to be updated based on device discovery. Two groups of options are supported: negotiated and forced. Negotiated options enable auto-negotiation and update the advertised speed capabilities. All capabilities less than or equal to the specified speed are advertised (include half and full duplex for each speed if applicable). Forced options disable auto-negotiation and set the port speed statically to the specified speed. In all cases the port is bounced following the settings update to ensure the new values take effect.
    - All updated port speed settings are restored to the previous statically configured value during the device cleanup phase.
- The PBA Auto-VLAN support can be globally enabled/disabled. Disabling the Auto-VLAN support clears all currently installed Auto-VLAN data (e.g., dynamic PBA rules/actions/policies and related settings updates) and blocks further processing of received Auto-VLAN PBA TLV data. Auto-VLAN support must be globally enabled before the per-port Auto-VLAN settings (e.g., PBA TLV status) impact Auto-VLAN PBA TLV processing.

- **Release 4.1**
  - Dynamic Actions
    - The LLDP Automatic Device Recovery (ADR) support initiates a PoE power toggle when a connected device's LLDP data expires. ADR must be enabled on a per-port basis. This setting can be dynamically controlled by PBA through the Automatic Device Recovery action.
- **Release 4.2**
  - Dynamic Actions
    - Automated VoIP support
      - With the introduction of the Automatic VoIP Configuration PBA action option, standard PBA operation can be used to identify connected VoIP devices and configure voice-related settings. When a PBA action is created/updated and the Automatic VoIP Configuration (Auto-VoIP) option is enabled, certain action options are automatically updated based on the current global voice VLAN settings:
        a. VLAN list – contains the voice VLAN and the data VLAN (if defined).
        b. Native VLAN – set based on the voice/data VLAN tagging status.
        c. Switch Port Mode – VoIP device ports are configured as Hybrid.
        d. QoS Trust – VoIP device ports are configured as 'dot1p' trusted.
        e. Uplink list – contains the voice VLAN uplink interface (if defined).

- If the user configures a value for any of these options, the value is overwritten based on the current global voice VLAN settings or the required VoIP device port setting:

  % Warning: Auto-VoIP PBA actions use global voice VLAN settings

- All other PBA options may be specified (based on platform applicability). A PBA Auto-VoIP policy (i.e., a PBA policy that references a PBA action with Auto-VoIP configuration enabled) is considered non-applicable/not-ready if the required global voice VLAN settings (i.e., the designated voice VLAN) are not defined.

- Previous releases restricted changes to settings that were temporarily under PBA control. These restrictions have been relaxed allowing dynamic settings to be updated by user configuration. Depending on the settings being updated, applied PBA policies may need to be reapplied to ensure the integrity of the configuration data.

- **Release 4.4**
  - Device Identification
    - PBA Rule modification is now supported. Rules that are referenced by an active PBA policy cause the policy to be reapplied (if still applicable) following the rule modification.
    - The LLDP-ANY rule type is enhanced to check all (PBA-supported) string-based LLDP TLVs for the target device identification data.
  - Policy Support
    - PBA Policy modification has been enhanced to allow the associated rule and/or action criteria to be updated without redefining the policy. Active policies are reapplied following modification, assuming they are still applicable.
    - PBA policy configuration allows the user to identify specific ports on which the policy can be applied. The effectively introduces a two-stage policy match: the associated rule criteria is first evaluated against the target device identification data. If a match is found, the policy port list is consulted to see if the device identification data was received through a port in the port list. If the port list is not empty, a port match is required for the policy to be applied. A port list is empty by default (i.e., with an empty port list policy behavior is the same as if previous releases).
- **Release 4.5**
  - Action Localization
    - PBA action localization allows the same PBA policies to apply different settings based on certain device characteristics (a.k.a. device localization). This simplifies policy definition (no need for multiple policies with different actions) and allows action criteria to be changed by updating the device localization data. Localization allows the user to design network-wide (represented by a cnMaestro switch group) PBA policies that can have their associated action settings (i.e., the action context) easily customized for specific devices as needed.
  - MAC List Support
    - PBA MAC list support allows PBA rules to be enhanced to support a non-contiguous range of MAC addresses for device identification. A user can download files that contain a list of MAC addresses. These named MAC lists can then be associated with rules using a new ‘MAC list’ rule type. When such a rule is associated with a PBA policy, the list of MAC addresses is consulted when determining if the policy matches the device identification data (i.e., a MAC address in this scenario) during the policy evaluation process.
- **Release 5.0**
  - Dynamic Actions

    VLANs associated with a PBA action can be specified using a comma-separated list of individual VLANs and VLAN ranges (e.g., 10, 15-20,100).

    The maximum count of VLANs that can be associated with a PBA action is increased to 200.
  - Policy Support

    VLANs associated with a PBA policy can be specified using a comma-separated list of individual VLANs and VLAN ranges (e.g., 10, 15-20,100).
  - MAC List File Support

    MAC OUIs can be intermixed with full MAC addresses in a MAC list file for enhanced device identification.
  - Interface Configuration

    Restricted MAC match processing can be enabled/disabled on a per-port basis, as well as globally (legacy operation). Restricted MAC match must be enabled globally for per-port settings to take effect.

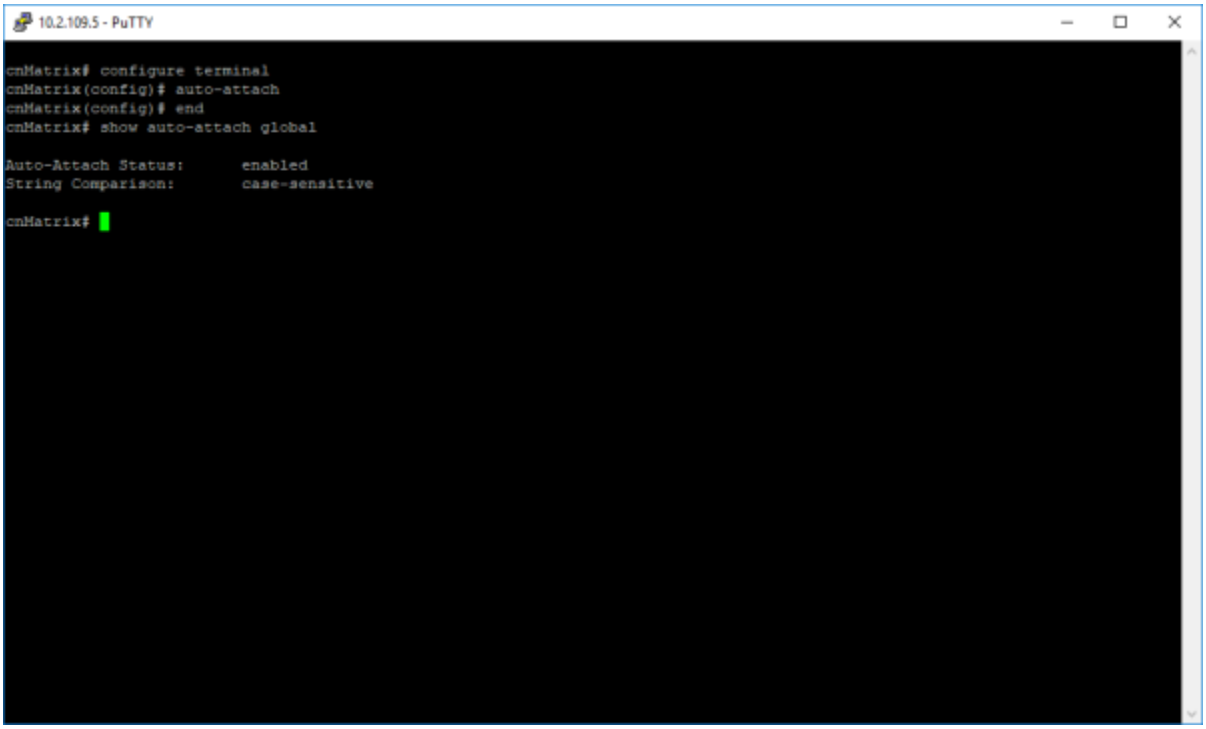
- **Release 6.1**
  - Dynamic Actions
    New action options introduced: DHCP Snooping trust state update, port STP Portfast enable/disable, static VLAN port membership exclusion/removal when a policy is being applied.
  - Policy Support
    Ability to enable/disable a policy's status based on the Time-of-Day. Track the applied policy history for up to 5 previously installed policies.
  - Time-of-Day (ToD) capabilities
    Support the definition of time windows within which a PBA policy is enabled and can be applied based on normal PBA device detection. Absolute (calendar date start/end) and relative (week-days) time windows can be defined along with intraday (hour/minutes start/end) times. A ToD policy that is outside of its time window is considered disabled and won't be evaluated duing device detection processing.
  - Auto-VLAN extensions
    Support a maximum of 200 Auto-VLAN VLANs (prior to 6.1 the limit was 20).

- **General Limitations**
  - Interactions with authentication (802.1x) support are not supported.
  - PBA policies are not applicable to port channels.
  - Traffic associated with the native VLAN egresses the switch as untagged traffic (i.e., the port is made an untagged member of the VLAN).

For more information, see Auto Attach Feature Description.

Network Diagram

How to Enable PBA/Auto Attach in CLI Interface

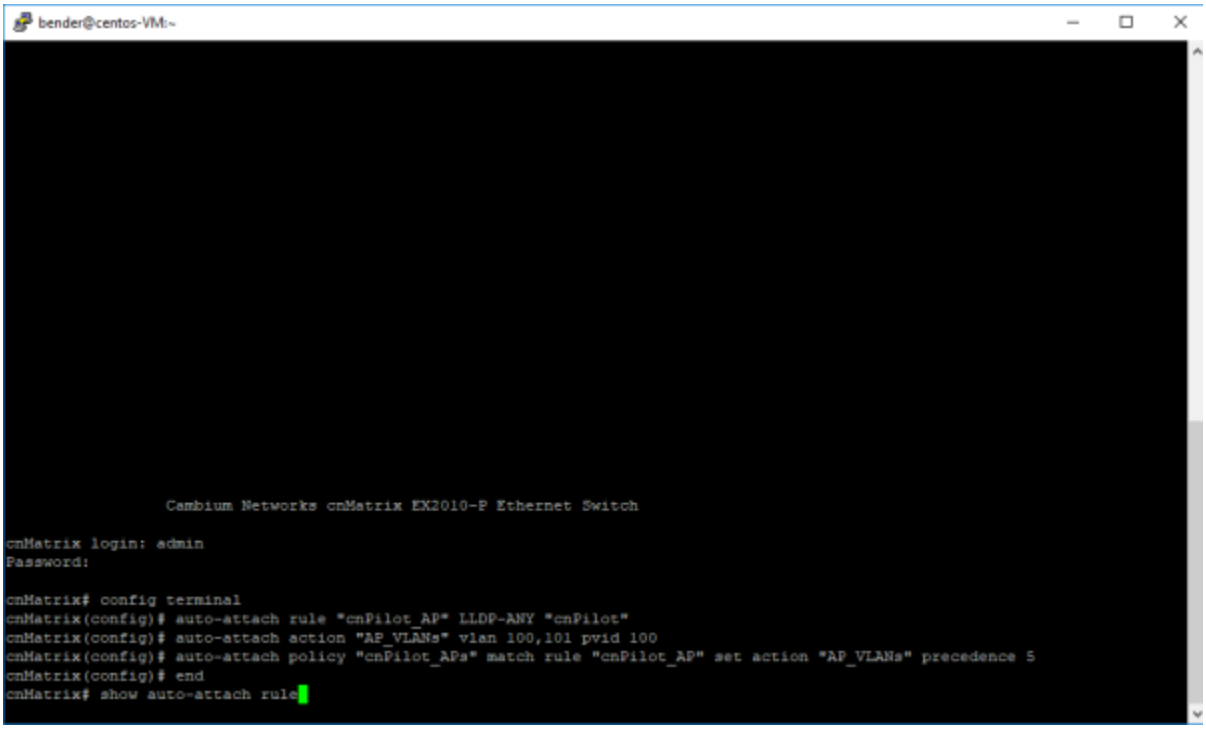


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **pba** (or **auto-attach**) command into the terminal to enable the PBA/Auto Attach feature. This feature is enabled by default. Press the **Enter** key.
3. Type the **end** command into the terminal.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

The **pba** (or **auto-attach**) command is also used to customize PBA behavior using the following options:

- **active-policy-reorder** – used to enable/disable active PBA policy reordering based on policy precedence.
- **auto-vlan-status** – enabled/disables Auto-VLAN processing for the device.
- **mac-policy-aging** – configures the MAC-based policy aging setting for non-verbose clients.
- **restricted-mac-match** – updates the MAC address-based policy matching mode.
- **string-comparison** – updates the PBA rule device data string comparison mode (default: ignore-case).
- **update-port-desc** – customizes the port description update mechanism when a policy is applied.
- **uplink** – configures global (default) uplinks for use with PBA policies.
- **localization** – configures the PBA switch localization value.

Configuring PBA/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 **pba rule** (or **auto-attach rule**) **"cnPilot_AP" LLDP-ANY "cnPilot"** command into the terminal to configure PBA/Auto-Attach rule information. Press the **Enter** key.

Note

cnPilot_AP = rule name; with this rule we match cnPilot Access Points.

cnPilot = matching string to be searched in all LLDP TLVs.

3. Rule type options include:
   - LLDP_ANY – match LLDP TLVs System Name, System Description, and Chassis ID.
   - LLDP_CAP – match LLDP System Capabilities flags.
   - LLDP-SYS-NAME – match LLDP System Name TLV data.
   - LLDP-SYS-DESC – match LLDP System Description TLV data.
   - LLDP-CHASSIS – match LLDP Chassis ID TLV data.
   - LLDP-PORT – match LLDP Port ID TLV data.
   - LLDP-PORT-DESC – match LLDP Port Description TLV data.
   - MAC-OUI – match learned MAC address OUIs against device ID data.
   - MAC-FULL – match learned MAC addresses against device ID data.
   - MAC-RANGE – compare learned MAC addresses against MAC address range device ID data.
   - MAC-LIST – compare learned MAC addresses against a non-contiguous MAC address range (MAC list file).
   - LLDP-IPV4-MGMT – match LLDP Management Address TLV IPv4 IP address data.
   - default - match any MAC address.
4. PBA rule usage restrictions:
   - Rule name is limited to 1 to 32 characters and must be unique.
   - Device identification string is limited to 1 to 60 characters.
   - Rules that are referenced by a policy cannot be deleted. Rules can be modified, even when referenced. Modification of a referenced rule causes the associated policy to be reapplied (if it is still applicable).

- A maximum of 100 rules can be defined.
- MAC address device identification format is xx:xx:xx (OUI), xx:xx:xx:xx:xx:xx (FULL) or xx:xx:xx:xx:xx:xx,yy:yy:yy:yy:yy:yy (RANGE).
- The low MAC address range value must be less that the high MAC address value (low and high).
- Only one rule with rule type ‘default’ can be defined.
- The device identification string for rule type default is ignored, if specified (optional for rule type default).
- A rule combination name is limited to 1 to 32 printable ASCII characters.
- A MAC list file must be downloaded before a rule referencing the MAC list can be created with the MAC-LIST rule type.

5. Type the **pba action** (or **auto-attach action**) **"AP_VLANs" vlan 100,101 pvid 100** command into the terminal to configure PBA/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.

6. Option: use the **pba action-ext** command to activate additional PBA action settings, including DHCP Snooping trust state update, port STP Portfast status and static VLAN membership exclusion/removal while the policy is applied.
7. PBA action usage restrictions:
   - Action name is limited to 1 to 32 characters and must be unique.
   - A VLAN range (vlan option) is comprised of 1 to 200 VLANs specified using a comma-separated list of individual VLANs and VLAN ranges (e.g., 10,15-20,100).
   - Specifying a native VLAN (pvid option) update requires a VLAN list containing the PVID VLAN be specified.
   - Updating the switch port mode automatically updates the port acceptable traffic type setting. A switch port mode setting of ‘access’ causes the acceptable traffic type to be set to ‘untagged’. Other switch port mode settings (i.e., ‘hybrid’, ‘trunk’) cause the acceptable traffic type to be set to ‘all’.
   - Actions that are referenced by a policy cannot be deleted. Action can be modified, even when referenced. Modification of a referenced action causes the associated policy to be reapplied (if it is still applicable).
   - A maximum of 100 actions can be defined.
   - An interface uplink list (uplink option) is comprised of 1 to 4 comma-separated interfaces identified using the interface type and slot/port convention (e.g., ‘Gi0/9,gi0/10,Ex0/1’).
   - The reset-link action modifier is treated as a no-op if the action does not modify the PVID.
   - If reset-link is enabled and the action updates the PVID, the show output indicates the reset-link status through the PVID display (“Link Reset Enabled”).
   - Action options that are not applicable to certain platforms (e.g., poe-priority, Cambium-Sync) may be specified but are ignored when the action data is applied.
   - VLAN exclusion will not remove all VLAN memberships if it will violate port configuration rules. Specifically, if the port Native VLAN (PVID) is not in the list of dynamic VLANs being added to the port, the static PVID VLAN membership will not be cleared.
8. Option: use the **pba tod** command to specify Time-of-Day (ToD) criteria to be used during policy definition.
9. PBA ToD usage restrictions:
   - ToD name is limited to 1 to 32 characters and must be unique.
   - An absolute (calendar date start/end) or a relative (week-days) date must be specified.
   - An intraday time (hour/minutes start/end) must be specified. Time specified using a 24 hour clock.
   - A ToD group name can be used to group different ToD specifications into a group/cluster that are treated as a single unit that identifies multiple time windows. The same group name (maximum 32 characters) is used to identify ToD specifications that are to be treated as a single unit.
   - An individual or group ToD specification must be defined before it can be referenced when defining a PBA policy using the policy **tod <tod-name>** option. The <tod-name> identifies either an individual ToD specification (ToD name is used) or a ToD group (ToD group name is used).
10. Type the **pba policy** (or **auto-attach**) **policy cnPilot_APs match rule cnPilot_AP set action AP_VLANs precedence 5** command into the terminal to configure PBA/Auto-Attach policy information. Press the **Enter** key.

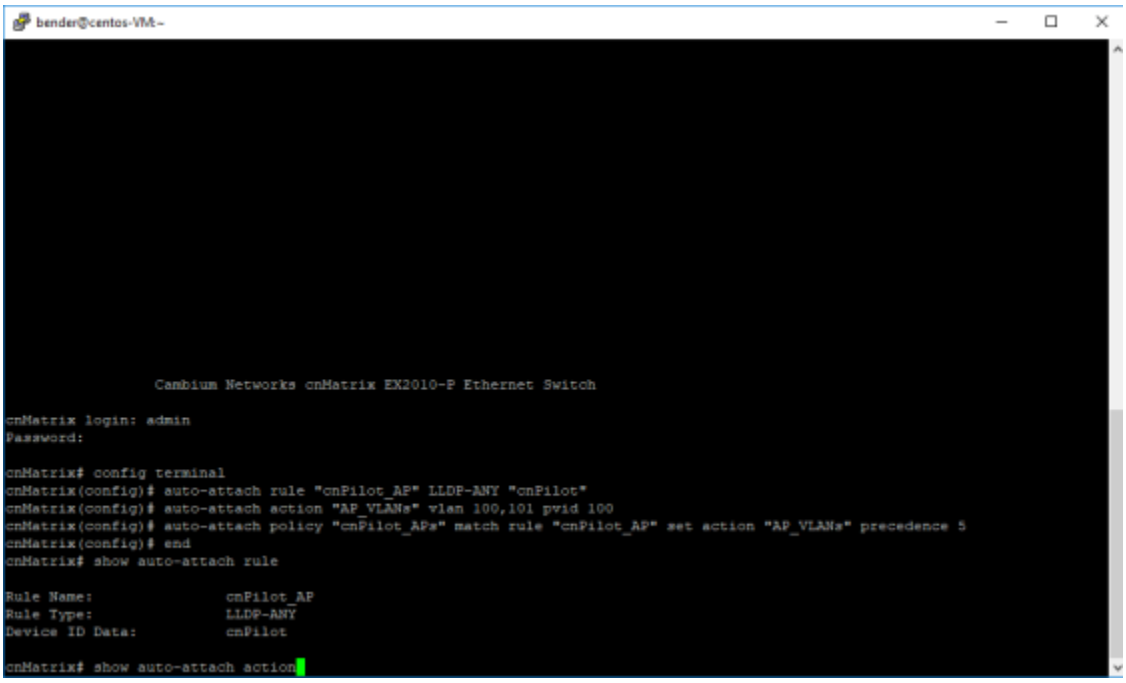
Note:

AP_VLANs = unique action name.

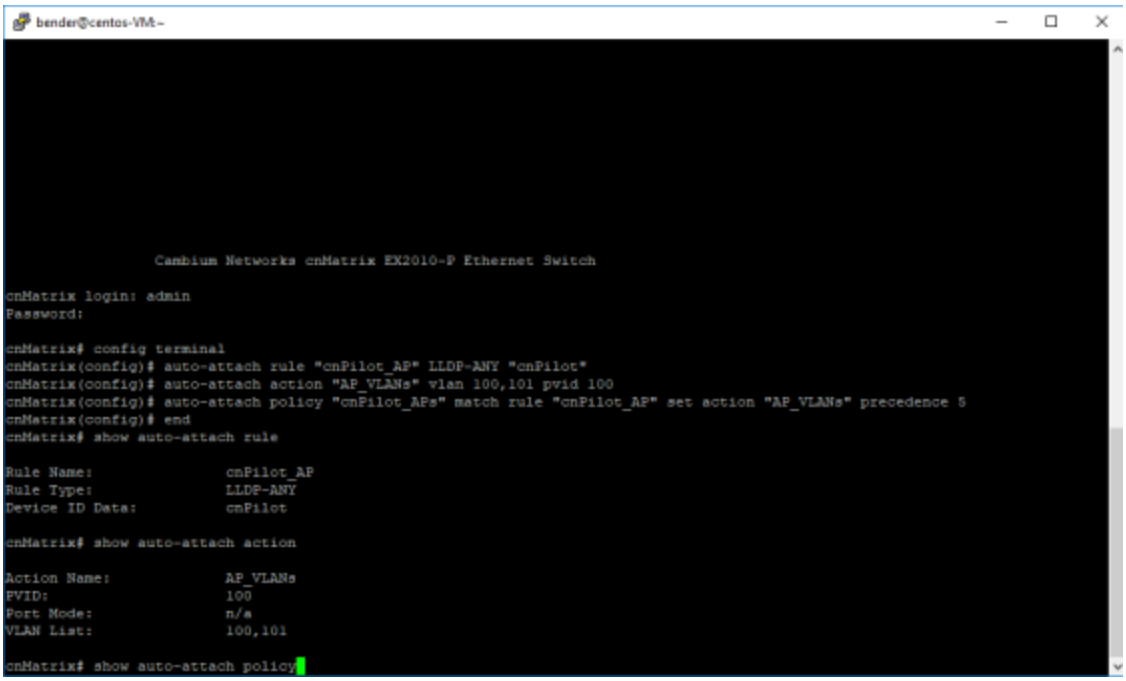
vlan 100, 101 = list of VLANs to be created.

pvid 100 = pvid value; this has to be a value specified in the VLAN list.

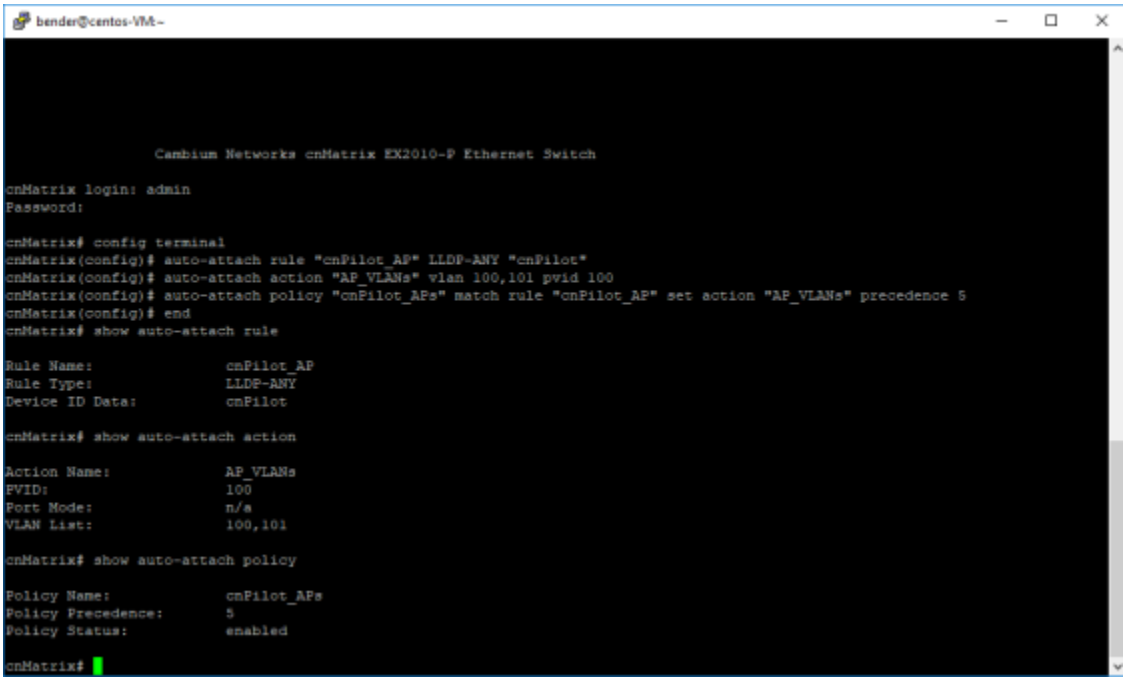
11. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.
12. Type the pba rule (or **show auto-attach rule)** command into the terminal to display PBA/Auto-Attach rule information. Press the **Enter** key.



13. Type the **pba action** (or **show auto-attach action**) command into the terminal to display PBA/Auto-Attach action information. Press the **Enter** key.



14. Type the **pba policy** (or **show auto-attach policy**) command into the terminal to display PBA/Auto-Attach policy information. Press the **Enter** key.



For more information, see Auto Attach Parameters and Commands.

PBA Action Localization (Version 4.5)

PBA action localization allows the same PBA policies to apply different settings based on certain device characteristics (device localization). This simplifies policy definition (no need for multiple policies with different actions) and allows action criteria to be changed by updating the device localization data. Localization allows the user to design network-wide (represented by a cnMaestro switch group) PBA policies that can have their associated action settings (i.e., the action context) easily customized for specific devices as needed.

PBA action localization support includes:

- Support for localized PBA action names. An action name always includes a base component (example, the current action name) and may also include a localization component. An '@' separates the base and localization components (example, baseActionName@localizationComponent).
- Introduction of a per-device localization label that specifies the context in which PBA actions are selected when a PBA policy is being evaluated.
- Updated PBA policy action reference support. A policy references an action using a non-localized or base action name (no change from the legacy behavior). When an action lookup occurs (during policy evaluation and installation), the device localization value is considered a lookup parameter (example, an action context identifier). If no device localization is defined, the action without any localization is selected (example, legacy PBA behavior is unchanged). If the device is localized, the action that is localized (with the localization component matching the device localization) is selected. If no such action is defined, the fallback non-localized action is selected.

Usage example

Two policies are defined (in order of their evaluation precedence) with their associated actions. Both match the traffic being received. These policies and actions are pushed by cnMaestro to all devices associated with a switch group.

Actions

- campus
- campus@studentDorm
- campus@adminDorm
- cameras@loading-dock

Policies

- cameras – action "cameras"
- campus – action "campus"

Device Localization: "" (no localization defined)

PBA Policy Evaluation Processing: localization label ""

- Policy "cameras" skipped – no matching action
- Policy "campus" applied using action "campus"

Update: Localization Label – "studentDorm"

PBA Policy Evaluation Processing: localization label "studentDorm"

- Policy "cameras" skipped – no matching action
- Policy "campus" applied using action "campus@studentDorm"

Update: Localization Label – "classroomBldA"

PBA Policy Evaluation Processing: localization label "classroomBldA"

- Policy “cameras” skipped – no matching action
- Policy “campus” applied using action “campus”

Update: Location Label – “”

PBA Policy Evaluation Processing: localization label “”

- Policy “cameras” skipped – no matching action
- Policy “campue” applied using action “campus”

Update: Location Label – “adminDorm”

PBA Policy Evaluation Processing: localization label “adminDorm”

- Policy “cameras” skipped – no matching action
- Policy “campus” applied using action “campus@adminDorm”

Delete action “campus” (deletion supported only when not in-use)

Update: Localization Label – “”

PBA Policy Evaluation Processing: localization label “”

- Policy “cameras” skipped – no matching action
- Policy “campus” skipped – no matching action

CLI/Web UI localization data configuration as follows:

- CLI: ‘[no] pba localization <string(32)>’
- CLI: ‘show pba global’
- CLI: ‘pba action baseActionName@localizedComponent …’
- CLI: ‘show pba action’
- CLI: ‘show pba policy detail’
- Web: Applications > Policy Based Automation > System > Device Localization
- Web: Applications > Policy Based Automation > Actions
- Web: Applications > Policy Based Automation > Policies

cnMaestro PBA localization data configuration as follows:

- Switch Groups/Configuration/Network/Policy Based Automation > Use Site name for localization
- Switch Groups/Configuration/Network/Policy Based Automation/Actions
- Switch Groups/Configuration/Network/Policy Based Automation/Policies
- Switches/Configuration/Advanced Settings/General > PBA Localization

PBA MAC List Support (Version 4.5)

PBA PBA MAC list support allows PBA rules to be enhanced to support a non-contiguous range of MAC addresses for device identification. You can download files that contain a list of MAC addresses. These named MAC lists can then be associated with rules using a new **MAC list** rule type. When such a rule is associated with a PBA policy, the list of MAC addresses is consulted when determining if the policy matches the device identification data (example, a MAC address in this scenario) during the policy evaluation process.

Operationally, a user downloads a PBA MAC list using existing file copy or download mechanisms (CLI – TFTP/SFTP/SCP/USB, Web – **System** > **Save/File Transfer** > **File Restore/Download**). During download processing, the MAC list file name and content is validated. Storage resource availability is confirmed as well.

PBA rule definition (CLI: ‘pba rule …’, Web: **Applications** > **Policy Based Automation** > **Rules**) references a MAC list by specifying the new MAC list rule type (MAC-LIST) and identifying a downloaded MAC list file. MAC list rules are no different from other PBA rules in terms of how they are used (i.e., referenced by PBA policies), displayed and managed. Policies that reference a MAC list rule (by specifying a MAC list rule name for the policy match criteria) are

processed in generally the same manner as other MAC-based PBA policies. One key difference is that a non-contiguous range of MAC addresses is used for device MAC address matching versus a MAC OUI (MAC-OUI rule type), a full MAC address (MAC-FULL rule type) or a contiguous range of MAC addresses (MAC-RANGE rule type).

PBA MAC list support includes:

- MAC list file download/delete (TFTP, SFTP, SCP, USB file copy/download available).
- MAC list file display (summary and content details display available).
- MAC list file validation. CSV file format allows comma-separated MAC addresses to be specified in four flexible formats: colon-separated octets, dash-separated octets, white-space separated octets and non-separated octets. Comma-separated non-MAC address data fields are ignored during file validation to support more flexible file formats. Up to 200 MAC addresses per file are supported.
- PBA rule MAC list (MAC-LIST) rule type to reference downloaded MAC list data.

Usage example

Download a previously created MAC list file: warehouse_macs.txt (contents as follows)

apMac1, 10/20/14, 58:c1:7a:00:83:0b, loading dock,

apMac2, 10/21/14, 58:c1:7a:11:83:1b, bookkeeping,

apMac3, 10/22/14, 58:c1:7a:01:83:2b,

apMac4, 10/23/14, 58:c1:7a:33:83:3b, bookkeeping,

apMac5, 10/24/14, 58:c1:7a:39:83:4b, bookkeeping,

apMac6, 10/25/14, 58:c1:7a:55:83:5b,

apMac7, 10/26/14, 58:c1:7a:61:83:6b, loading dock,

apMac8, 10/27/14, 58:c1:7a:c3:83:7b, public.1,

apMac9, 10/28/14, 58:c1:7a:ab:83:8b, public.2,

apMac10, 10/29/14,58:c1:7a:00:83:9b

```
EX2010# show pba mac-list-files
```

No MAC list files currently downloaded

```
EX2010# copy tftp://10.140.134.6/warehouse_macs.txt pba_mac_list
```

File transfer completed in 0 seconds

PBA MAC list file copied successfully

```
EX2010# show pba mac-list-files
```

MAC List File Name: warehouse_macs.txt

MAC List File Status: downloaded

MAC List MAC Count: 10

MAC List File Refresh: enabled

```
EX2010# show pba mac-list-files warehouse_macs.txt
```

MAC List File Name: warehouse_macs.txt

MAC List File Status: downloaded

MAC List MAC Count: 10

MAC List File Refresh: enabled

58c17a00830b, 58c17a11831b, 58c17a01832b, 58c17a33833b,

58c17a39834b, 58c17a55835b, 58c17a61836b, 58c17ac3837b,

58c17aab838b, 58c17a00839b

EX2010# con t

```
EX2010(config)# pba rule warehouseMacs MAC-LIST warehouse_macs.txt

EX2010(config)# pba action warehouseMacs vlan 200 user-priority 5

EX2010(config)# pba policy warehouseMacs match rule warehouseMacs set action
warehouseMacs

EX2010# exit

EX2010# show pba rule
```

Rule Name: warehouseMacs

Rule Type: MAC-LIST

Device ID Data:

Data File Name: warehouse_macs.txt

Rule Combination Name:

```
EX2010# show pba policy detail
```

Policy Name: warehouseMacs

Policy Precedence: 50

Policy Status: enabled

Policy Ports: all

Rule Name: warehouseMacs

Rule Type: n/a

Rule Device ID Data: n/a

Action Name: warehouseMacs

Action PVID: n/a

Action Port Mode: n/a

Action VLAN List: n/a

```
EX2010# clear pba mac-list-files
```

% PBA MAC list files deleted: 1

```
EX2010# show pba mac-list-files
```

No MAC list files currently downloaded

PBA MAC list file restrictions

1. A MAC list file must contain a single MAC address or a comma-separated list of 2..200 MAC addresses (e.g., 11:22:33:44:55:66,88 99 aa bb cc dd,334455667788).
2. Comma-separated non-MAC address data in the file is automatically skipped during data parsing.
3. Acceptable MAC address formats:
    - Colon-separated octets – 11:22:33:44:55:66
    - Dash-separated octets – 11-22-33-44-55-66
    - Whitespace-separated octets – 11 22 33 44 55 66
    - Non-separated octets – 112233445566
4. A maximum of ten (10) MAC list files can be stored on the switch at any time.
5. A MAC list file name must be 1..64 alphanumeric characters (plus '-', '_' and '.').
6. Defining a PBA MAC-LIST rule requires a MAC list file to be specified at the same time. Only currently downloaded MAC list files can be referenced by a PBA rule.
7. MAC list files that are referenced by a rule cannot be deleted.
8. Starting with the 5.0 release, MAC OUIs can be intermixed with full MAC addresses in a MAC list file.

CLI/Web UI MAC list file display and control as follows:

- CLI: 'copy tftp://… pba_mac_list'
- CLI: 'copy sftp://… pba_mac_list'
- CLI: 'copy scp://… pba_mac_list'
- CLI: 'copy usb:… pba_mac_list'
- CLI: 'clear pba mac-list-files'
- CLI: 'clear pba mac-list-file <macListFileName>'
- CLI: 'show pba mac-list-files'
- CLI: 'show pba mac-list-files <macListFileName>'
- CLI: 'show pba download settings'
- CLI: 'pba rule <ruleName> MAC-LIST <macListFileName>'
- Web: System > Save/File Transfer > File Download/Restore
- Web: Applications > Policy Based Automation > System > MAC List Files
- Web: Applications > Policy Based Automation > System > Data File Download Settings
- Web: Applications > Policy Based Automation > Rules

cnMaestro support

The cnMaestro PBA MAC list file support includes the ability to configure the PBA MAC list filenames to be downloaded to the switch (the what to download) and the download/transfer settings (the how to download). cnMaestro does not support PBA MAC list file construction or storage. The user is responsible for producing an appropriately formatted PBA MAC list file and for providing access to a server from which the file can be downloaded.

Two new components are introduced by cnMaestro to support PBA MAC lists. The MAC Lists tab is added to the PBA Policy/Action/Rule configuration table to allow the user to specify (currently up to 10) PBA MAC list files that the switch is requested to download. The PBA Server Settings section allows the user to specify the download settings to be used (only) by PBA to download the identified PBA MAC list files to the switch.

Typical server settings are supported:

- Transfer method (TFTP, SFTP, SCP)
- Server IP address (IPv4, IPv6, DNS)
- Download path (if required for the specified transfer method)
- Username (required for SFTP, SCP)
- Password (required for SFTP, SCP)

Through the PBA MAC Lists tab, the user configures the names of the MAC list files that the switch should attempt to download from the user-maintained file server using the configured server download settings. Following a cnMaestro

configuration push, the PBA agent attempts to download all of the configured MAC list files using the provided download settings/credentials.

cnMaestro PBA MAC list file data configuration

- Switch Groups/Configuration/Network/Policy Based Automation > MAC List File Server Settings
- Switch Groups/Configuration/Network/Policy Based Automation/MAC Lists
- Switch Groups/Configuration/Network/Policy Based Automation/Rules

PBA Time-of-Day Support (Version 6.1)

PBA Time-of-Day (ToD) support allows PBA policies to be dynamically enabled/disabled based on the current system time. The user can define ToD specifications that can be linked to a PBA policy if ToD-based policy evaluation is desired. A ToD spec provides relative (weekday-based) or absolute (date-based) time parameters that are compared against the system clock to determine if the ToD spec is ‘active’ or ‘inactive’. A policy is operationally disabled (i.e., skipped during PBA LLDP/MAC-based device detection) if it is associated with a ToD spec that is currently inactive. A policy is operationally enabled (i.e., available for normal evaluation during device detection processing) if it is associated with a ToD spec that is currently active (or if the policy is not associated with a ToD spec at all, i.e., the legacy behavior).

A new core PBA table, the Time-of-Day (ToD) table, is introduced to allow the user to specify absolute or relative time parameters, a.k.a. ToD specifications. A named ToD spec defines either a start/end date (absolute timing) or weekdays (relative timing) together with a start/end time related to those days/dates. Together, these components establish a window of time that, when compared to the current system clock value, determines if the ToD specification is considered active (i.e., within the time window) or inactive (i.e., outside of the time window). A policy is operationally (ToD) enabled if the ToD specification that it is associated with is active and operationally (ToD) disabled if it is inactive. A policy’s operational state determines its eligibility for evaluation during device detection processing and possible installation on a device port.

One or more ToD specifications can be grouped/joined to allow multiple activation time windows to be associated with a PBA policy. A policy can reference a standalone ToD spec, a ToD group (i.e., one or more ToD specs evaluated in a cumulative fashion) or no ToD data at all.

Terminology

- Absolute time - time specification using mm/dd/yyyy data and a 24-hour clock for intradate timing.
- Relative time - time specification using week-days data and a 24-hour clock for intraday timing.
- Active time window - the period of time a policy associated with a ToD spec may be applied to a port if the policy criteria dictates (i.e., matches port LLDP/MAC address event data).
- Eligible policy - a PBA policy with an administrative status of 'enabled' that doesn't include a ToD reference or that references a ToD specification that places the policy in an active time window based on the system clock. An operationally enabled policy.
- Ineligible policy - a PBA policy with an administrative status of 'disabled' or that references a ToD specification that places the policy outside of an active time window based on the system clock. An operationally disabled policy.
- ToD group – a set of ToD specifications that share the same group name.

Additional Operational Details

A. Day-based (relative) timing is defined using a comma-separated list of one or more days. Days are specified by their standard abbreviations (e.g., “sun,mon,tue,wed,thu,fri,sat”, “su,mo,tu,we,th,fr,sa” or “su,m,tu,w,th,f,sa”) or using full names (e.g., “Sunday,Monday,Tuesday,Wednesday,Thursday, Friday,Saturday”. Configuration data is case-insensitive.

B. Start date and end date (absolute) timing is defined using the standard “mm/dd/yyyy” (month/day/ year) data format. Data is validated for range (e.g., mm – 1..12, dd – 1..31, yyyy – first allowed year is 2023) and calendar correctness (e.g., days per month). The start date must be less than or equal to the end date.

C. Start time and end time data is defined using the standard 24-hour clock “hh:mm” (hour/minutes) format. Data is validated for range (e.g., hh – 0..23, mm – 0..59). The start time must be less than or equal to the end time.

D. ToD group active/inactive status is determined by evaluating each ToD spec in the group. If the individual ToD spec is active, the ToD group is active. If all individual ToD specs that comprised the ToD group are inactive, the ToD group is inactive. A maximum of 21 individual ToD specifications can be added to a group (7 days * 3 time windows per day).

E. In-use ToD specifications can be updated. Policies that reference the ToD data being updated, if active and applied to a port, are bounced to facilitate re-evaluation of the associated time data.

F. In-use ToD groups can be updated. Policies that reference the ToD group being updated, if active and applied to a port, are bounced to facilitate re-evaluation of the associated time data. A ToD group must contain at least one member (i.e., the last group member can’t be deleted if the ToD group is referenced by a PBA policy).

G. A PBA policy that is operationally enabled and applied to a port can have its associated ToD data updated. The policy is bounced to facilitate re-evaluation of the updated ToD data.

New/Updated CLI Command Summary

A. PBA Time-of-Day specification configuration

```
pba tod <tod-name> { week-days <days-of-the-week> |
                     start-date <mm/dd/yyyy> end-date <mm/dd/yyyy> }
                     start-time hh:mm end-time hh:mm
                     [ group <group-name> ]


no pba tod <tod-name>
```

where:

- tod-name - 1..32 character ToD specification name. Same syntax/limitations as other PBA table name objects. A PBA policy references this name to associate the policy with ToD parameters.
- week-days - Configure day-based (relative) ToD data.
- days-of-the-week - Days of the week are specified using a comma-separated list of day abbreviations (e.g., "M,Tu,Th,F,Sa" or "Mon,Tue,Thu,Fri,Sat" for Monday, Tuesday, Thursday, Friday, Saturday). Case-insensitive abbreviations or full day names are accepted.
- start-date - Configure starting date for date-based (absolute) ToD data.
- end-date - Configure ending date for date-based (absolute) ToD data.
- mm/dd/yyyy - Date specification (month, day, year).
- start-time - Configure starting time for intraday/intradate ToD data.
- end-time - Configure ending time for intraday/intradate ToD data.
- hh:mm - Time specification (hours, minutes - 24 hour clock).
- group-name - 1..32 character ToD group name. Allows multiple ToD entries to be joined and treated as a single cumulative specification. A PBA policy references this name to associate the policy with ToD parameters.

B. PBA Time-of-Day specification display

show pba tod [name <tod-name> | group <group-name>]

where:

- tod-name - 1..32 character ToD specification name.
- group-name – 1..32 character ToD group identifier.

Notes:

- CLI ToD display output includes operational state data that indicates if the individual ToD specification is active or inactive, based on the specification data and the current system clock time. ToD group operational state data is also displayed for group members. A ToD group is active if any of the individual ToD specs that comprise the group are active.

C. Related PBA configuration / display updates

pba policy <policy-name> match rule <rule-name>
set action <action-name>
tod <tod-name | tod-group-name> …

show pba policy [detail | tod-xray | …]

where:

- tod-name - 1..32 character ToD specification name.
- tod-group-name – 1..32 character ToD group identifier.
- tod-xray – displays policy ToD data (individual ToD specification or ToD group members).

Notes:

- Updated PBA policy ‘show’ output includes ‘Time-of-Day Qualifier’ data that presents the associated ToD data (individual ToD specification or ToD group) and its status (active or inactive). If the associated ToD data is inactive, the policy is operationally disabled.

Example: ToD specification configuration, display and usage

```
EX2010P-EE0000(config)# pba tod relative-time-1 week-days m,tu,w,th,f
start-time 09:00 end-time 17:00 group all-week-days

EX2010P-EE0000(config)# pba tod relative-time-2 week-days saturday,sunday
start-time 00:00 end-time 23:59 group all-week-days

EX2010P-EE0000(config)# pba tod absolute-time start-date 02/01/2025
end-date 02/28/2025 start-time 17:00 end-time 23:00

EX2010P-EE0000# show pba tod

Time-of-Day Name:   absolute-time
Weekdays:
Start Date:         02/01/2025
End Date:           02/28/2025
Start Time:         17:00
End Time:           23:00
Group Name:
Operational State:  inactive

*************************************************

Time-of-Day Name:   relative-time-1
Weekdays:           mon,tue,wed,thu,fri
```

```
Start Date:
End Date:
Start Time:          09:00
End Time:            17:00
Group Name:          all-week-days (inactive)
Operational State:   inactive

**************************************************

Time-of-Day Name:    relative-time-2
Weekdays:            sun,sat
Start Date:
End Date:
Start Time:          00:00
End Time:            23:59
Group Name:          all-week-days (inactive)
Operational State:   inactive

EX2010P-EE0000# show pba tod name absolute-time

Time-of-Day Name:    absolute-time
Weekdays:
Start Date:          02/01/2025
End Date:            02/28/2025
Start Time:          17:00
End Time:            23:00
Group Name:
Operational State:   inactive

EX2010P-EE0000# show pba tod group all-week-days

Time-of-Day Name:    relative-time-1
Weekdays:            mon,tue,wed,thu,fri
Start Date:
End Date:
Start Time:          09:00
End Time:            17:00
Operational State:   inactive
------
Time-of-Day Name:    relative-time-2
Weekdays:            sun,sat
Start Date:
End Date:
Start Time:          00:00
End Time:            23:59
Operational State:   inactive
```

PBA Auto-VLAN Server Support (Version 6.1)

Phase 1 PBA Auto-VLAN server support has two components:

- Auto-VLAN server discovery
- Auto-VLAN server VLAN advertisement

cnMatrix automatically discovers Auto-VLAN server devices that are connected to any port. The first Auto-VLAN server device supported is Cambium's NSE product. Multiple such devices can be connected to a switch, though a single ("uplink") Auto-VLAN server connection is the recommended (and expected) configuration. Discovery may initiate specific actions, such as a switch port mode update (e.g., dynamically update the switch port mode to 'Trunk') and Auto-VLAN processing (with the switch acting as the client), based on new Auto-VLAN server operation configuration settings. All Auto-VLAN server-related dynamic updates are cleared (i.e., settings revert to their previous value) when the device is no longer connected to the port.

Auto-VLAN server discovery is enabled by default but may be disabled on a per-port basis. Using LLDP, a discovered Auto-VLAN server is passed VLAN information (i.e., the list of VLANs associated with the server-connected port and the port's native VLAN/PVID) using the Auto-VLAN infrastructure. Ports on which an Auto-VLAN server is discovered can be automatically transitioned to 'Trunk' mode from a non-trunk mode ('Hybrid', 'Access'). The dynamic port mode update is maintained for the duration of the server connection. When the server is longer present, the port mode reverts to its previous mode (or to default settings if the previous settings can't be restored). The user controls this operation through a new global PBA setting ('auto-vlan-server-trunk'). This dynamic operation is disabled by default.

New/Updated CLI Command Summary

A. Auto-VLAN server discovery control (per-interface setting). Enables/disables automatic Auto-VLAN server discovery (default setting: enabled):

pba auto-vlan-server-discovery

no pba auto-vlan-server-discovery

B. Auto-VLAN server port mode update (global setting). When enabled, the port through which an Auto-VLAN server is discovered is automatically transitioned to 'Trunk' mode (default setting: disabled). When the server is no longer detected, the port mode reverts to its previous value:

pba auto-vlan-server-trunk [enable | disable]

C. PBA dynamic uplink support (global setting). When enabled, Auto-VLAN server discovery causes the global PBA uplink list to the updated to include the port through which the Auto-VLAN server is discovered (default setting: enabled). When the server is no longer detected, the Auto-VLAN interface is removed from the PBA global uplink list.

pba dynamic-uplink [enable | disable]

D. Current Auto-VLAN server-related settings are exposed through the existing/new 'show' commands:

show pba global

show pba interface auto-vlan-server

```
EX2010P-EE0000# show pba global

PBA Status:                enabled
String Comparison:         case-ignored
Update Port Description:   pba-policy-name
Restricted MAC Match:      enabled
Active Policy Reordering:  enabled
MAC-based Policy Aging:    disabled
Auto-VLAN Status:          enabled
Auto-VLAN Server Trunk:    disabled
Dynamic Uplink Support:    enabled
Dynamic Policy Uplinks:
Device Localization:

EX2010P-EE0000# show pba interface auto-vlan-server

           Auto-VLAN  Device
           Server     Settings
Interface  Discovery  TLV Status  Server Status
---------  ---------  ----------  -------------
Gi0/1      enabled    enabled
Gi0/2      enabled    enabled
Gi0/3      enabled    enabled
Gi0/4      enabled    enabled
Gi0/5      enabled    enabled
Gi0/6      enabled    enabled
```

```
Gi0/7       enabled    enabled
Gi0/8       enabled    enabled
Gi0/9       enabled    enabled
Gi0/10      enabled    enabled
```

Dynamic ARP Inspection (Starting with version 2.1)

Managing Dynamic ARP Inspection

Feature Overview

The **Dynamic ARP Inspection (DAI)** feature has been added to enhance the security of your network. DAI validates network ARP response packets to be securely validated in the network. Without DAI, 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 configured on the switch. You have to consider that the CPU utilization will increase with the number of DAI-enabled VLANs and also with the number of network ARP packets.

Limitations

- The DAI feature is limited to the number of VLANs in the system.
- Number of entries in the binding database.
- The DAI feature per port-channel interfaces is supported from version 4.3.

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.

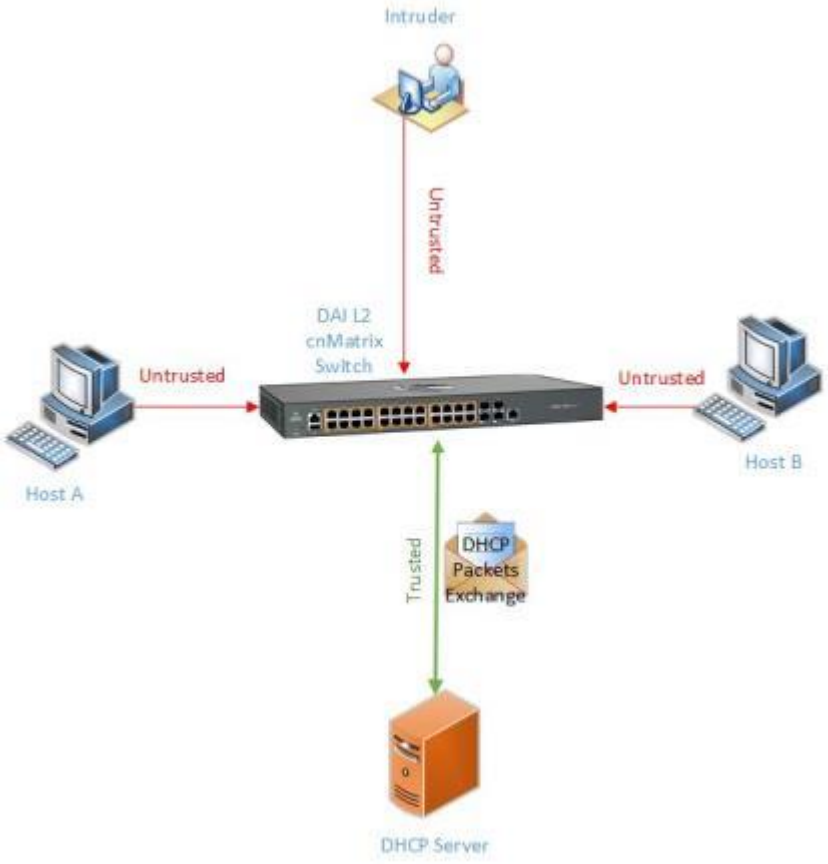
Prerequisites

- 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 by-pass 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.

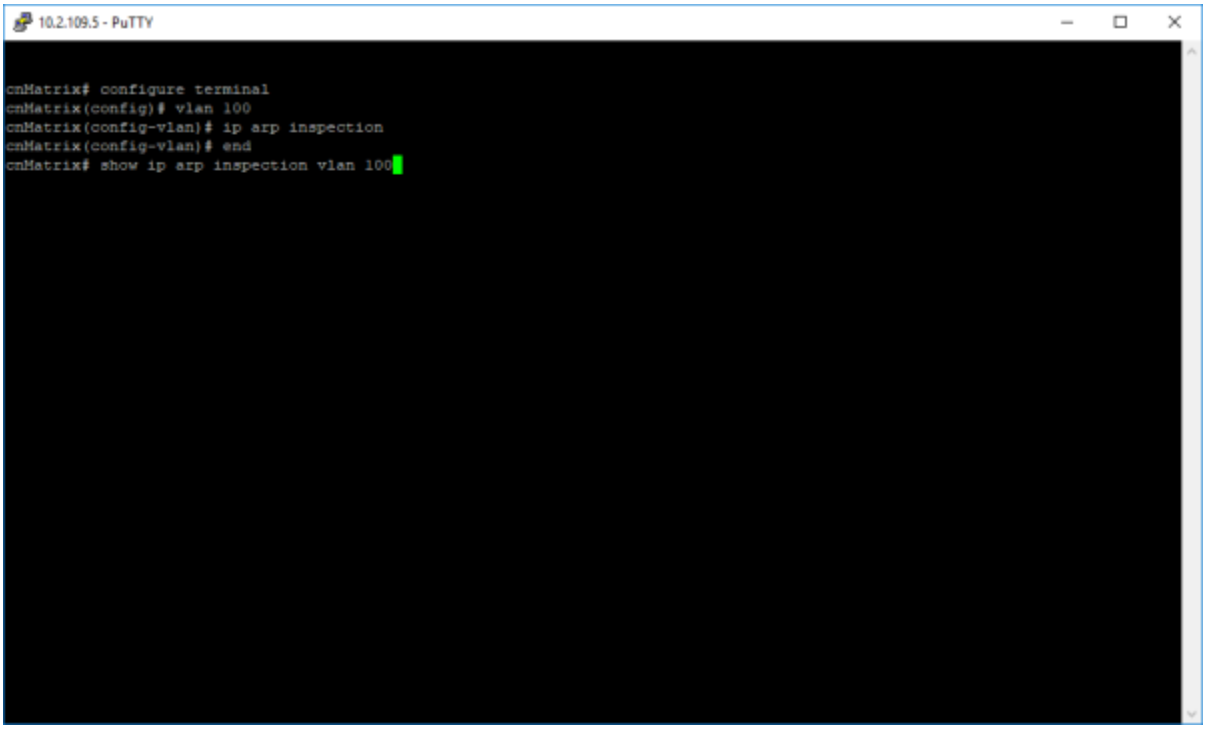
Note

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.

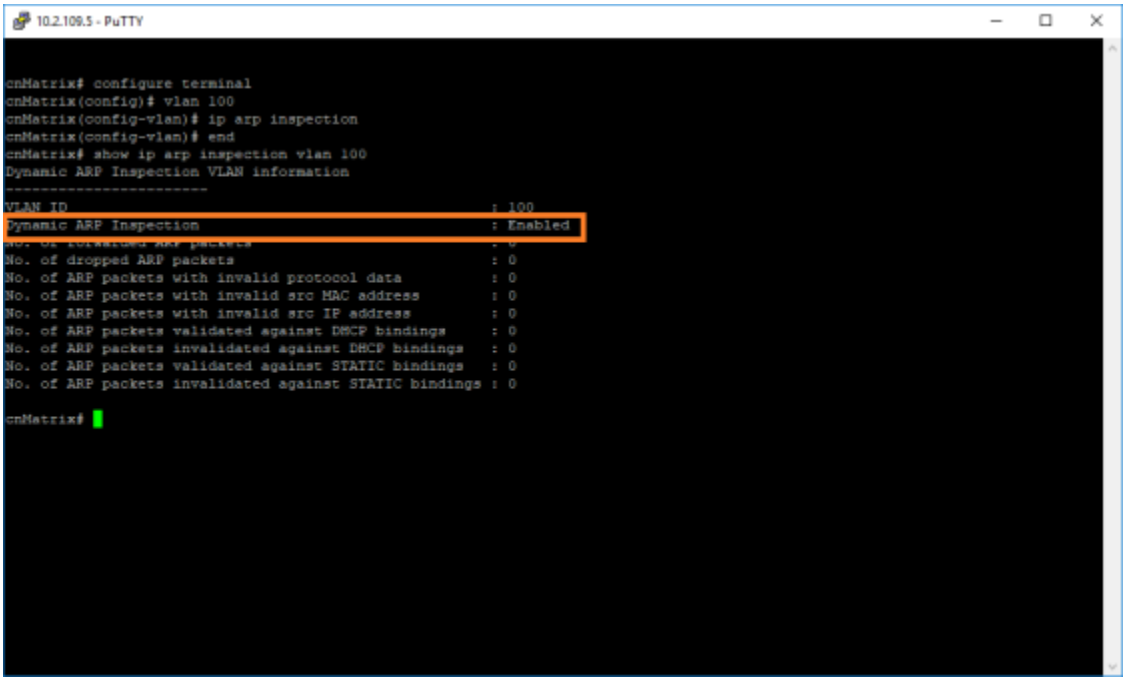
Network Diagram



How to Enable DAI on VLANs in CLI Interface

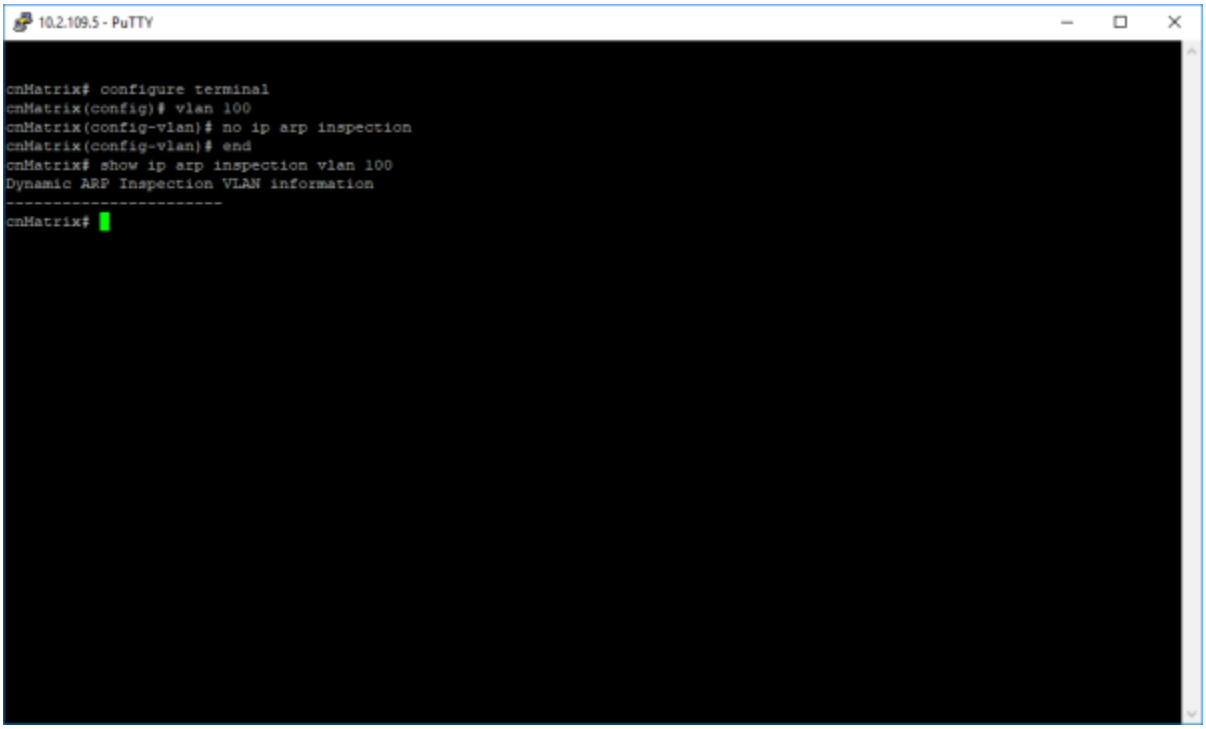


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **vlan 100** command into the terminal to configure vlan 100. Press the **Enter** key.
3. Type the **ip arp inspection** command into the terminal to enable DAI on the selected VLAN. Press the **Enter** 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 DAI status for vlan 100 (verify if DAI is enabled).



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

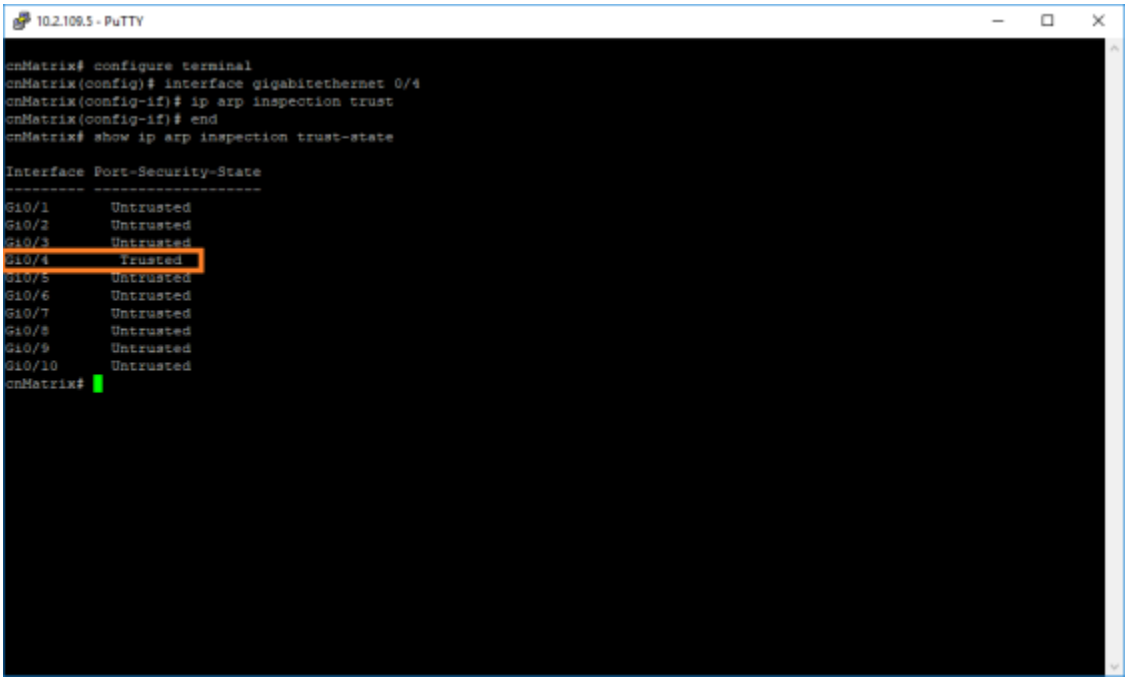
How to Disable DAI on VLANs in CLI Interface



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 DAI 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 DAI 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.

Configuring the DAI 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 DAI 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.

Energy Efficient Ethernet (starting with version 4.1)

Managing Energy Efficient Ethernet

Feature Overview

Energy Efficient Ethernet (EEE) is an 802.3az standard that is designed to reduce the power consumption of copper interfaces during idle periods. Idle periods are periods in which no data is being transmitted. EEE can be configured on a port basis and has two possible states: Enabled or Disabled. EEE is supported networks that run in 100Base-TX, 1000Base-T, or 2500Base-T.

Note

The **EEE** feature can be configured via CLI, Web and SNMP.

Attention

EEE capable switch is supported starting with cnMatrix release 4.0.

Starting with cnMatrix release 6.1, EEE can be controlled globally as well as per-port. When EEE is globally enabled, the EEE per-port settings take precedence and dictate the port behavior. When EEE is globally disabled, EEE behavior is automatically disabled on all ports and the per-port EEE settings are ignored.

Standard

802.az

Scaling Numbers

EEE works on all copper-ports and can be enabled or disabled on a port basis.

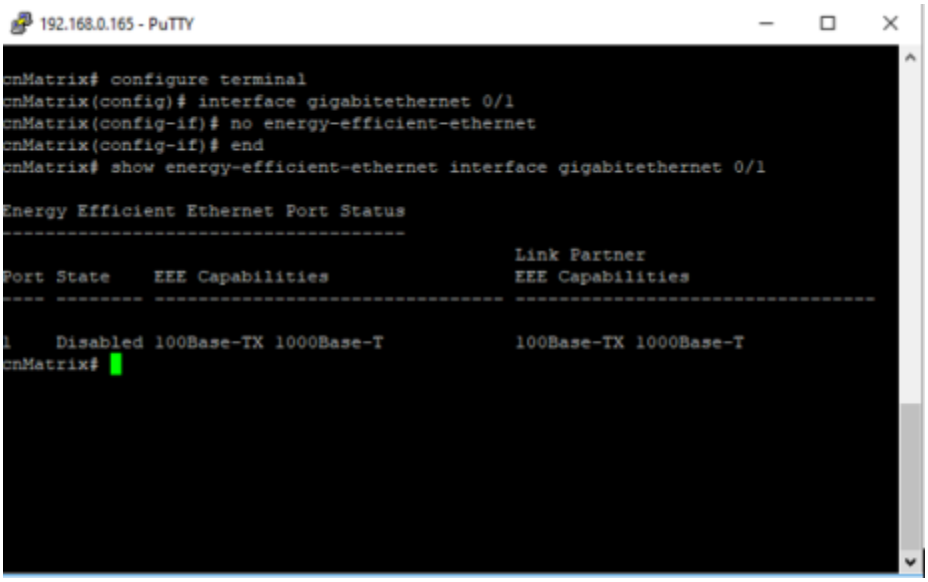
Limitations

EEE is not supported on fiber ports.

Default Values

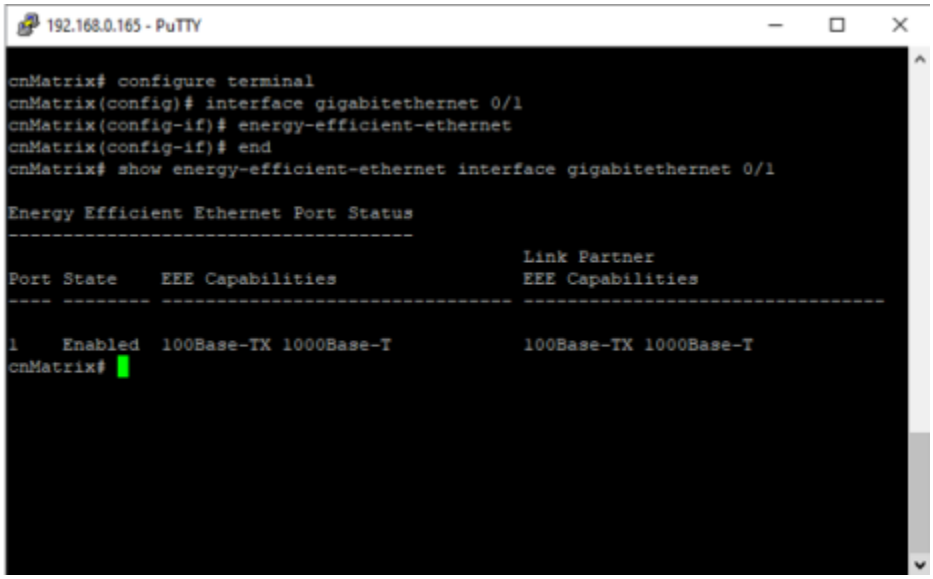
By default, all interfaces have EEE enabled and support all of the available EEE capabilities.

How to disable EEE on an 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 energy-efficient-ethernet** command into the terminal. Press the **Enter** key.

How to enable EEE on an 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 **energy-efficient-ethernet** command into the terminal. Press the **Enter** key.

Troubleshooting EEE

Useful command for troubleshooting EEE:

```
cnMatrix# show energy-efficient-ethernet
```

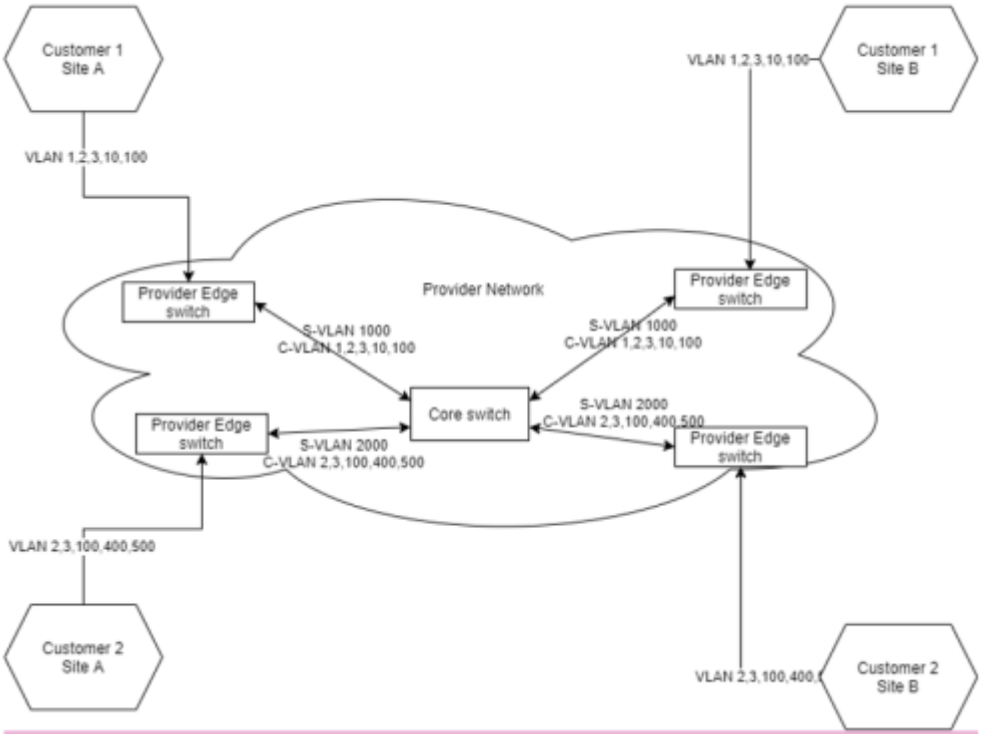
This command displays the state of all ports. Also, if the link partner is EEE capable, its capabilities should appear under the **Link Partner Capabilities** column.

Q-in-Q

Feature Description

This feature allows service providers to use a single VLAN to forward traffic for customers who use multiple VLANs, while keeping the traffic from different customers segregated. To accomplish this, a Service VLAN is assigned to each customer, based on the ingress port and VLAN ID, and all forwarding is done in the service VLAN. To forward traffic over the network, an additional VLAN tag (the S-TAG) is added to the packets egressing on network.

This way, multiple customers may use their VLAN tagging.



In this use case, Customers 1 and 2 have set up overlapping sets of VLAN IDs in their networks, and by using Q-in-Q, the network administrator of the provider network can keep the packets originating from Customer 1 away from the interfaces of Customer 2 and vice-versa.

The provider network is comprised by one or several **provider edge** switches – where the customers connect to the provider cloud, and one or several **core** switches, that can be qinq-unaware with the single purpose of bridging traffic from VLANs 1000 and 2000 (the S-VLANs).

The **provider-edge** bridge mode is a global mode in which the switch ports can be either customer-edge ports or provider ports. Their role is configurable by the user, depending on if they connect to a customer or the network provider core.

C-VLAN (Customer-VLAN) – the VLAN id assigned by the customer network. In case the packet is untagged, the C-VLAN can be assigned by the provider bridge at ingress. Original C-VLANs are kept as part of the packet payload.

S-VLAN (Service-VLAN) – the VLAN id assigned upon ingress on a customer-edge port. This is the VLAN id used in the bridging process.

S-VLAN tag – an additional VLAN tag added to the customer packet, containing the VLAN id, the 802.1ad ethernet type, and the S-TAG dot1p user priority. This tag is added when the packets egress via a provider port and stripped when the packets egress via a customer-edge port.

Double-tagged packet – A packet that has both the S-TAG and the C-TAG. These packets are forwarded via the provider ports. The S-TAG is referred to as the **external** tag, while the C-TAG is the **internal** tag,

The user will need to do configure the following:

- Change the bridge mode to provider edge and reboot.
- Configure port types to either customer-edge or provider.
- Configure the port/C-VLAN to S-VLAN translation.

Additionally, the user will be able to configure:

- The ingress/egress ethernet type for the S-VLAN.
- The default C-VLAN for a provider port, in case there are packets arriving as C-untagged.
- The default S-TAG dot1-p priority.

Configuring Q-in-Q via CLI

```
cnMatrix# boot default bridge-mode {customer | provider-edge}
```

- **Customer** - Sets the bridge to Customer Bridge Mode which allows the switch to operate as a 802.1Q VLAN Bridge.
- **Provider** - Sets the bridge to Provider Bridge Mode which allows the bridge to operate as a normal Q-in-Q Bridge.

By default, the switch is configured as **customer**.

```
cnMatrix# show bridge-mode

The current bridge mode is: provider-edge
```

After booting into the **provider-edge** mode, the user needs to assign customer-edge and provider edge ports:

```
cnMatrix(config-if)# bridge port-type {customer-edge | provider}
```

- **Customer-edge** – Denotes that the port is connected to a single customer. The packets received on this port are initially classified as a C-VLAN. C-VLAN classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service VLAN selection is done for a frame based on the entry present in the C-VID registration table for the pair (C-VID, reception port).
- **Provider** – Denotes that the port is connected to a single provider.

On customer-edge ports

- cnMatrix(config-if)# switchport [customer-vlan <integer(1-4094)>] service-vlan <vlan_id>
- cnMatrix(config-if)# no switchport [customer-vlan <integer(1-4094)>] [service-vlan]

If **customer-vlan** is not specified, the service-vlan will be applied to all incoming packets, regardless of C-VLAN:

```
cnMatrix(config-if)# switchport service-vlan <vlan_id>

cnMatrix(config-if)# no switchport service-vlan <vlan_id>
```

```
cnMatrix(config-if)# switchport [customer-vlan %d] svlan-prio {<0-7> | none}
```

Specifies which dot1p priority to be used in the S-TAG: either a fixed user-set value, or none. If **customer-vlan** is not specified, the S-VLAN-prio will be applied to all incoming packets, regardless of C-VLAN.

```
cnMatrix(config-if)# switchport customer-vlan pvid <vlan_id>
```

Specifies which C-VID value to use for untagged packets received on the customer-edge port. The specified VLAN Id must be already configured on the port as a customer-vlan.

```
cnMatrix(config-if)# service-vlan <svlan> pvid <pvid>
```

If C-untagged packets are received on the provider port, a C-TAG needs to be added. The PVID configured here will be the VLAN id from the C-TAG. This command is configured on the customer port, but the value set here is applied on all network provider ports from the S-VLAN.

```
cnMatrix(config-if)# service-vlan <svlan> def-user-priority <value>
```

If C-untagged packets are received on the provider port, a C-VLAN needs to be added. The default priority value configured here will be the dot1p used in the C-TAG. This command is configured on the customer port, but the value set here is applied on all network provider ports from the S-VLAN.

On provider ports:

```
cnMatrix(config-if)# switchport egress ether-type {x8100 | x88a8 | x9100}
```

Specifies which TPID to be used in the S-TAG of the frames egressing on this port.

```
cnMatrix(config-if)# no switchport egress ether-type
```

Defaults which TPID to be used in the S-TAG of the frames egressing on this port.

```
cnMatrix(config-if)# switchport ingress ether-type {x8100 | x88a8 | x9100}
```

Specifies which TPID to use to determine the S-TAG of the frames ingressing on this port.

```
cnMatrix(config-if)# no switchport ingress ether-type
```

Defaults the TPID used to determine the S-TAG of the frames ingressing on this port.

```
cnMatrix# show provider-bridge port config

Provider Bridge Port configuration table
```

Port Gi0/1

Port Type : Customer-edge Port

Dot1x Protocol Tunnel Status : Peer

LACP Protocol Tunnel Status : Peer

Spanning Tree Tunnel Status : Discard

LLDP Protocol Tunnel Status : Peer

Service VLAN Classification : Customer-VLAN

Unicast MAC Learning Status : Enable

Customer-VLAN : 10

Port Gi0/2

Port Type : Provider Network Port

Service VLAN Classification : PVID

```
cnMatrix# show service-vlan
```

```
Customer-VLAN Id Registration Table
```

Service VLAN	Port	Customer-VLAN	S-VLAN Priority
1000	Gi0/1	ALL	NONE

Provider-edge Port Configuration

Service VLAN	Port	PVID	Default Prio
1000	Gi0/1	NONE	5

Configuration example

1. Configure global settings:

   ```
   cnMatrix# boot default bridge-mode provider-edge
   ```

   The switch reboots to the default configuration, in “provider-edge” mode.

   Configure port modes:

   ```
   cnMatrix(config)# interface gigabitethernet 0/1
   ```

   ```
   cnMatrix(config-if)# bridge port-type customer-edge
   ```

   default is provider, so for the other ports, we do not have to configure anything.

2. Create S-VLANs

   ```
   cnMatrix(config)# vlan 100
   ```

   ```
   cnMatrix(config)# vlan 102
   ```

   ```
   cnMatrix(config)# vlan 103
   ```

   S-VLANs must be created before assigning customer-Vlans to them.

3. Map Customer VLANs to SVANs

   ```
   cnMatrix(config-if)# switchport customer-vlan 2 service-vlan 102
   ```

   ```
   cnMatrix(config-if)# switchport customer-vlan 3 service-vlan 103
   ```

   ```
   cnMatrix(config-if)# switchport service-vlan 100
   ```

   Traffic from VLAN 2 will go to S-VLAN 102, traffic from VLAN 3 will go to S-VLAN 103. All other traffic will go to S-VLAN 100.

4. Configure the dot1p priority in the S-VLAN.

   This is configured at the ingress of the customer port, and will be visible at egress on any provider port:

   ```
   cnMatrix(config-if)# switchport customer-vlan 2 svlan-prio {<0-7> | none}
   ```

   let’s say 5 in our example.

This means that any packet that ingresses on the customer port on C-VLAN 2 will have an S-TAG containing S-VLAN 102 and dot1p 5.

5. For untagged traffic ingressing on customer ports:

```
cnMatrix(config-if)# switchport customer-vlan pvid 2
```

Untagged traffic will get C-VLAN 2, and will go to S-VLAN 102 (as C-VLAN 2 is associated to S-VLAN 102).

or

```
cnMatrix(config-if)# switchport customer-vlan pvid 5
```

Untagged traffic will get C-VLAN 5, and will go to S-VLAN 100 (as C-VLAN 5 is not associated to any S-VLAN, it will go to the default S-VLAN).

or

```
cnMatrix(config-if)# switchport customer-vlan pvid disable
```

Untagged traffic will be left untagged. If a default service-vlan is configured for the port, it will go to that S-VLAN, if not, it will be dropped.

6. Add provider ports to the desired S-VLANs.

```
cnMatrix(config) #vlan 100

cnMatrix(config-vlan)# ports add gi 0/2

cnMatrix(config) #vlan 102

cnMatrix(config-vlan)# ports add gi 0/2

cnMatrix(config) #vlan 103

cnMatrix(config-vlan)# ports add gi 0/2
```

7. Add customer-edge ports to the S-VLANs. Customer-edge ports must be added as untagged ports.

```
cnMatrix(config) #vlan 100

cnMatrix(config-vlan)# ports add gi 0/1 untagged gi 0/1

cnMatrix(config) #vlan 102

cnMatrix(config-vlan)# ports add gi 0/1 untagged gi 0/1

cnMatrix(config) #vlan 103

cnMatrix(config-vlan)# ports add gi 0/1 untagged gi 0/1
```

8. Configure additional parameters, if needed

```
cnMatrix(config-if)# #switchport ingress ether-type x88a8
```

this is the default setting, but we support also 0x8100 and 0x9100.

```
cnMatrix(config-if)# #switchport egress ether-type x88a8
```

same thing, but for egress.

```
cnMatrix(config-if)# service-vlan <vlan-id> pvid
```

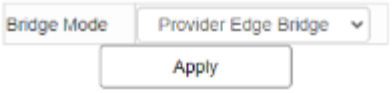
S-TAGGED but not C-TAGGED traffic will get the inner tag from this value. The PVID is configured on a customer-edge port and is applied on all provider ports which are members in the service VLAN.

```
cnMatrix(config-if)# service-vlan <vlan-id> def-user-pri
```

S-TAGGED but not C-TAGGED traffic will get the inner tag from this value. The default priority is configured on a customer-edge port and is applied on all provider ports which are members in the service VLAN.

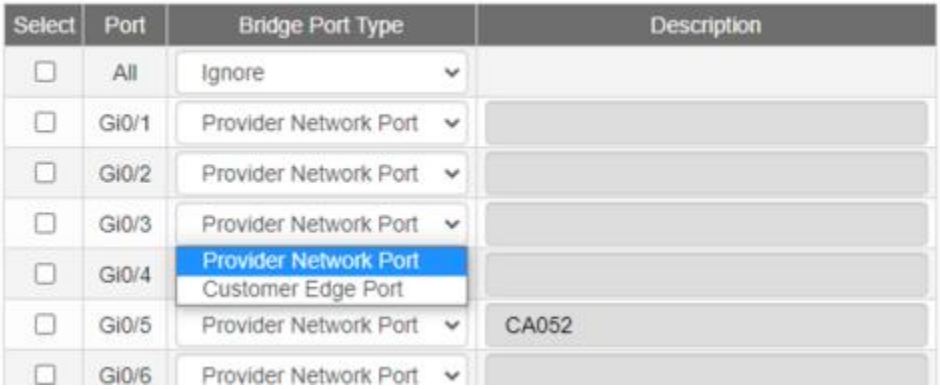
Configuring Q-in-Q via the Web GUI

Bridge mode selection

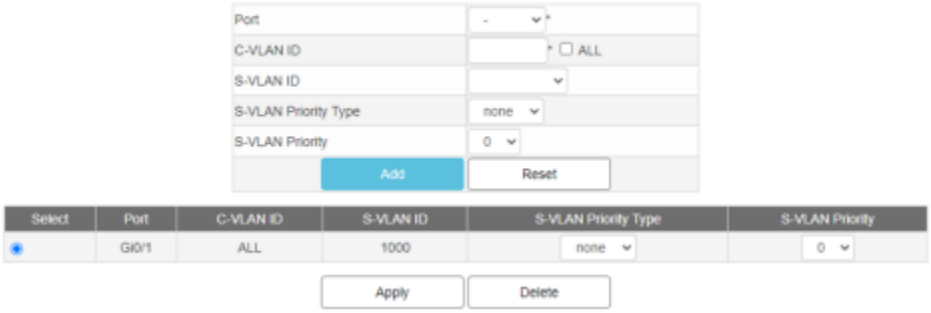


After selecting the desired bridge mode, the switch will reboot to the default settings.

Bridge Port Type Configuration



C-VID registration



When **ALL** is checked, all the traffic coming in on the customer port is mapped to the S-VLAN.

ether-type Config

Customer-Edge Port Configuration

Note:

Value zero for Customer PVID disables the assignment of a Customer-VLAN ID.

Provider Edge Port Configuration

Note:

Value zero for PVID disables the assignment of a Customer-VLAN ID.

Ethernet Ring Protection Switching

Feature Description

ERPS (Ethernet Ring Protection Switching) provides highly reliable and stable protection mechanism in ring networks and provides mechanism to avoid formation of loops, which would fatally affect network operation and service availability.

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This link is called the ring protection link (**RPL**), and under normal conditions this link is blocked, i.e., not used for traffic. One designated node, the **RPL owner**, is responsible to block traffic over the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the **RPL neighbor node**, may also participate in blocking or unblocking its end of the RPL.

ERPS uses the continuity check (CCM) capability from CFM to monitor the link status and to transmit/receive APS PDUs. This functionality is setup after ring setup is configured after the ring links are configured.

How to configure ERPS

Create and reserve a VLAN for ERPS control traffic

The following will create a configuration for the following network diagram:

Prerequisites

Ring ports must be members of the ERPS ring VLAN

i. Enter vlan 3500 configuration

Node1(config)# vlan 3500

ii. Add ERPS ports to the VLAN

Node1(config-vlan)# port add gigabitethernet 0/3

Node1(config-vlan)# port add gigabitethernet 0/5

ERPS configuration

1. Enable ERPS Globally

```
Node1(config)# aps ring enable
```

2. Configure an ERPS ring

```
Node1(config)# aps ring group 1
```

3. Create a ring

a. Configure ring member ports and control VLANs

Prerequisite: Create VLAN 3500 and add the given ports

```
cnMatrix(config-ring)# aps working gig 0/5 gig 0/3 vlan 3500
```

b. Optional: Configure the node role, here Node1 is the RPL owner

```
Node1(config-ring)# aps protect gig 0/5
```

c. Set the MEPs for local and remote ports (other CFM settings will be configured automatically)

```
Node1(config-ring)# aps working port1 local-mep 41 remote-mep 42
Node1(config-ring)# aps working port2 local-mep 32 remote-mep 34
```

d. Activate the ring group

```
Node1(config-ring)# aps group active
```

```
Node1 configuration:

       aps ring enable
aps ring group 1
aps working gigabitethernet 0/5 gigabitethernet 0/3 vlan 3500
aps protect gigabitethernet 0/5
aps working port1 local-mep 41 remote-mep 42
aps working port2 local-mep 32 remote-mep 34
       aps group active

Node2 configuration:

       aps ring enable
       aps ring group 1
       aps working gigabitethernet 0/5 gigabitethernet 0/6 vlan 3500
       aps working port1 local-mep 42 remote-mep 41
       aps working port2 local-mep 51 remote-mep 52
       aps group active


Node3 configuration:

       aps ring enable
       aps ring group 1
       aps working gigabitethernet 0/6 gigabitethernet 0/5 vlan 3500
       aps working port1 local-mep 52 remote-mep 51
       aps working port2 local-mep 34 remote-mep 32
       aps group active
```

Troubleshooting Ring failures

Run the following command:

Node1(config-ring)# do sh aps ring

If there is an issue, it can easily be seen after the CFM port status header:

Here port 2 of the ring has been misconfigured.

First thing to make sure is that the ring links are matching on both ends and are members of the same VLAN that is configured for ERPS. Second step is to check if the local MEP on current switch matches remote MEP on the remote, check if the other pair remote/local also matches.
The connectivity issues can be sorted without enabling ERPS, after solving them you can enable ERPS, and the ring will transition to Idle state after the timers have finished.

LimitationsAll limitations that ERPS version 1 has apply to the current implementation:

- No compatibility with version 2, as they have different state machines
- Not supported: manual switch, force switch and non-revertive mode, if the fault(s) are cleared ring will revert to the initial state regardless of what has happened to the network
- It is recommended to use different VLAN for each ring, as ERPS messages could hop between rings
- Rings can't share the same link as it will cause network segmentation
- Only port-based configuration can be set, service based will be supported in version 2
- Router ports can't be part of an ERPS ring.
- STP can't be used on ports part of the ring. Configuring ring links will disable STP for those ports. When removing the ring configuration STP will be left disabled and will have to be enabled manually.

L3 Features

DHCP Relay

Managing DHCP Relay

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 of 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.

Attention

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

Network Diagram

How to Enable DHCP Relay in CLI Interface

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.
6. For more information, see DHCP Relay Parameters and Commands.

Routed Interface

Managing Routed Ports

Feature Overview

Starting with version 4.2, the switch dynamically allocate routed ports VLAN IDs as opposed to reserve the upper-portion of VLAN IDs for that purpose.

The VLAN ID could be provided on the command line when the command that create the router port is issued or, if omitted, it would be used the greatest VLAN ID available.

The available range for VLAN ID is: 1 – 4094.

The number of routed ports that can be created is 8.

Note:

The Routed Ports feature can be configured via CLI, Web and SNMP.

Attention!

Routed Ports(VLAN ID dynamic allocation) feature is supported starting with cnMatrix release 4.2.

Standards

N/A

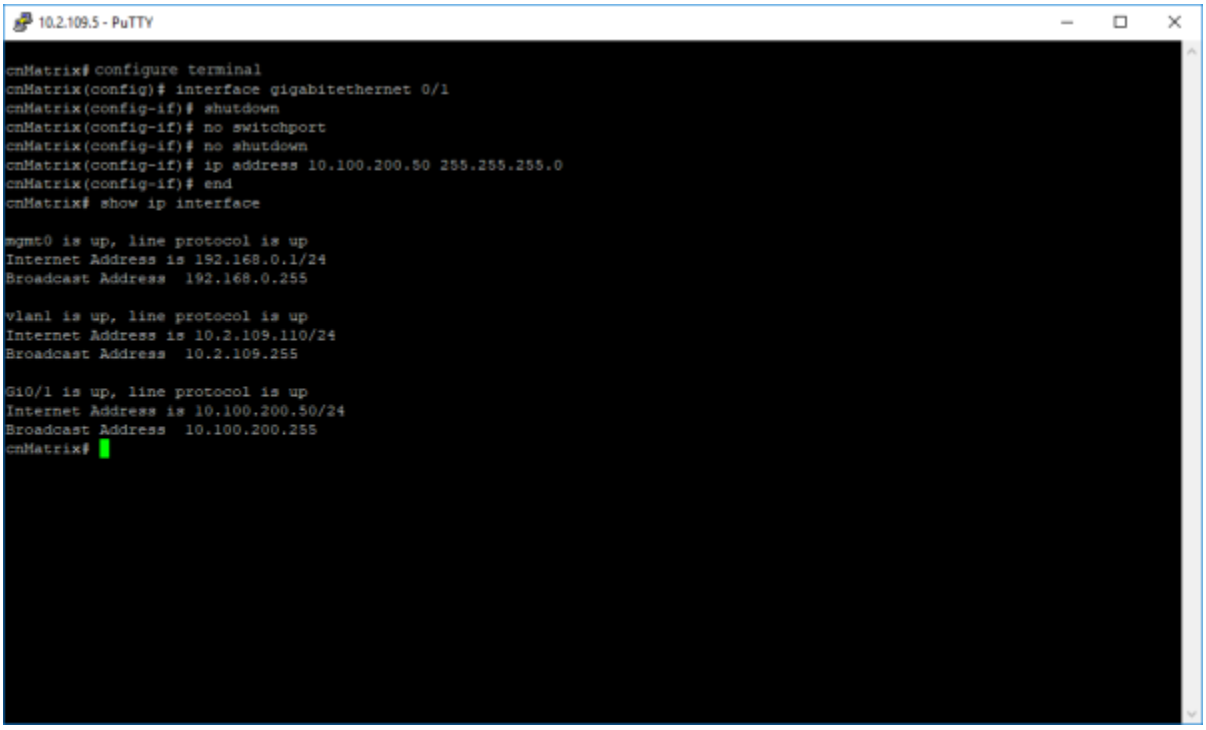
Limitations

N/A

Default Values

N/A

How to Enable Routed Interfaces in CLI Interface (Example 1)



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.

Note:

In case the command is used without the **vid** parameter the system allocates the greatest VLAN ID available.

How to Enable Routed Interfaces in CLI Interface (Example 2)

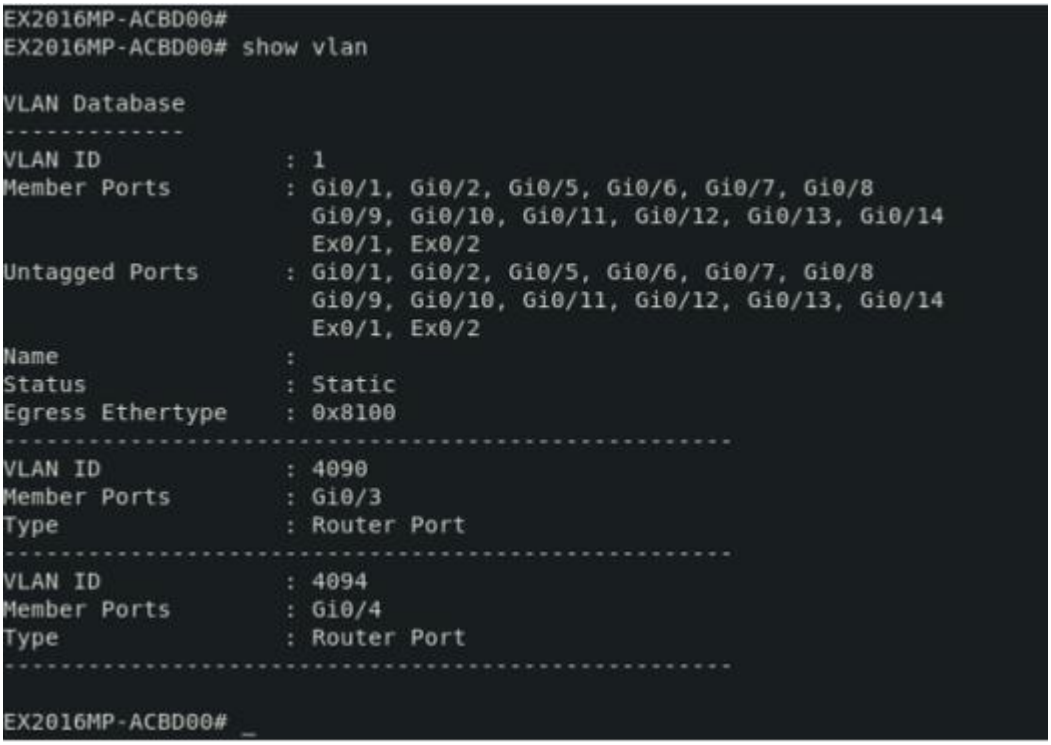
```
EX2016MP-ACBD00# config terminal
EX2016MP-ACBD00(config)# interface gigabitethernet 0/3
EX2016MP-ACBD00(config-if)# shutdown
EX2016MP-ACBD00(config-if)# no switchport vid 4090
EX2016MP-ACBD00(config-if)# no shutdown
EX2016MP-ACBD00(config-if)# end
EX2016MP-ACBD00#
```

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/3** command into the terminal to select the interface to be configured. Press the **Enter** key.
3. Type the **shutdown** command into the terminal to disable the interface. Press the **Enter** key.
4. Type the **no switchport vid 4090** command into the terminal to set the port(interface) as a routed port. Press the **Enter** key.
5. Type the no **shutdown** command into the terminal to enable the interface. Press the **Enter** key.

Note:

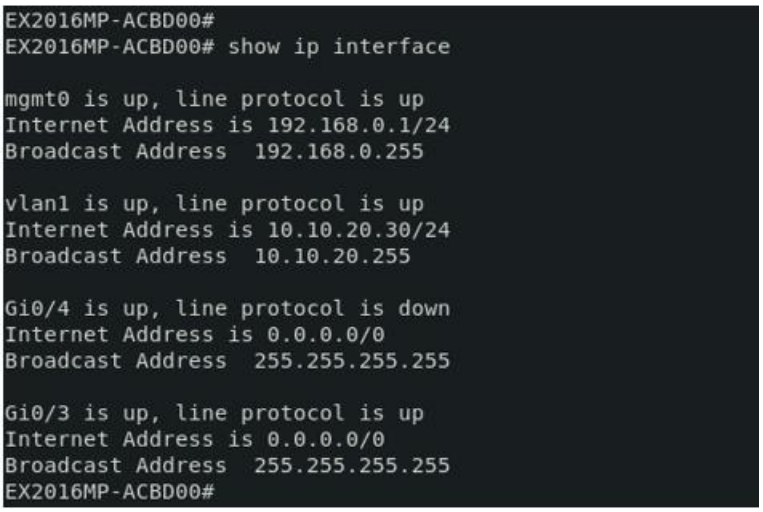
Once a **VLAN ID** is used for a Router port it cannot be used when creating a new VLAN and consequently, once an ID is used for a VLAN, the same ID cannot be used when creating a Router port.

How to show Routed Ports using show VLAN command



Type the **show vlan** command into the terminal. Press the **Enter** key.

How to show Routed Ports using show ip interface command



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

How to change Routed Ports vid

```
EX2016MP-ACBD00#
EX2016MP-ACBD00# config terminal
EX2016MP-ACBD00(config)# interface gigabitethernet 0/4
EX2016MP-ACBD00(config-if)# shutdown
EX2016MP-ACBD00(config-if)# port-vid 4093
EX2016MP-ACBD00(config-if)# no shutdown
EX2016MP-ACBD00(config-if)# end
EX2016MP-ACBD00#
```

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 the interface to be configured. Press the **Enter** key.
3. Type the **shutdown** command into the terminal to disable the interface. Press the **Enter** key.
4. Type the **port-vid 4093** command into the terminal to change the VLAN ID used for that router port. Press the **Enter** key.
5. Type the **no shutdown** command into the terminal to enable the interface. Press the **Enter** key.

Note:

If an ID is used for a VLAN, the same ID cannot be used for a Router Port.

How to disable a Routed Port

```
EX2016MP-ACBD00#
EX2016MP-ACBD00# config terminal
EX2016MP-ACBD00(config)# interface gigabitethernet 0/3
EX2016MP-ACBD00(config-if)# shutdown
EX2016MP-ACBD00(config-if)# switchport
EX2016MP-ACBD00(config-if)# no shutdown
EX2016MP-ACBD00(config-if)# end
EX2016MP-ACBD00#
```

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/3** command into the terminal to select the interface to be configured. Press the **Enter** key.
3. Type the **shutdown** command into the terminal to disable the interface. Press the **Enter** key.
4. Type the **switchport** command into the terminal to set the port(interface) into a switch port. Press the **Enter** key.
5. Type the **no shutdown** command into the terminal to enable the interface. Press the **Enter** key.

Troubleshooting Routed Ports

Useful commands for troubleshooting

- cnMatrix# show ip interface
- cnMatrix# show running-config ip
- cnMatrix# show running-config

IP Routing

Managing IP Routing

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

Note

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.

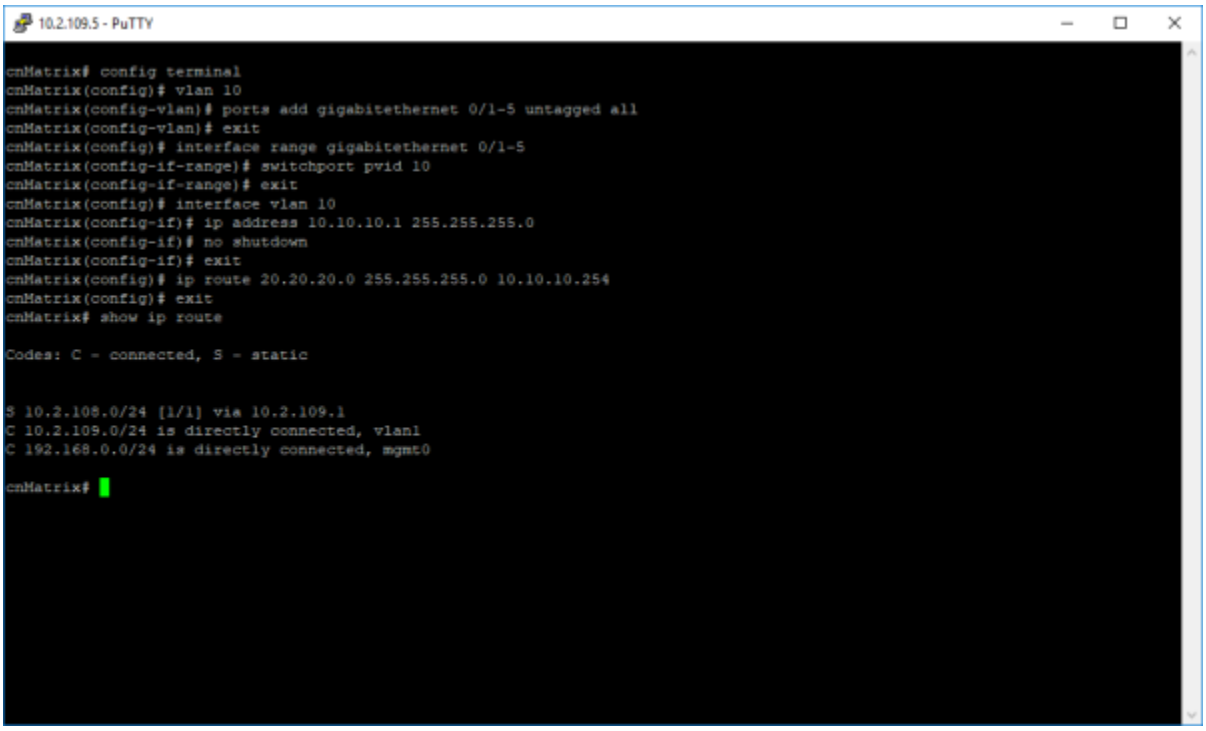
Default Values

- 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

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.

RIP (Starting with version 2.1)

Managing RIP

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 the 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.

Attention

Dynamic Routing is not supported on EX1028, EX1028-P, EX1010, and EX1010-P switches, therefore RIP functionality is not available for cnMatrix EX1028, EX1028-P, EX1010, and EX1010-P.

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.

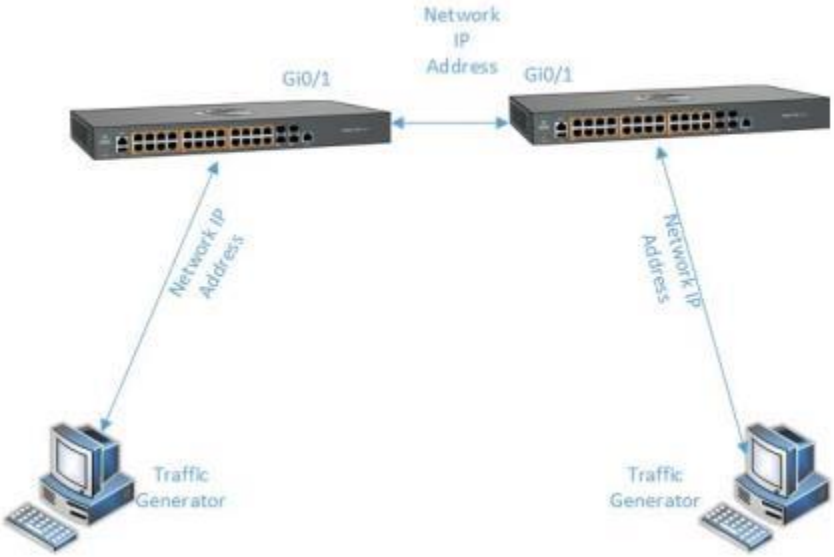
Default Values

- 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.

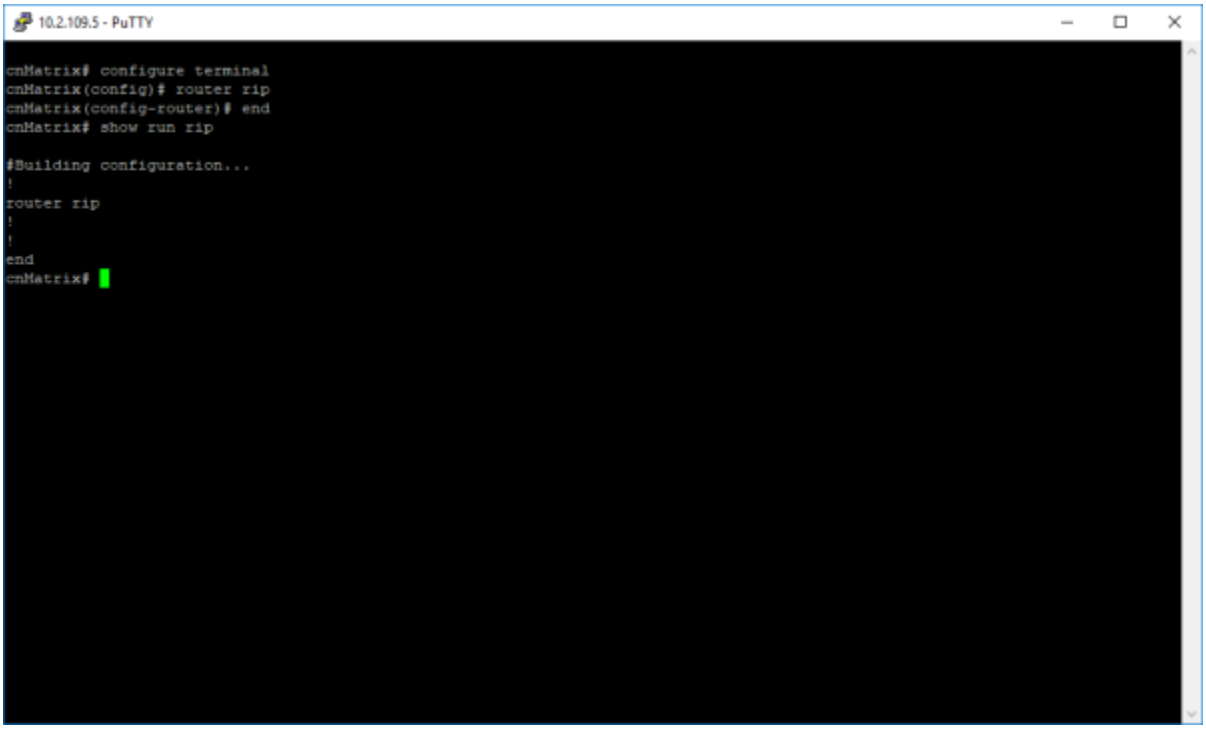
Prerequisites

- 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.

Network Diagram

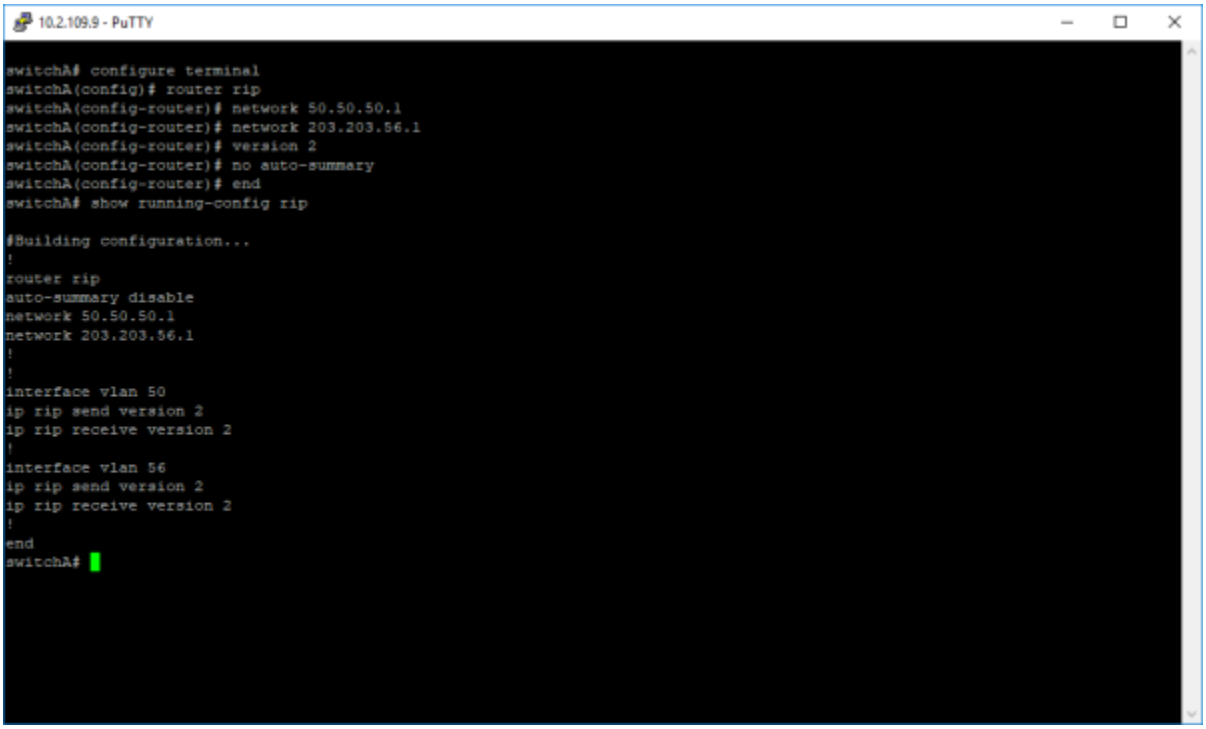


How to Enable RIP in CLI Interface



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 current operating configuration. Press the **Enter** key.

How to Configure RIP in CLI Interface (example)



Before configuring RIP, ensure that the following are configured previously:

Configuration example 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

Configuration example 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

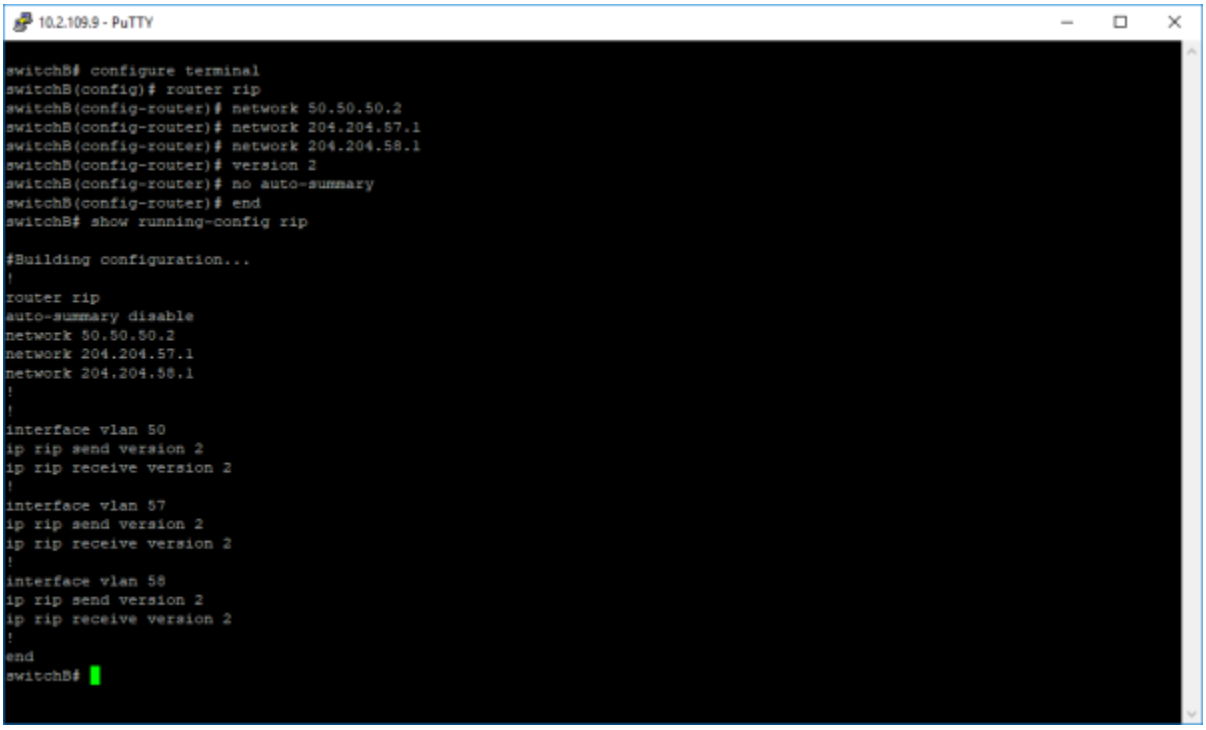
vlan 57
ports gigabitethernet 0/2 untagged gigabitethernet 0/2

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

interface gigabitethernet 0/2
switchport pvid 57
no shutdown

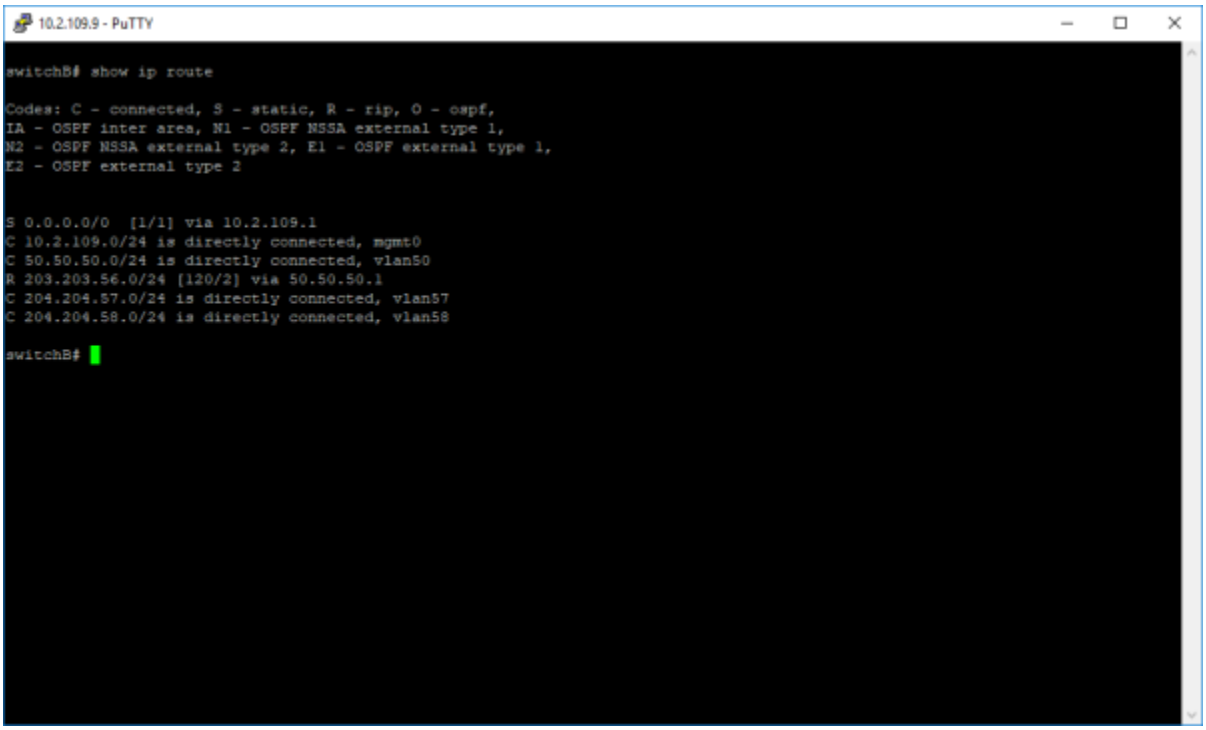
SWITCH A

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **router rip** command into the terminal to enable the RIP feature and to enter the router configuration mode. Press the **Enter** key.
3. 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.
4. 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.
5. Type the **version 2** command into the terminal to configure the global version of the RIP feature. Press the **Enter** key.
6. Type the **no auto-summary** command into the terminal to disable auto summarization in RIP. 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 running-config rip** command into the terminal. Press the **Enter** key.



SWITCH B

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **router rip** command into the terminal. Press the **Enter** key.
3. Type the **network 50.50.50.2** command into the terminal. Press the **Enter** key.
4. Type the **network 204.204.57.1** command into the terminal. Press the **Enter** key.
5. Type the **network 204.204.58.1** command into the terminal. Press the **Enter** key.
6. Type the **version 2** command into the terminal. Press the **Enter** key.
7. Type the **no auto-summary** command into the terminal. 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 running-config rip** command into the terminal. Press the **Enter** key.
10. Type the **show ip route** command into the terminal. Press the **Enter** key.



OSPF (Starting with version 2.1)

Managing OSPF

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.

Caution

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

Attention

Dynamic Routing is not supported on EX1028, EX1028-P, EX1010, and EX1010-P switches, therefore OSPF functionality is not available for cnMatrix EX1028, EX1028-P, EX1010, and EX1010-P.

Standards

- RFC 1583
- RFC 3509
- RFC 2328

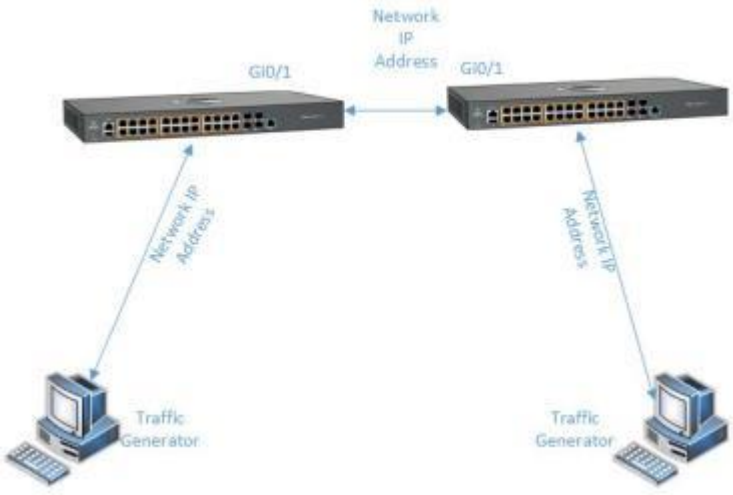
Default Values

- 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.

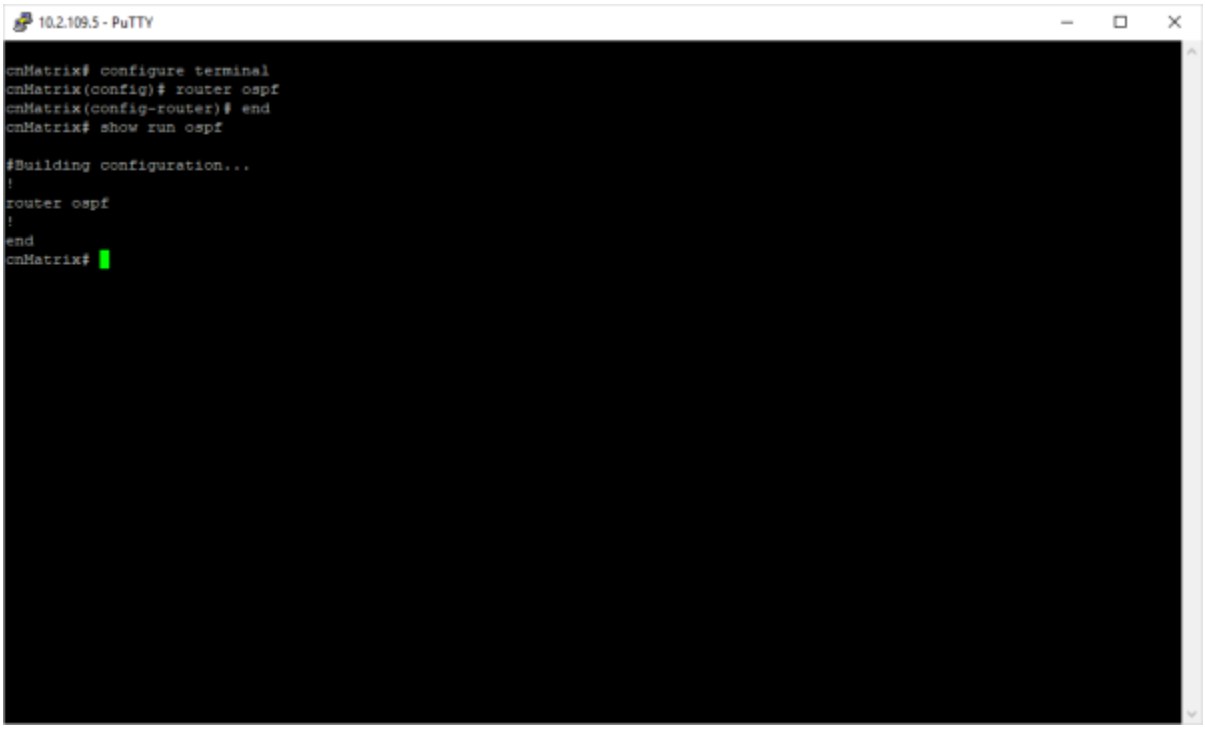
Prerequisites

- N/A

Network Diagram

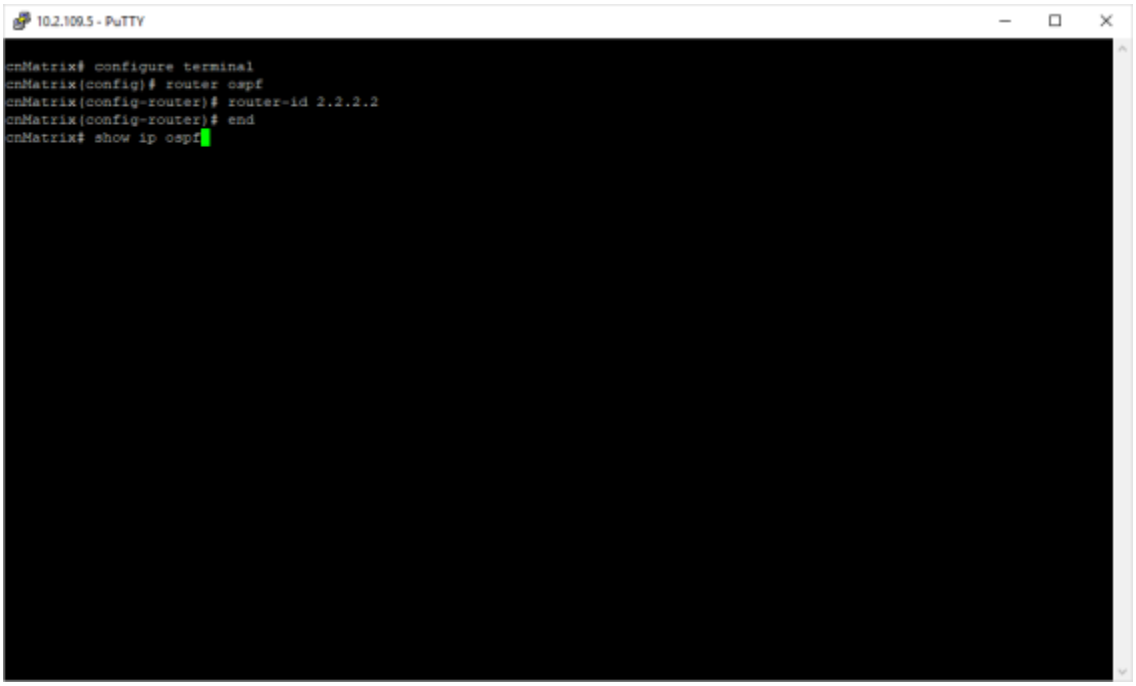


How to Enable OSPF in CLI Interface

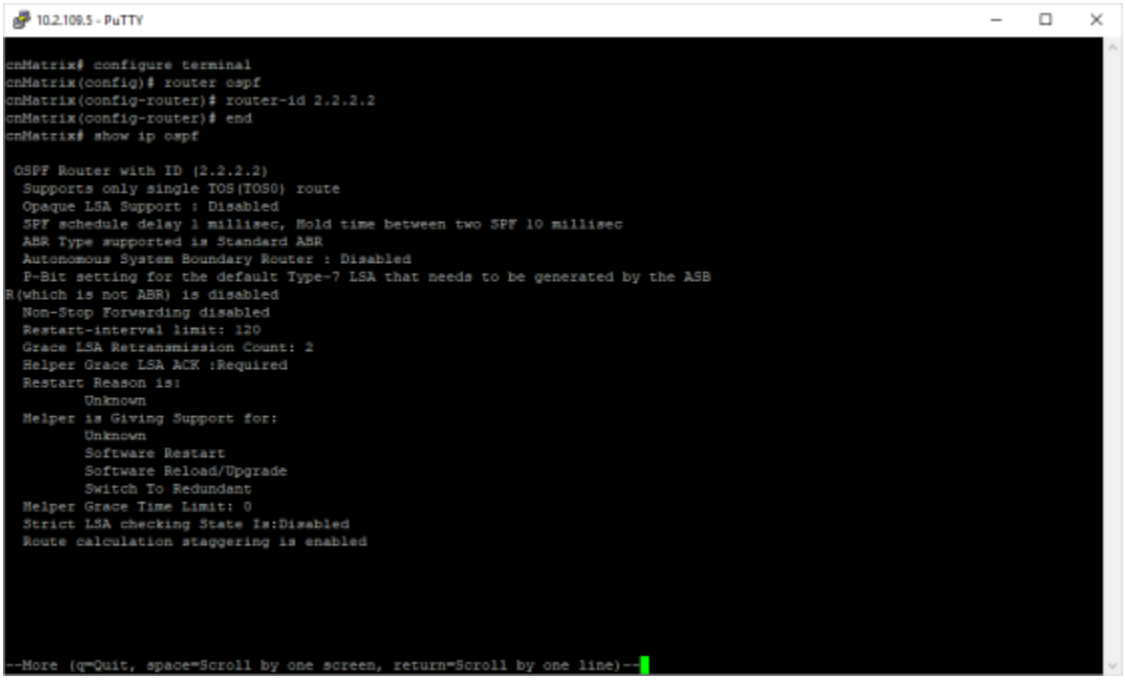


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **router ospf** command into the terminal to enable the OSPF feature. Press the **Enter** key.
3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.
4. 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.

How to Configure OSPF Router ID in CLI Interface

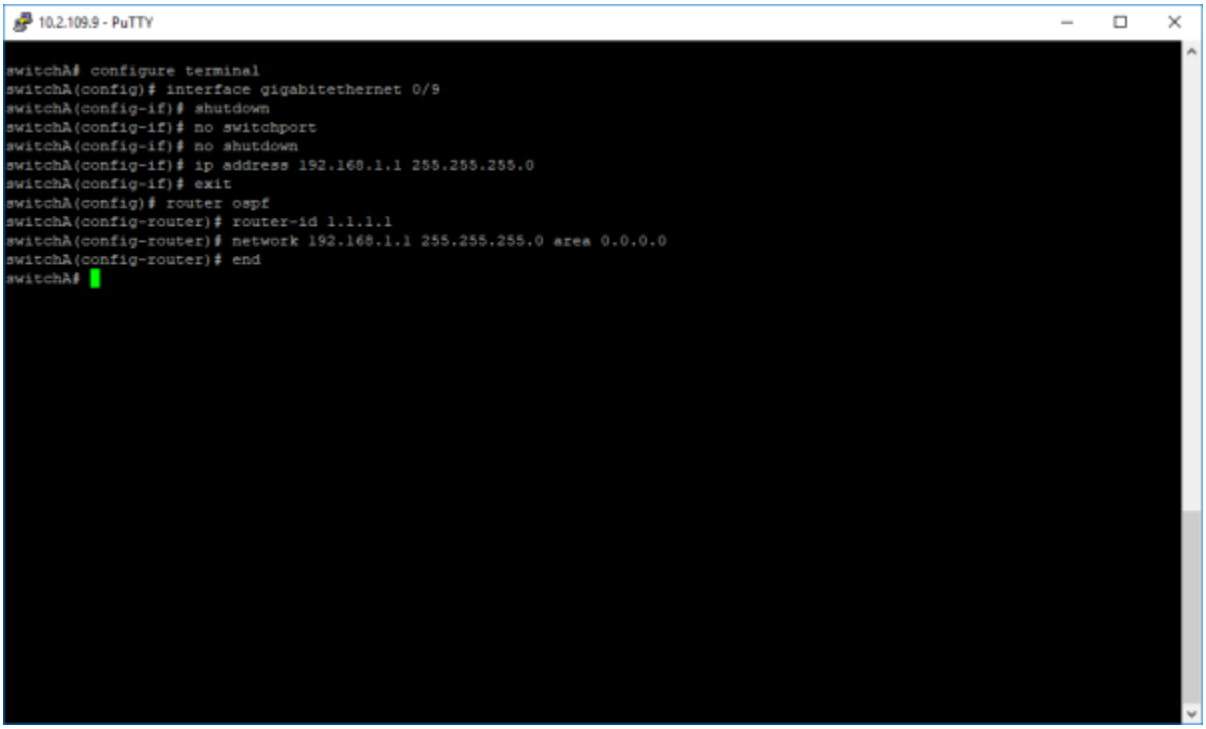


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **router ospf** command into the terminal to enable the OSPF feature. Press the **Enter** key.
3. Type the **router-id 2.2.2.2** command into the terminal to set the router ID for the OSPF process. Press 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).



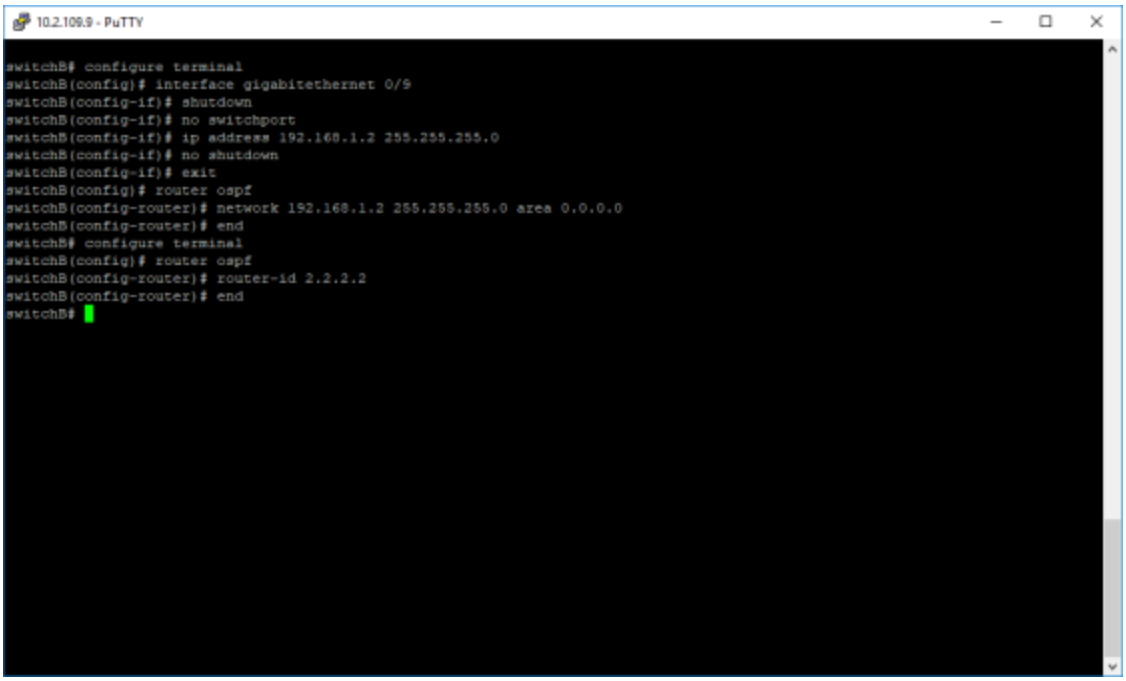
For more information, see OSPF Parameters and Commands.

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 Privileged EXEC mode on switch A. Press the **Enter** key.



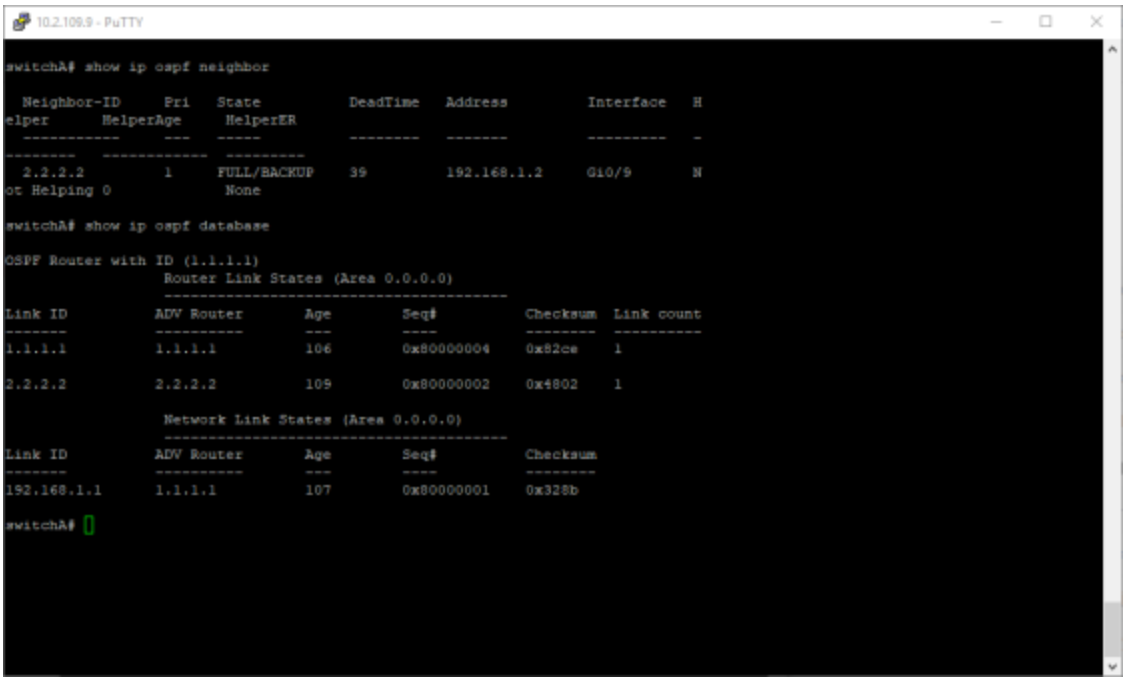
SWITCH B

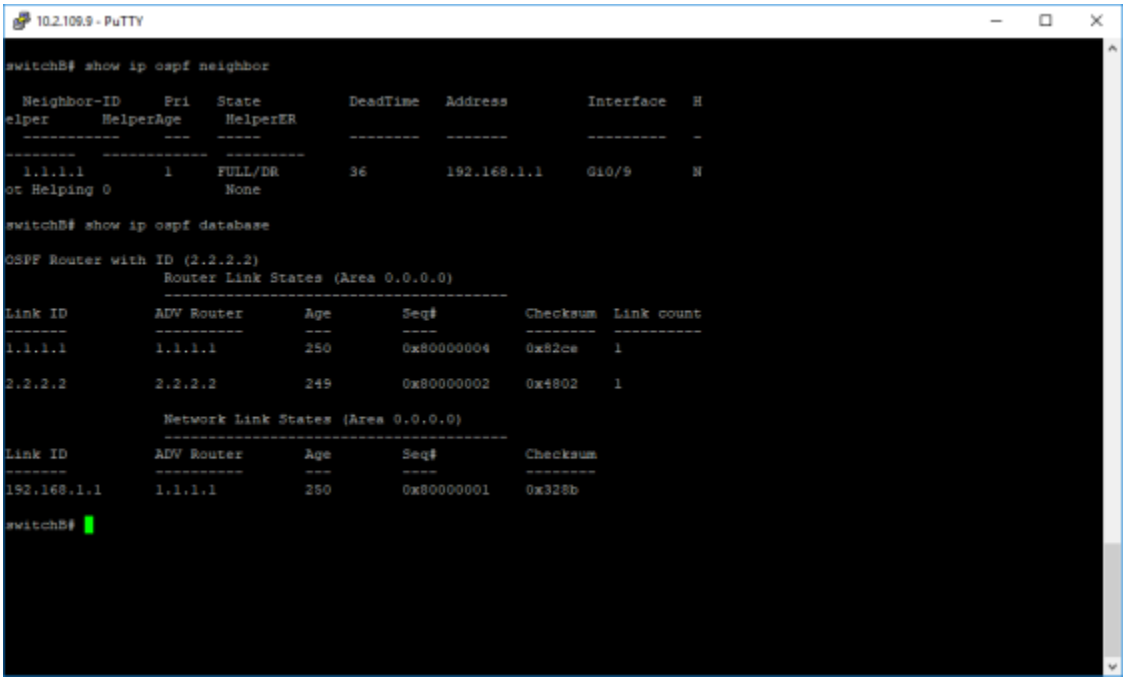
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/9** command into the terminal to select the interface to be configured on switch B. Press the **Enter** key.
3. Type the **shutdown** command into the terminal. Press the **Enter** key.
4. Type the **no switchport** command into the terminal. Press the **Enter** key.
5. Type the **ip address 192.168.1.2 255.255.255.0** command into the terminal. Press the **Enter** key.
6. Type the **no shutdown** command into the terminal. 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 field to enable the OSPF routing process and to enter the configuration router mode on switch B. Press the **Enter** key.
9. Type the **network 192.168.1.2 255.255.255.0 area 0.0.0.0** command into the terminal. Press the **Enter** key.
10. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the **Enter** key.

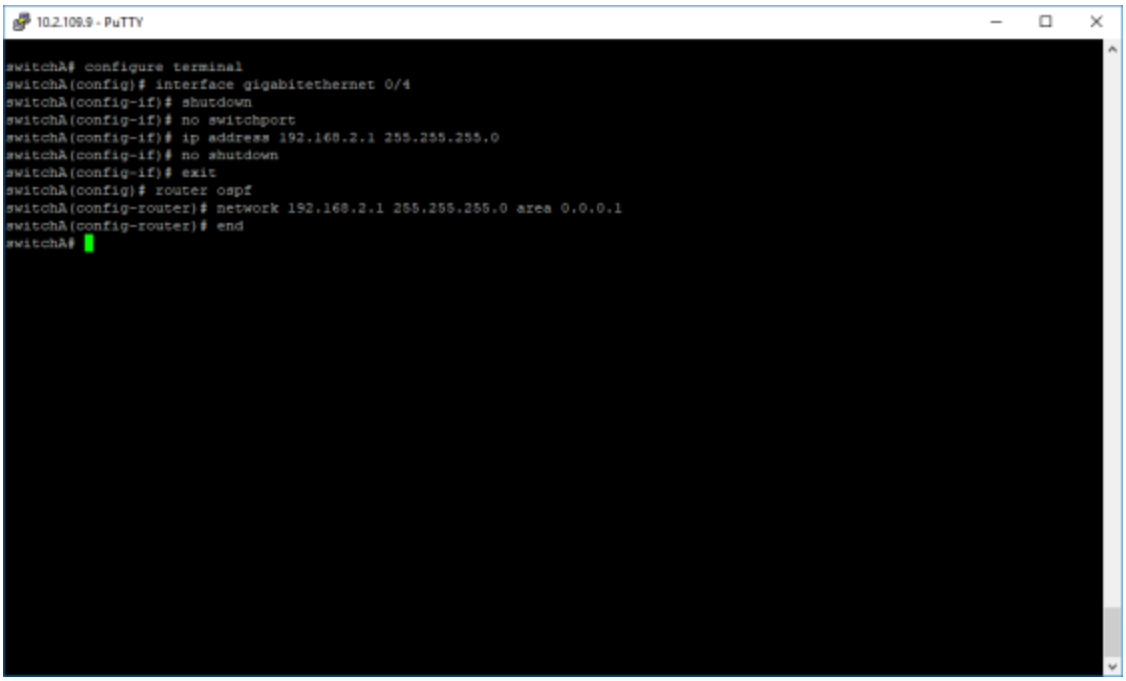
Note

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:

11. Type the **configure terminal** command into the terminal. Press the **Enter** key.
12. Type the **router ospf** command into the terminal. Press the **Enter** key.
13. Type the **router-id 2.2.2.2** command into the terminal. Press the **Enter** key.
14. Type the **end** command into the terminal to go back to the Privileged EXEC mode on switch B. Press the **Enter** key.
15. This is how you can verify if the configuration was successful on both switches:
16. 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.
17. 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.

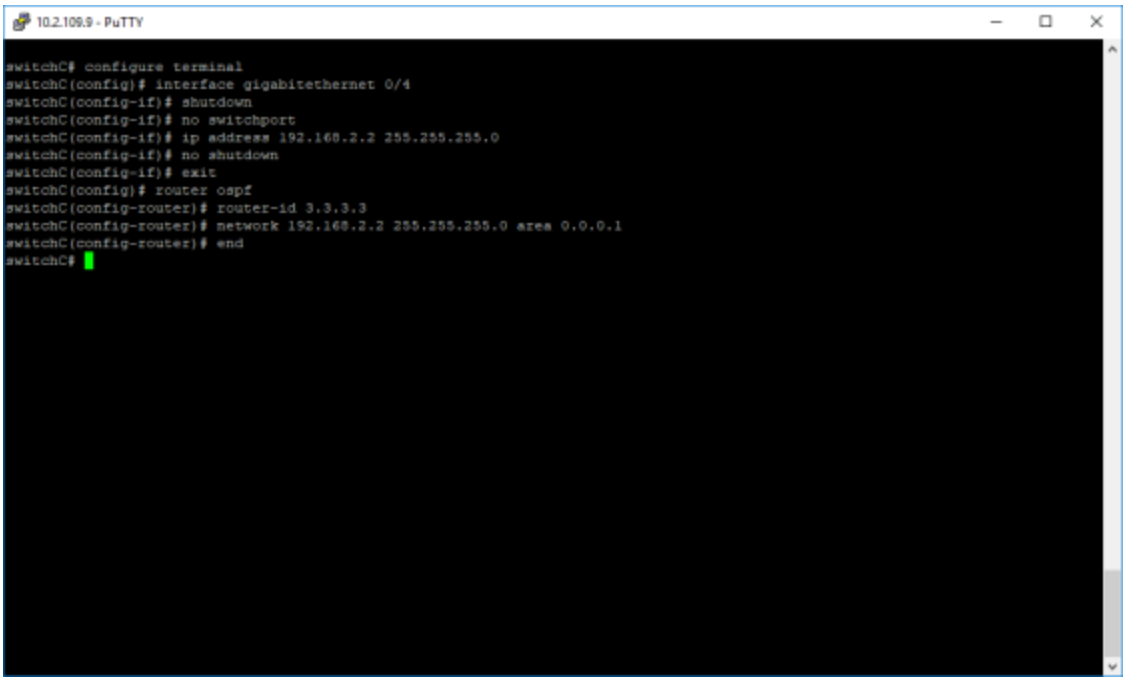

10.2.109.9 - PuTTY
switchA# show ip ospf neighbor
Neighbor-ID Pri State DeadTime Address Interface H
elper HelperAge HelperER
2.2.2.2 1 FULL/BACKUP 39 192.168.1.2 Gi0/9 N
ot Helping 0 None
switchA# show ip ospf database
OSPF Router with ID (1.1.1.1)
Router Link States (Area 0.0.0.0)
Link ID ADV Router 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#



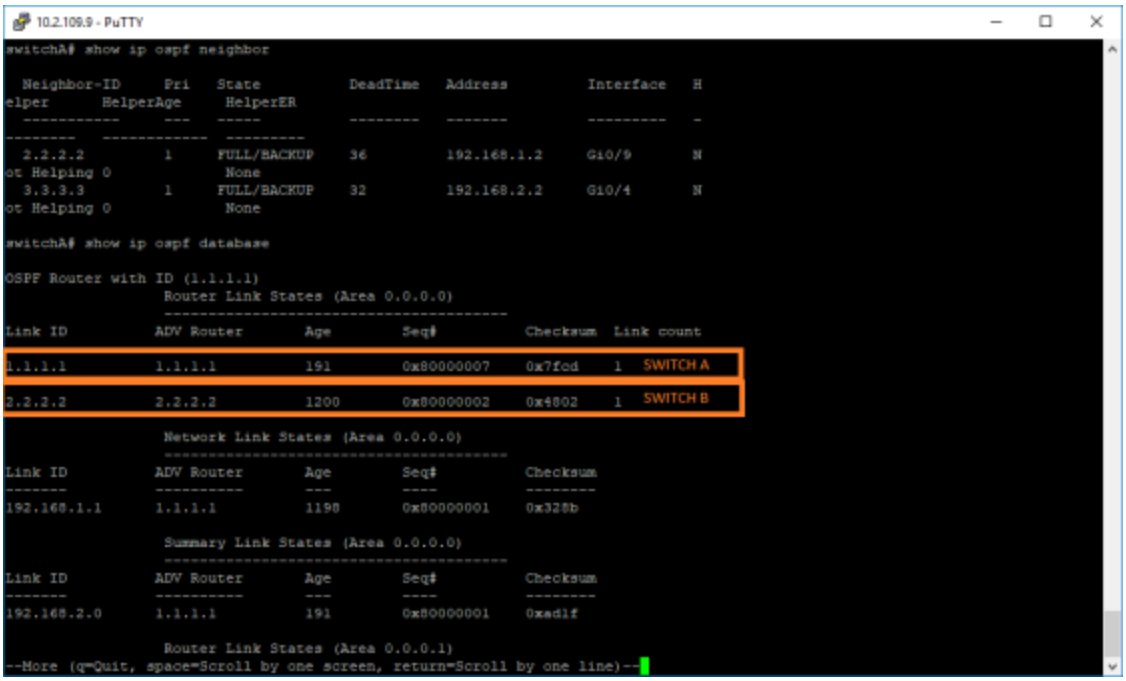
SWITCH A

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/4** command into the terminal. Press the **Enter** key.
3. Type the **shutdown** command into the terminal. Press the **Enter** key.
4. Type the **no switchport** command into the terminal. Press the **Enter** key.
5. Type the **ip address 192.168.2.1 255.255.255.0** command into the terminal. Press the **Enter** key.
6. Type the **no shutdown** command into the terminal. 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. Press the **Enter** key.
9. Type the **network 192.168.2.1 255.255.255.0 area 0.0.0.1** command into the terminal. Press the **Enter** key.
10. Type the **end** command into the terminal to go back to the Privileged EXEC mode on switch A. Press the **Enter** key.

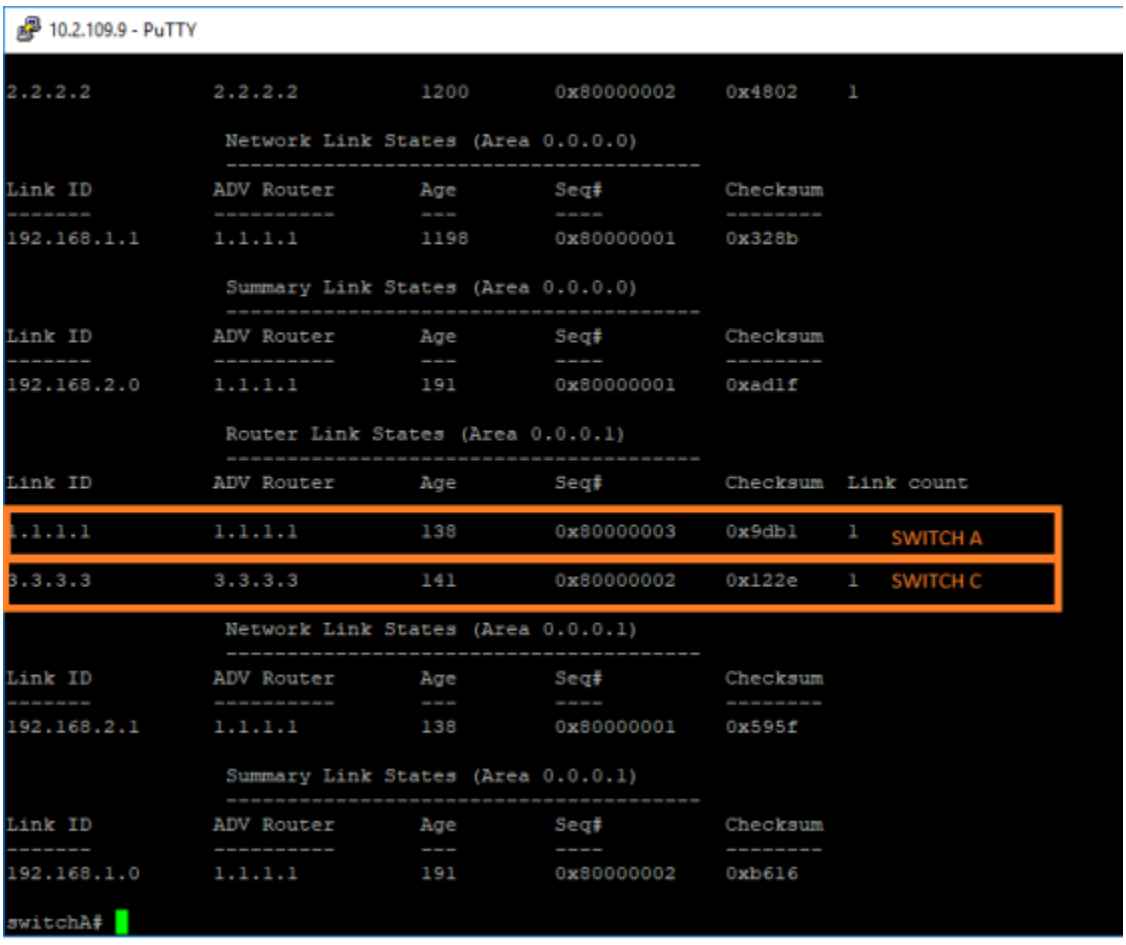


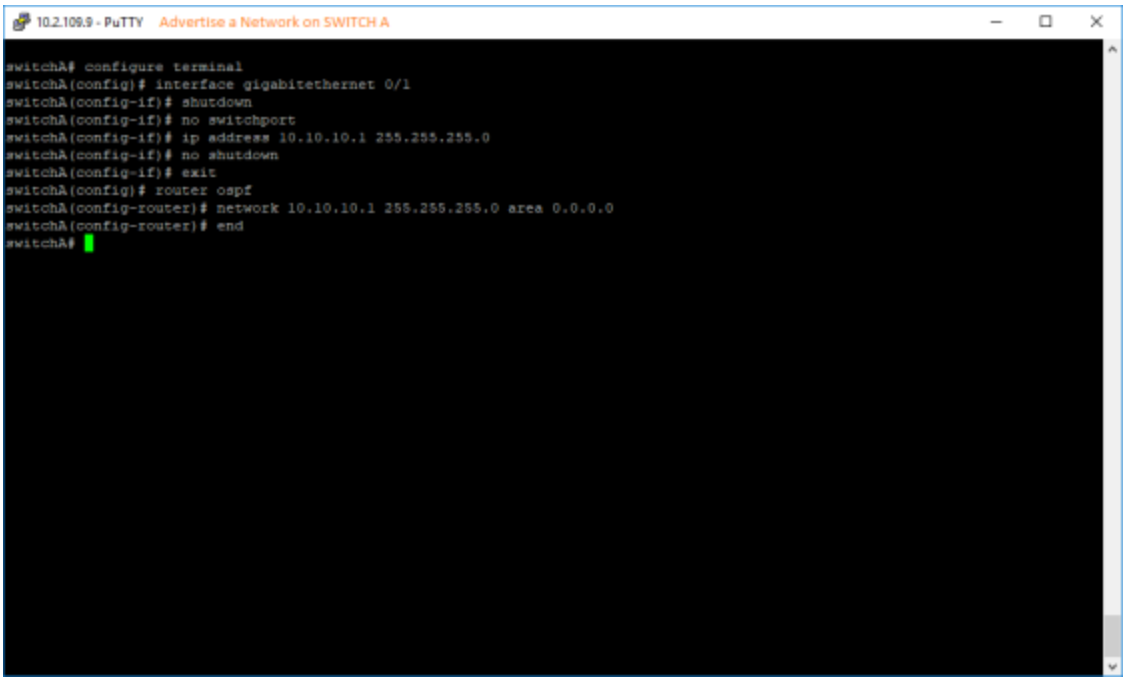
SWITCH C

1. Type the **configure terminal** command into the field. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/4** command into the terminal. Press the **Enter** key.
3. Type the **shutdown** command into the terminal. Press the **Enter** key.
4. Type the **no switchport** command into the terminal. Press the **Enter** key.
5. Type the **ip address 192.168.2.2 255.255.255.0** command into the terminal. Press the **Enter** key.
6. Type the **no shutdown** command into the terminal. 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. Press the **Enter** key.
9. Type the **router-id 3.3.3.3** command into the terminal. Press the **Enter** key.
10. Type the **network 192.168.2.2 255.255.255.0 area 0.0.0.1** command into the terminal. Press the **Enter** key.
11. Type the **end** command into the terminal. Press the **Enter** key.
12. 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.
13. Type the **show ip ospf database** command into the (in switch A and switch C) to display the OSPF Link State Database.



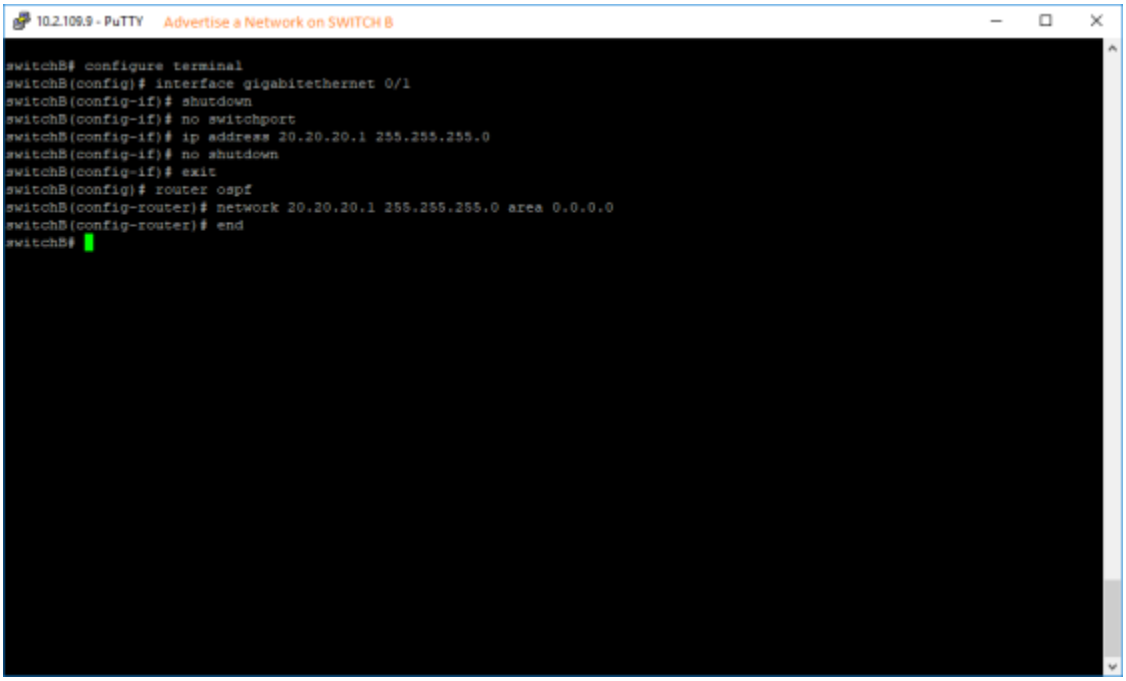
14. Press the **Enter** key.





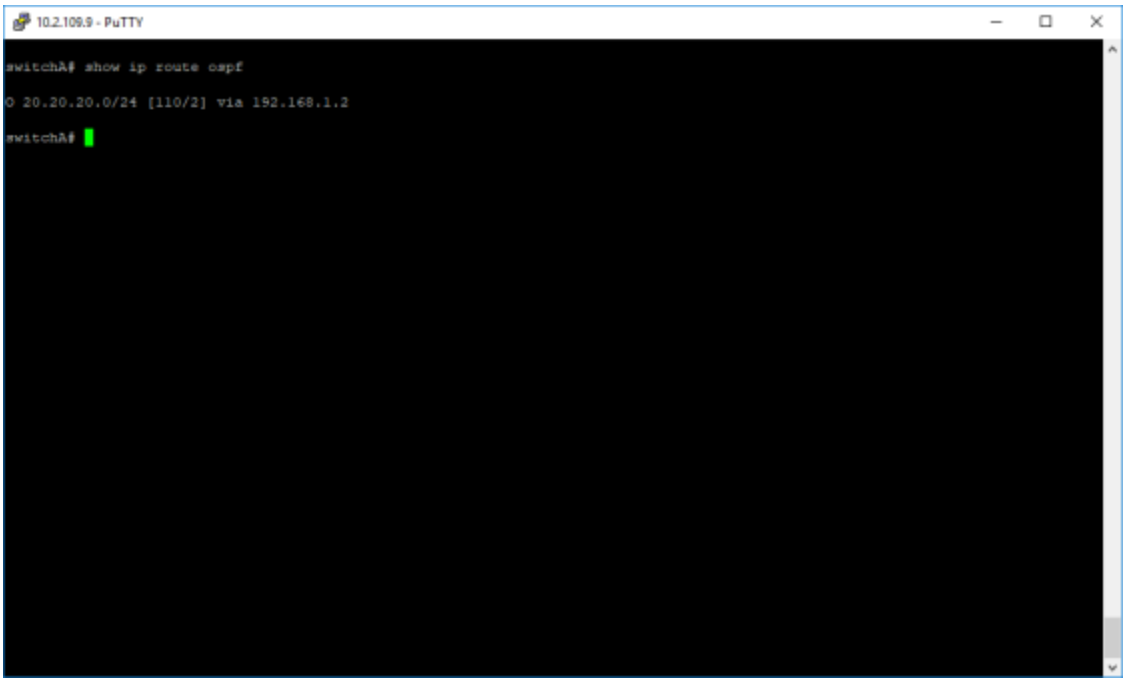
SWITCH A

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 **shutdown** command into the terminal. Press the **Enter** key.
4. Type the **no switchport** command into the terminal. Press the **Enter** key.
5. Type the **ip address 10.10.10.1 255.255.255.0** command into the terminal. Press the **Enter** key.
6. Type the **no shutdown** command into the terminal. 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. Press the **Enter** key.
9. Type the **network 10.10.10.1 255.255.255.0 area 0.0.0.0** command into the terminal. Press the **Enter** key.
10. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.

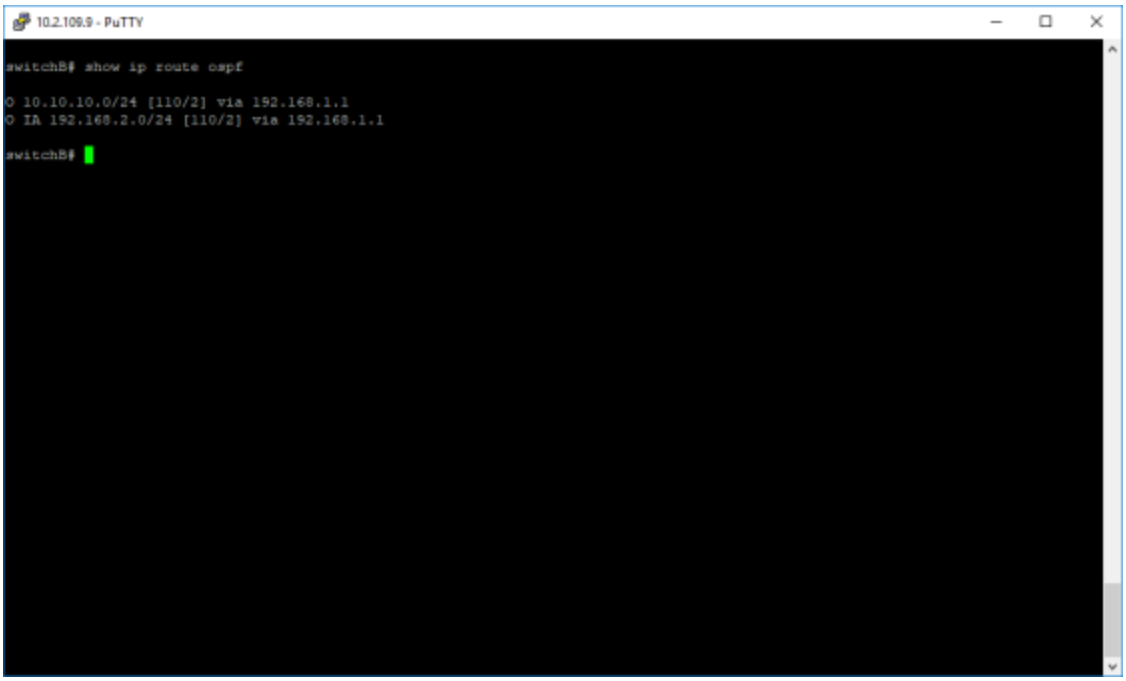


SWITCH B

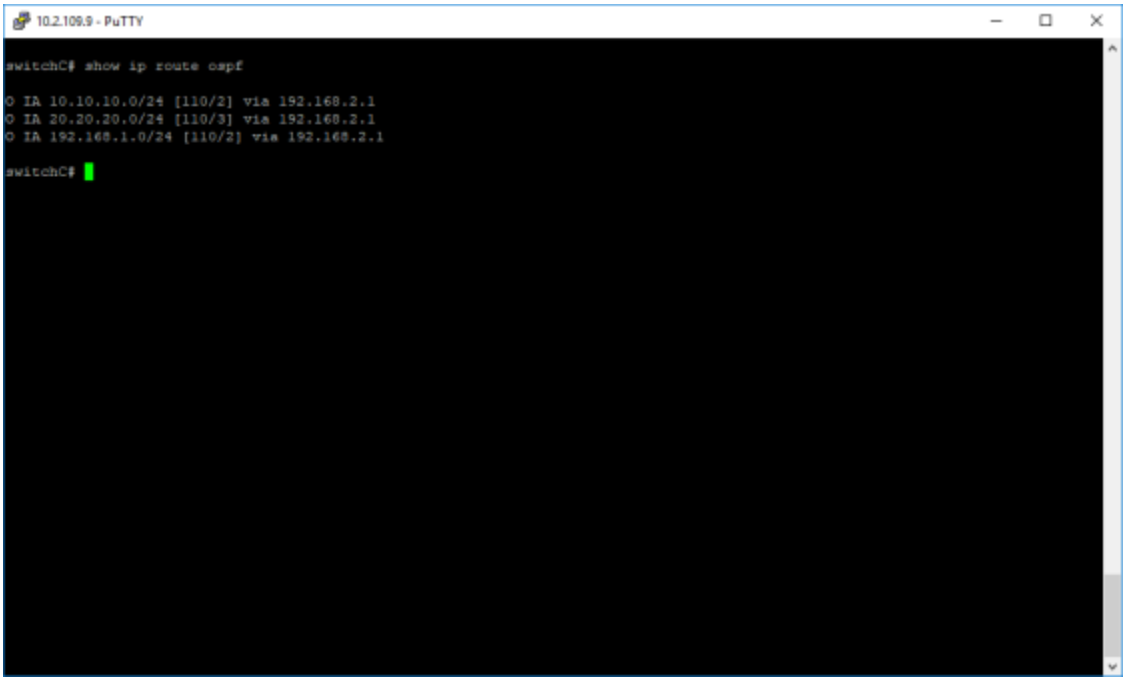
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/1** command into the terminal. Press the **Enter** key.
3. Type the **shutdown** command into the terminal. Press the **Enter** key.
4. Type the **no switchport** command into the terminal. Press the **Enter** key.
5. Type the **ip address 20.20.20.1 255.255.255.0** command into the terminal. Press the **Enter** key.
6. Type the **no shutdown** command into the terminal. 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. Press the **Enter** key.
9. Type the **network 20.20.20.1 255.255.255.0 area 0.0.0.0** command into the terminal. Press the **Enter** key.
10. Type the **end** command into the terminal. Press the **Enter** key.



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



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



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

How to configure OSPF network type

Starting with version 4.4, additional OSPF network types are supported for Non-broadcast, Point-to-Multipoint Non-Broadcast, and Point-to-Point.

Web configuration is not available in 4.4.

Command	Explanation
# configure terminal	Enter global configuration mode.
(config)# interface ip-interface	Enter interface configuration mode on the IP interface that you want to change OSPF network type on.
(config-if)# ip ospf network {broadcast | non-broadcast | point-to-multipoint non-broadcast | point-to-point}	Configure the desired OSPF network type. **Default**: broadcast
(config-if)# exit	Exit interface configuration mode.
(config)# router ospf	Enter OSPF router configuration mode.
(config-router)# neighbor neighbor-ip	Configure static neighbors for non-broadcast network types.

Protocol Independent Multicast – Sparse Mode

Feature Description

PIM is IP routing protocol-independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Open Shortest Path First (OSPF), and static routes. PIM uses this unicast routing information to perform the multicast forwarding function.
Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

PIM-SM uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees, it
requires the use of a rendezvous point (RP). The RP address is used by first-hop routers to send, PIM register messages on behalf of, a host sending a packet to the group. The RP address is also used by last-hop routers to send, PIM join/prune messages to the RP to inform it about, group
membership. The RP must be administratively configured in the network. A PIM router can be an RP for more than one group. A group can have more than one RP. The conditions specified by the access list determine for which groups the router is an RP.

Sources register with the RP and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S, G) join messages towards that

source. Each router along the reverse path compares the unicast routing metric of the RP address to the metric of the source address. If the metric for the source address is better, it will forward a PIM (S, G) join message towards the source. If the metric for the RP is the same or better, then the
PIM (S, G) join message will be sent in the same direction as the RP. PIM-SM is useful and applicable in large networks like in medium to large enterprises or small service provider networks. In such environments, the multicast traffic receivers tend to be scattered across the network resulting in a sparse multicast tree.

Supported functionality

- PIM Sparse Mode version 2
- Processes notifications from an IGMP module about changes in multicast membership on attached interfaces, and uses the notifications to trigger appropriate PIM messages.
- Manages establishment and removal of (*, G) or (S, G) entries.
- Implements the Hello state machine to periodically send Hello messages to discover neighboring PIM routers and to maintain neighbor information received through Hello messages.
- Performs DR (Designated Router) election for PIM-SM, on each interface based on the priority and IP address of the PIM routers on that interface.
- Maintains timers to age out stale neighboring router information.
- Uses Asserts for PIM-SM groups to elect a single forwarder in each multi access LAN that this router is a part of, when multiple routers are forwarding on that same interface.
- Exchanges Join / Prune messages with neighbors to manage the multicast delivery tree.
- Can be configured to be a RP (Rendezvous Point).
- Supports flexible group mask length configuration for static RP and candidate RP configuration.
- Points the multicast tree core towards the multicast source, when configured as a RP.
- Builds and maintains the RP, rooted shared trees (Multicast delivery trees) using periodic and triggered Join/ Prune messages.
- Implements register messages for PIM-SM groups to the RP encapsulate packets initially when a source first sends traffic to a group.
- Implements the RPF (Reverse Path Forwarding) algorithm.
- Calculates the shortest path and constructs the multicast tree, for PIM-SM groups, after which further Register messages are avoided and the multicast flows freely.
- Adapts to unicast route changes and attached interface state changes to appropriately trigger the necessary protocol actions.
- Supports regular housekeeping functions such as ND and timeout, BSR (Bootstrap Router) election, transmitting periodic C-RP (Candidate-RP) advertisements to the BSR, RP-Set distribution by BSR to all PIM routers.
- The Bootstrap router will trigger the update RP-Set as soon as it receives updated RP-candidate information from other PIM routers.
- A single PIM domain is supported.
- Uses checksums to validate PIM messages.
- Provides complete support for SNMP-based management by implementing the MIB in the RFC 2934.
- Uses the interface prune state and unicast metrics to appropriately process State Refresh messages.
- Manages the multicast delivery tree and makes hardware abstraction layer callouts when the multicast delivery tree is modified, so that a separate datapath (for example in hardware) can be populated.
- Operates periodic timers to age out multicast information that is not refreshed through the protocol.
- The minimum and default hold-time for RP-set is updated as 2.5 times the RP-candidate advertisement interval. If a router receives a RP-candidate advertisement with advertisement interval below 60 seconds, then the router shall override the RP-set hold-time with 2.5 times 60seconds (i.e. 150 seconds).How to configure PIM-SM

Prerequisites

Before configuring PIM on the desired SVIs (switched virtual interfaces), IP addresses should be configured on the same SVIs.

Configure OSPF for the PIM interfaces.

How to configure PIM-SM via CLI interface

1. Enable PIM-SM globally.

```
cnMatrix-R10(config)# ip pim
```

2. Enable PIM-SM on a SVI.

```
cnMatrix(config)# interface vlan 100

cnMatrix(config-if)# ip pim componentId 1
```

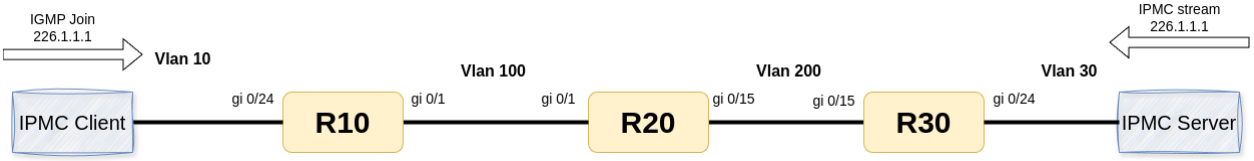
3. Enable PIM-SM BSR on a SVI.

```
ip pim bsr-candidate 30
```

4.Configure the RP candidate address for a particular multicast group or multicast network.

```
cnMatrix(config)# ip pim component 1

cnMatrix(pim-comp)# rp-candidate rp-address 226.1.1.0 255.255.255.0 110.0.0.1
```

Configuration example



Preliminary configuration:

Router R10 configuration

```
vlan 10
ports gigabitethernet 0/24

vlan 100
ports gigabitethernet 0/1-2

interface vlan 10
ip address 10.0.0.1 255.255.255.0
no shutdown

interface vlan 100
ip address 110.0.0.1 255.255.255.0
no shutdown

router ospf
network 10.0.0.1 area 0.0.0.0
network 110.0.0.1 area 0.0.0.0
```

Router R20 configuration

```
vlan 100
ports gigabitethernet 0/1

vlan 200
ports gigabitethernet 0/15

interface vlan 100
ip address 110.0.0.2 255.255.255.0
no shutdown

interface vlan 200
ip address 120.0.0.2 255.255.255.0
no shutdown

router ospf
network 110.0.0.2 area 0.0.0.0
network 120.0.0.2 area 0.0.0.0
```

Router R30 configuration

```
vlan 30
ports gigabitethernet 0/24

vlan 200
ports gigabitethernet 0/15

interface vlan 30
ip address 30.0.0.3 255.255.255.0
no shutdown

interface vlan 200
ip address 120.0.0.3 255.255.255.0
no shutdown

router ospf
network 30.0.0.3 area 0.0.0.0
network 120.0.0.3 area 0.0.0.0
```

PIM-SM configuration

Router R10 PIM-SM configuration

```
ip pim

interface vlan 10
ip pim componentId 1

interface vlan 100
ip pim componentId 1
```

Router R20 PIM-SM configuration

```
ip pim

interface vlan 100
ip pim bsr-candidate 30
```

```
ip pim componentId 1

interface vlan 200
ip pim componentId 1

ip pim component 1
rp-candidate rp-address 226.1.1.0 255.255.255.0 110.0.0.2
```

Router R30 PIM-SM configuration

```
ip pim

interface vlan 30
ip pim componentId 1

interface vlan 200
ip pim componentId 1
```

Troubleshooting

Show component

Display domain information like the elected BSR and Candidate RP Holdtime.

```
cnMatrix-R20# show ip pim component

PIM Component Information
--------------------------
Component-Id: 1
  PIM Mode: sparse,   PIM Version: 2
  Elected BSR: 110.0.0.2
  Candidate RP Holdtime: 150
```

Show bootstrap

```
cnMatrix-R20# show ip pim bsr

PIMv2 Bootstrap Configuration For Component 1
-----------------------------------------------
This system is the PIMv4 Bootstrap Router (BSR)
  BSR Address : 110.0.0.2
  BSR Priority : 30, Hash Mask Length : 30
BSR UpTime: 00:33:52
```

Show PIM-SM interfaces

Display the router's PIM interfaces information: interface address, DR address/priority, Hello interval, neighbor count.

```
cnMatrix-R20# show ip pim interface
PIM is globally enabled
Context Id 0 for Socket Id 35

Address                  IfName/IfId Ver/Mode  Nbr   Qry            DR-Address
         DR-Priority
                                               Count Interval
```

```
-------                 ----------- --------  ----- --------       ----------
         -----------
110.0.0.2               vlan100/63    2/Sparse  1      30            110.0.0.2
                1
120.0.0.2               vlan200/65    2/Sparse  1      30            120.0.0.3
                 1

cnMatrix-R20# show ip pim interface vlan 100 detail
PIM is globally enabled
Context Id 0 for Socket Id 35

vlan100 (Interface Index:63) is up
  Internet Address is 110.0.0.2
  Muticast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
    PIM version : 2, mode: Sparse
    PIM DR : 110.0.0.2
    PIM DR Priority : 1
    PIM Neighbour Count : 1
    PIM Hello/Query Interval : 30
    PIM Message Interval : 60
    PIM Override Interval : 0
    PIM Lan Delay : 0
    PIM Lan-Prune-Delay : Disabled
    PIM Component Id : 1
    PIM RPF Status : Disabled
    PIM Interface Statistics
        General (Sent/Received):
            Hellos: 75/74,  JP's: 36/0,  Assert's: 0/0,
        Errors:
            Checksum error: 0,  Invalid packet types/DF subtypes: 0/0
            Authentication Failed: 0
            Packet length errors: 0,     Bad version packets: 0,     Packets
fro
m self: 0
            Packets from Non-Neighbors : 1
            Packets received on RPF interface : 0
            (*,G) Joins received with no/wrong RP: 0/0
```

Show mroute

Displays the PIM multicast routing table.

```
cnMatrix-R20# show ip pim mroute

IP Multicast Routing Table
--------------------------
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
IIF State P: Pruned F: Forwarding A: Graft Ack Pending
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table For Component 1
```

```
Total number of Multicast Routes is 2

(10.0.0.100,226.1.1.1) ,00:36:32/00:53:46
  Incoming Interface : vlan100 ,RPF nbr : 110.0.0.1 ,Route Flags : S
  Outgoing InterfaceList :
    vlan200, Forwarding/Sparse ,00:36:32/00:53:46

(*, 226.1.1.1) ,00:36:51/--- ,RP : 110.0.0.2
  Incoming Interface : vlan100 ,RPF nbr : NULL ,Route Flags : WR
  Outgoing InterfaceList :
    vlan200, Forwarding/Sparse ,00:36:51/00:00:00
```

Show rendezvous candidate

Display the candidate RP information: the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

```
cnMatrix-R20# show ip pim rp-candidate

CompId    GroupAddress      Group Mask       RPAddress/Priority   Context
------    ------------      ----------       ---------- -------   -------
     1       226.1.1.0   255.255.255.0       110.0.0.2/192        default
```

Show rendezvous hash

Display the elected RP for the multicast group address with the mask length.

```
cnMatrix-R20# show ip pim rp-hash

Component 1
-----------
Group Address/Network Mask: 226.1.1.0/255.255.255.0
RP Address: 110.0.0.2
Priority: 192, Hold Time: 150
```

Show rendezvous set

Display the RP-set information: the Group Prefix, RP address, Hold time and Expiry Time.

```
cnMatrix-R20# show ip pim rp-set

PIM Group-to-RP mappings
------------------------
Group Address : 226.1.1.0 Group Mask : 255.255.255.0
   RP: 110.0.0.2
  Component-Id : 1
    Hold Time : 150, Expiry Time : 00:02:03
```

Limitations

	No.	Description

PIM routing interfaces	64	Interfaces on which PIM routes Multicast traffic.
PIM neighbors	8	PIM router neighbors
Multicast streams	512	S,G multicast traffic
RP MC Group mappings	32	Rendezvous point candidate group mappings for the entire PIM domain.

Management Features

DHCP Client

Managing DHCP Client

Feature Overview

DHCP Client uses DHCP protocol to dynamically 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, and SNTP Server IP address from the DHCP server.

DHCP Client can be enabled on any IPv4 interface associated with existing VLANs, on Routed Interfaces, or the Out-Of-Bandinterface.

Standards

- RFC 2131

Scaling Numbers

- DHCP Client can be enabled on 64 IPv4 Interfaces.

Limitations

N/A

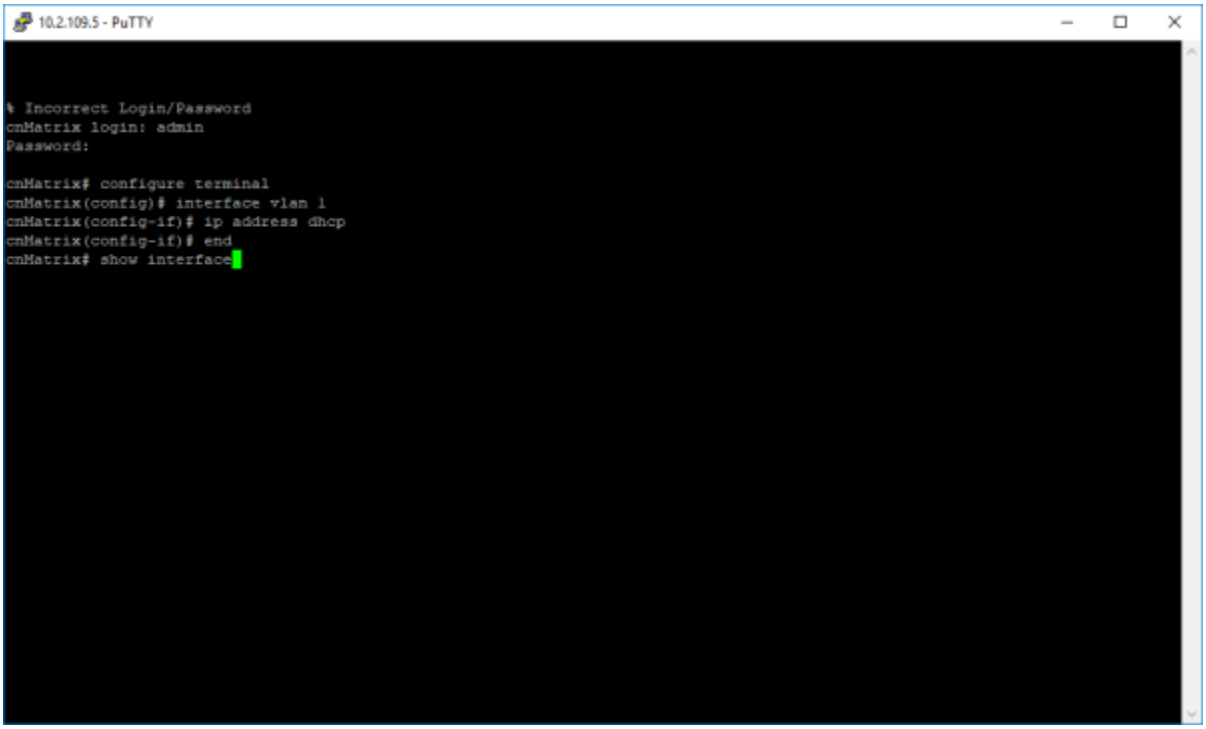
Default Values

- 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.

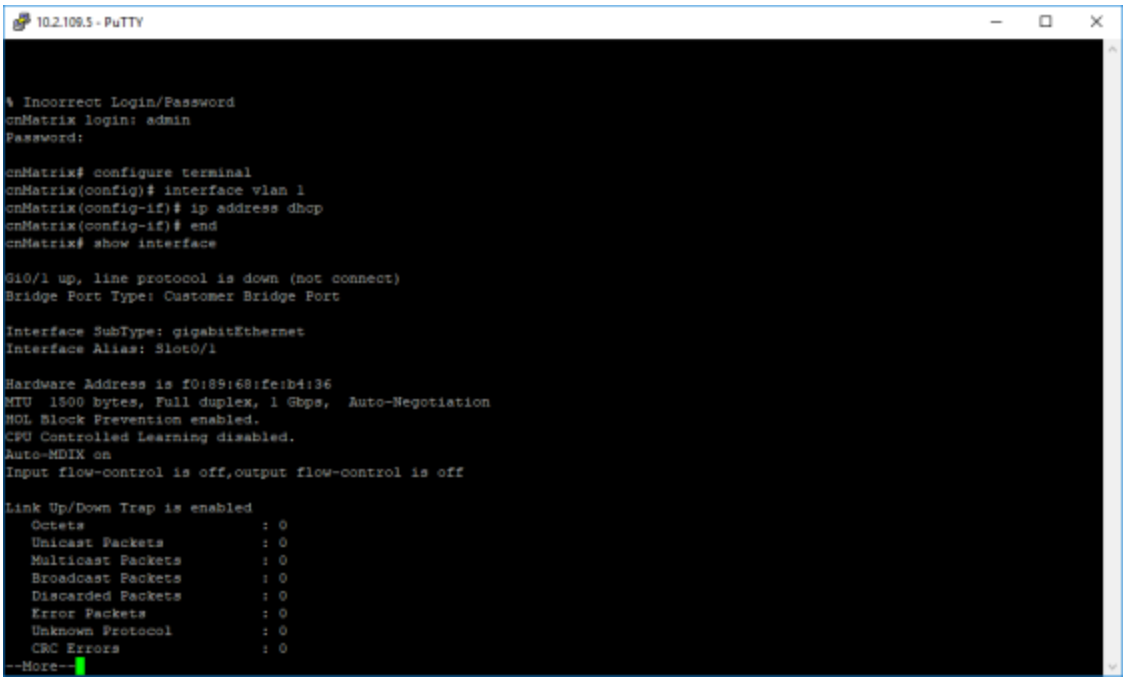
Prerequisites

N/A

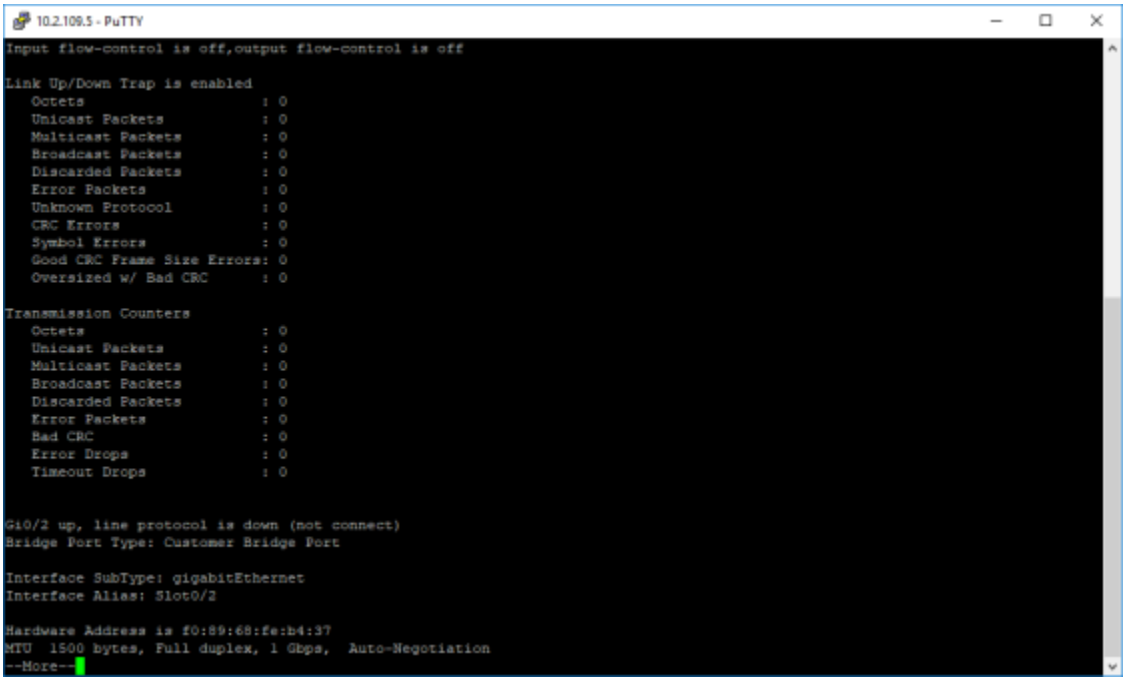
How to Enable DHCP Client in CLI Interface



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 **Enter** key to move down one page.



For more information, see DHCP Client Parameters and Commands.

DHCP Server

Managing DHCP Server

Feature Description

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.

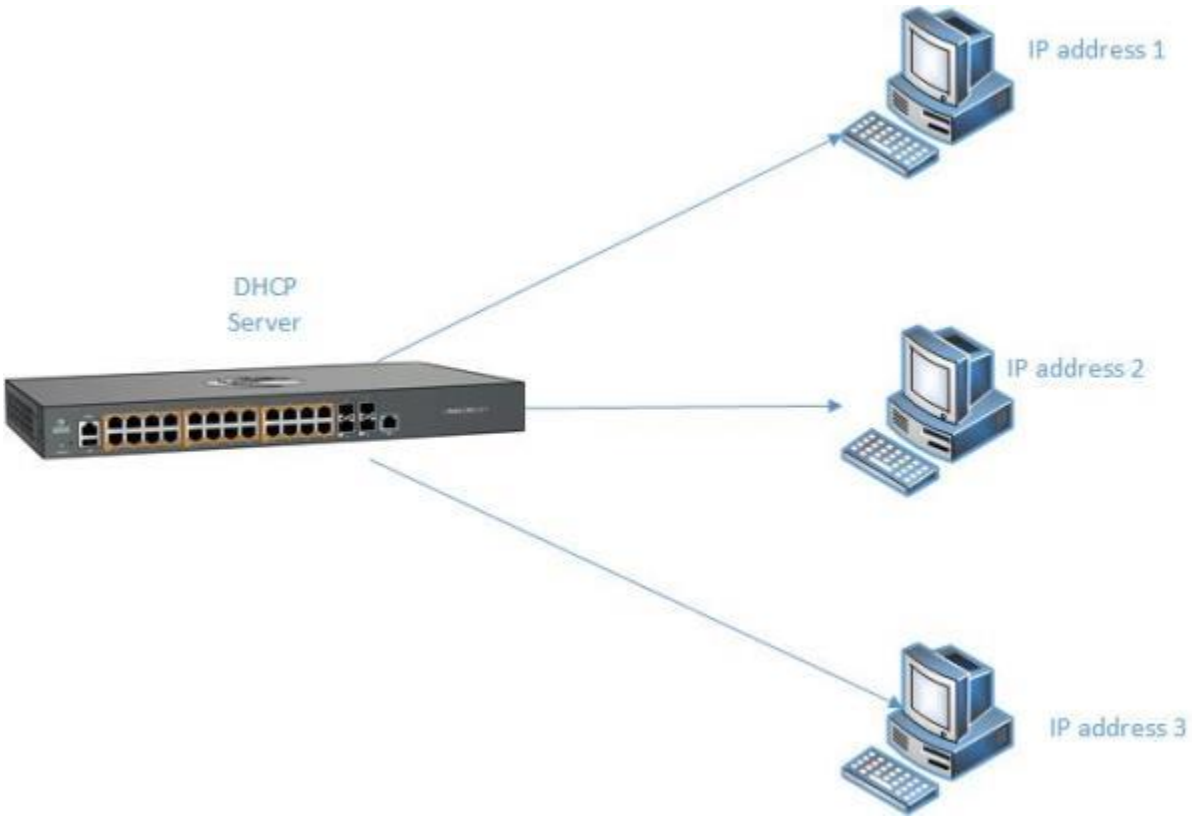
Default Values

- 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

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

Network Diagram



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#
```

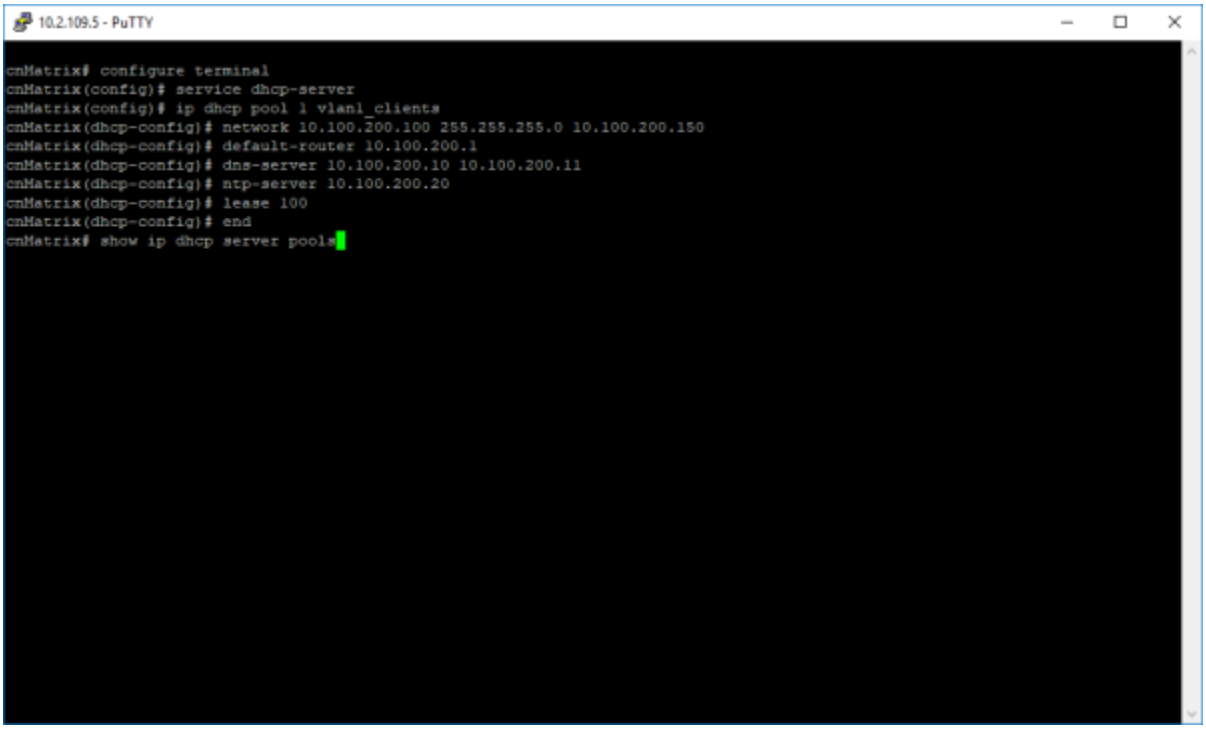
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **ip dhcp pool 1** command into the terminal to create the DHCP address pool. Press the **Enter** key to create a DHCP address pool.
3. Type the **host hardware-type 1 client-identifier 00:11:22:33:44:04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

> Note
>
> 00:11:22:33:44:04 = MAC address

> Note
>
> 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.

Configuring DHCP Address Pool

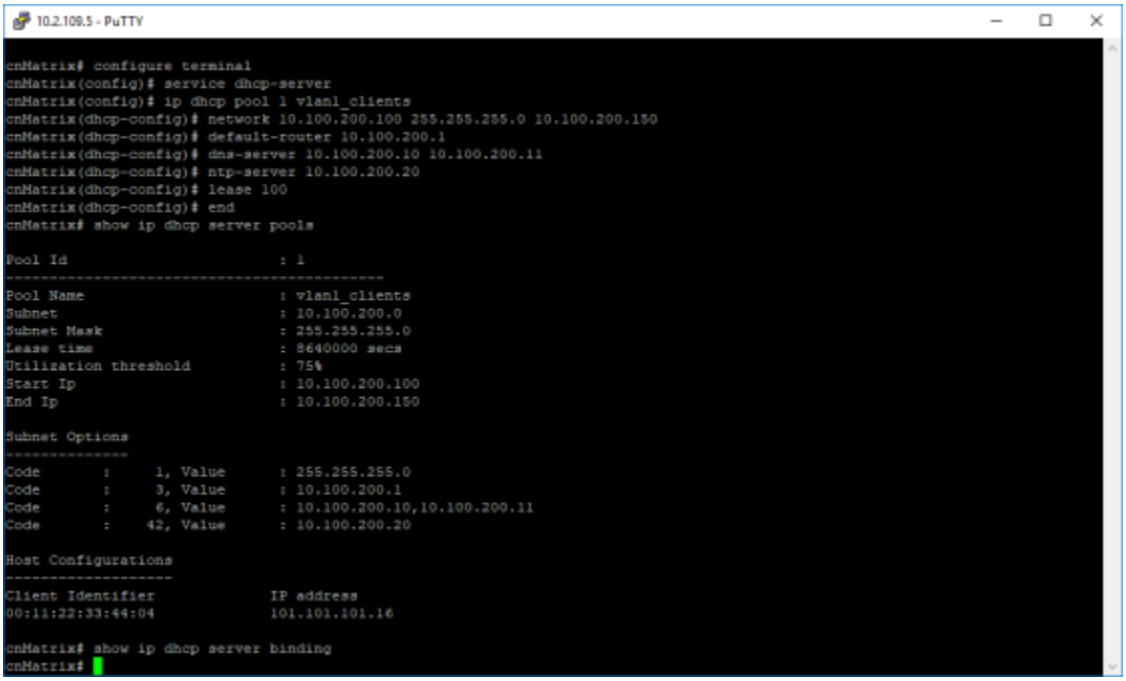


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **service dhcp-server** command into the terminal to enable the DHCP Server feature. Press the **Enter** key
3. Type the **ip dhcp pool 1 vlan1_clients** command into the terminal to create a name for the 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.

> Note
>
> 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.

Out-of-Band Management

Managing Out-of-Band Ethernet Management

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.

Attention

EX1028, EX1028-P, EX1010, and EX1010-P switches do not have a physical OOB port. OOB management is not supported on these switches.

Standards

N/A

Scaling Numbers

N/A

Limitations

- IPv6 not supported on OOB port.

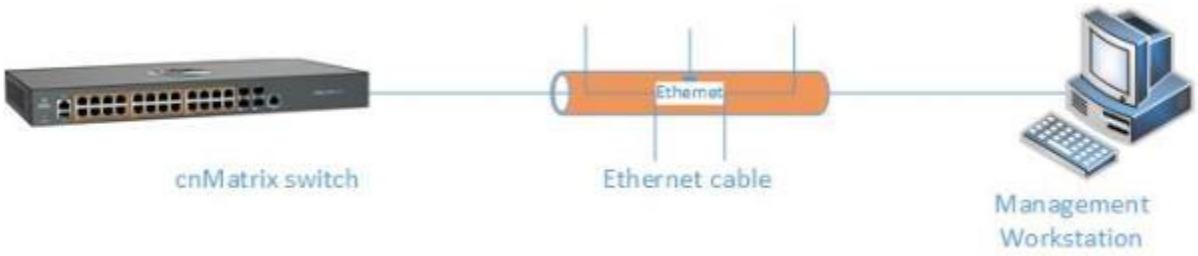
Default Values

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

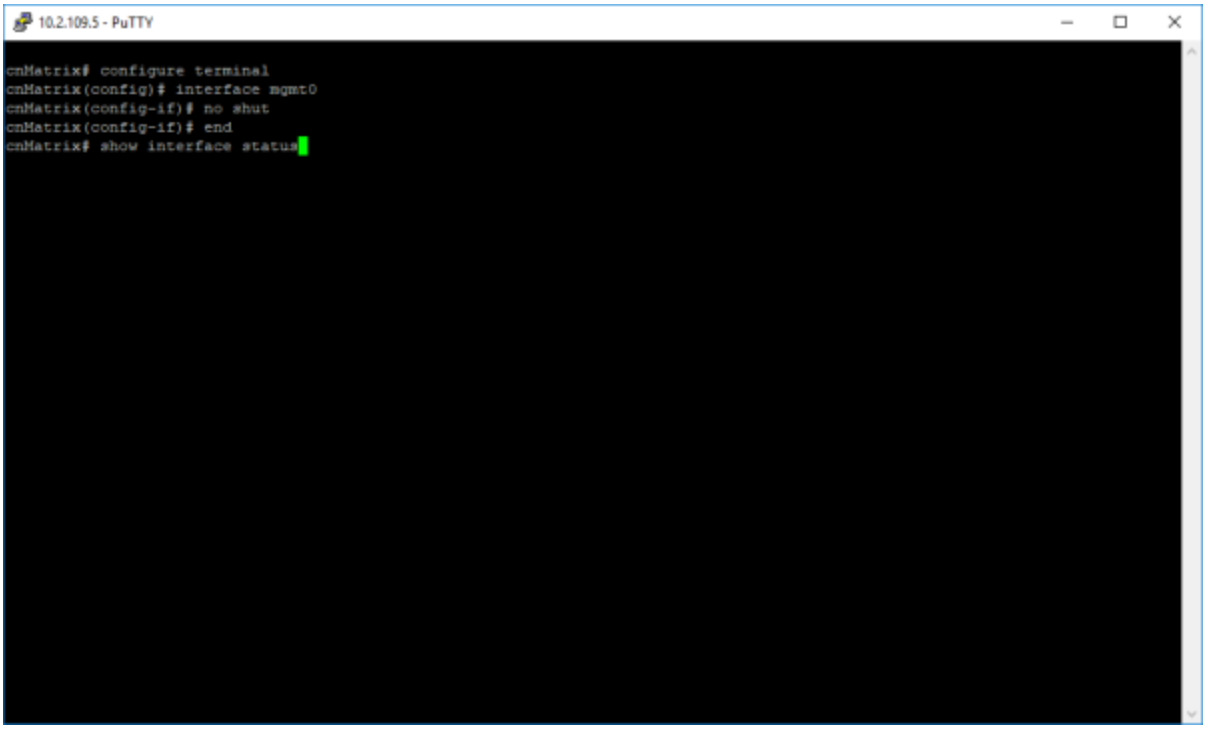
Prerequisites

N/A

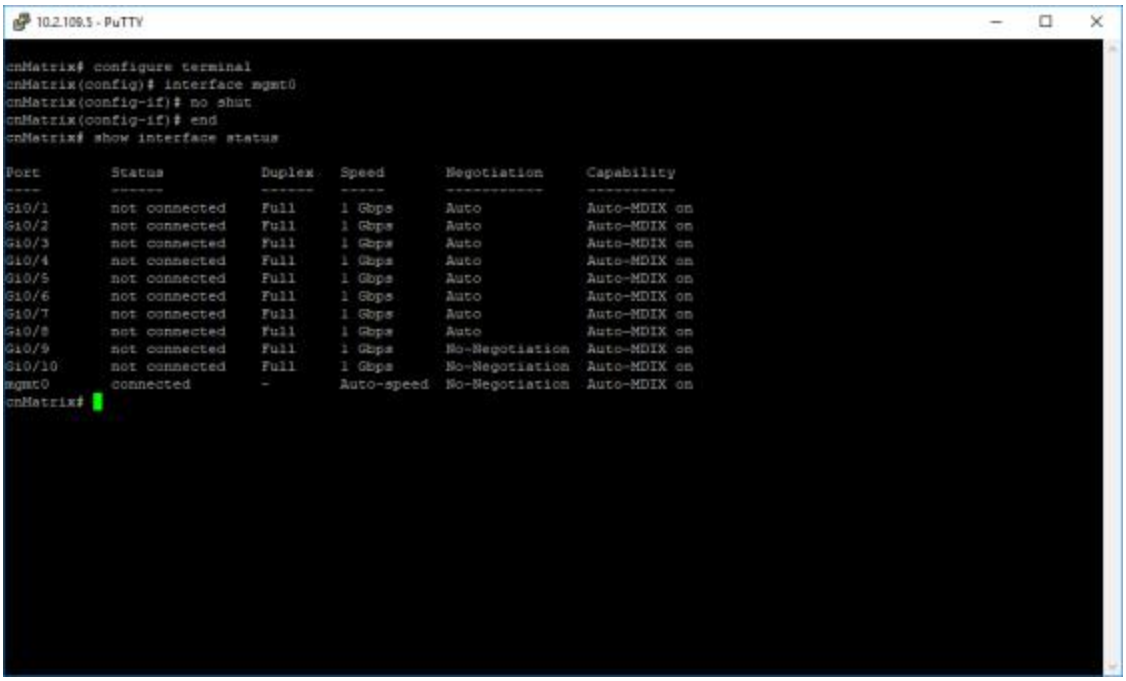
Network Diagram



Configuring OOB 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-BandEthernet Management Parameters and Commands.

Telnet Server

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 a user and a password and then provides 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

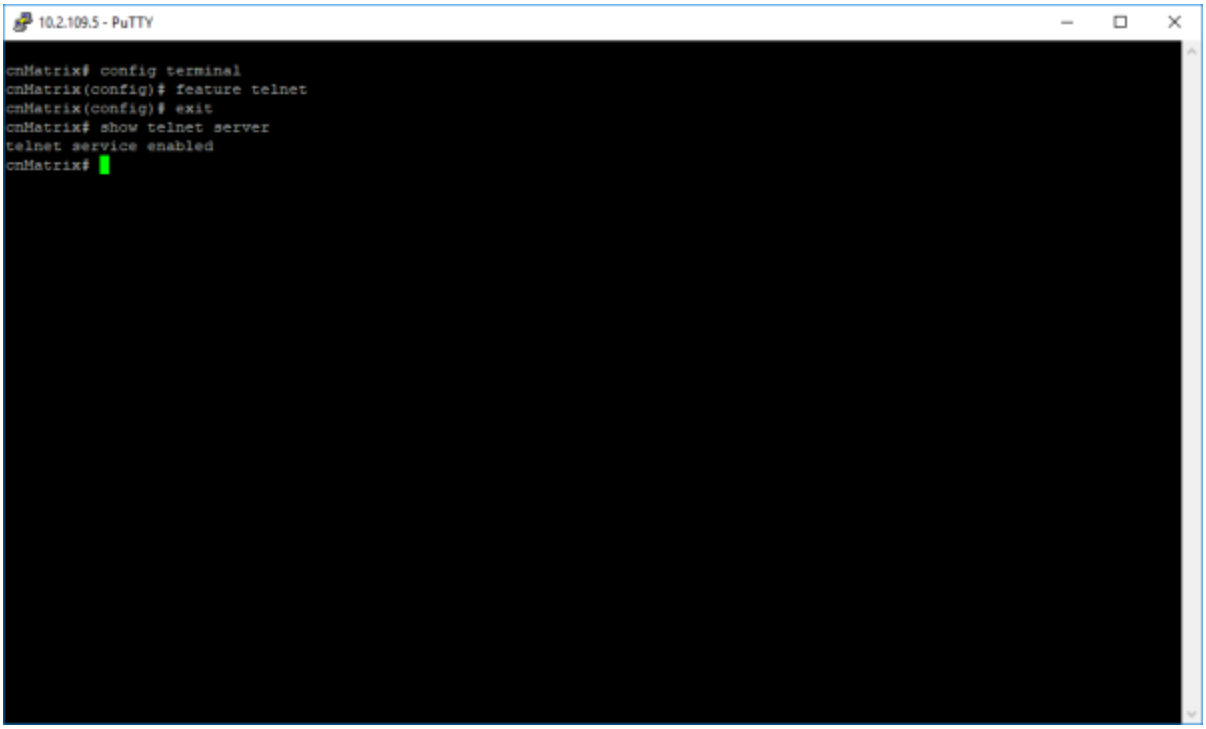
Default Values

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

Prerequisites

N/A

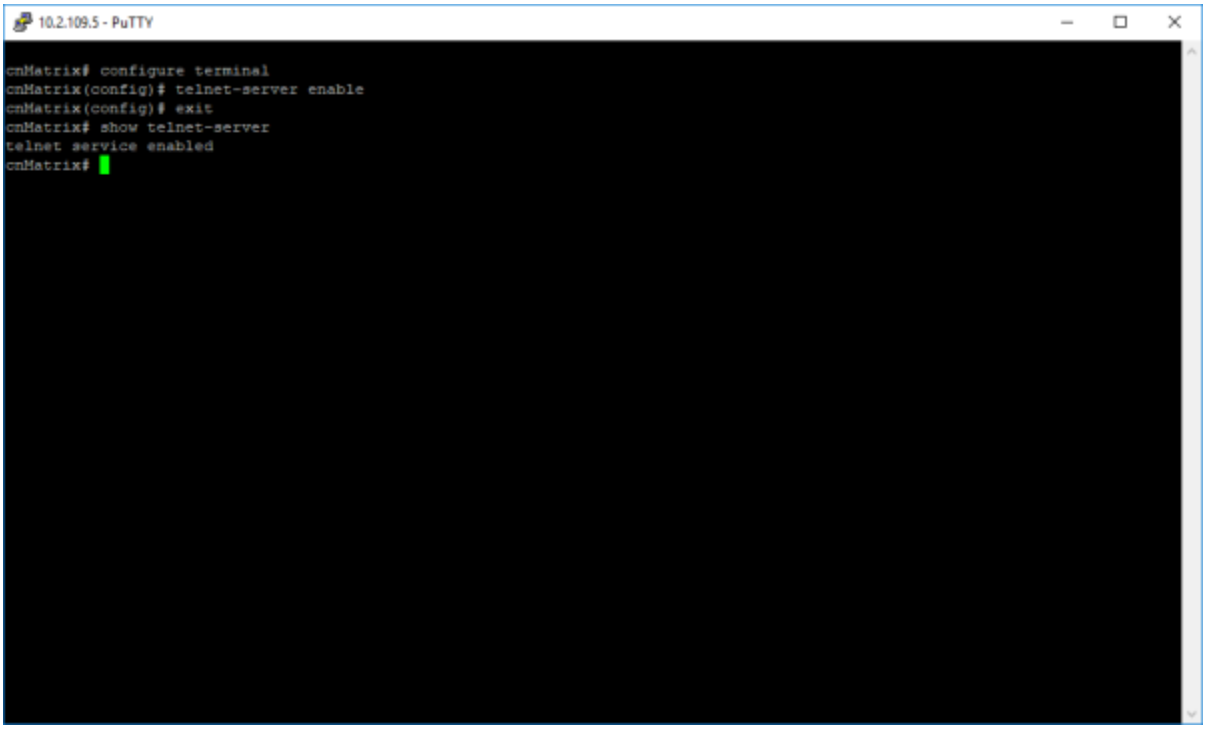
How to Enable Telnet Server in CLI Interface



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.

How 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.

Troubleshooting Telnet Client/Telnet Server

Useful commands for troubleshooting:

- cnMatrix#show telnet-client
- cnMatrix#show telnet server
- cnMatrix#show users – see active connections

System Resource Monitoring

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.

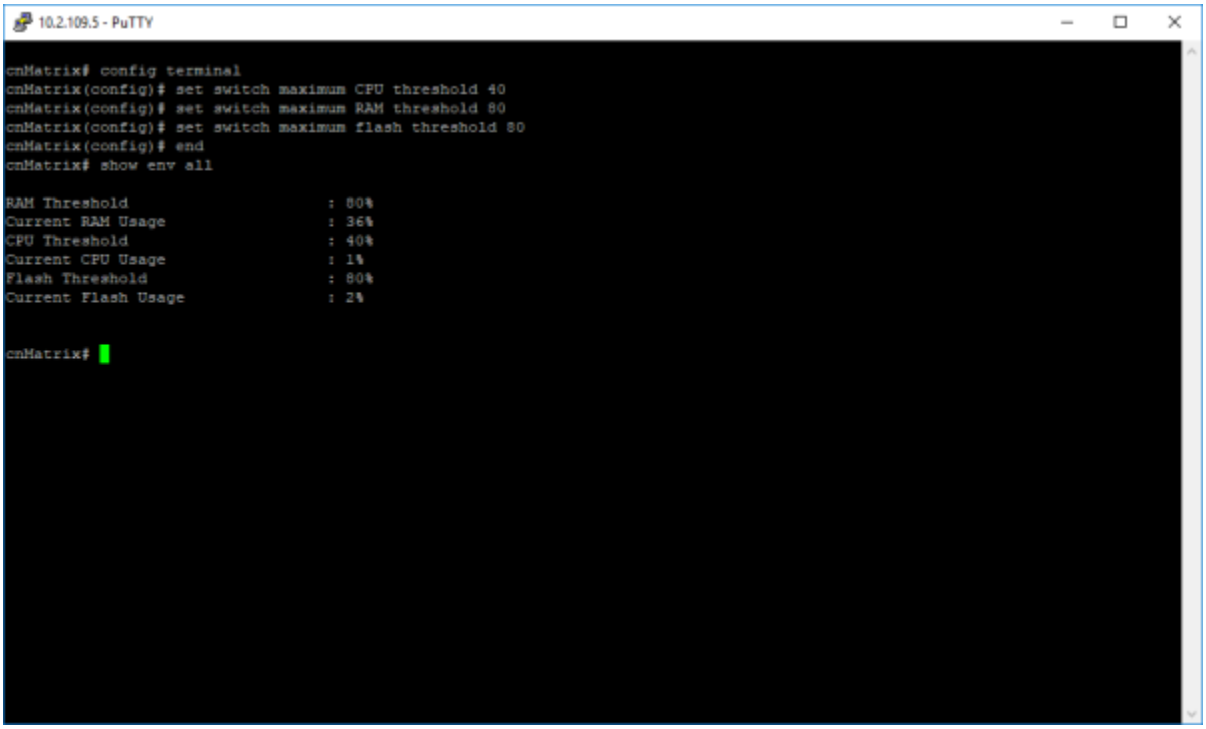
Default Values

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

Prerequisites

N/A

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.

Troubleshooting System Resource Monitoring

Useful commands for troubleshooting:

- cnMatrix#show env all

Syslog

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, and 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.

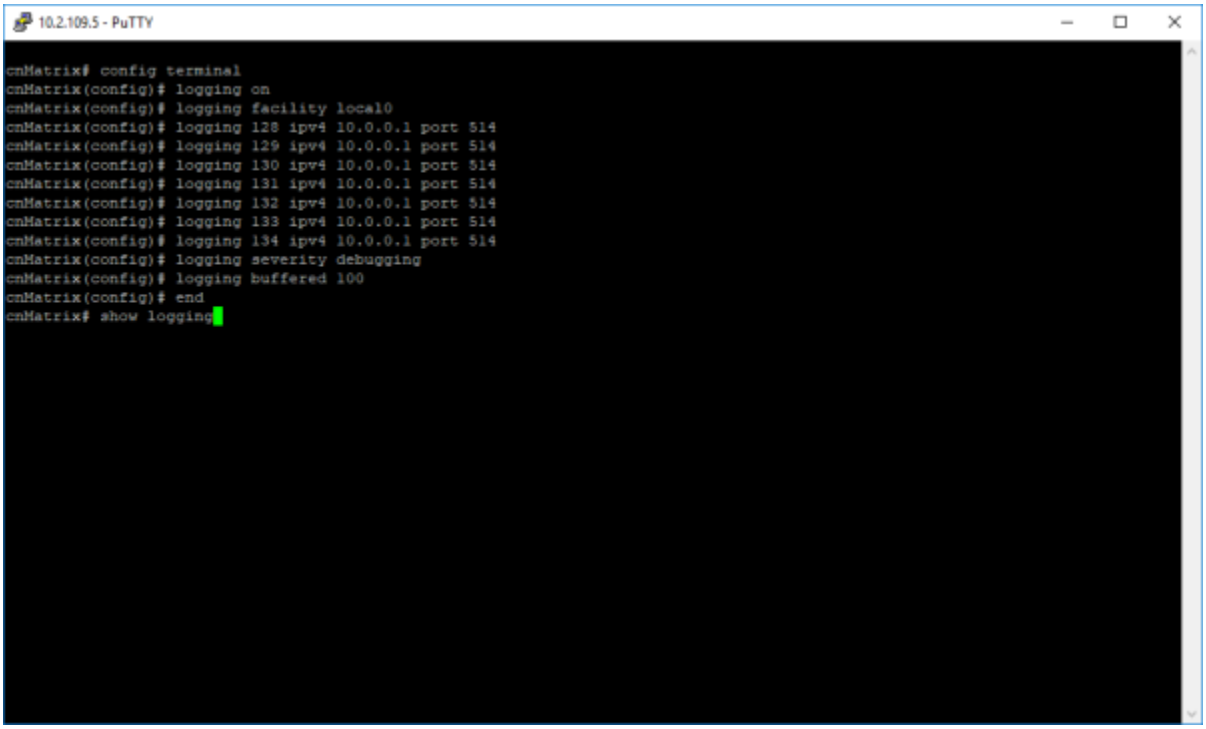
Default Values

- 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.

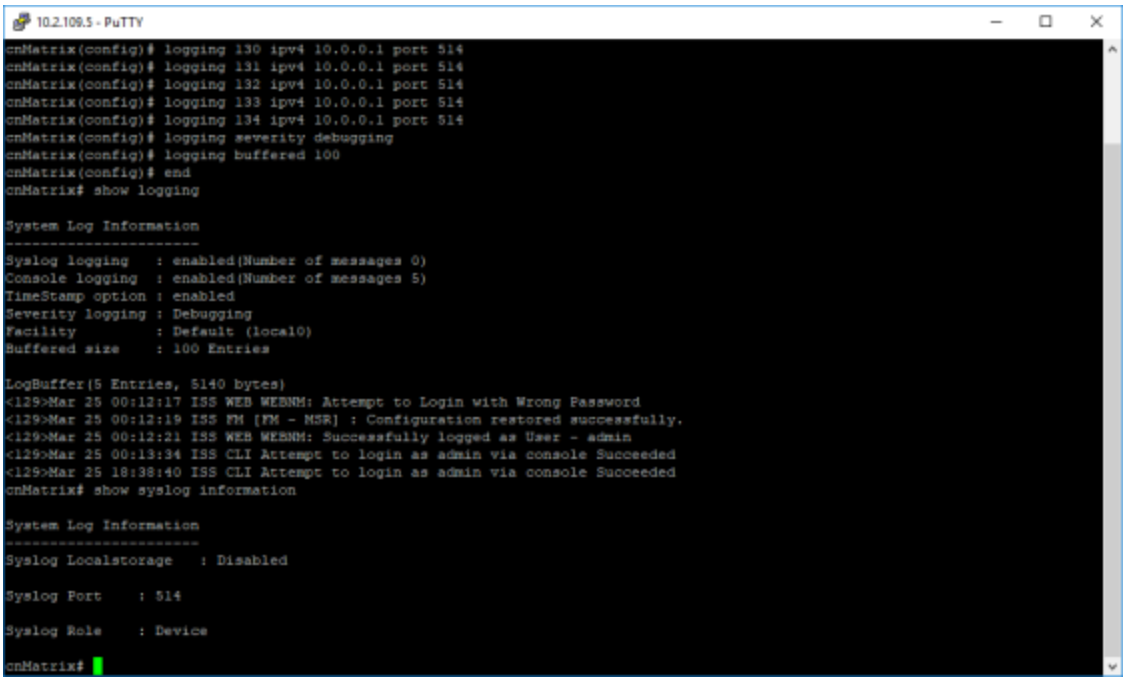
Prerequisites

- 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.

How 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.

Troubleshooting Syslog

Useful commands for troubleshooting:

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

SNMP

Managing SNMP

Feature Description

SNMP (Simple Network Management Protocol) is the most widely used network management protocol on TCP or 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

Web User Interface

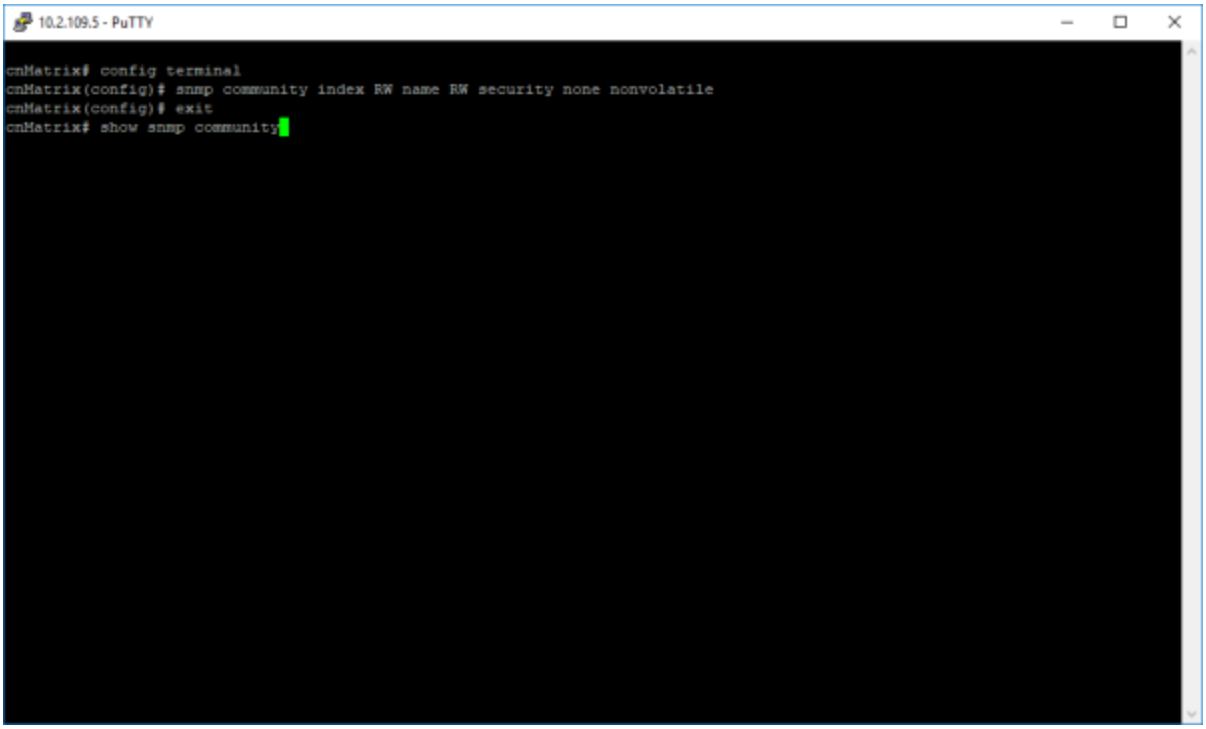
- All individual SNMP agent configuration tables are configurable via the Web UI (**System** > **SNMP**).
- SNMP Quick Start configuration is available through the Web UI (**System** > **SNMP** > **Quick Start**). The SNMP Quick Start page supports streamlined configuration of SNMPv2c read-only/read-write community strings, trap receiver address data and SNMPv3 user and related security parameters.

Default Values

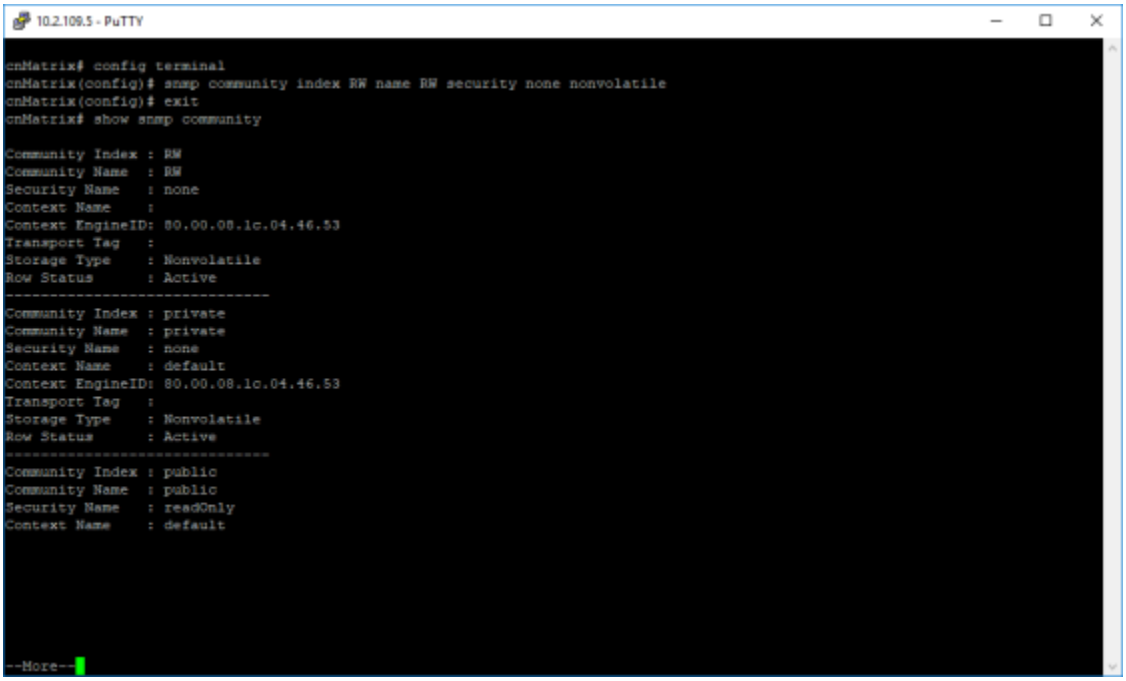
- SNMP agent is enabled by default.
- SNMP Coldstart trap is enabled by default.
- Storage Type: Non-Volatile by default.
- Row Status: Active by default.
- Sub-tree OID: 1 by default.
- Sub-tree Mask: 1 by default.
- Community names: private, public.
- Group security models: v1, v2c, v3.

Network Diagram

How to Enable and Configure SNMP V2 in CLI Interface



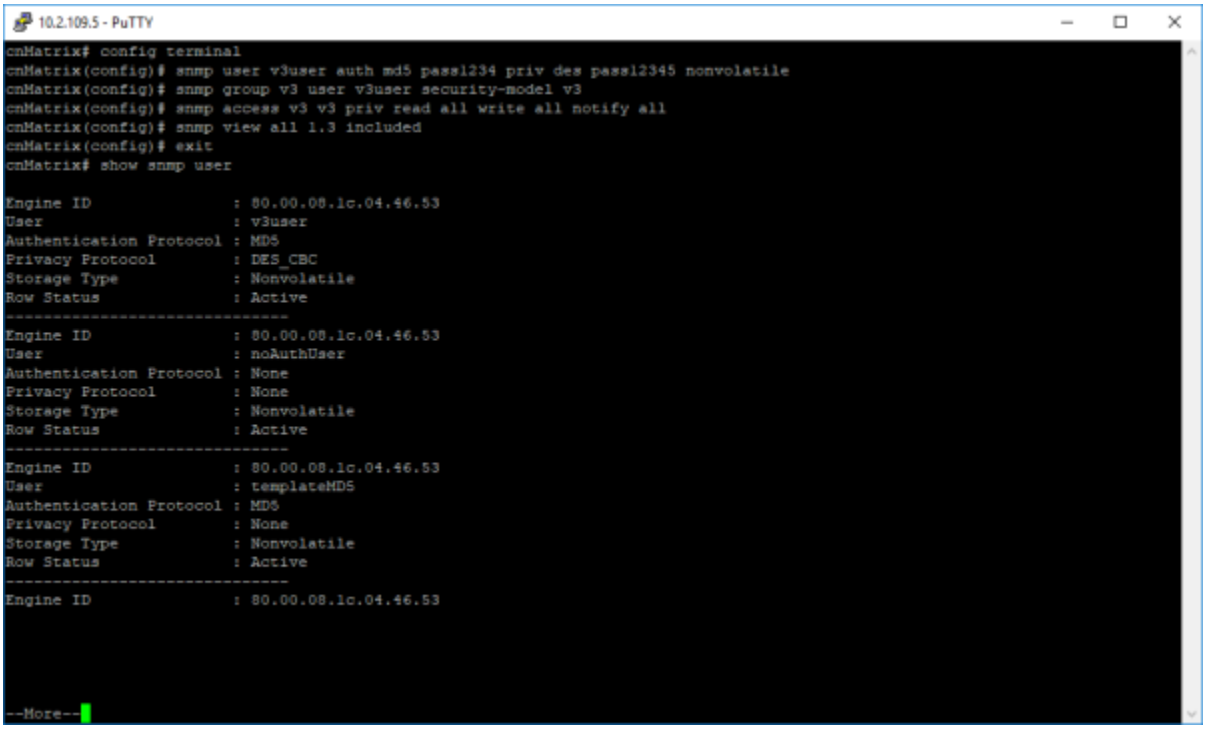
1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **snmp community index RW name RW security none nonvolatile** command into the terminal to configure the SNMP community details. Press the **Enter** key.
3. Type the **exit** command into the terminal to go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

For more information, see SNMP Parameters and Commands.

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.

SSH

Managing SSH

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 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 and client are using OpenSSH version 9.7. 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. But it can be configured to a smaller value.

Default Values

- The SSH server and SSH client are enabled by default.
- The SSH version is 2.
- The debugging option is disabled by default.
- The default primary port number: 22.
- The following cipher algorithms are set by default: CHACHA20-POLY1305, 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-SHA2-256.
- The default SSH maximum sessions: 8

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

The cnMatrix SSH server implementation supports the following:

- Algorithms:
- Cipher algorithms – CHACHA20-POLY1305, 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.
- The key exchange algorithms supported are SNTRUP761X25519-SHA512@OPENSSH.COM,CURVE25519-SHA256,CURVE25519-SHA256@LIBSSH.ORG,ECDH-SHA2-NISTP256,ECDH-SHA2-NISTP384,ECDH-SHA2-NISTP521,DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA256,DIFFIE-HELLMAN-GROUP16-SHA512,DIFFIE-HELLMAN-GROUP18-SHA512,DIFFIE-HELLMAN-GROUP14-SHA256. 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-ED25519-CERT-V01@OPENSSH.COM,ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM,ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM,ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM,SK-SSH-ED25519-CERT-V01@OPENSSH.COM,SK-ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM,RSA-SHA2-512-CERT-V01@OPENSSH.COM,RSA-SHA2-256-CERT-V01@OPENSSH.COM,SSH-ED25519,ECDSA-SHA2-NISTP256,ECDSA-SHA2-NISTP384,ECDSA-SHA2-NISTP521,SK-SSH-ED25519@OPENSSH.COM,SK-ECDSA-SHA2-NISTP256@OPENSSH.COM,RSA-SHA2-512,RSA-SHA2-256

- Authentication using username and password.
- SSH max-startups options:
    - drop-all: All connection attempts are refused if the number of unauthenticated connections reaches this value
    - rate-drop: SSH server will refuse connection attempts with a probability of the rate drop
    - start-drop: Number of concurrent unauthenticated connections to the SSH server from which it starts to drop connections
- Timer for authentication and sends a disconnect message in case the timer expires. The timeout period is 120 seconds. This can be changed with the command ssh login grace time.
- Session re-keying after a specified time interval or after a specified amount of data transfer. The options can be specified with command ip ssh rekey interval and limit.
- SSH client alive options:
    - messages: Number of client alive messages which may be sent without SSH server receiving any messages back from the client. If this threshold is reached, SSH server will terminate the session
    - Interval: Timeout interval in seconds after which if no data has been received from the client, SSH server will send a message to request a response from the client

The SSH server implementation does not support the following:

- Certificates for server and user authentication.
- 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 OOB 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 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.

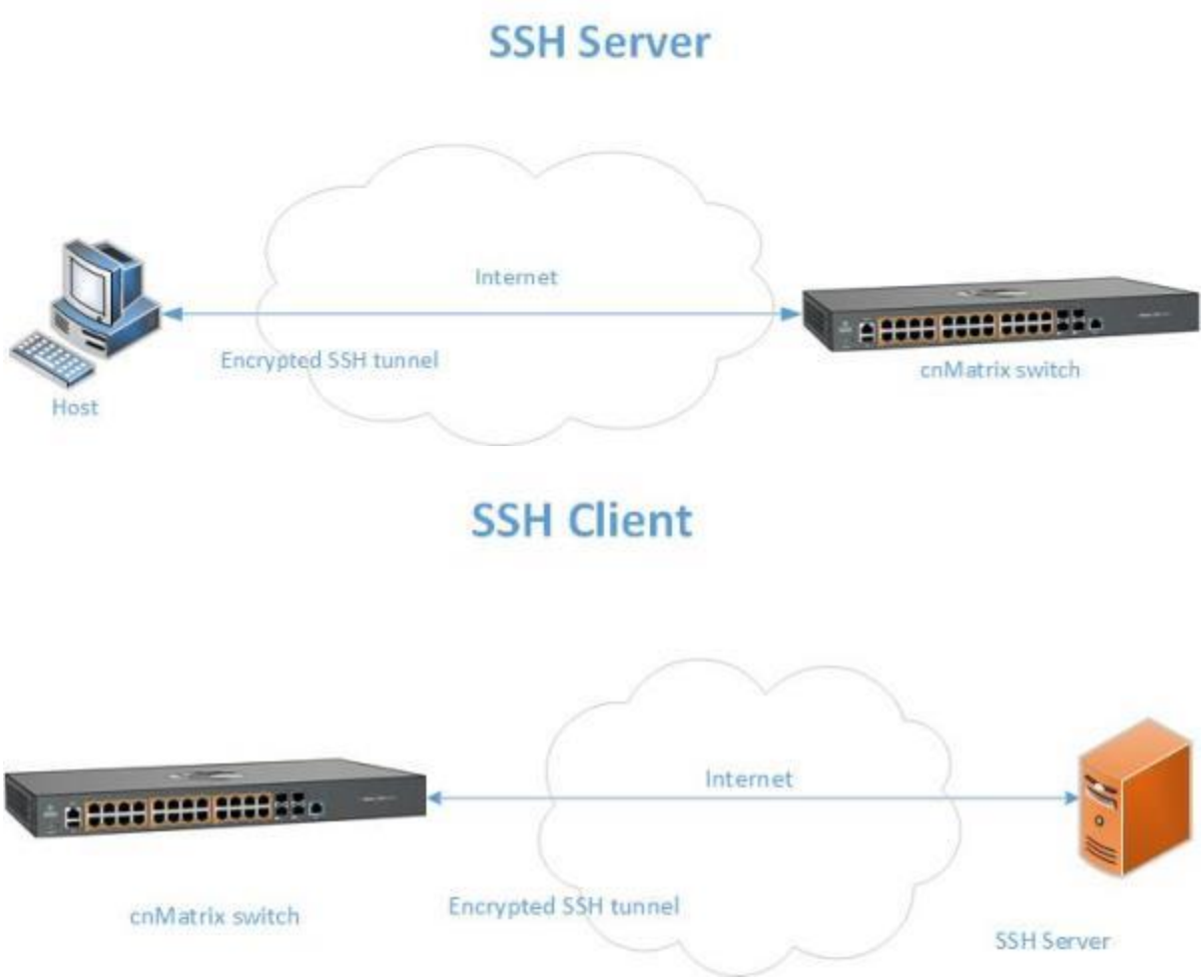
Options supported in SSH client:

- <string> It can be username@ip_address or ipv4 address or ipv6 address
- - 4 - Forces SSH to use Ipv4 addresses only.
- - 6 - Forces SSH to use Ipv6 addresses only.
- - a - Enables forwarding of the authentication agent connection.
- - b - Disables forwarding of the authentication agent connection.
- - c - Requests compression of all data.
- - p - To specify port to connect on remote host
- -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.

- <string> Remote command to be executed. If it is more than one argument use double quotes

After the ssh client connects to a remote ssh server you cand view the known host with command “show ssh known-hosts". In case you know for sure that the host has changed and needs an update, then you can remove the known host with command “no ssh known-host" and reconnect to the remote server.

Network Diagram



How to Enable SSH Server in CLI Interface

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

Attention

The SSH server is enabled by default

Troubleshooting SSH

Useful command for troubleshooting:

- cnMatrix# show ssh client
- cnMatrix# show ssh server
- cnMatrix# show ssh known-hosts
- cnMatrix# show users – see active connections
- cnMatrix# debug ssh all
- cnMatrix# debug ssh client all

Max SSH Sessions

The total number of CLI remote sessions (Telnet + SSH) is 8. For security reasons, the number of SSH sessions should be limited and configurable.

Note:

The maximum number of SSH sessions is 8.

Even if the maximum number of SSH sessions is 8, the number of telnet sessions will not be affected: the sessions will be still allocated on a first-come-first-served basis.

For example, even if SSH max sessions is set to 3, I still can have 5 telnet sessions.

The number of SSH sessions can be limited with the command:

```
cnMatrix(config)# ssh max-sessions (1-8)
```

It can be configured to default by using the following command:

```
cnMatrix(config)# default ssh max-sessions
```

Note:

The user can disable the SSH server.

Command is:

```
cnMatrix(config)# ssh disable
```

If eight SSH sessions are opened and the user wants to decrease the number of SSH sessions, the user is asked to close SSH sessions first.

Helpful commands for closing a certain session.

- Displays details about CLI active sessions.

  ```
  cnMatrix# show users
  ```

- Displays vty of current session.

  ```
  cnMatrix# show line vty
  ```

- Close a certain session by its vty.

```
cnMatrix# clear line vty {(3-10) | all}
```

IPv6 Management

Managing IPv6 Management

Feature Overview

Internet Protocol version 6 (IPv6) has been added as a successor of Internet Protocol version 4, which expands the number of network address bits from 32 bits to 128 bits. cnMatrix supports IPv6 host mode on its Layer 3 interfaces. IPv6 addresses can be configured using manually (stateful) or dynamically (stateless) using DCHPv6 or Router Advertisement mechanism.

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.
- IPv6 is not supported on OOB interface.

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.

How to Enable and Configure IPv6 in CLI Interface

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface vlan 1** command into the terminal to select the interface to be configured. Press the **Enter** key.
3. Type the **ipv6 enable** command into the terminal to enable IPv6 on the selected interface. Press the **Enter** key.
4. Type the **ipv6 address 2000::50/64** command into the terminal to configure IPv6 address and Prefix length on the interface. 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 ipv6 interface** command into the terminal to display the IPv6 interface information. Press the **Enter** key.
7. Press the **Enter** key.

For more information, see IPv6 Management Parameters and Commands.

Reload (Starting with version 2.1)

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 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.

Note

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

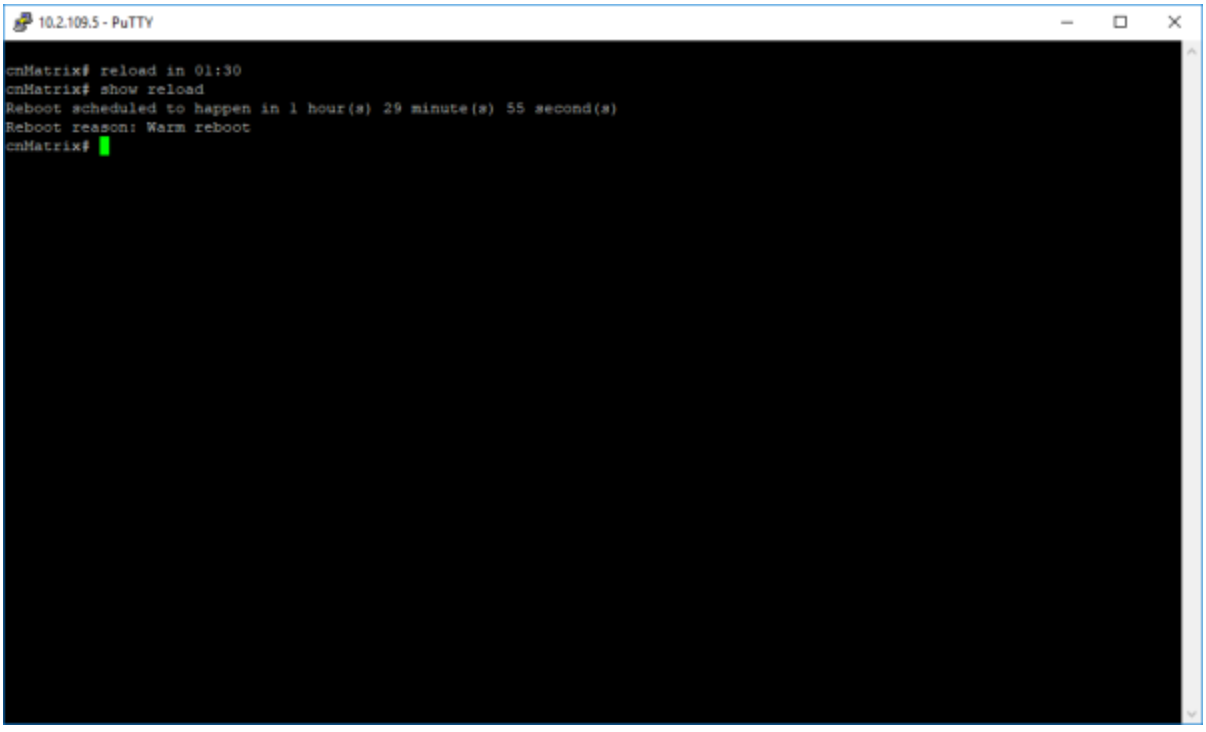
- No reload is scheduled by default.

Prerequisites

- N/A

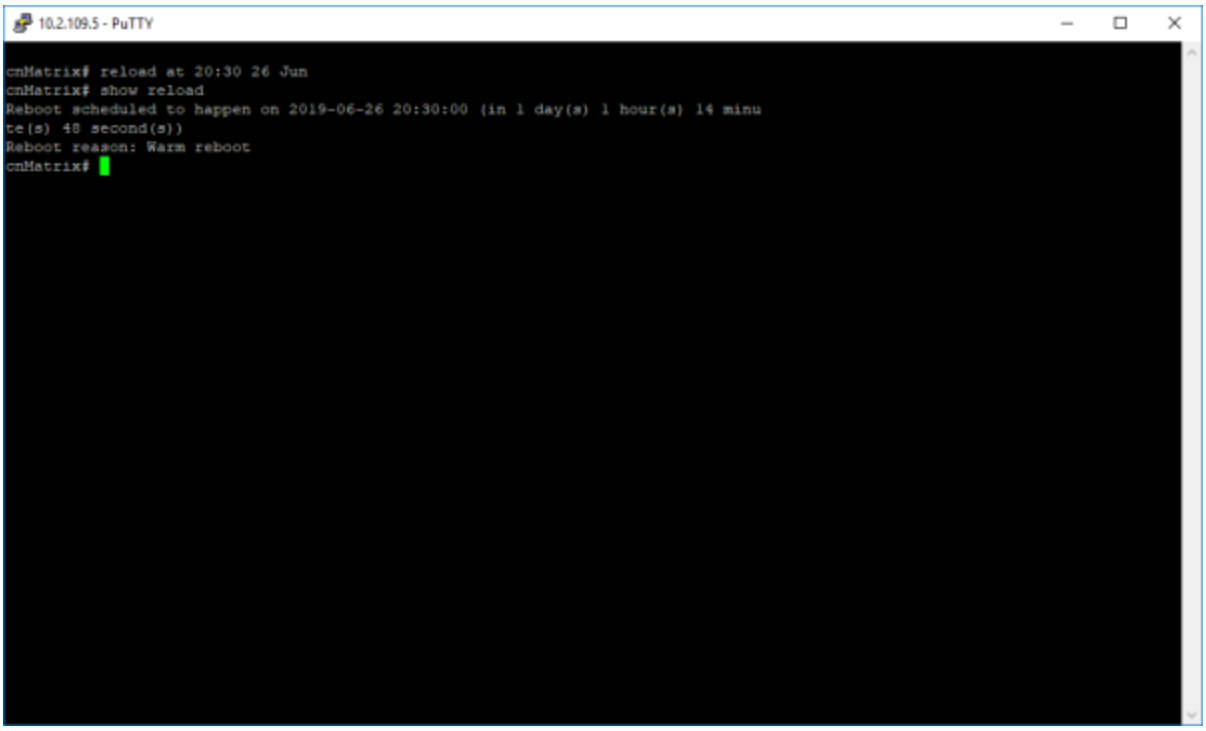
How to Schedule Reload on your cnMatrix Switch in CLI Interface

Schedule Reload in a Specific Amount of Time



1. Type the **reload in 01:30** command into the terminal to schedule 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.

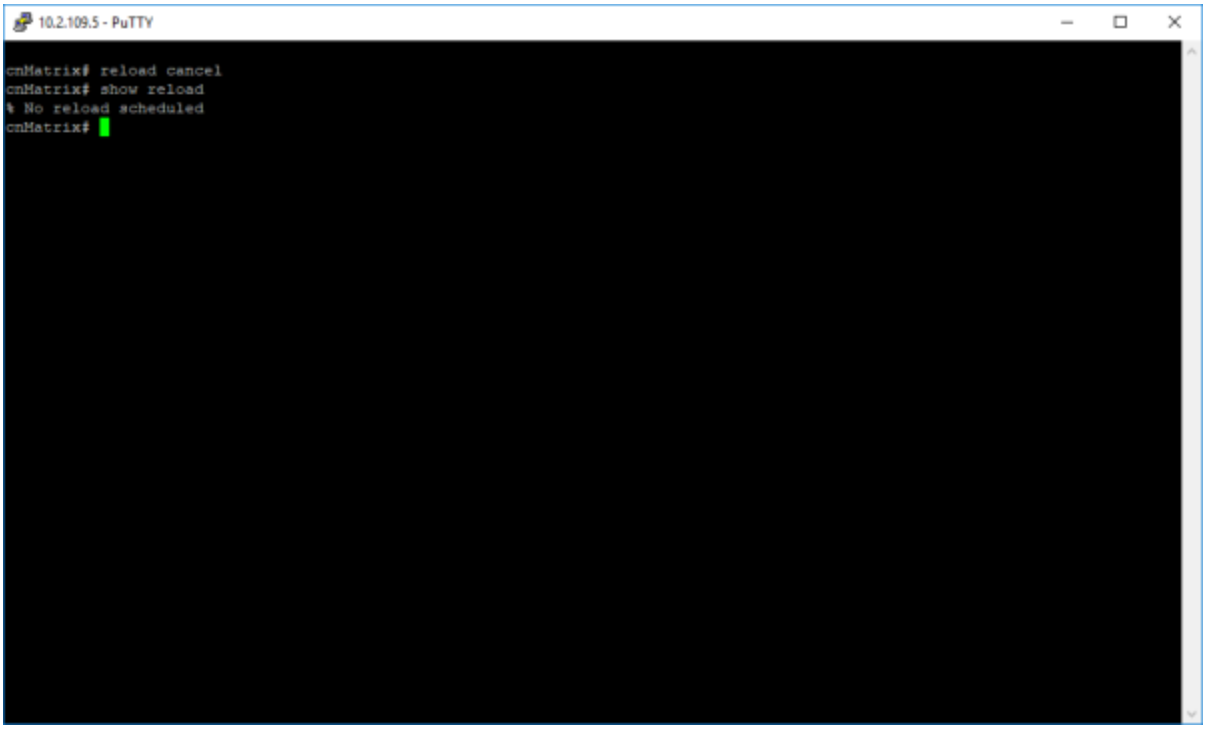
Schedule Reload at a Specific Time and Date



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.

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.

USB (Starting with version 2.1)

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 a USB device.
4. Access the files and folders that are on a USB device.
5. Access device information and vendor information (Vendor Name, Product ID, Total Capacity etc).

Note

The USB feature can be used as a back-up solution for software upgrades.

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

Tip

Manually mounting the device is not mandatory.

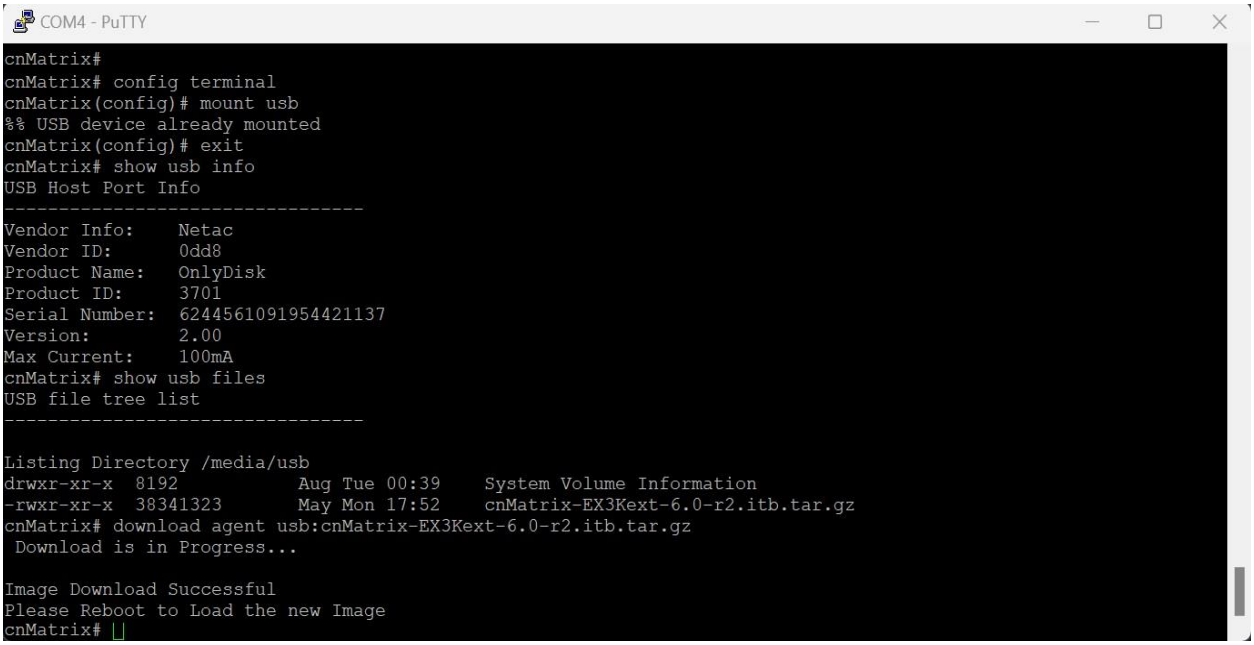
Limitations

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

Default Values

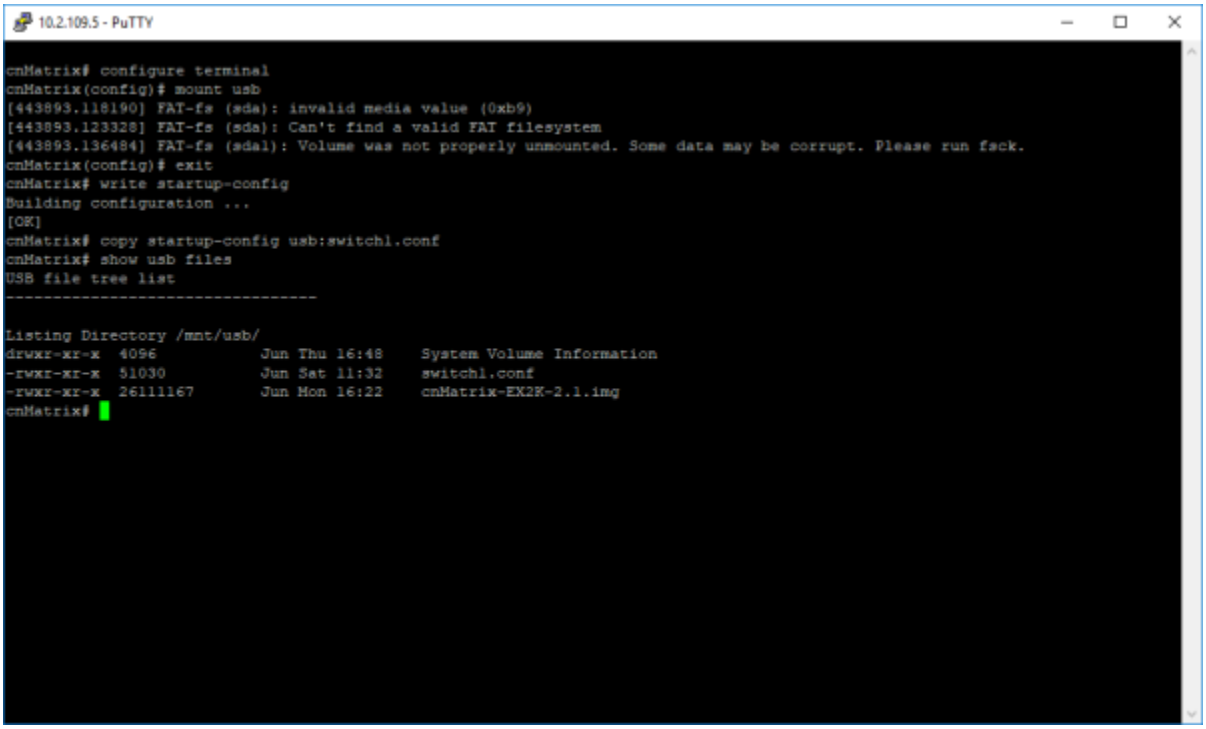
- No USB device is present by default.

How to Upgrade/Downgrade your Software Using USB



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 **show usb info** command into the terminal to display USB information. Press the Enter key.
5. Type the **show usb files** command into the terminal to display the files that are currently on the USB. Press the **Enter** key.
6. Type the download **agent usb:imageName.itb.tar.gz** command into the terminal to copy an existing image file from the USB to your cnMatrix switch. Press the **Enter** key.

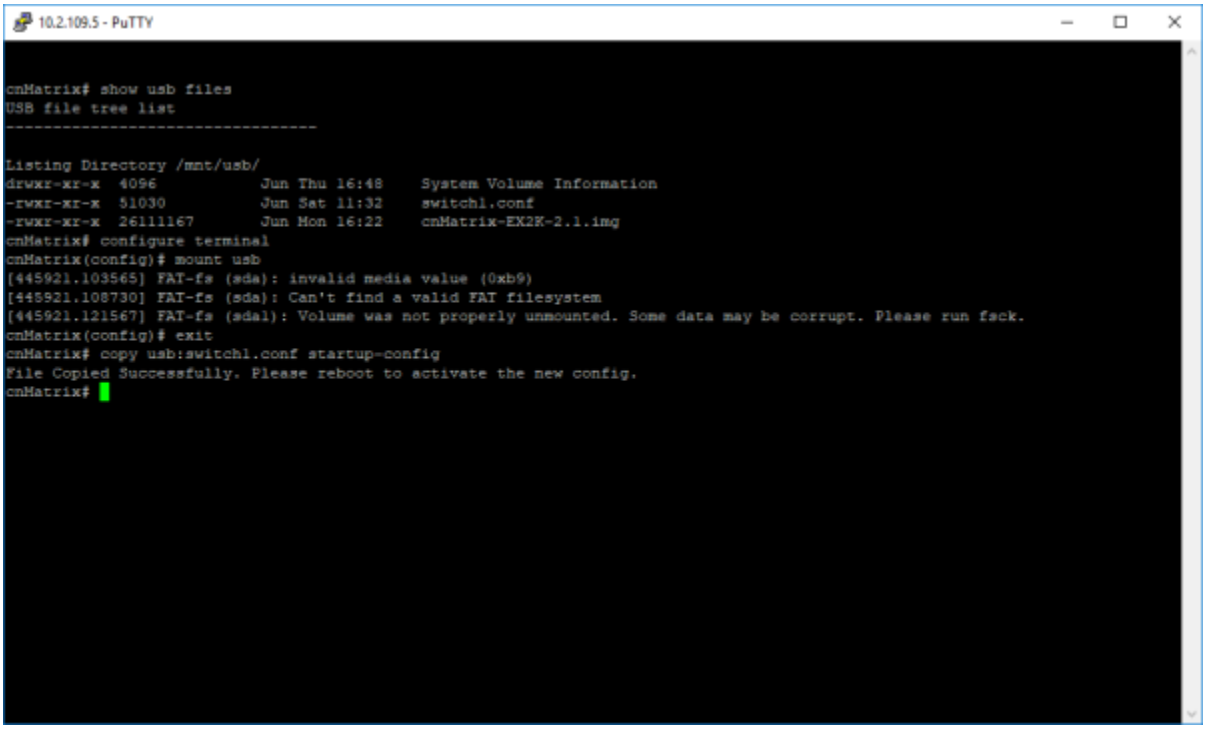
How to Copy Startup Config from Switch to USB (Example)



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.

How to Copy Startup Config from USB to Switch (Example)



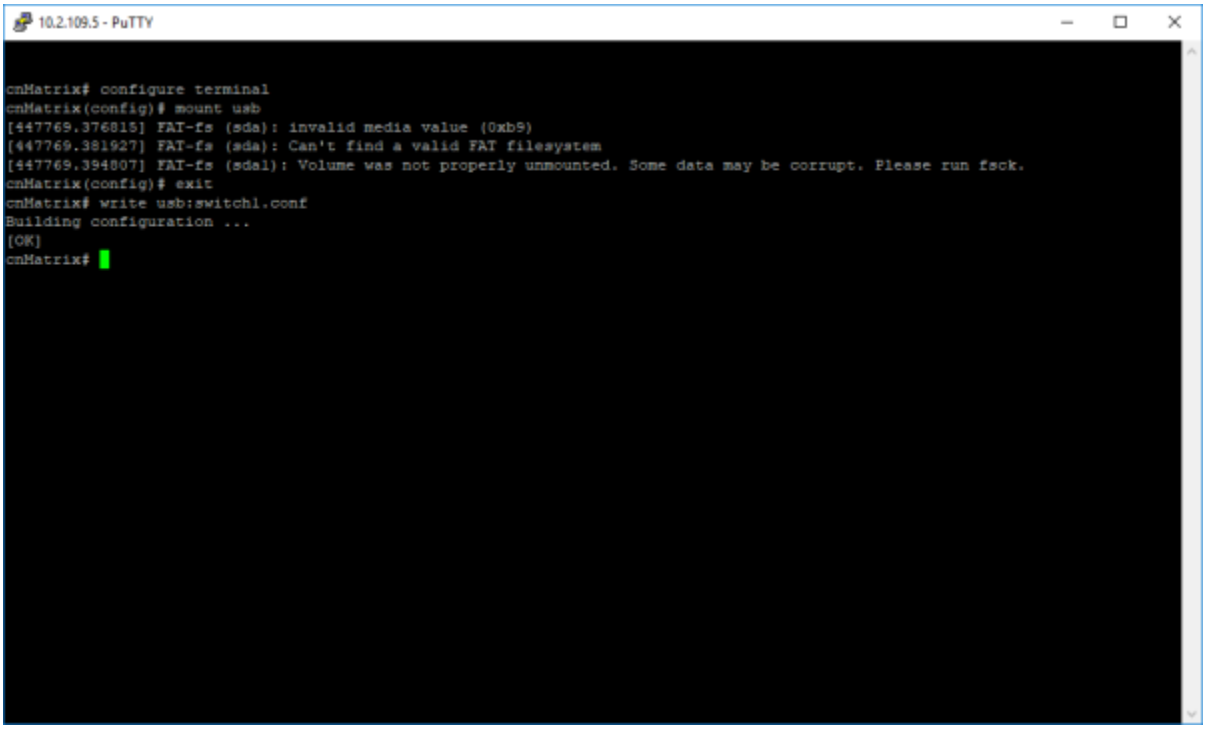
7. Type the **show usb files** command into the terminal to display the files that are currently on the USB. Press the **Enter** key.
8. Type the **configure terminal** command into the terminal. Press the **Enter** key.
9. Type the **mount usb** command into the terminal to mount a USB stick. Press the **Enter** key.
10. Type the **exit** command into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.
11. 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.

Caution

Please reboot your switch to activate the new configuration.

For more information, see USB Parameters and Commands.

How to Copy Running-Config to Switch



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

Troubleshooting USB

Useful commands for troubleshooting:

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

IP Quick Start

Managing IP Quick Start

Feature Overview

The IP Quick Start feature implements a CLI command that updates core IPv4 network settings on a defaulted switch:

1. Settings for (default) VLAN 1 are updated.
2. DHCP-based IP address allocation is updated to 'manual'.
3. The IP address and subnet mask associated with VLAN 1 are updated to the specified values.

4. A default route (0.0.0.0/0) for the designated default gateway is added to the routing database.
5. A DNS server is configured (when specified) for URL resolution.

Note:

The IP Quick Start feature can be configured via CLI and Web.

Attention

IP Quick Start feature is supported starting with cnMatrix release 4.2.

Standards

N/A

Limitations

N/A

Default Values

N/A

Configuring IP Quick Start (Example)

1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **ip Quick Start 10.10.20.30 255.255.255.0 gateway 10.10.20.10 name-server 8.8.8.8** command into the terminal to set on the default vlan (VLAN 1).
3. Static ip – 10.10.20.30
4. Subnet mask – 255.255.255.0
5. Default route to gateway – 10.10.20.10
6. Name server – 8.8.8.8
7. Press the Enter key.

Note:

Gateway and name-server parameters are optional.

Take care when manually configuring an IP address without specifying a default gateway. DHCP-based settings are cleared and the device may become unreachable until a gateway is configured.

How to show IP Quick Start settings (Example)

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

Troubleshooting IP Quick Start

Useful commands for troubleshooting

- cnMatrix# show running-config

Banners

Feature Overview

Banners are customized messages that are presented to a user in the terminal or in the Web UI. The login banner will be presented before the user logs in and the message-of-the-day (MOTD) banner will be presented after the user logs in.

Limitations

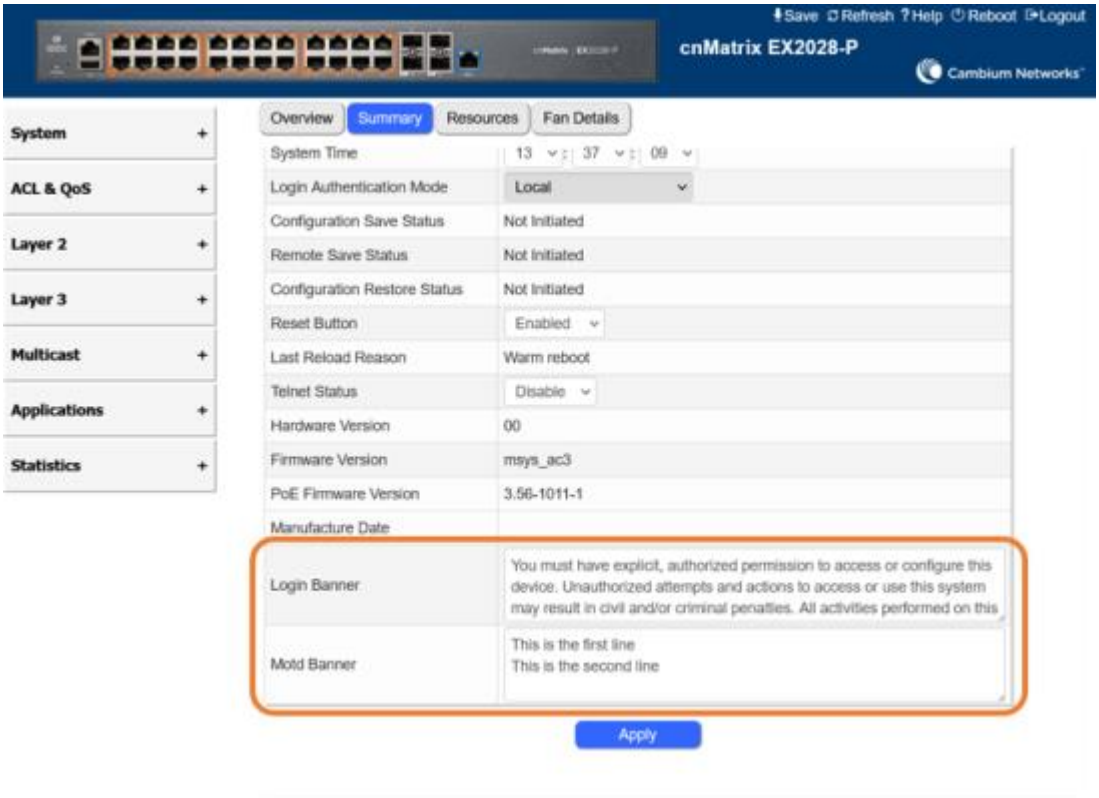
Maximum banner length is 256 characters.

Default Values

No banner is configured.

How configure the login and MOTD banners (Example)

```
cnMatrix# configure terminal
cnMatrix(config)# banner login "You must have explicit, authorized permission to
 access or configure this device. Unauthorized attempts and actions to access or
 use this system may result in civil and/or criminal penalties. All activities p
erformed on this device are logged and monitored"
cnMatrix(config)# banner motd "This is the first line\nThis is the second line"

cnMatrix(config)# end
```

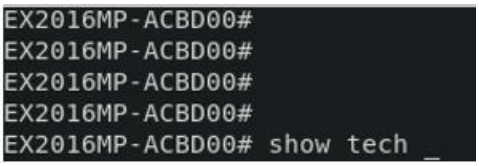


Show Tech

Feature Overview

The **Show Tech** command displays most common data from various show commands for debugging purposes.

How to display critical device state and debug information using Show Tech command (Example)

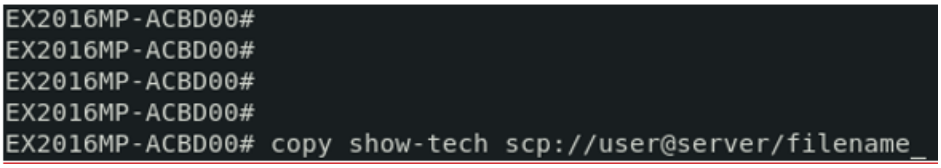


Type the show tech command into the terminal. Press the **Enter** key.

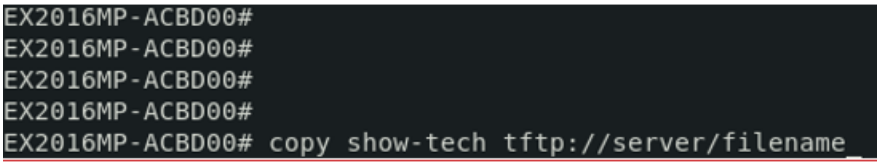
Note:

The output of the **Show Tech** command can be very large. You can save the output to a file on a remote server and inspect the data there.

How to copy the output of the Show Tech command to a remote file (Example)



Type the **copy show-tech scp://user@server/filename** command into the terminal. Press the **Enter** key.



Type the **copy show-tech tftp://server/filename** command into the terminal. Press the **Enter** key.

SCP

Feature Overview

The SCP is a network protocol, based on the BSD RCP protocol, which supports file transfers between hosts on a network. SCP uses Secure Shell (SSH) for data transfer and uses the same mechanisms for authentication, thereby ensuring the authenticity and confidentiality of the data in transit. A client can send (upload) files to a server, optionally including their basic attributes (permissions, timestamps). Clients can also request files or directories from a server (download).

The SCP protocol uses a client server model. cnMatrix contains only the SCP client implementation.

Default Values

The SPC client is enabled by default.

How to download software images using SCP (Example)

```
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00# download agent scp://user@server/cnMatrix-EXTX-4.4.0-b2.img.tar
.gz
```

1. Type the **download agent scp://user@server/filename** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password**: Enter the password and press the **Enter** key.

How to upload startup config using SCP (Example)

```
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00# copy startup-config scp://user@server/filename_
```

1. Type the **copy startup-config scp://user@server/filename** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password:** Enter the password and press the **Enter** key.

How to download startup config using SCP (Example)

```
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00# copy scp://user@server/filename startup-config _
```

1. Type the **copy scp://user@server/filename startup-config** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password**: Enter the password and press the **Enter** key.

How to upload running config using SCP (Example)

```
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00# copy running-config scp://user@server/filename_
```

1. Type the **copy running-config scp://user@server/filename** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password**: Enter the password and press the **Enter** key.

How to download running config using SCP (Example)

```
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00#
EX2016MP-ACBD00# copy scp://user@server/filename running-config _
```

1. Type the **copy scp://user@server/filename running-config** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password**: Enter the password and press the **Enter** key.

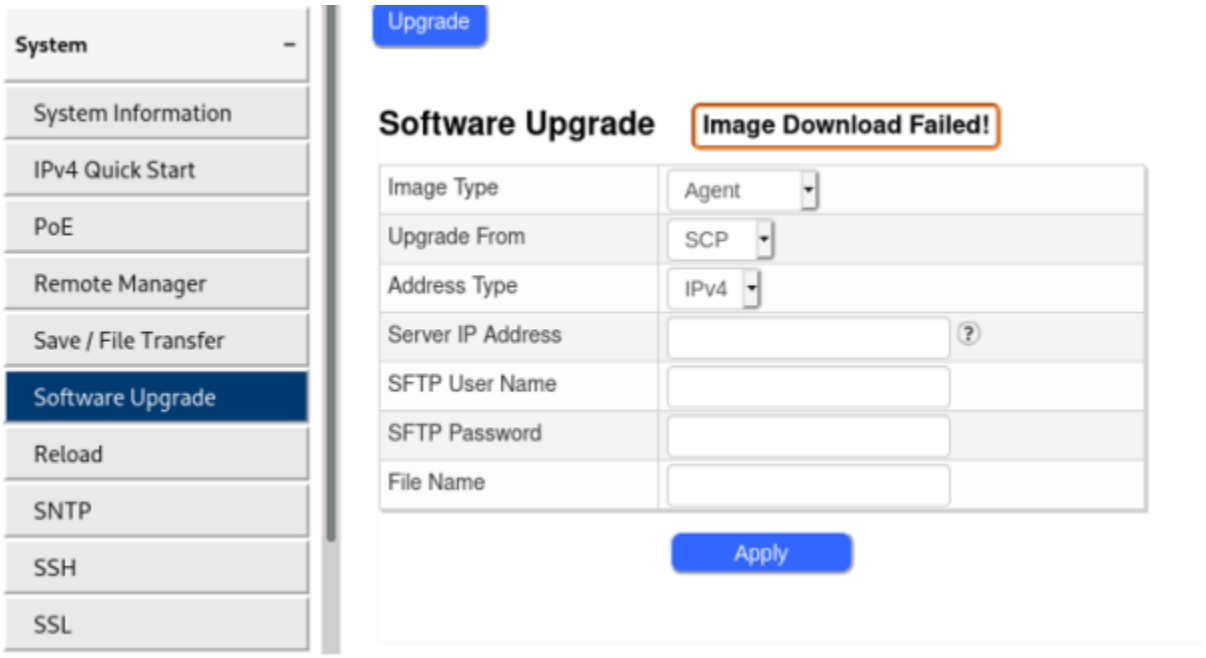
Troubleshooting SCP

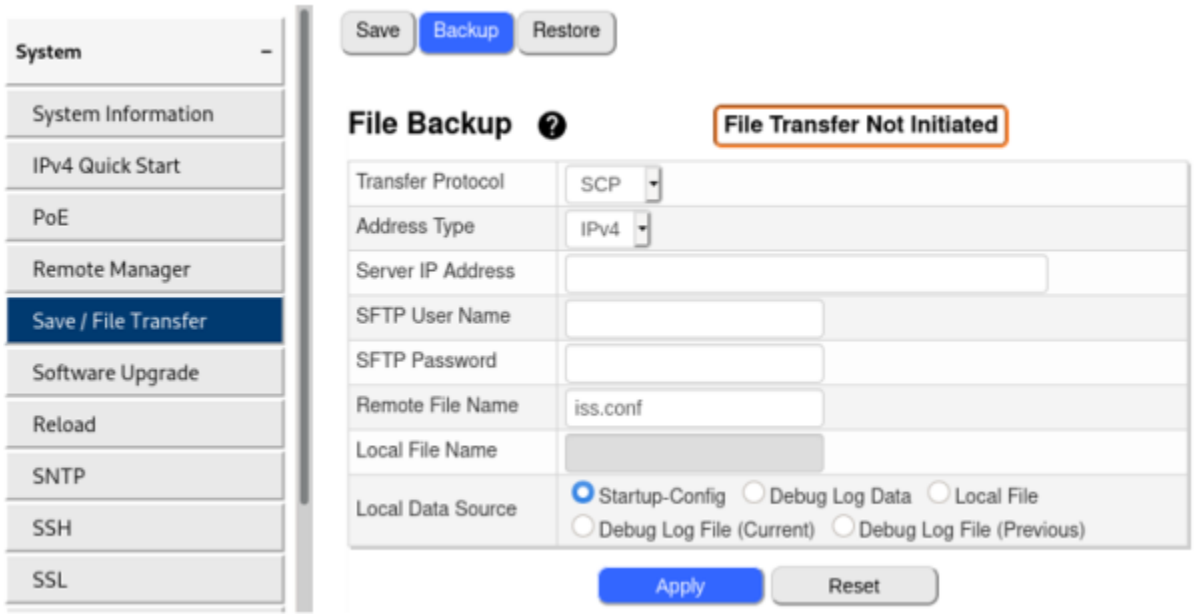
Useful commands for troubleshooting

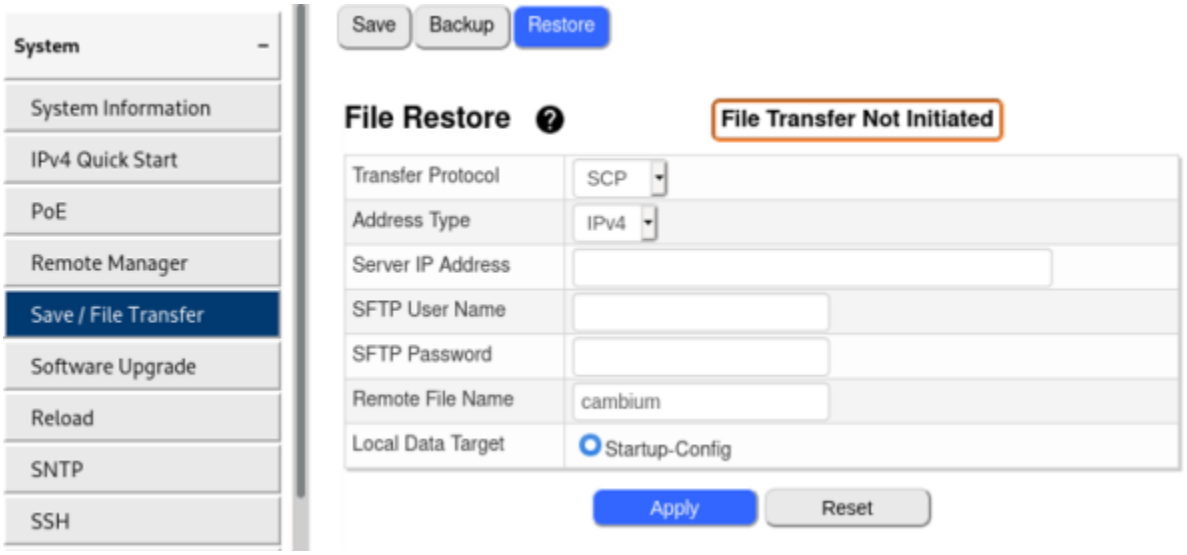
- cnMatrix# debug scp
- cnMatrix# no debug scp

```
EX2016MP-ACBD00#
EX2016MP-ACBD00# debug scp
EX2016MP-ACBD00#
EX2016MP-ACBD00# download agent scp://klu@10.2.109.2:/tftpboot/uImage_25_07_2022
_cs
 Download is in Progress...
*   Trying 10.2.109.2:22...
* Connected to 10.2.109.2 (10.2.109.2) port 22 (#0)
* SSH MD5 fingerprint: 5868a0f2b66a85b57af296a9f36de28f
* SSH authentication methods available: publickey,gssapi-keyex,gssapi-with-mic,password
* Initialized password authentication
* Authentication complete
* SSH CONNECT phase done
* Connection #0 to host 10.2.109.2 left intact

Image Download Successful
Please Reboot to Load the new Image
EX2016MP-ACBD00#
```

```
EX2016MP-ACBD00#
EX2016MP-ACBD00# no debug scp
EX2016MP-ACBD00#
EX2016MP-ACBD00#
```


System
System Information
IPv4 Quick Start
PoE
Remote Manager
Save / File Transfer
Software Upgrade
Reload
SNTP
SSH
SSL
Upgrade
Software Upgrade
Image Download Failed!
Image Type
Agent
Upgrade From
SCP
Address Type
IPv4
Server IP Address
SFTP User Name
SFTP Password
File Name
Apply


System
System Information
IPv4 Quick Start
PoE
Remote Manager
Save / File Transfer
Software Upgrade
Reload
SNTP
SSH
SSL
Save
Backup
Restore
File Backup
File Transfer Not Initiated
Transfer Protocol
SCP
Address Type
IPv4
Server IP Address
SFTP User Name
SFTP Password
Remote File Name
iss.conf
Local File Name
Local Data Source
Startup-Config
Debug Log Data
Local File
Debug Log File (Current)
Debug Log File (Previous)
Apply
Reset



Automatic configuration using DHCP and TFTP

Feature Overview

Zero-touch configuration can also be implemented with the help of a DHCP server and a TFTP server. A switch running factory default configuration will look for DHCP option 66 in the DHCP offers and if the option is present, the switch will attempt to contact the TFTP server at the address given in option 66, download the configuration file and execute it.

Detailed Behavior

The file to download from the TFTP server can be specified using DHCP option 67. If not specified, the switch will try the following file names in this order: network-config, cambium.cnf, cambium.conf, and hostname where hostname is the current hostname of the switch.

If no DHCP offer contains option 66 or the TFTP download failed, the switch will release the IP address and try to acquire a new one after 30 seconds and will keep doing this until the DHCP-based automatic configuration is either successful or cancelled.

The automatic configuration is cancelled by entering global configuration mode in the CLI, logging into the Web UI, onboarding on cnMaestro or when 170 seconds have passed since the first DHCP offer.

The automatic configuration is considered successful even if the execution of the script terminated with errors.

Saving the configuration either manually or via the automatic configuration script will disable the automatic configuration mechanism until the next factory reset. If the configuration is not saved, the mechanism will download and execute the configuration on every boot.

Troubleshooting Automatic Configuration

Useful commands for troubleshooting

- cnMatrix# show logging

CPU Monitor

Managing CPU Monitor

Feature Overview

When enabled, the cnMatrix switch captures the received packets that hit CPU. The packets are saved within a buffer in RAM and do not persist through a reboot. Once the data is captured, it can be displayed in hex format to CLI console. CPU Monitor process it will stop automatically if a configuration limit is reached or if the RAM usage is above 85%.

Data can be exported as a packet capture (PCAP) file to allow for further examination. Parameters are configured in exec mode and they are temporary. As result, the configuration is not stored within the switch configuration and does not remain in place after a system reboot.

Limitations

CPU Monitor captures packets only on Rx. The limits are 32 MB for buffer size or 10000 for number of packets.

Default Values

CPU Monitor is inactive by default.

- Buffer size value is 10KB.
- Packet size value is 64 bytes.
- Number of packets to be captured is 10.

How to Enable and Configure CPU Monitor

```
EX2010-EC9EC0# show cpu-monitor config
 Info                  Actual value       Limit / filter type
 --------------     -----------------     -------------------
 Buffer size                       0                    10 KB
 Packet size                      na                    64
 Nr of Packets                     0                    10
 Direction                        Rx                    na
 Status                     INACTIVE                    na
EX2010-EC9EC0# config terminal
EX2010-EC9EC0(config)# cpu-monitor buffer-size 20
EX2010-EC9EC0(config)# cpu-monitor packet-size 128
EX2010-EC9EC0(config)# cpu-monitor packets-limit 50
EX2010-EC9EC0(config)# exit
EX2010-EC9EC0# show cpu-monitor config
 Info                  Actual value       Limit / filter type
 --------------     -----------------     -------------------
 Buffer size                       0                    20 KB
 Packet size                      na                   128
 Nr of Packets                     0                    50
 Direction                        Rx                    na
 Status                     INACTIVE                    na
EX2010-EC9EC0# cpu-monitor start
EX2010-EC9EC0# show cpu-monitor config
 Info                  Actual value       Limit / filter type
 --------------     -----------------     -------------------
 Buffer size                       3                    20 KB
 Packet size                      na                   128
 Nr of Packets                    50                    50
 Direction                        Rx                    na
 Status                       DONE                      na
EX2010-EC9EC0#
```

1. Type the **show cpu-monitor config** command into the terminal to see the initial config. Press the **Enter** key.
2. Type the **configure terminal** command into the terminal. Press the **Enter** key.
3. Type **cpu-monitor buffer-size 20** to set another buffer size. Press the **Enter** key.
4. Type **cpu-monitor packet-size 128** to set the maximum size which the packets are saved to the buffer. Press the **Enter** key.
5. Type **cpu-monitor packets-limit 50** to set the maximum number of packets that will be saved in the buffer. Press the **Enter** key.
6. Type **Exit** command to go back to the global configuration mode. Press the **Enter** key.
7. Type **cpu-monitor start** command to start capturing packets process. Press the **Enter** key.
8. Type **cpu-monitor stop** command at any time stop the capturing process. Press the **Enter** key.

How to dump to CLI captured packets

```
EX2052-EC0880# show cpu-monitor config
 Info                  Actual value       Limit / filter type
 --------------      ----------------     -------------------
 Buffer size                      <1                    10 KB
 Packet size                      na                    64
 Nr of Packets                    10                    10
 Direction                        Rx                    na
 Status                         DONE                    na
EX2052-EC0880# show cpu-monitor output

2022/11/17 13:17:00.363013 64

0000 58 C1 7A EC 08 81 8C 8C AA D4 32 14 08 00 45 00
0010 00 28 3D 96 40 00 80 06 96 8D C0 A8 52 7E C0 A8
0020 52 DD FD A7 00 16 A1 D8 F2 0B D1 4E EE 8D 50 10
0030 04 02 33 A7 00 00 00 00 00 00 00 00 55 55 55 55

2022/11/17 13:17:00.408948 64

0000 58 C1 7A EC 08 81 8C 8C AA D4 32 14 08 00 45 00
0010 00 28 3D 97 40 00 80 06 96 8C C0 A8 52 7E C0 A8
0020 52 DD FD A7 00 16 A1 D8 F2 0B D1 4E EF 9D 50 10
0030 04 01 32 98 00 00 00 00 00 00 00 00 55 55 55 55

2022/11/17 13:17:05.101189 64

0000 58 C1 7A EC 08 81 60 A4 B7 9B 69 2C 08 06 00 01
0010 08 00 06 04 00 01 60 A4 B7 9B 69 2C C0 A8 52 01
0020 00 00 00 00 00 00 C0 A8 52 DD 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 55 55 55 55

2022/11/17 13:17:15.240832 64
--More (q=Quit, space=Scroll by one screen, return=Scroll by one line)--
```

1. Type the **show cpu-monitor config** command into the terminal to check that cpu-monitor capturing process is finished, it is in the DONE state. Press the **Enter** key.
2. Type the **show cpu-monitor output** command into the terminal to display the contents of the captured packets. Press the **Enter** key.

How to upload CPU Monitor buffer using SCP

In order to upload a captured session, it must first be ended, be in the DONE state.

```
EX2010-EC9EC0# show cpu-monitor config
 Info                  Actual value       Limit / filter type
 --------------      ----------------     -------------------
 Buffer size                      3                    20 KB
 Packet size                     na                   128
 Nr of Packets                   50                    50
 Direction                       Rx                    na
 Status                        DONE                    na
EX2010-EC9EC0# copy cpu-monitor scp://user-name@server:/fullpath/filename.pcap
%% Password:
```

1. Type **copy cpu-monitor scp://user@server:/fullpath/filename.pcap** command into the terminal. Press the **Enter** key.
2. You will be prompted for the **%%Password**: Enter the password and Press the **Enter** key.

How to upload CPU Monitor buffer using SFTP

```
EX2010-EC9EC0#
EX2010-EC9EC0# copy cpu-monitor sftp://user-name:password@server/filename.pcap
```

Type **copy cpu-monitor sftp://user:passwrd@server/filename.pcap** command into the terminal. Press the **Enter** key

How to upload CPU Monitor buffer using TFTP

```
EX2010-EC9EC0#
EX2010-EC9EC0# copy cpu-monitor tftp://server/filename.pcap
```

Type **copy cpu-monitor tftp://server/filename.pcap** command into the terminal. Press the **Enter** key.

Security Features

LOCAL AUTHENTICATION

User authentication retries

For security reasons, if a user tries to login with wrong credentials several times, it will be blocked for a certain amount of time. By default, if the user fails to authenticate 3 times, the user will be locked for 10 minutes.

Note:

User **admin** will be blocked just on remote sessions (SSH, Telnet, and Web), not on serial console.

The number of retries and the block period can be configured using the following command:

```
cnMatrix(config)# login block-for <30-900secs> attempts <1-10>
```

To set to default values, use:

```
cnMatrix(config)# default login block-for
```

Even if a user gets locked after it reached the maximum of login retries, it can be unlocked. Only user ‘admin’ can unblock other users.

Correspondent command:

```
cnMatrix(config)# enableuser<username>
```

To check if a user is blocked or not use the following commands:

```
cnMatrix# show blocked users
```

Inactivity Timeout

After an inactivity timeout expired on a certain session, the user will be logged out. The inactivity timeout is configurable and has correspondent command for both CLI and Web sessions.

CLI session:

- Inactivity timeout can be set with the command:

  ```
  cnMatrix(config)# exec-timeout <1-18000secs>
  ```

- The default value is 1800 secs. The value can be restored to default value using:

  ```
  cnMatrix(config)# default exec-timeout
  ```

Web session:

- Inactivity timeout can be set with the command:

  ```
  cnMatrix(config)# Web-session timeout <1-15mins>
  ```

- The default value is 15 min. The Inactivity timeout can be set to default value using:

```
cnMatrix(config)# default Web-session timeout
```

To display inactivity timeout can be used following command:

```
cnMatrix# show sessions timeout
```

RADIUS

Managing RADIUS

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.

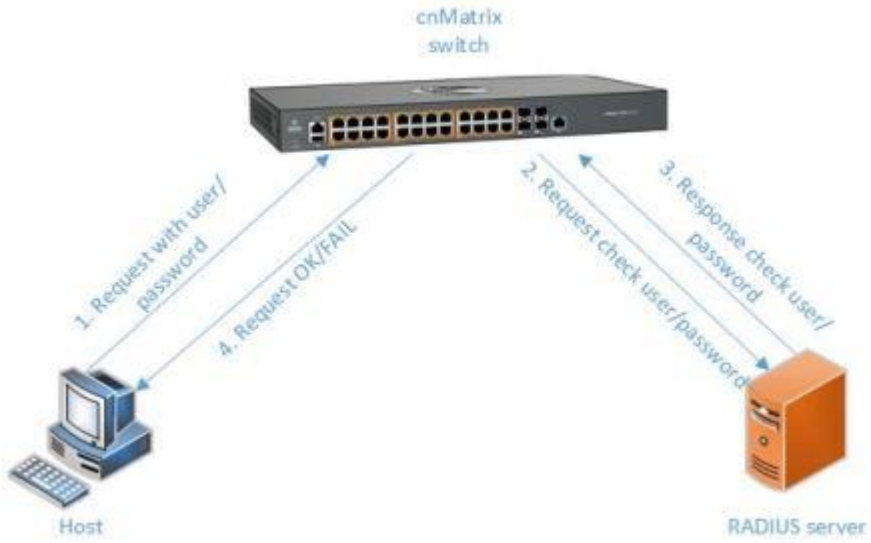
Default Values

- 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.

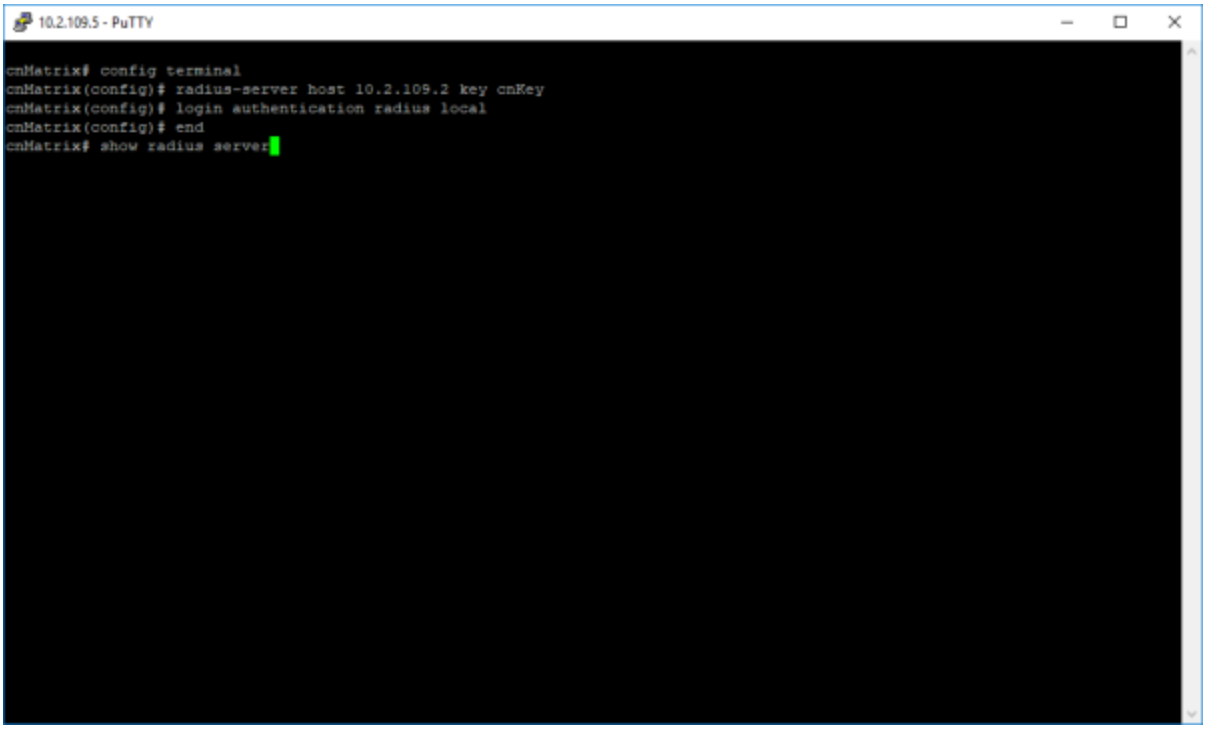
Prerequisites

N/A

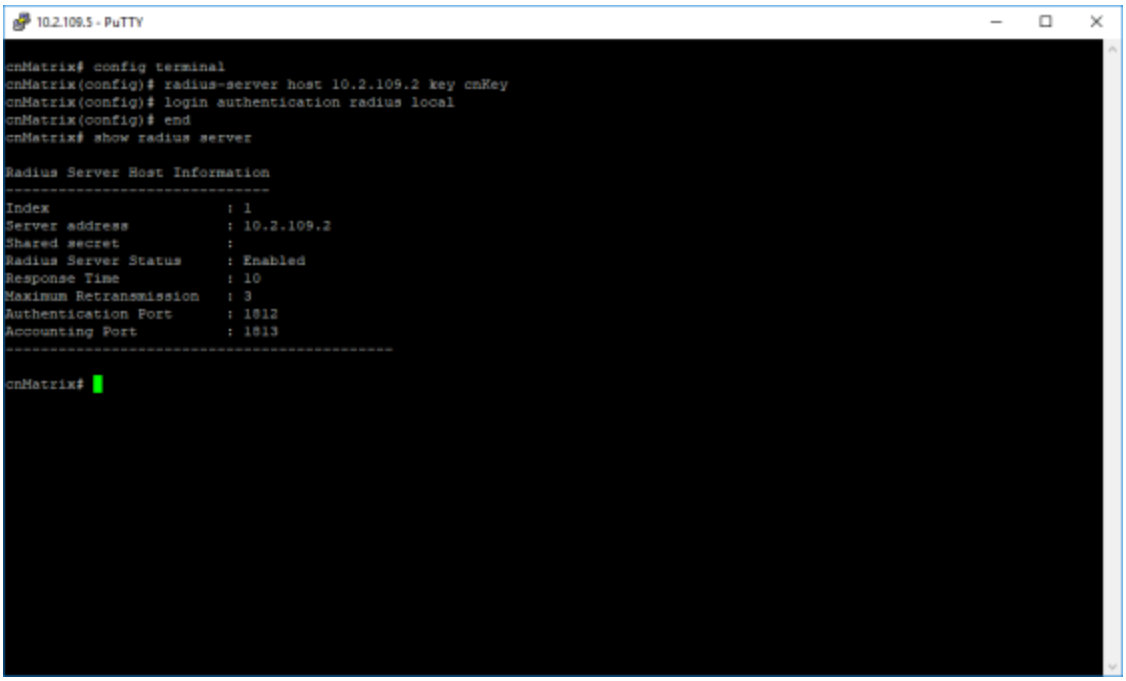
Network Diagram



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.

Troubleshooting RADIUS

Useful commands for troubleshooting:

- cnMatrix# show radius server
- cnMatrix# show radius statistics
- cnMatrix# debug radius all

RADIUS Dynamic Authorization

Feature Description

cnMatrix RADIUS Dynamic Authorization is a feature that allows cnMatrix to accept authorization changes from a RADIUS client with the purpose of changing the authorization of already connected users. cnMatrix RADIUS Dynamic Authorization is used with PNAC features.

Standards

- cnMatrix RADIUS Dynamic Authorization is RFC 3576 compliant.

Scaling Numbers

- cnMatrix RADIUS Dynamic Authorization accept requests from 32 clients.
- The maximum length of the secret key is 48 characters.

Limitations

- Clients can only be registered with their IPv4 address.

Default Values

- The default listen port is 3799.
- The debugging option is disabled by default.

Prerequisites

N/A

How to configure RADIUS Dynamic Authorization

1. Type **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **aaa server radius dynamic-author** command into the terminal to enter the RADIUS dynamic authorization configuration mode. Press the **Enter** key.
3. Type the **port 3799** command into the terminal to set the listen port to 3799. Press the **Enter** key.
4. Type the **client 192.168.0.10 server-key cnKey** into the terminal to specify a RADIUS client. 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 aaa clients** command into the terminal to display RADIUS dynamic authorization client configurations. Press the **Enter** key.

Troubleshooting RADIUS Dynamic Authorization

Useful commands for troubleshooting:

- cnMatrix# show aaa clients
- cnMatrix# debug aaa coa

Terminal Access Controller Access Control System (TACACS)

Managing TACACS

Feature Description

TACACS 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 TACACS+ 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

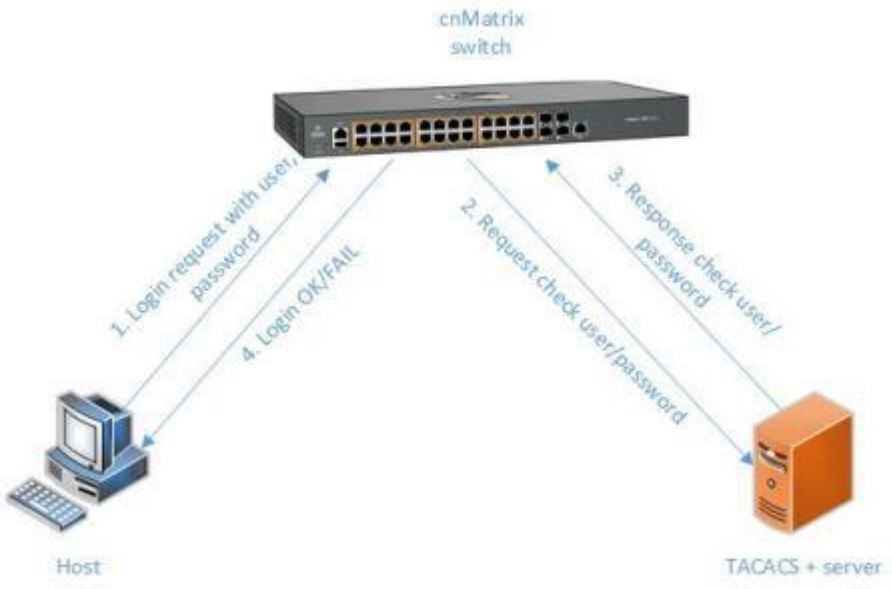
- The default TCP port number: 49.

- 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

Network Diagram



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.

Troubleshooting TACACS

Useful commands for troubleshooting:

- cnMatrix# debug tacacs
- cnMatrix# show tacacs server
- cnMatrix# show tacacs statistics

IGMP Snooping

Managing IGMP Snooping

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 512 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.

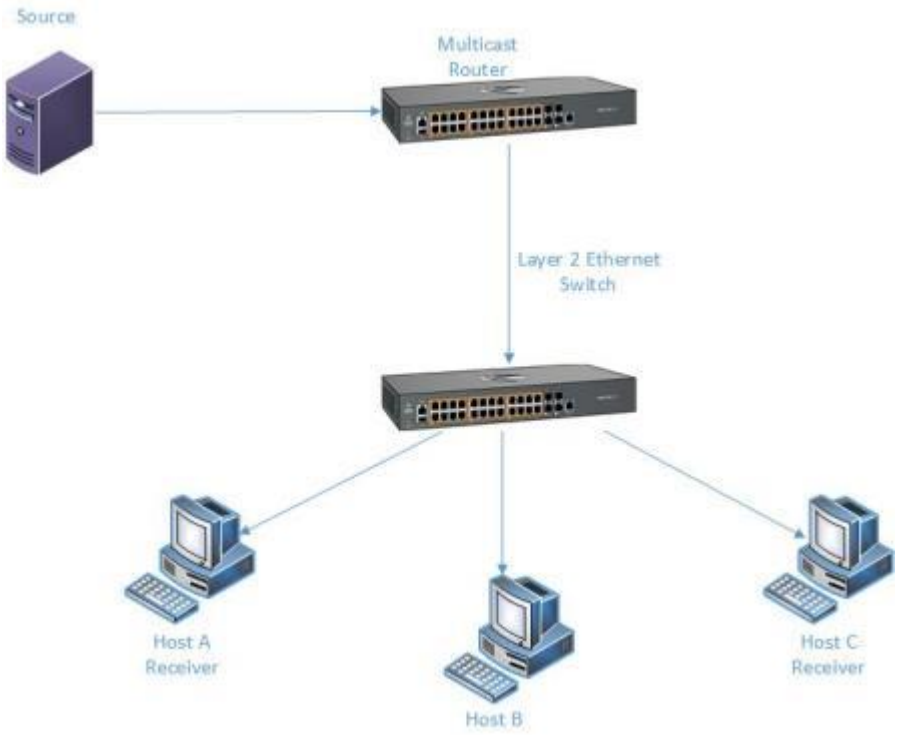
Prerequisites

- N/A

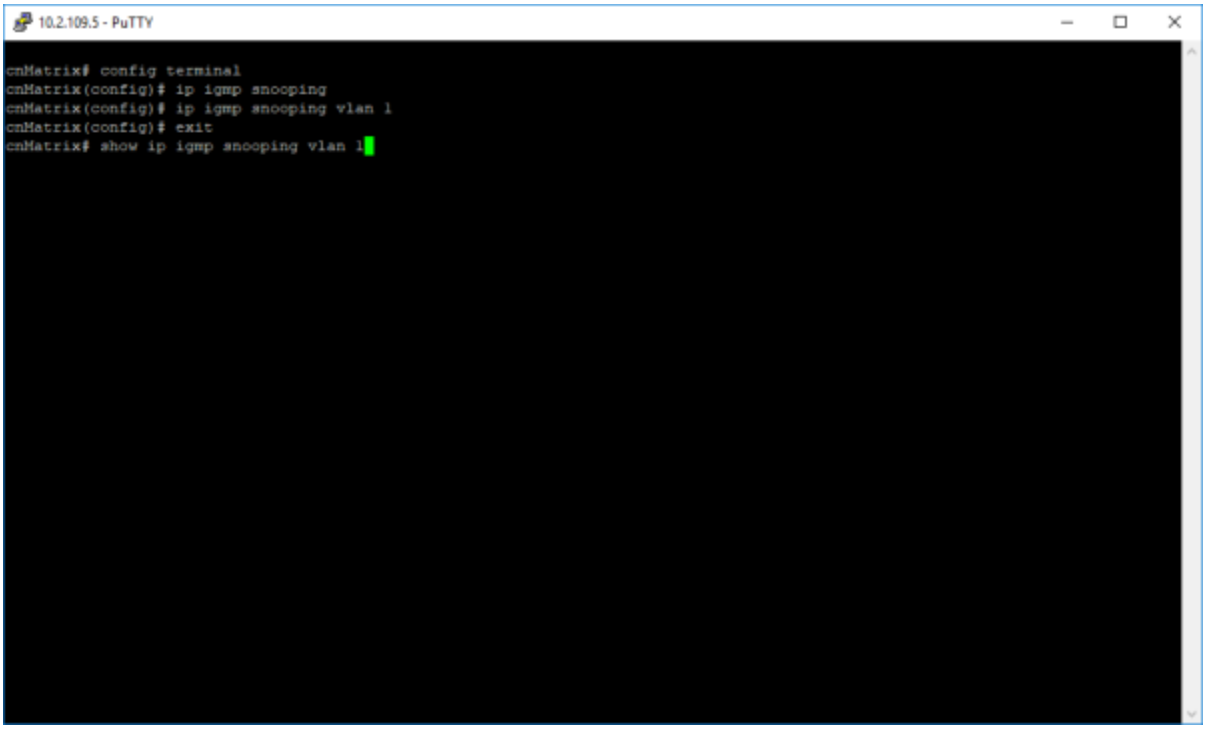
SNMP

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

Network Diagram

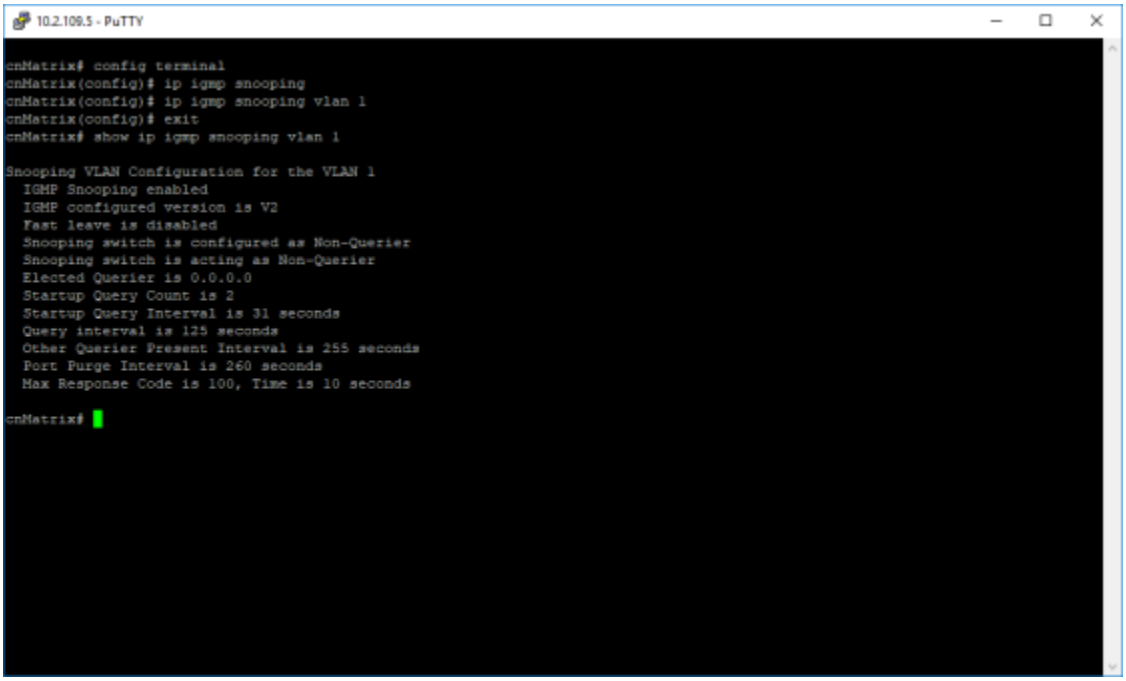


How to Enable IGMP Snooping in CLI Interface



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.

Troubleshooting IGMP Snooping

Useful commands for troubleshooting:

- cnMatrix# show ip igmp snooping
- cnMatrix#show ip igmp snooping globals
- cnMatrix#show ip igmp snooping statistics

IGMP Snooping Filtering

Managing IGMP Snooping Filtering

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

Note

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: 512.
- No IGMP filter is applied by default.

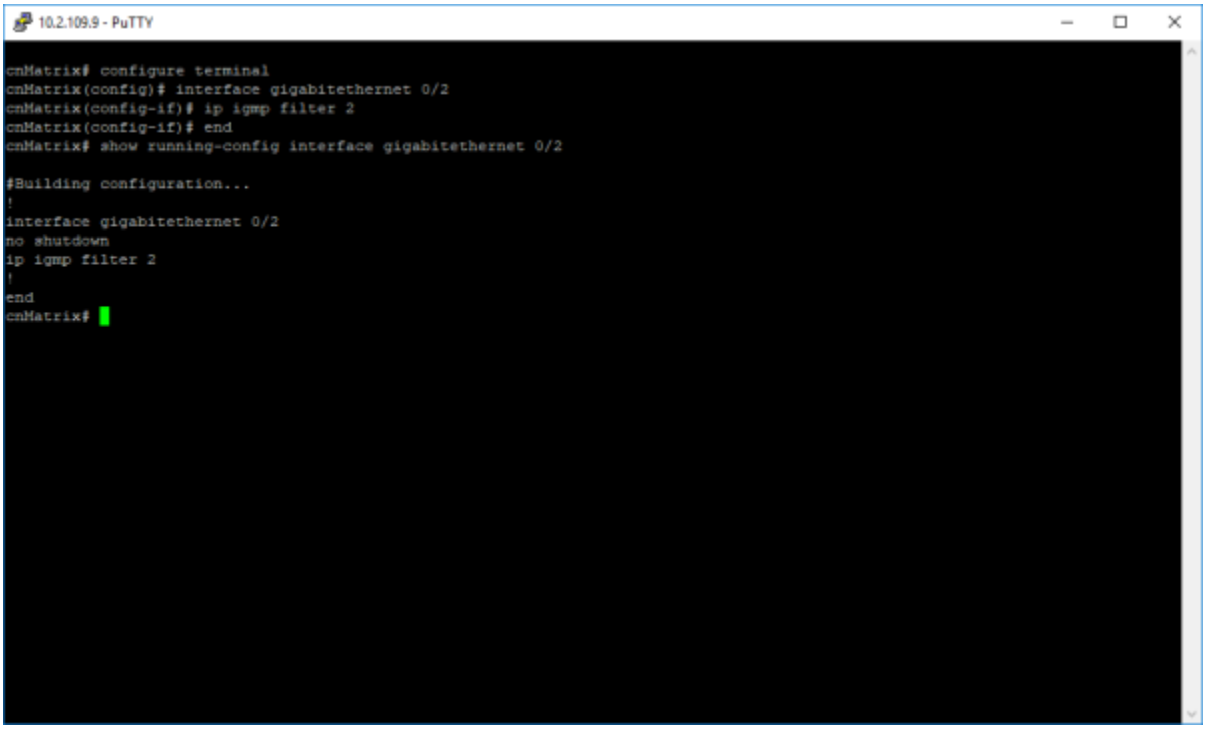
Prerequisites

Enable the IGMP Snooping feature:

- cnMatrix# configure terminal
- cnMatrix(config)# ip igmp snooping

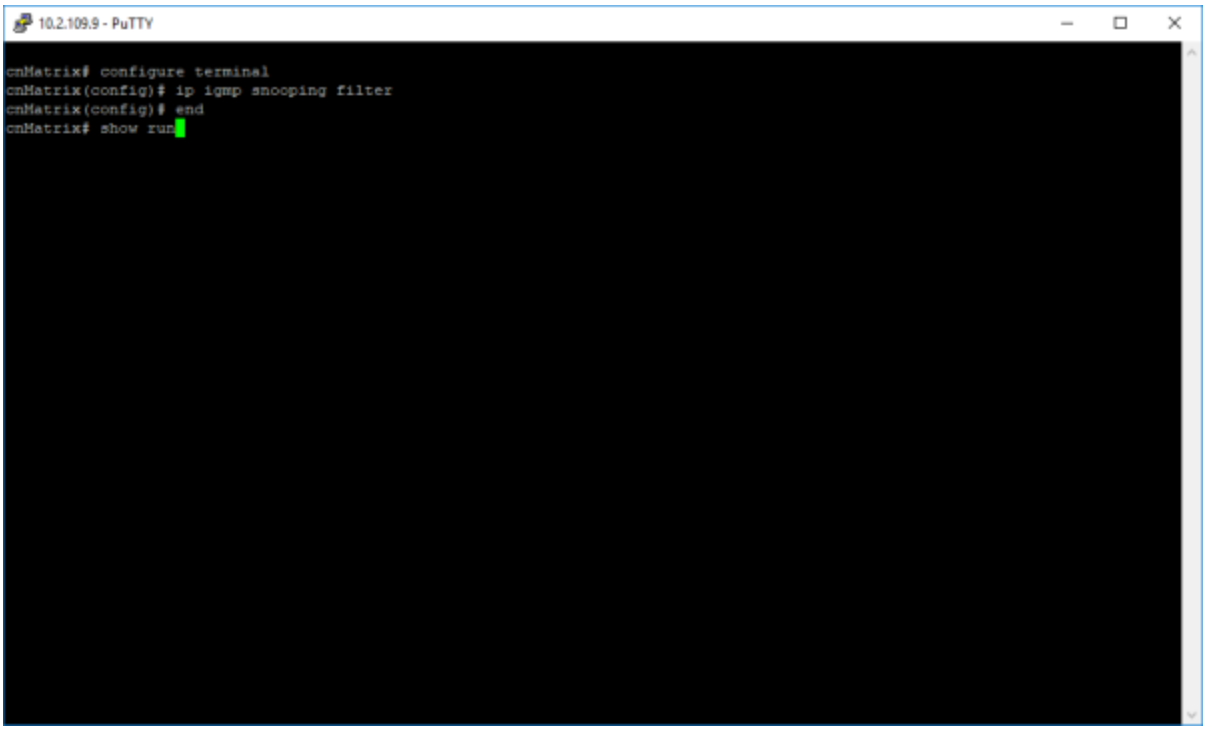
How to Enable, Configure and Apply IGMP Profiles in CLI Interface

Applying IGMP Profiles

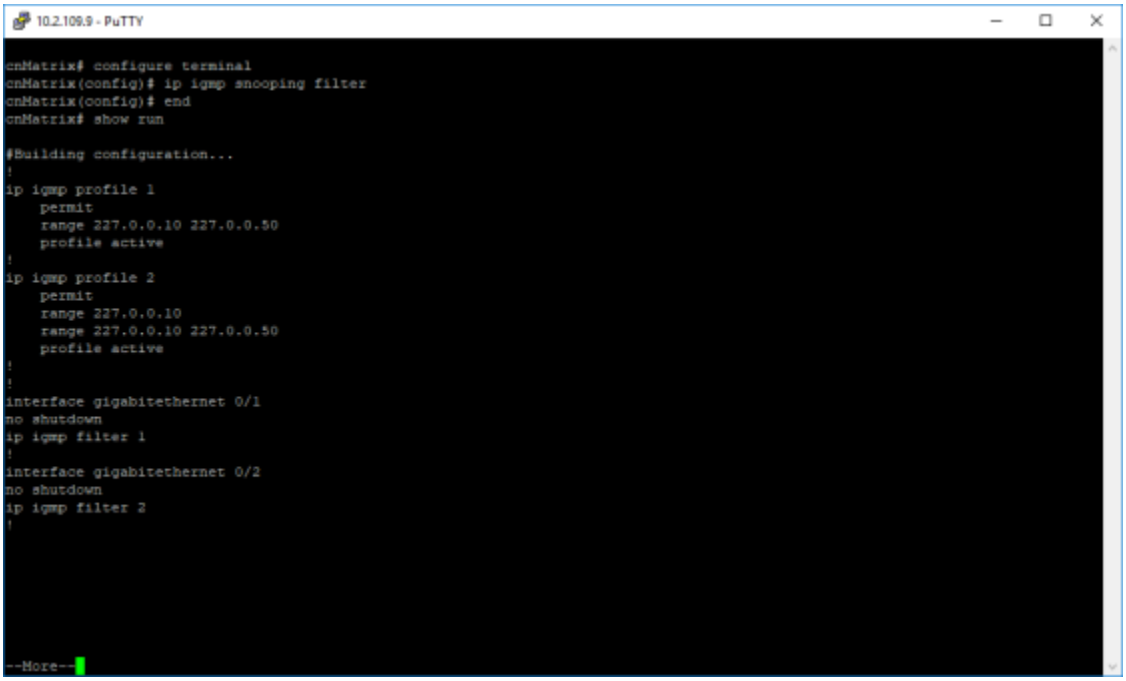


1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/2** command into the terminal. Press the **Enter** key.
3. Type the **ip igmp filter 2** command into the terminal. Press the **Enter** key to apply the specified IGMP profile 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.

Enabling IGMP Snooping Filter



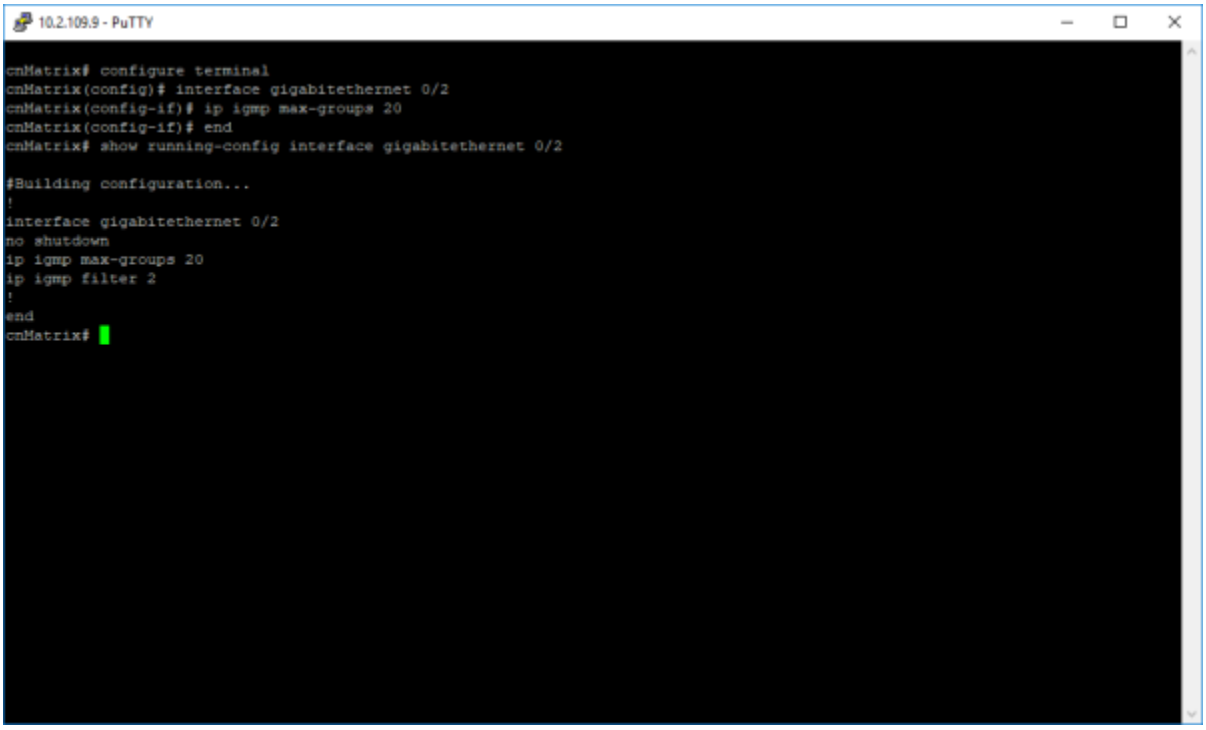
1. Type the **configure terminal** command into the terminal. Press the **Enter** key.
2. Type the **ip igmp snooping filter** command into the terminal to enable the IGMP Snooping filter. Press the **Enter** key.
3. Type the **end** command into the terminal to go to the Privileged EXEC mode. Press 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.



5. Press the **Enter** key.

For more information, see IGMP Snooping Parameters and Commands.

Setting 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.

   Note

   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.

DHCP Snooping

Managing DHCP Snooping

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 that 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.

Web User Interface

- DHCP Snooping parameters are configurable via the Web UI. Global DHCP Snooping status can be enabled or disabled and operational parameters configured on **Layer 2** > **DHCP Snooping** > **System**.
- Per-VLAN DHCP Snooping status is controlled through **Layer 2** > **DHCP Snooping** > **VLAN Settings**.
- Per-port DHCP Snooping trust state configuration is supported on **Layer 2** > **DHCP Snooping** > **Interfaces**.
- DHCP IP binding data is displayed through **Layer 2** > **DHCP Snooping** > **IP Bindings**.

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.

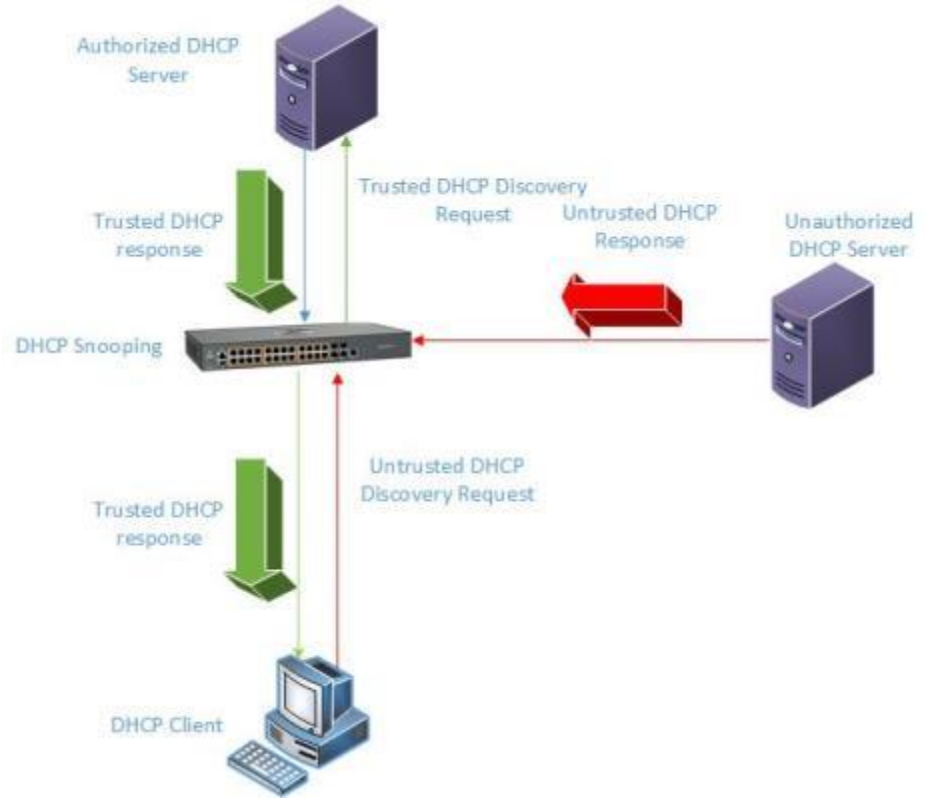
Prerequisites

- N/A

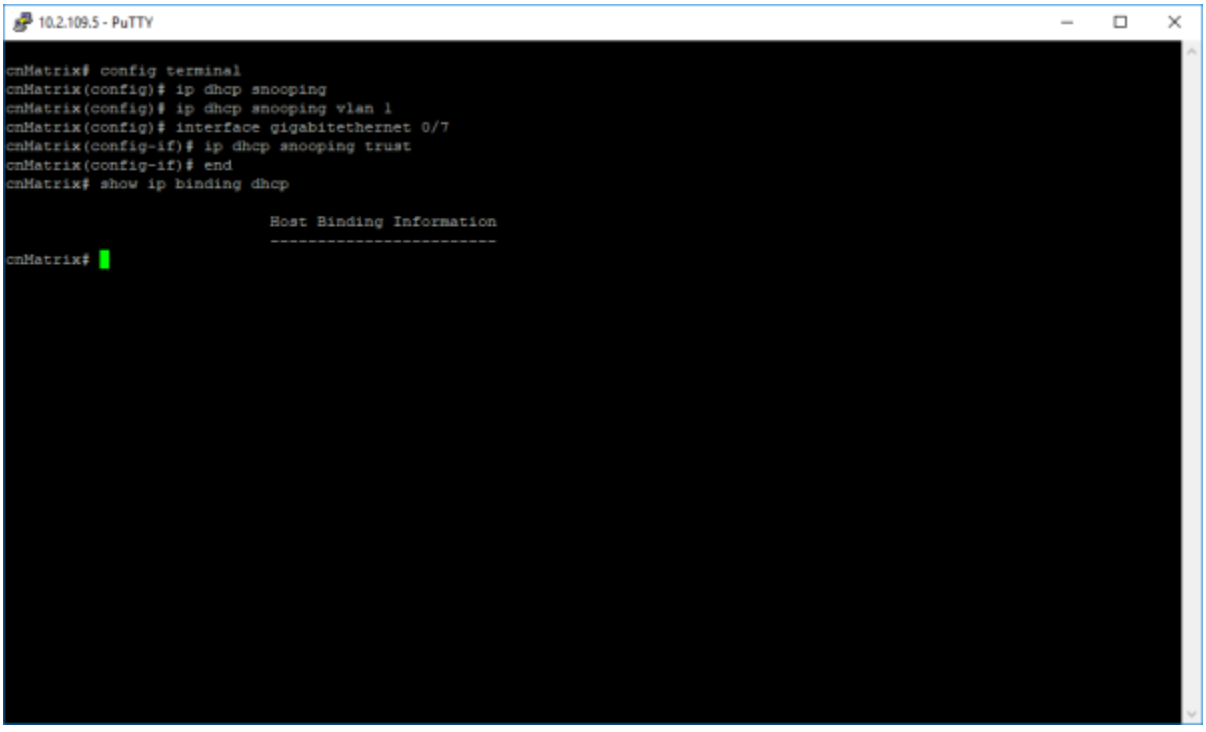
Note

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

Network Diagram



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.

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

Access Control List (ACL)

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 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 must 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 commit 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. The default mode is immediate.

Standards

N/A

Scaling Numbers

- The maximum number of ACLs that can be configured on a system is limited by the number of hardware policies available.: One ACL takes up one hardware policy for each port on which is applied. There is a total of 145 IPv4 policies available, while MAC and IPv6 ACLs share a total of 145 policies. One ACL applied on all ports takes up a single hardware policy.
- The usage of hardware policies can be displayed at any moment by issuing the **show access-lists resources** command.

Note

On **EX3K** units only, there is a total of 512 IPv4 and 512 MAC/IPv6 hardware policies available.

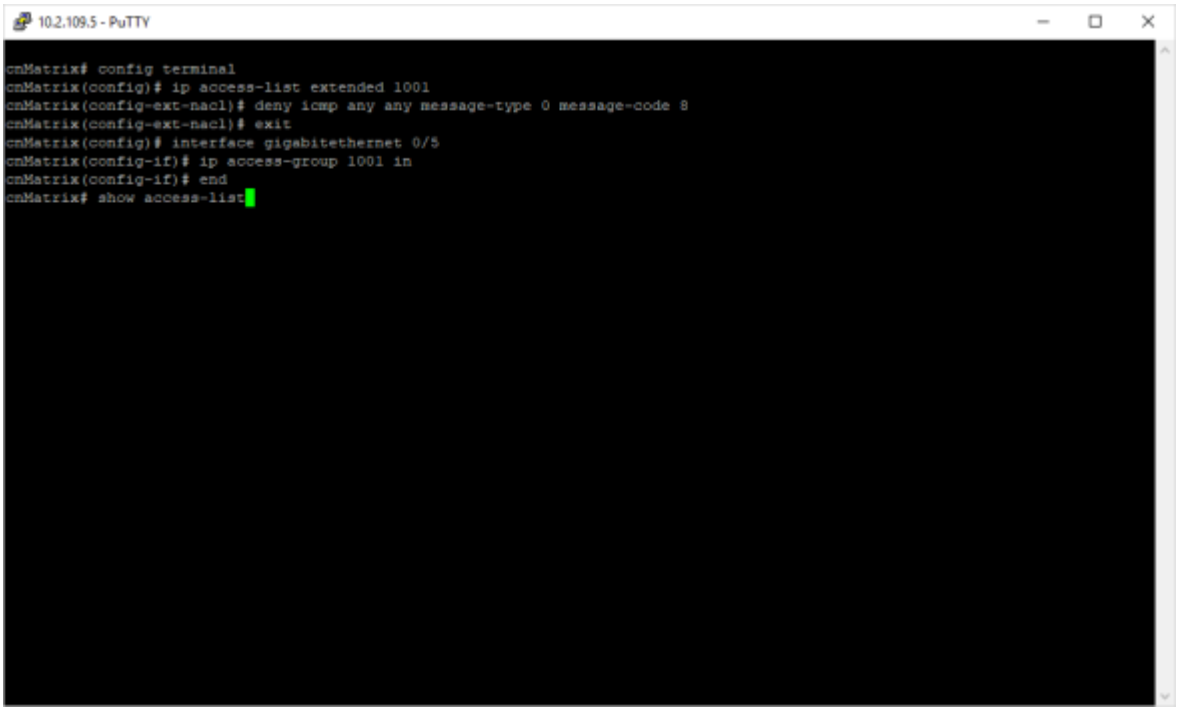
Limitations

- 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.

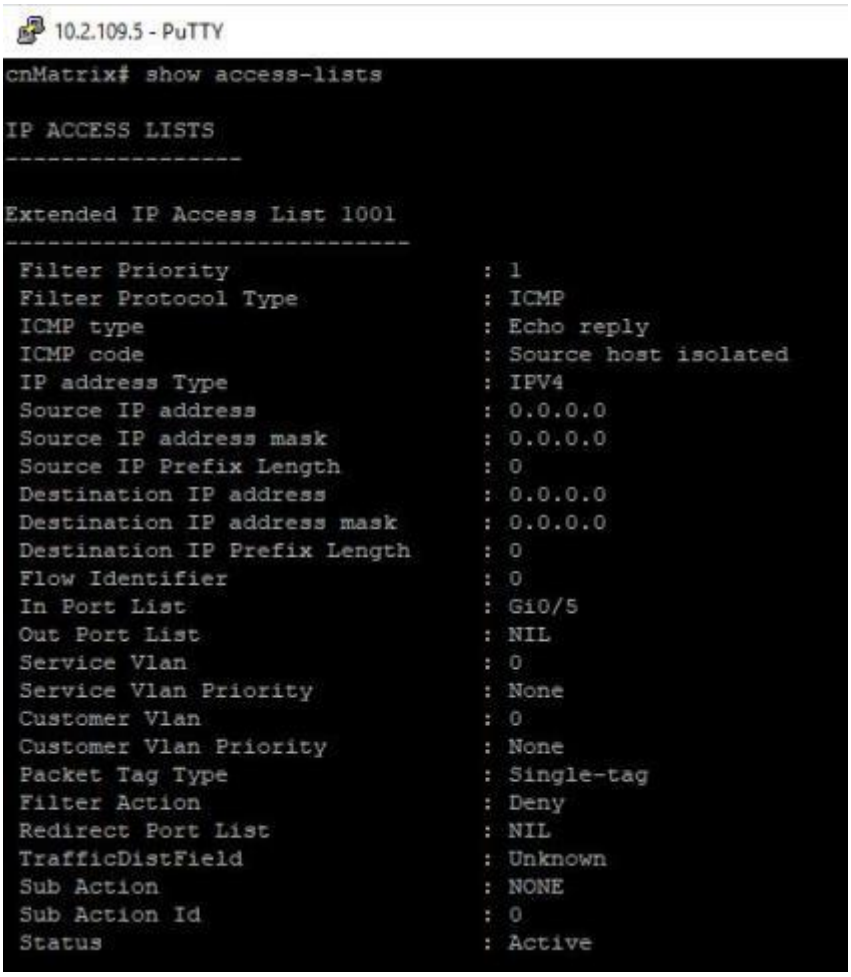
Default Values

- The default provisioning mode: immediate.
- No ACLs are preconfigured on the switch.

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.



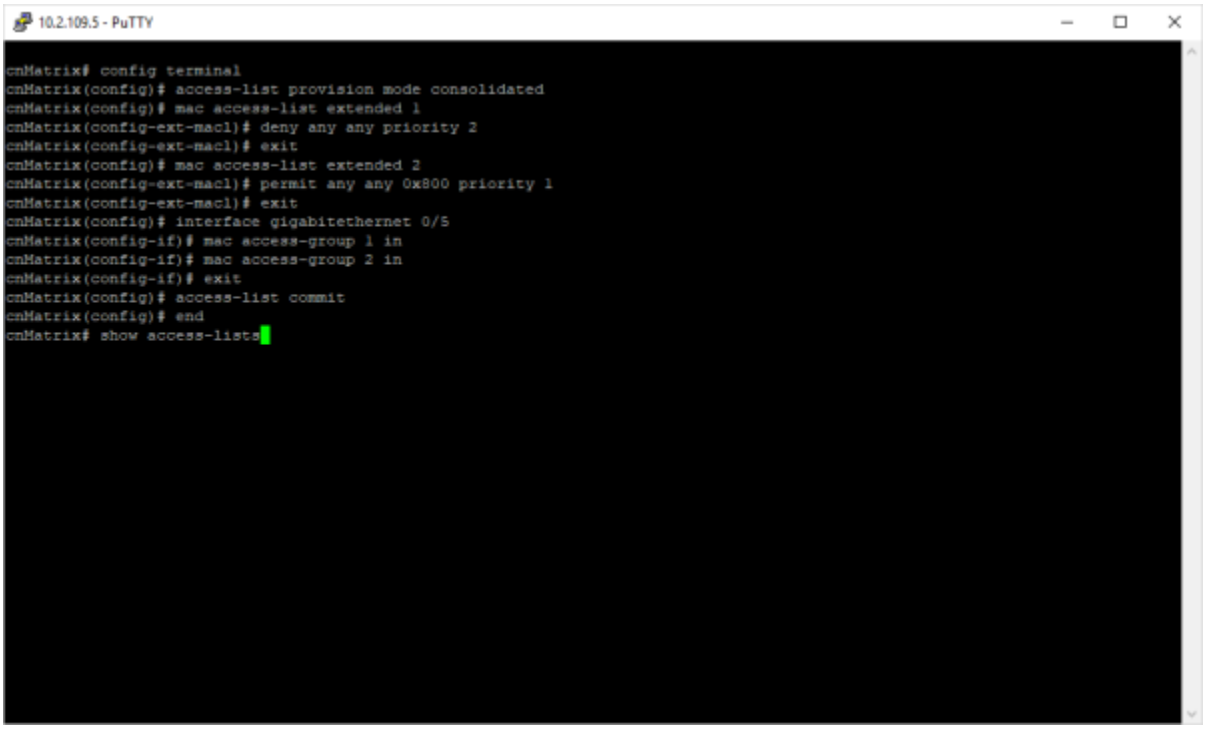
For more information, see ACL Parameters and Commands. **Starting with version 2.1**, see ACL Parameters and Commands version 2.1.

Configuring ACL in CLI Interface for a Vlan - Immediate Mode

```
EX2016MP-ACBD00# config terminal
EX2016MP-ACBD00(config)# ip access-list extended 1001
EX2016MP-ACBD00(config-ext-nacl)# deny icmp any any message-type 0 message-code
8
EX2016MP-ACBD00(config-ext-nacl)# exit
EX2016MP-ACBD00(config)# vlan 2
EX2016MP-ACBD00(config-vlan)# ip access-group 1001 in
EX2016MP-ACBD00(config-vlan)# end
EX2016MP-ACBD00# show access-lists ip 1001

Extended IP Access List 1001
----------------------------
 Filter Priority                 : 1
 Filter Action                   : Deny
 Filter Protocol Type            : ICMP
 ICMP type                       : Echo reply
 ICMP code                       : Source host isolated
 IP address Type                 : IPV4
 Source IP address               : ANY
 Source IP address mask          : ANY
 Source IP Prefix Length         : 0
 Destination IP address          : ANY
 Destination IP address mask     : ANY
 Destination IP Prefix Length    : 0
 Flow Identifier                 : 0
 In Port List                    : Gi0/1 , Gi0/2 , Gi0/3 , Gi0/4
                                 , Gi0/5 , Gi0/6 , Gi0/7 , Gi0/8
                                 , Gi0/9 , Gi0/10 , Gi0/11 , Gi0/12
                                 , Gi0/13 , Gi0/14 , Ex0/1 , Ex0/2
 Out Port List                   : NIL
 VLAN Id                         : 2
 VLAN Priority                   : None
 Sub Action                      : NONE
 Sub Action Id (New VLAN Id)     : 0
 Status                          : Active
 Match Count                     : 0

EX2016MP-ACBD00#
EX2016MP-ACBD00#
```

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 **vlan 2** 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 ip 1001** command into the terminal to display the IP access lists. Press the **Enter** key.

Configuring ACL in CLI Interface- Consolidated Mode

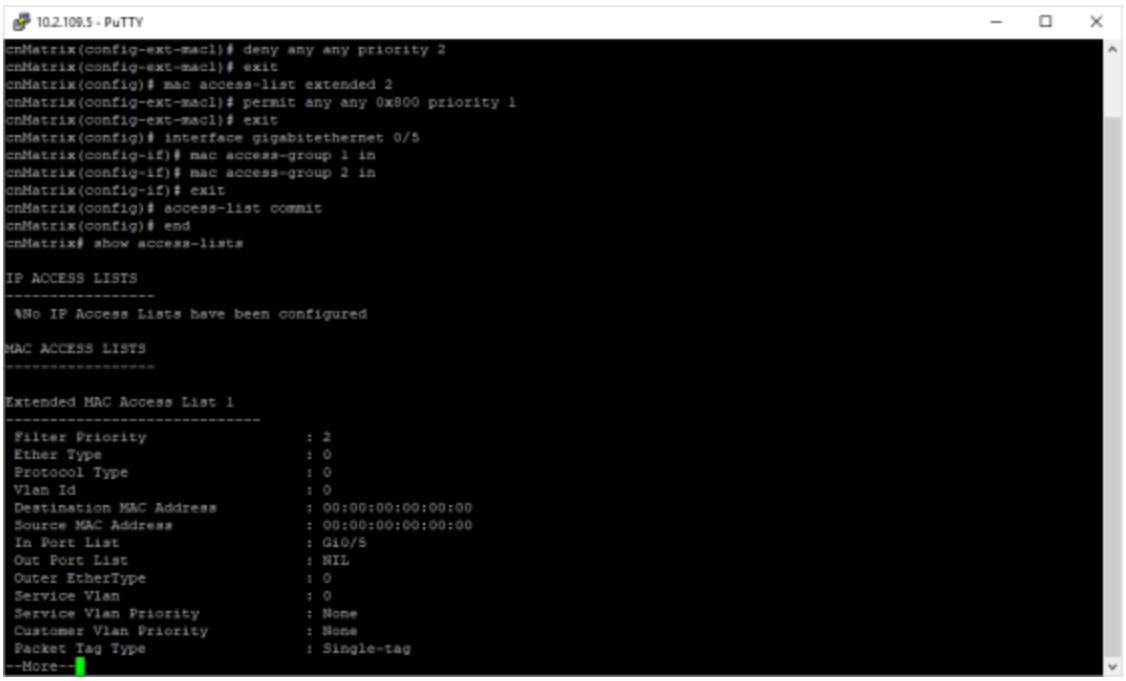


1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **access-list provision mode consolidated** command into the terminal to configure access-list provision mode as consolidated. Press the **Enter** key.
3. Type the **mac access-list extended 1** command into 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 rejected 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 ACL one 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.

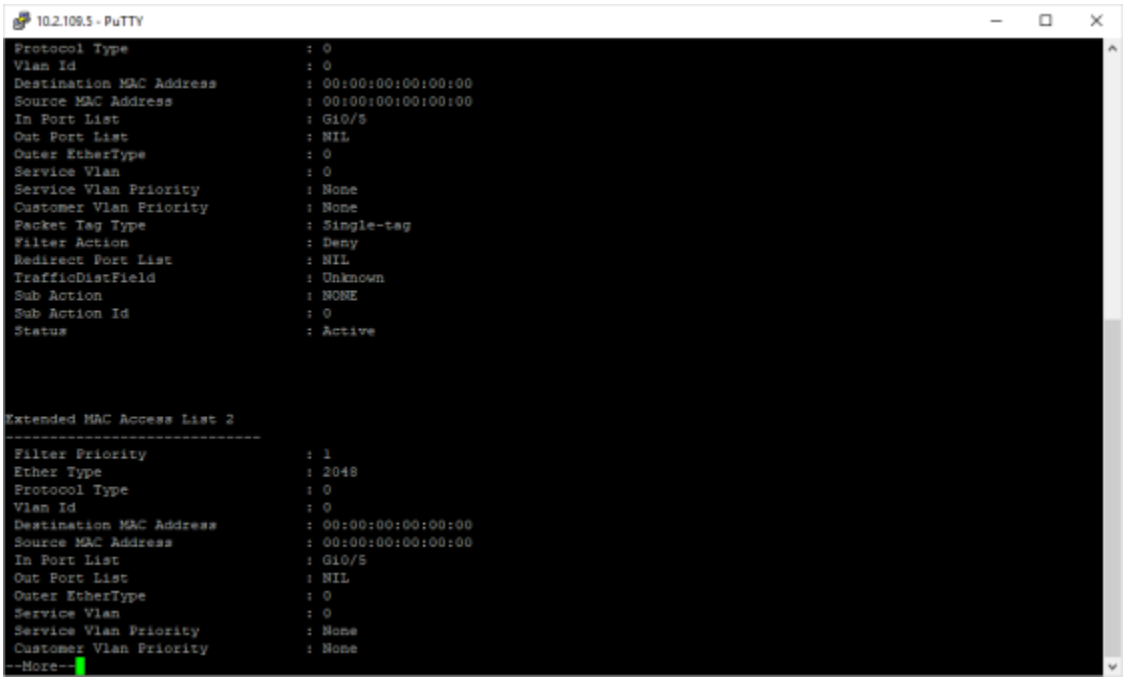
Note

This command is applicable only when the provision mode is consolidated.

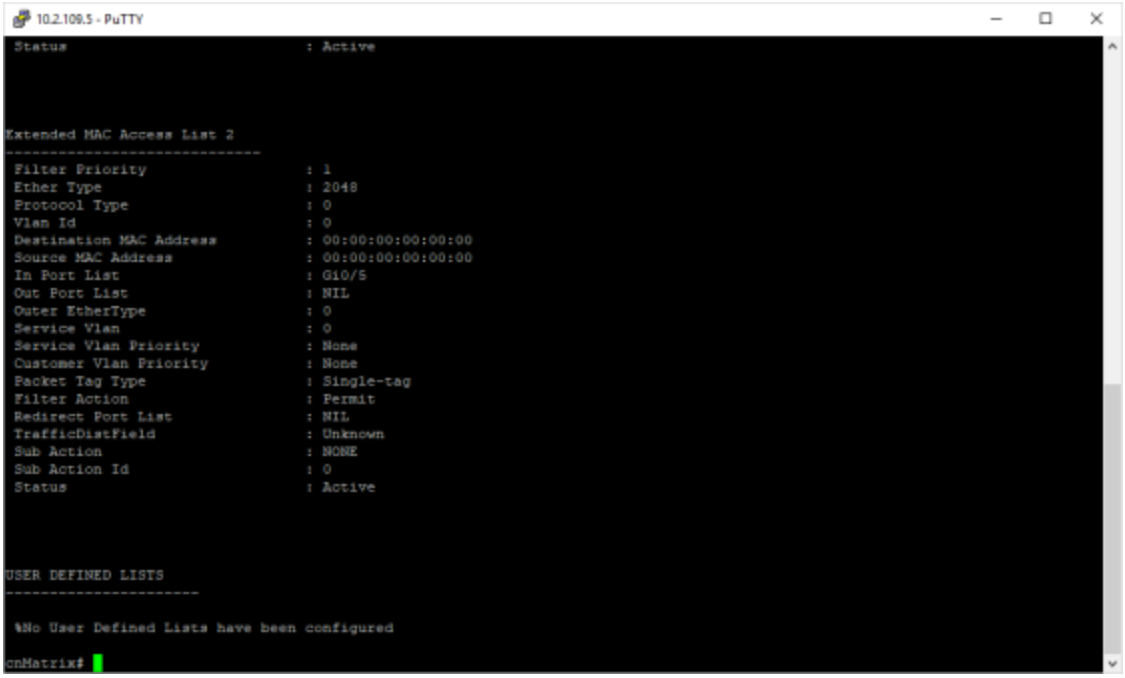
14. Type the **end** into the terminal to go to the Privileged EXEC mode. Press the **Enter** key.
15. Type the **show access-lists** command into the terminal to display IP access lists. Press the **Enter** key.



16. Press the **Enter** key.



17. Press the **Enter** key.



For more information, see ACL Parameters and Commands. Starting with version 2.1, see ACL Parameters and Commands version 2.1.

Troubleshooting access lists

Check if an ACL is active or not:

- Run the command **show access-lists** and identify the desired ACL.
  - Identify the value of the **Status** field.
  - If the value of the **Status** field is **Inactive** then:
    - Identify the value of the **In Port List** and **Out Port List** fields. If both are **NIL**, the ACL is inactive, as it has not been applied on any port.
- Run the command **show access-lists resources**.
  Check if the number of hardware policies reached the maximum. Once the number of hardware policies in use reaches the maximum, new rules will be marked as inactive.

Static MAC

Managing Static MAC

The switch allows the user to configure a **static MAC** address and assign it to a specific VLAN ID and 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 unicast MAC addresses can be configured using this switch.
- A valid entry in the mac-address-table is a MAC or 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.

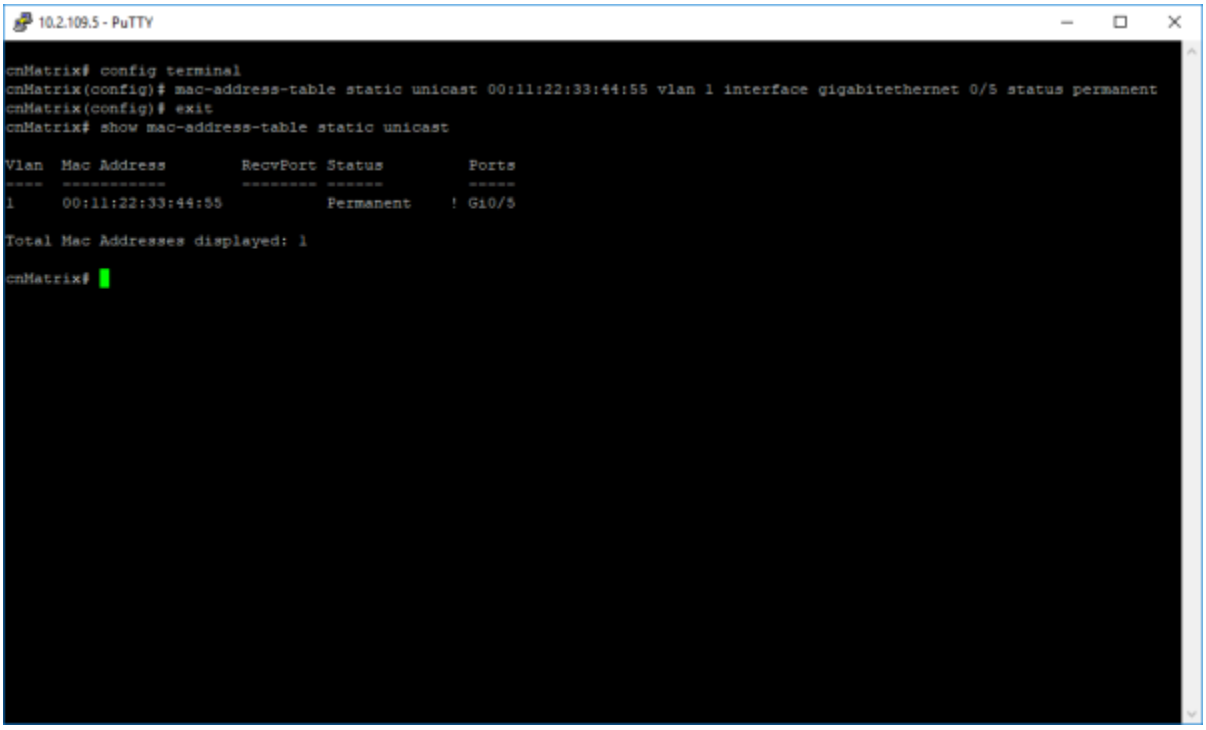
Prerequisites

- 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.

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.

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 static unicast address.
- cnMatrix# show mac-address-table static unicast interface.
- cnMatrix# show mac-address-table count.

Locally Managed Username and Password

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

How to Create Username and Password in CLI Interface

```
cnMatrix# configure terminal
cnMatrix(config)# username user1 secret pa$$w0RD privilege 15
cnMatrix(config)# exit
cnMatrix# listuser

User                    Role(Privilege)
--------------------    ----------------
admin                   administrator(15)
guest                   guest(1)
user1                   administrator(15)

cnMatrix#
```

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, password, 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.

Note:

A role option is presented that can be used instead of specifying a privilege. This maps the role type to a privilege.

```
username <user> password <pass> [ role { guest | tech | admin } |
privilege <1-15> ]
```

Starting with release 3.2-r4 default password usage is no longer supported.

For more information, see Local Management User Name Password Parameters and Commands.

Password encryption service

Feature Overview

This feature encrypts cleartext passwords in the configuration. When enabled, all existing passwords and new passwords will be encrypted. When disabled, existing passwords will remain encrypted, but all new passwords will no longer be encrypted.

```
cnMatrix# configure terminal
cnMatrix(config)# service password-encryption
```

Default Values

Password encryption service is disabled by default.

HTTPS

Managing HTTPS

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.
- 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 1024 or 2048 bits.
- The default crypto pair that can be generated is 2048 bits.

Default Values

- The SSL feature is enabled by default and uses a self-signed certificate. For security, this certificate should be replaced with a CA-signed certificate.
- The default chipersuites are TLS-AES-128-GCM-SHA256, TLS-AES-256-GCM-SHA384, TLS-CHACHA20-POLY1305-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 TLSv1.2 and TLSv1.3.

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 an 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:

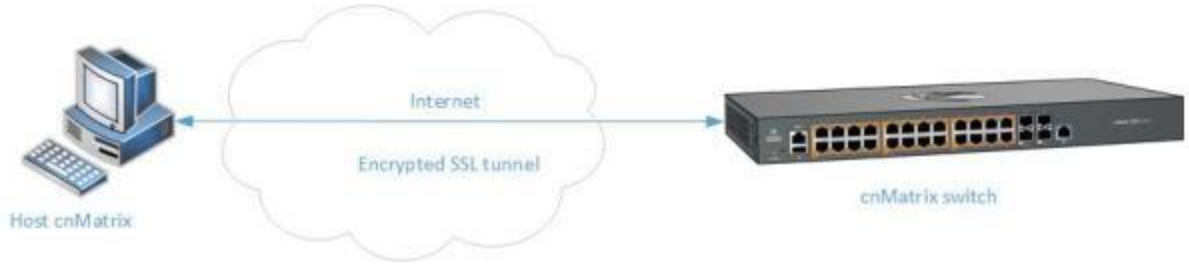
- Google Chrome version 125.
- Mozilla Firefox version 126.
- Microsoft Edge version 125.

The TLS server supports the following:

- Algorithms
- The key encryption algorithm: AES.
- 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:
    - TLS-AES-128-GCM-SHA256
    - TLS-AES-256-GCM-SHA384
    - TLS-CHACHA20-POLY1305-SHA256

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 Website 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.

Network Diagram



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** 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.

How to install a CA-signed certificate

1. In the Privileged EXEC mode, type the **ssl gen cert-req algo rsa sn *<hostname>*** command into the terminal, where *<hostname>* is the hostname you will use to access the switch. This will be used as the common-name in the Certificate Signing Request. Press the **Enter** key.
2. Copy the output from the terminal into a file with **.csr.pem** extension and send this file to your Certificate Authority for signing.
3. Upon receiving the signed certificate from your CA, type the **ssl server-cert** command into the terminal. Press the **Enter** key.
4. The prompt "Enter Cert:" will be displayed in the terminal. Open the signed certificate with a text editor.
5. Concatenate the base 64 text between the BEGIN and END CERTIFICATE markers into a single line.
6. Copy the base 64 text, without the BEGIN and END CERTIFICATE markers and paste it into the terminal. Press the **Enter** key.
7. Type the **show ssl server-cert** command into the terminal to display the HTTPS server certificate. Press the **Enter** key.

Troubleshooting HTTPS

Useful commands for troubleshooting:

- cnMatrix#show ip http secure server
- cnMatrix#debug ssl all
- cnMatrix#show ssl server-cert

HTTP

Managing HTTP

Feature Description

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 Web UI 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 Web UI 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 run-time 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.

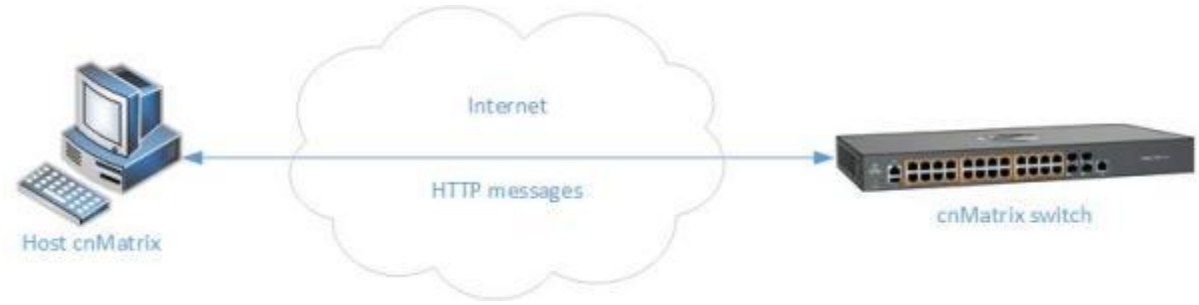
Scaling Numbers

- The HTTP server supports maximum 4 HTTP Web UI sessions opened simultaneously.
- The maximum number of HTTP sessions supported is 10.

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.

Network Diagram



How to Enable HTTP in CLI Interface

```
cnMatrix#
cnMatrix# configure terminal
cnMatrix(config)#
cnMatrix(config)# ip http enable
cnMatrix(config)#
cnMatrix(config)# exit
cnMatrix#
cnMatrix# show http server status

HTTP server status              : Enabled
HTTP port is                    : 80
HTTP Requests In                : 0
HTTP Invalids                   : 0
cnMatrix#
cnMatrix#
```

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.

Troubleshooting HTTP

Useful commands for troubleshooting:

- cnMatrix# show http server status

HTTP or HTTPS client

Feature Description

The HTTP or HTTPS client is used for connecting to cnMaestro management server.

Standards

- HTTP or HTTPS Client is RFC 1945, RFC 4346 and RFC 7230 compliant.

Scaling Numbers

N/A

Limitations

N/A

Default Values

N/A

How to configure HTTP or HTTPS proxy and authentication

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **ip http client proxy-server 192.168.0.10 proxy-port 8080** command into the terminal to configure the proxy server address and port. Press the **Enter** key.
3. Type the **ip http client username myuser** command into the terminal to configure the username. Press the **Enter** key.
4. Type the **ip http client password mypassword** command into the terminal to configure the password. Press the **Enter** key.

Troubleshooting HTTP or HTTPS client

To confirm the configuration of the feature;

- cnMatrix# show running-config

For more information, see troubleshooting cnMaestro.

Max sessions for HTTP or HTTPS

For security reasons, the number of HTTP/HTTPS sessions can be limited. By default, the number of Web sessions is 10.

The http or https sessions can be set using command:

```
cnMatrix(config)# ip http max-sessions <1-10>
```

The number of http(s) sessions are set to default using command:

```
cnMatrix(config)# default ip http max-sessions
```

Note:

If the new value of http(s) max sessions is smaller than the current one, automatically all the sessions will be closed before setting it.

If needed, HTTP or HTTPS authentication can be also disabled:

- Disable http status in the system

  ```
  cnMatrix(config)# ip http disable
  ```

- Disable https status in the system

  ```
  cnMatrix(config)# no ip http secure server
  ```

802.1x Authentication

Managing 802.1x Authentication

The **802.1X** feature enables network device 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 submit 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

Note

The switch has a local authentication server to support local authentication without the RADIUS server.

Standards

- IEEE 802.1X
- RFC 2865

Scaling Numbers

- N/A

Limitations

- N/A

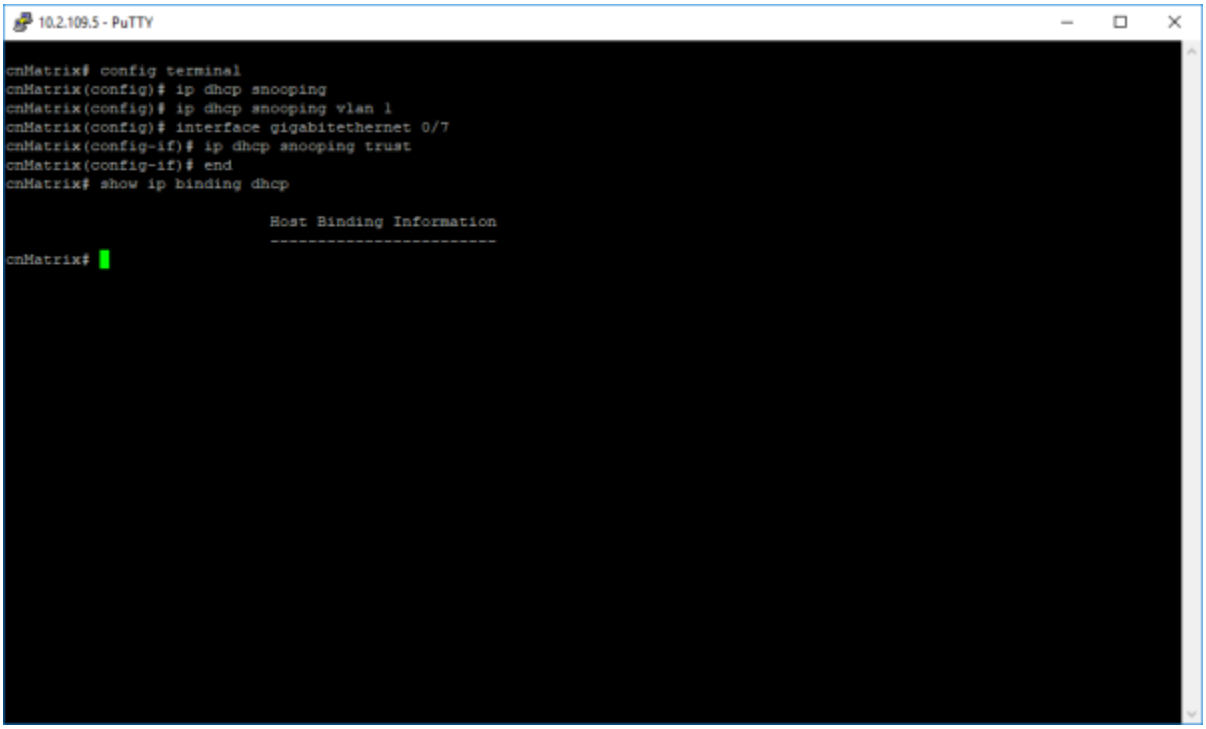
Default Values

- 802.1X is disabled by default.
- 802.1X per-port Authentication Mode is set to Multi-Host by default.
- MAB (MAC Authentication By-Pass) is disabled by default.
- 802.1x is enabled globally by default.
- 802.1x is disabled per-port by default (dot1x port-control force-authorized).
- AAA authentication default users database is local.
- AAA authorization is disabled by default.

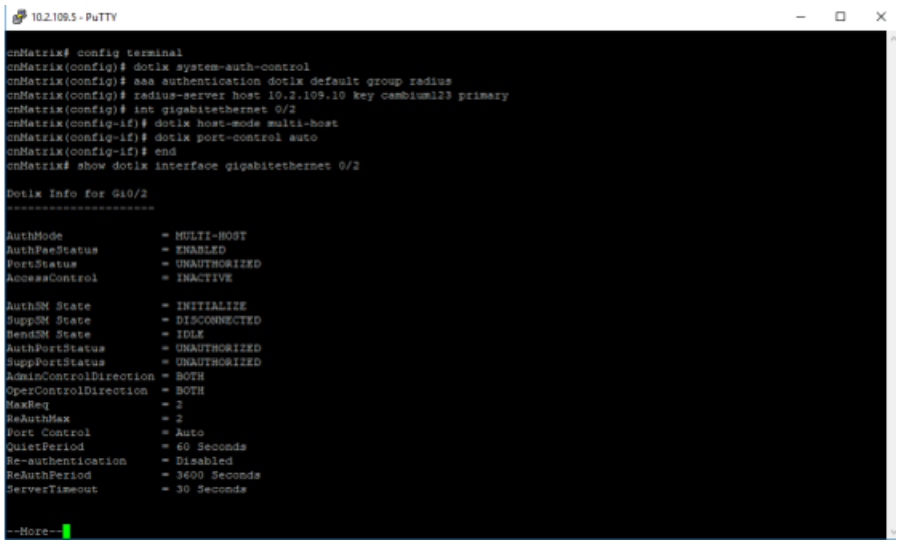
Prerequisites

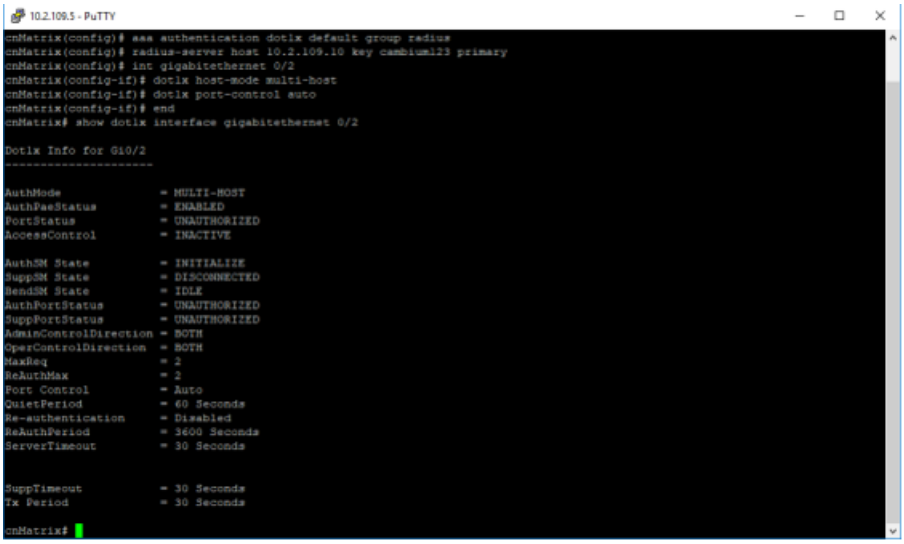
- N/A

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 **aaa authorization network default group radius** command into the terminal to enable the RADIUS authorization method for all ports. Note that only access ports can be authorized – hybrid and trunk ports will ignore radius authorization. Press the **Enter** key. (Starting with release 4.1).
5. 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.
6. Type the **int gigabitethernet 0/2** command into the terminal to select the interface to be configured. Press the **Enter** key.
7. Type the **dot1x host-mode multi-host** command into the terminal to configure port authentication mode. Press the **Enter** key.
8. Type the **dot1x port-control auto** command into the terminal to configure the authentication port control. Press the **Enter** key.
9. Type the **dot1x mac-auth-bypass** command into the terminal to configure the authentication of mac address based clients Press the **Enter** key. (Starting with release 4.1)
10. Type the **dot1x reauthentication** command into the terminal to enable the re-authentication process – default value is 3600 seconds. 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 **dot1x interface gigabitethernet 0/**2 command into the terminal to display the information of the 802.1X authentication for the gi0/2 interface in Multi-Host mode. Press the **Enter** key.
13. Type the show **dot1x mac-info** command into the terminal to display the information of the 802.1X authentication for the Single-Host mode. Press the **Enter** key.
14. Type the show **dot1x** command into the terminal to display the global 802.1x settings. Press the **Enter** key.





For more information, see 802.1x Authentication Parameters and Commands.

IPv6 Neighbor Discovery Router Alert Guard

Managing IPv6 ND RA Guard

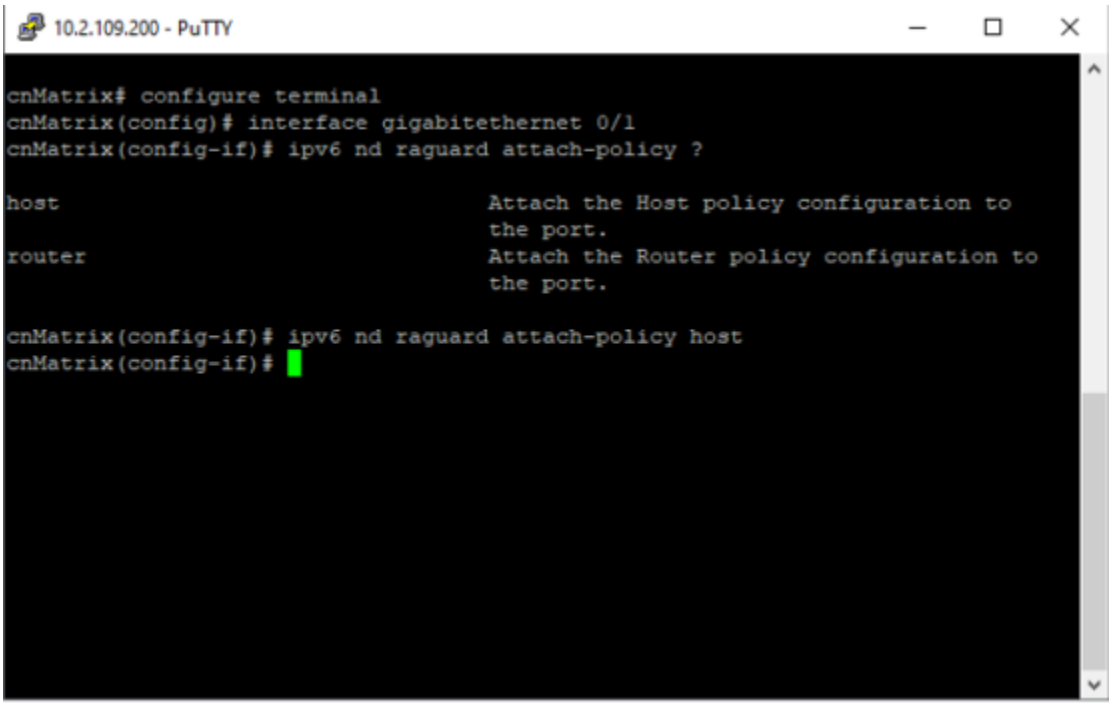
This feature prevents malicious and unwitting IPv6 Neighbor Discovery Router Advertisement packets from entering the network at the edge, so that only specific devices, connected usually to uplink ports can assign IPv6 addresses to other network devices.

This feature can be enabled on a per-port basis. By attaching the **host** policy to a port, the IPv6 ND RA packets received on that port will be dropped at ingress. By attaching the **router** policy, the IPv6 ND RA packets will be allowed on that port.

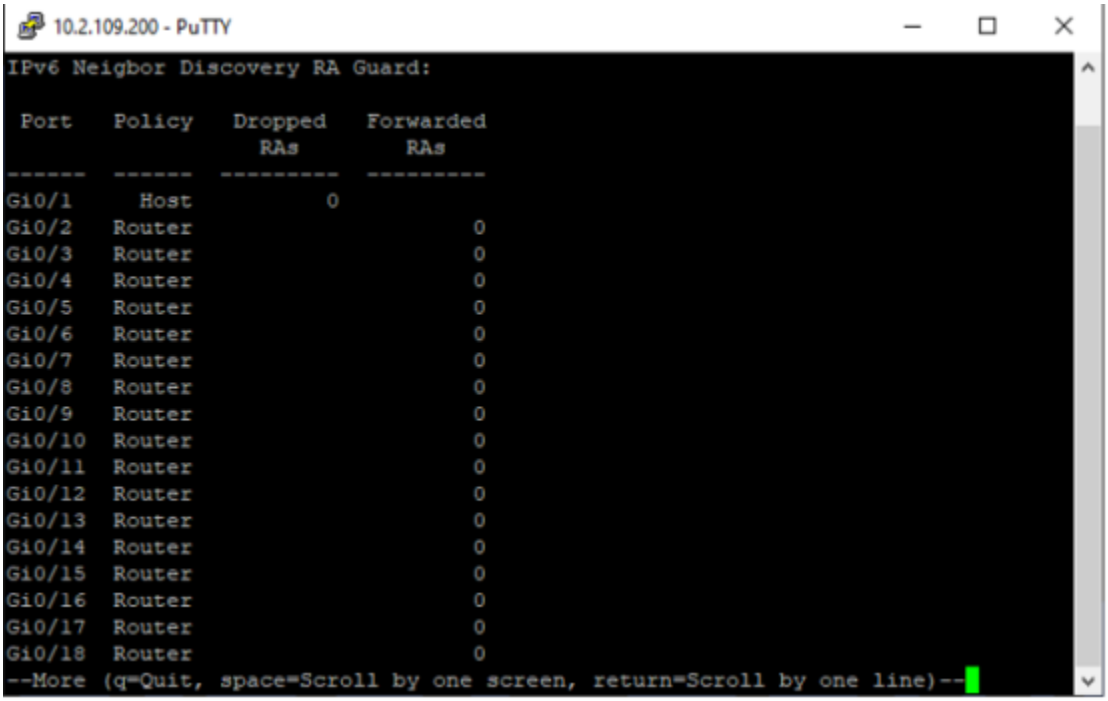
By default, the “router” policy is attached to all ports.

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

3. Type the **ipv6 nd raguard attach-policy host** command into the terminal to attach the “host” policy to the selected 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 ipv6 nd raguard** command into the terminal to display the IPv6 ND RA guard configuration and statistics. Press the **Enter** key.



Troubleshooting IPv6 ND RA Guard

When an IPv6 ND RA Guard **host** policy is attached to an uplink port, it also prevents the switch from obtaining an IPv6 address from the network. This is usually an unwanted behavior. To avoid this problem, please keep a **router** policy attached to uplink ports.

Port MAC Limit

Managing Port MAC Limit

Feature Overview

The Port MAC Limit feature offers the possibility for the switch to restrict the access to the network to a certain number of devices, based on their MAC address. It provides a way of configuring the number of allowed MAC addresses on a per-port basis and a selection of configurable actions to be taken to MAC addresses found in violation. The feature show statistics about the number of violations that occurred.

Note

The Port MAC Limit feature can be configured via CLI, Web, and SNMP.

Attention

Port MAC Limit feature is supported starting with cnMatrix release 4.1.

Standards

N/A

Limitations

N/A

Default Values

- The feature is disabled by default.
- When enabled, the default maximum is set to **1** and the action is set to **protect**.

Configuring and enabling Port MAC Limit - Port Based in CLI Interface (Example)

```
TX2020RP-EC4C40#
TX2020RP-EC4C40# config terminal
TX2020RP-EC4C40(config)# interface gigabitethernet 0/1
TX2020RP-EC4C40(config-if)# switchport port-security maximum 5
TX2020RP-EC4C40(config-if)# switchport port-security violation protect
TX2020RP-EC4C40(config-if)# switchport port-security
TX2020RP-EC4C40(config-if)# end
TX2020RP-EC4C40#
```

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 **switchport port-security maximum 5** command into the terminal to set the maximum number of MAC addresses allowed. Press the **Enter** key.
4. Type the **switchport port-security violation protect** command into the terminal to set the action in case of violation occurs. Press the **Enter** key.
5. Type the **switchport port-security** command into the terminal to enable the feature on that port(interface). Press the **Enter** key.

Note

If the feature is enabled on port without setting the maximum number of MACs or the action, the default maximum is set to **1** and the action is set to **protect**.

Example: cnMatrix(config-if)# switchport port-security

How to disable Port MAC Limit - Port Based in CLI Interface (Example)

```
TX2020RP-EC4C40#
TX2020RP-EC4C40# config terminal
TX2020RP-EC4C40(config)# interface gigabitethernet 0/1
TX2020RP-EC4C40(config-if)# no switchport port-security
TX2020RP-EC4C40(config-if)# end
TX2020RP-EC4C40#
```

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 **no switchport port-security** command into the terminal to disable the feature on that port(interface). Press the **Enter** key.

How to show Port MAC Limit settings

```
TX2020RP-EC4C40# show port-security

Interface  Status    Max-Addr  Action
---------  --------  --------  ---------
Gi0/1      Enabled      5      Protect
Gi0/2      Disabled     1      Protect
Gi0/3      Disabled     1      Protect
Gi0/4      Disabled     1      Protect
Gi0/5      Disabled     1      Protect
Gi0/6      Disabled     1      Protect
Gi0/7      Disabled     1      Protect
Gi0/8      Disabled     1      Protect
Gi0/9      Disabled     1      Protect
Gi0/10     Disabled     1      Protect
Gi0/11     Disabled     1      Protect
Gi0/12     Disabled     1      Protect
Gi0/13     Disabled     1      Protect
Gi0/14     Disabled     1      Protect
Gi0/15     Disabled     1      Protect
Gi0/16     Disabled     1      Protect
Ex0/1      Disabled     1      Protect
Ex0/2      Disabled     1      Protect
Ex0/3      Disabled     1      Protect
Ex0/4      Disabled     1      Protect
TX2020RP-EC4C40#
```

Type the show port-security command into the terminal. Press the **Enter** key.

How to show Port MAC Limit statistics

```
TX2020RP-EC4C40# show port-security statistics

Interface  Status    Max-Addr  Action    Num-Addr   Num-Vio
---------  --------  --------  --------  ---------  -------
Gi0/1      Enabled      5      Protect       5         1349
Gi0/2      Disabled     1      Protect       0         0
Gi0/3      Disabled     1      Protect       0         0
Gi0/4      Disabled     1      Protect       0         0
Gi0/5      Disabled     1      Protect       0         0
Gi0/6      Disabled     1      Protect       0         0
Gi0/7      Disabled     1      Protect       0         0
Gi0/8      Disabled     1      Protect       0         0
Gi0/9      Disabled     1      Protect       0         0
Gi0/10     Disabled     1      Protect       0         0
Gi0/11     Disabled     1      Protect       0         0
Gi0/12     Disabled     1      Protect       0         0
Gi0/13     Disabled     1      Protect       0         0
Gi0/14     Disabled     1      Protect       0         0
Gi0/15     Disabled     1      Protect       0         0
Gi0/16     Disabled     1      Protect       0         0
Ex0/1      Disabled     1      Protect       0         0
Ex0/2      Disabled     1      Protect       0         0
Ex0/3      Disabled     1      Protect       0         0
Ex0/4      Disabled     1      Protect       0         0

Interface  Last-Mac           Last-Violation
---------  -----------------  ------------------
Gi0/1      0a:85:e1:78:0d:c0  2021-07-01 15:04:20
Gi0/2
Gi0/3
Gi0/4
Gi0/5
Gi0/6
Gi0/7
```

Type the show port-security statistics command into the terminal. Press the **Enter** key.

Note

The statistics information also includes the settings information.

Troubleshooting Port MAC Limit

Useful commands for troubleshooting

- cnMatrix# show port-security statistics

WISP Features

This chapter presents new functionality available only on the WISP switches, i.e. the TX2020R-P, TX2012R-P, and the TX2028RF-P.

Power over Ethernet

Note

- For TX2020R-P, ports 1-8 are 4-Pair PoE ports, and ports 9-16 are 2-Pair PoE ports.
- For TX2012R-P, ports 1-4 are 4-Pair PoE ports, and ports 5-8 are 2-Pair PoE ports.
- For TX2028RF-P, ports 1-8 are 4-Pair PoE ports, and ports 9-16 are 2-Pair PoE ports.
- 4-Pair ports support up to 90w (802.3bt Type4/Class8).
- 2-Pair ports support up to 30w (802.3bt Type3/Class4).
- For TX2020R-P the maximum PoE budget is 960W.
- For TX2012R-P the maximum PoE budget is 480W.
- For TX2028-RF-P the maximum PoE budget is 960W.

PoE configurable power modes

Passive 24V mode

Passive 24V mode is a Cambium-specific implementation of passive PoE to function at 24V, as oppose to standard 802.3 PoE which delivers power at 54V. In this mode, no detection or classification is performed. 24V is forced on the port.

Note that the voltage output range from cnMatrix is 22V to 26V.

For this mode, the PoE LED will light up green. For standard 802.3bt mode, the PoE LED will light up amber.

Note

Passive 24V mode is only available on ports 9-16 of TX2020R-P or TX2028RF-P and ports 5-8 of TX2012R-P.

Caution

Passive 24V mode may cause damage to devices since it automatically puts power on the line. Check that a device is compatible with this passive power mode before using it.

Passive 54V mode

Passive 54V is a mode in which no detection and no classification is performed. As the name describes it functions at standard 54V.

For this mode, the PoE LED will light up green. For standard 802.3bt mode, the PoE LED will light up amber.

Note

Passive 54V mode is available on all ports of the WISP switches.

Caution

Passive 54V mode may cause damage to devices since it automatically puts power on the line. Check that a device is compatible with this passive power mode before using it.

Hybrid mode

Hybrid is a mode in which detection is still performed, but the classification is no longer performed. Hence this mode has two major advantages: one, it offers protection by still performing standard 802.3 detection (as oppose to passive PoE modes), and second, it offers the possibility for a device to draw-up as much power as it desires regardless of the advertised class.

For this mode, the PoE LED will light up amber, same as for 802.3 mode, since this mode requires detection and it is not a true passive mode.

Note

Hybrid mode is available on all ports of the WISP switches.

Configuring a power mode (example)

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/3** command. Press the **Enter** key.
3. Type the **power inline mode passive-24V** command into the terminal to configure the power mode to passive 24V on port gi0/3. 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 power inline** command into the terminal to display the per-port PoE information. Press the **Enter** key.

PoE auto-detect mode for cnMedusa (450m) or cnWave (v3000 and v5000)

By default, the cnMedusa or cnWave advertises itself as a Class4 device and so, in 802.3 mode it cannot receive more than 30w of power. With this auto-detect feature, if a cnMedusa or cnWave is detected on a port via LLDP information the power mode on that port will be automatically changed to hybrid so that the cnMedusa or cnWave can draw as much as 90w of power regardless of the class it advertises itself as. By default, this feature is enabled.

Useful information:

- Changing the power mode implies a power-off/power-on on the port. So, once a cnMedusa or cnWave is detected and the power mode is changed successfully, it will reboot and come back online with the new

power mode. After coming back online, the cnMatrix waits for 2 minutes to confirm again that it is a cnMedusa or cnWave via the same LLDP information. The port is kept intentionally powered-off for 12 seconds (PoE LED will be blinking green) to avoid the cnMedusa or cnWave booting-up in SPC mode. All of these events can be followed via logging.

- If the cnMedusa or cnWave is unplugged or if the port is administratively powered-off, cnMatrix will revert the power mode to 802.3 on that port.

Note

This feature requires SW version R20.0.1 on the cnMedusa or cnWave. If the customer uses R16.2.3 or earlier then he must manually set the port in hybrid mode to be able to draw the full 90w.

Note

This feature is only available on the 4-Pair PoE ports which support up to 90w. These are 1-8 on the TX2020R-P or TX2028RF-P and 1-4 on TX2012R-P.

PoE high temperature mode

High temperature is a mode that protects the switch from overheating by reducing the total PoE power budget. This mode is useful when the switch operates in an extreme temperature environment.

The amount by which the PoE budget is reduced depends on the power supply model:

- The PoE budget for the 1200W CRPS is reduced from a maximum of 960W to 700W.
- The PoE budget for the 930W CRPS is reduced from a maximum of 840W to 600W.
- The PoE budget for the 600W CRPS is reduced from 500W to 450W.

Removable power supplies

The TX2020R-P model offers two removable power supplies slots for two reasons: redundancy and flexible power budget requirements.

The TX2012R-P model offers one removable power supply slot for flexible power budget requirements.

The TX2028RF-P model offers one removable power supply slot for flexible power budget requirements.

As long as one power supply remains installed, inserting or removing a power supply will not cause the switch to power down.

The detection of a power supply is installed or removed upon insertion is done automatically and the power budget is adjusted accordingly on the fly.

Table 1: PoE budget based on power supply model

Power Supply	Type (AC/DC)	DC – in Voltage	Available PoE Load
1200W (110V)	AC	NA	900W
1200W (220V)	AC	NA	960W
1200W	DC	48-72V	960W
1200W	DC	36-47V	740W

Power Supply	Type (AC/DC)	DC – in Voltage	Available PoE Load
930W	AC	NA	840W
930W	DC	48-72V	840W
930W	DC	36-47V	740W
600W	AC	NA	500W
600W	DC	48-72V	500W
600W	DC	36-47V	500W

Troubleshooting

- cnMatrix# show power detail
- cnMatrix# show power inline
- cnMatrix# show power inline measurements
- cnMatrix# show system power-supplies

Default Values

- Standard 802.3 mode is the default power mode on all ports.
- PoE auto-detect cnMedusa or cnWave is enabled by default.
- PoE high temperature mode is disabled by default.

Cambium-Sync

Cambium-Sync has two sync sources:

- A built in GPS module, with a connected antenna (internal source).
- A Cambium cnPulse device (external source).

The sync source is inductively coupled and available on any of the Ethernet ports.

Cambium-Sync sources

The two Cambium-Sync sources be selectively enabled/disabled by the user. If, for whatever reason, one of the sync sources is not functioning properly, (GPS module loses signal or cnPulse device becomes defective), Cambium-Sync may become unreliable. This feature is a way to remotely disable either sync source without actually going onsite.

The SYNC LED will be Green if sync is detected from either source or Amber if no sync is detected from both sources.

Configuring Cambium-Sync source (example)

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **no cn-sync source cnpulse** command into the terminal to ignore the cnPulse as sync source. Press the **Enter** key.
3. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the **Enter** key.
4. Type the **show cn-sync** command into the terminal to display the Cambium-Sync information. Press the **Enter** key.

Similarly, type the cn-sync source cnpulse command to enable the cnPulse as sync source.

For the antenna, type [no] cn-sync source antenna for the same results.

Cambium-Sync output per-port

Cambium-Sync can be enabled or disabled on a per-port basis by the user, depending on what ports devices that require sync signal are plugged in.

Configuring Cambium-Sync output (example)

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **interface gigabitethernet 0/3** command. Press the **Enter** key.
3. Type the **cn-sync output** command into the terminal to enable Cambium-Sync on port gi0/3. 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 cn-sync** command into the terminal to display the Cambium-Sync information. Press the **Enter** key.

Similarly, type **no cn-sync output** command to disable Cambium-Sync on a certain port.

Configuring cnPulse power-on or power-off

The power on the cnPulse port is disabled by default for safety reasons since it is passive power and always puts out 5V on the line. To power-on the cnPulse port type the following commands:

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type the **cn-sync cnpulse power** command into the terminal to power-on the cnPulse port. Press the **Enter** key.
3. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the **Enter** key.
4. Type the **show cn-sync** command into the terminal to display the Cambium-Sync information. Press the **Enter** key.

Similarly, type the **no cn-sync cnpulse power** command to power-off the cnPulse port.

Troubleshooting

1. For displaying the current Cambium-Sync configuration:

   cnMatrix# show cn-sync

2. For displaying the GPS statistics for both sync sources:

   cnMatrix# show cn-sync statistics both

3. For power-cycling the sync sources if one of them is not functioning properly:

   cnMatrix# debug cn-sync source cnpulse power-cycle

4. For checking the status of the sync signal:

   cnMatrix# show cn-sync

   In the output of the command find CN-SYNC Signal Status field. Possible states are Sources Disabled (both sync sources are disabled by the user), In-Sync, and Not In-Sync.

Default Values

- Both sync sources are enabled by default.
- Cambium-Sync is disabled on all the ports by default.
- cnPulse port is powered-off by default.

DC-in voltage range

This feature allows the user to specify the input voltage range in which the TX1012-P-DC will be powered-up. This is used internally by the switch to automatically adjust the available power budget. The possibilities are:

- For 9-29V input voltage range the available power budget is 120W.
- For 30-60V input voltage range the available power budget is 170W.

Configuring DC-in voltage range

1. Type the **config terminal** command into the terminal. Press the **Enter** key.
2. Type **power mode DC-in-voltage-range 30-60V** to change the input voltage range to 30-60V.
3. Type the **end** command into the terminal to go back to the Privileged EXEC mode. Press the **Enter** key.
4. Type the **show power detail** command into the terminal to display the DC-in voltage range information. Press the **Enter** key.

Default Values

By default, the TX1012-P-DC starts configured in 9-29V input voltage range, so it will have 120W of available power budget. This setting is persistent across reboots if the user manually saves the configuration or if the auto-save feature is enabled.

Note:

This feature is only applicable to the TX1012-P-DC model.

Regulatory and Compliance

Legal and Regulatory Information

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:

Cambium Networks End User License Agreement

- Open Source Components incorporated in the Hardware and associated notices
- Hardware Warranty
- Limitation of Liability
- Compliance with Safety Standards

Cambium Networks End User License Agreement

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 OR INSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT 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 **Documentatio**n 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, non-exclusive, 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 back-up 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 back-up 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 back-up 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.

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 license 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 license [including the GNU Public license.]

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 damages 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 license 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 license including the GNU Public license.

Open SSH 5.1	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 other 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 licensed 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 CORRECTION.

	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. 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>; 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. 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. 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.

Remaining components of the software are provided under a standard 2-term BSD license 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 (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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) 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.

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. 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 PROVIDE 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!

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.

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.

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:

- 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.

Cambium Networks complies with the European Regulation 2023/988 of 10 May 2023 on General Product Safety. EU Authorized Representative: Cambium Networks Europe B.V., Muiderstraat 1, 1011PZ Amsterdam, Netherlands. Contact Information: GPSR@cambiumnetworks.com.

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

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Installation and User Guides	http://www.cambiumnetworks.com/guides
Technical training	https://learning.cambiumnetworks.com/learn
Support website (enquiries)	https://support.cambiumnetworks.com
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list to contact	http://www.cambiumnetworks.com/contact-us/
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™

www.cambiumnetworks.com