Cambium Networks™

cnMatrix User Guide

Web GUI Configuration v2.1

Table of Contents

1 Getting Started

1.1 Interfaces

1.1.1 WEB

WEB

This section describes the configuration of cnMatrix using the WEB interface.

The WEB can be used to configure, show the configuration, monitor statistics and troubleshoot the switch. You can access the WEB interface by typing the user name and password in the authentication page.

The following tabs are available in the WEB interface:

System Tab

The following menu items are available in the **System** tab:

System Information

General information about the switch is available in this tab, such as Hardware Version, Software Version and System Name. Here you can configure global information such as the System Name, System Time, as well as the System Time and Telnet Server Status.

Field	Description
Hardware Version	Displays the hardware version number of the system.
Firmware Version	Displays the firmware version number of the system.
CNS Software Version	Displays the Cambium networking switch version.
Hardware Part Number	Displays the hardware part number of the system.
Software Serial Number	Displays the software serial number of the system.
Manufacture Date *Starting with version 2.1*	Displays the manufacture date of your cnMatrix switch.
System Description	Displays the model name.
System Name	The name for identifying the device.
System Contact	The contact person details for this managed node.
System Location	The physical location of this node.
Device Up Time	Displays the time from which the device is up.
System Time	The current date and time
Login Authentication Mode	The login authentication mode.
Configuration Save Status	Displays the configuration save status.
Remote Save Status	Displays the remote save status.
Configuration Restore Status	Displays the configuration restoration status.
Last Reload Reason *Starting with version 2.1*	Displays the last reload reason.
Telnet Status	The status of TELNET in the system.

System Resources

System Temperature, CPU and RAM and Flash Memory Usage are available in this tab.

Thresholds can be configured for these values, so that SYSLOG messages can be generated when they are reached.

The following fields are available in the **System Resources** page:

Field	Description
CurrentTemperature(celsius)	The current temperature of the switch in Celsius.
CPU Threshold(%)	The maximum CPU usage of the switch in percentage
Current CPUUsage(%)	Displays the current CPU usage of the switch in percentage.
RAM Threshold(%)	The maximum RAM usage of the switch in percentage.
Current RAMUsage(%)	Displays the current RAM usage of the switch in percentage.
Flash Treshold(%)	The maximum Flash usage of the switch in percentage
Current Flash Usage(%)	Displays the current Flash usage of Switch in percentage.

The following fields are available in the **Fan Details** page:

Field	Description
Fan No	Displays the Fan number in the Switch.
Fan Status	Displays the Fan status in the Switch.

The EX2028-P switch is the only model that has a fan included.

PoE (*Starting with version 2.1*)

The following fields are available in the **Power Supply Status** page:

Field	Description
PoE Global Admin State	Displays the admin state of the PoE feature.
Power Supply Status	Displays he operational status of power supply.
Max Power Supplies	Displays the number of power supplies present on the switch.
Total Power	Displays the maximum available power for PoE use.
Total Power Consumed	Displays the instant PoE power consumption.

The following fields are available in the **PoE Interface** page:

Field	Description
Select	Selects the port for which the configuration needs to be done.
Port	Displays the port number for which the configuration needs to be done.
PoE Admin State	Enables/Disables PoE on the port.
Detection Status	Displays the detection status for the port.
Power Class	Displays the power class of the device powered on the port.
Priority	Sets the priority of the port. Available options: ■ Critical ■ High ■ Low Note: If the maximum power availability is exceeded, the devices will be powered off in the order of the priority
Volt(V)	Displays the instant voltage on the port.
Current(mA)	Displays the instant drawn current on the port.

Power(Watt)	Displays the instant power consumption on the port.

cnMaestro (*Starting with version 2.1*)

The following fields are available in the **cnMaestro** page:

Field	Description
cnMaestro Management	Enables/Disables cnMaestro the ability to manage the switch from cnMaestro.
Static URL	Specifies the URL of the cnMaestro server.
Validate Certificate	Validates the SSL certificate of the cnMaestro server.

Save and Restore

The configuration files can be uploaded or downloaded to/from the switch's Flash memory. Files can also be erased form the Flash using this tab, including the startup config file, or even the entire contents of the Flash memory.

The following fields are available in the **Save Configuration** page:

Field	Description
Save Option	Specifies the save option to be used for the Switch.
Transfer Mode	Specifies the transfer mechanism to save the Switch configurations in the remote system.
Address Type	The IP Address type of the remote system in which the Switch configurationsare to be saved.
IP Address	The IP Address of the remote system in which the Switch configurations are tobe saved.
SFTP User Name	The user name required for saving the Switch configurations to the remotesystem in SFTP mode.
SFTP Password	The password required for saving the Switch configurations on to the remotesystem in SFTP mode.
File Name	The name of the file in which the Switch configurations are to be saved.

The following fields are available in the **Restore Configuration** page:

Field	Description
Restore Option	Specifies whether the Switch configurations have to be restored.

The following fields are available in the **Erase Configuration** page:

Field	Description
Erase Option	Specifies the erase or delete configuration or file.
File Name	The configuration file name to be erased.

Image Download

Starting with version 2.1, the **Image Download** menu item has been renamed to **Software Upgrade.**

A software image upgrade can be performed in this menu item. The switch will connect to a TFTP or SFTP server, will download the specified upgrade file and will program it on the box. A reboot is needed to run the new software.

Field	Description
Upgrade From	The type of server from which the image is to be downloaded. *Starting with version 2.1*, the **USB** option has been added.
Address Type	The IP Address type of the machine from which the image is to be downloaded.

Server IP Address	The IP address of the machine from which the image is to be downloaded.
SFTP User Name	The user name required for downloading the image from SFTP server.
SFTP Password	The password required for downloading the image from SFTP server.
File Name	The name of the image to be downloaded from the remote system.

File Transfer

The custom files can be uploaded or downloaded to/from the switch's Flash memory.

The following fields are available in the **File Upload** page:

Field	Description
Transfer Protocol	The transfer mode for uploading file to the remote system.
Address Type	The transfer mode for uploading file to the remote system.
Server IP Address	IP Address Enter the IP address of the machine to which the file is to be uploaded.
SFTP User Name	The user name required for uploading file in SFTP mode.
Remote File Name	The filename or filename with path to which the local file need to be copied in the remote system.
Source File Name	The filename or filename with path from which the local file need to be copied in the remote.

The following fields are available in the **File Download** page:

Field	Description
Transfer Protocol	The transfer mode for downloading file from the remote system.
Address Type	The IP Address of machine to which the log file is to be downloaded.
Server IP Address	The IP address of the machine to which the file is to be downloaded.
SFTP User Name	The user name required for downloading file in SFTP mode.
SFTP Password	The password, required for downloading the file in SFTP mode
File Name	The name of the file to be downloaded from the remote system.

For more information, see Save/ Restore/Erase/ Download Configurations in WEB Interface.

SNTP

Simple Network Time Protocol can be configured using this tab. SNTP is disabled by default. Configuration options are available for:

- SNTP Scalars Configuration
- SNTP Unicast Table Configuration
- SNTP Broadcast Configuration
- SNTP Multicast Configuration
- SNTP Manycast Configuration

For more information, see SNTP Web Fields.

SSH

Secure Shell can be enabled or disabled via this page. Supported ciphers and HMAC types can be configured. SSH server is enabled by default.

The following fields are available in the **SSH Global Settings** page:

Field	Description

SSH Status	The status of the SSH module
SSH Version Compatibility	The version of the SSH..
SSH Cipher List	The Cipher-List. The cipher list takes values as bit mask.
SSH HMAC List	The hash message authentication code.
Max Packet size	The maximum number of bytes allowed in an SSH transport connection.

SSL

The HTTP Secure Server can be enabled and configured. A SSL certificate can be uploaded, or one can be generated on request.

The following fields are available in the **SSL Global Settings** page:

Field	Description
HTTP Secure Server	The status of the HTTP secure server.
SSL Version	The protocols to configure the SSL version.
HTTP Secure Ciphersuite	The cipher suite from the list for providing the input.

The following fields are available in the **SSL Digital Certificate** page:

Field	Description
Generate CertificateSigning Request	Used to generate certificate based on the RSA key size and common name.
RSA Key Size	The desired Key size.
Common Name	The details of the user requesting for the Digital Certificate.

SNMP

The Simple Network Management Protocol can be configured. The protocol is enabled by default. Configuration options are available for:

- SNMP Community Settings
- SNMP GROUP Settings
- SNMP Group Access Settings
- SNMP Target Address Settings
- SNMP Target Parameter Settings
- SNMP Security Settings
- SNMP Trap Settings
- SNMP Filter Settings
- SNMP Basic Settings

For more information, see SNMP Web Fields.

Attention: "private" and "public" community names must be changed from their defaults. Running SNMP with the default cmmunity names is a major security issue.

Reload (*Starting with version 2.1*)

The following fields are available in the **Reload** page:

Field	Description
Reload Reason	Specifies the reason for reloading.

Reload in	Specifies the remaining time until reboot.
Reload at	Specifies the specific time and date bto reboots the switch.
Last Reload Reason	Displays the reason for the last reload performed on the switch.
Set	Submits the configurations to the switch.

If a delayed boot is already configured on the switch, the **Reload** page will display the delay time in the HH:MM format. In this case, all the input boxes will be greyed out and you will only have the option to cancel the existing delayed boot.

ACL & QoS Tab (*Starting with version 2.1*)

The following menu items are available in the **ACL &QoS** tab:

ACL

The following fields are available in the **MAC ACL Configuration** page:

Field	Description
ACL Number	An extended MAC access list number. This value ranges from 1 to 65535.
Priority	The priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rules.
Action	The action for the incoming packets of the specified access list. The default option is **Permit.**
Source MAC	The source MAC Address for which the access list must be applied. Note: The source and destination MAC addresses must be configured, in order for you to have the acceess list in active status.
Destination MAC	The destination MAC Address for which the access list must be applied.
Ethernet Type	The Ethernet type.
VLAN ID	The VLAN ID for which the access list has to be applied.
Vlan Priority	The priority outbound packets containing the specified VLAN-ID.
Port List (Incoming)	The port list for the incoming ports for which the access list has to be applied.
Port List (Outgoing)	The port list for the outgoing ports for which the access list has to be applied.
Sub-Action	Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
Sub-Action: VLAN ID	The unique identifier for the new VLAN to be assigned to the packet.

The following fields are available in the **IP Standard ACL Configuration** page:

Field	Description
ACL Number	The unique standard access-list number.
Priority	The priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rules.
Action	The action for the incoming packets of the specified access list. The default option is **Permit.**
Source IP Address	The source IP Address for which the access list must be applied.

Subnet Mask	The address mask corresponding to the source IP Address.
Destination IP Address	The destination IP Address for which the access list must be applied.
Subnet Mask	The address mask corresponding to the destination IP Address.
Port List (Incoming)	The incoming port list for which the access lists has to be applied.
Port List (Outgoing)	The outgoing port list for which the access lists has to be applied

The following fields are available in the **IP Extended ACL Configuration** page:

Field	Description
ACL Number	The unique ID for the access list.
Priority	The priority for the filter.
Action	The action for the incoming packets of the specified access list. The default option is **Permit.**
Address Type	The type of IP address prefix. Available options: ■ ipv4 – Sets the type of IP address prefix as IP version 4. ■ ipv6 – Sets the type of IP address prefix as IP version 6.
Source IP Address	The source IP address through which the packets are forwarded.
Subnet Mask	The address mask corresponding to the IP Address.
Destination IP Address	The IP Address for which the access list must be applied.
Subnet Mask	The destination subnet mask address through which the packets are forwarded
Port List (Incoming)	The incoming port range.
Port List (Outgoing)	The outgoing port range.
Protocol	The protocol type for which the packets are permitted when a match is found. The default option is **icmp.** Available options: ■ ICMP – Specifies that the filter will be applied for Internet Control Message Protocol packets. ■ IP – Specifies that the filter will be applied for Internet Protocol packets. ■ TCP – Specifies that the filter will be applied for Transmission Control Protocol packets. ■ UDP – Specifies that the filter will be applied for User Datagram Protocol packets. ■ OSPF– Specifies that the filter will be applied for Open Shortest Path First packets. ■ PIM – Specifies that the filter will be applied for Protocol Independent Multicasting packets. ■ OTHER – Specifies that the filter will be applied for any other protocol packets.
Message Code	The message code to be checked for ICMP (Internet Control Message Protocol) Packets.
Message Type	The message type to be checked for ICMP Packets.
Dscp	The Differentiated Services Code Point value to be checked against the packet.

	Note: If the **ICMP** option is selected in the **Protocol** field, this field will be greyed out.
TOS	The TOS value to be matched against the packets. Available options: ■ None - Specifies that the TOS value is not matched. ■ High Reliability - Matches the protocol packets having TOS field set as high reliability. ■ High Throughput - Matches the protocol packets having TOS field set as high throughput. ■ High Reliability and High Throughput - Matches the protocol packets having TOS field set either as high reliability or high throughput. ■ Low Delay - Matches the protocol packets having TOS field set as low delay. ■ Low Delay and High Reliability - Matches the protocol packets having TOS field set either as low delay or high reliability. ■ Low Delay High Throughput - Matches the protocol packets having TOS field set either as low delay or high throughput. ■ Low Delay High Throughput and High Reliability - Matches the protocol packets having TOS field set either as low delay or high reliability or high throughput. Note: If the **ICMP** option is selected in the **Protocol** field, this field will be greyed out.
ACK Bit	Indicates the TCP Ack Bit to be checked against the incoming packet. The default value is **Any.** Available options: ■ Establish - Specifies that ACK Bit is set as Establish. ■ Not Establish - Specifies that ACK Bit as set as Not Establish. ■ Any - Specifies that ACK Bit is not considered and can take any value. Note: This field is enabled and can be configured only if **Protocol** is set as **TCP.**
RST Bit	Indicates the TCP Reset Bit to be checked against the incoming packet. Available options: ■ Set - Specifies that RST Bit is Set. ■ Not Set - Specifies that RST Bit is not Set. ■ Any - Specifies that RST Bit is not considered and can take any value. Note: This field is enabled and can be configured only if **Protocol** is set as **TCP.**
Source Port	The TCP/UDP (User Datagram Protocol) source port from which the access list has to be applied.
Destination Port	The TCP/UDP destination port from which the access list has to be applied.
Destination Prefix Lenght	The length of the CIDR (Classless Inter Domain Routing) prefix carried in the destination IP address.
Source Prefix Lenght	The length of the CIDR prefix carried in the source IP address.
Flow ID	The flow identifier in an IPv6 header.
Sub-Action	Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
SubAction-ID (VLAN-ID)	The unique identifier for the new VLAN to be assigned to the packet.

The following fields are available in the **Provision Mode** page:

Field	Description
ACL Provisioning Mode	The commit support for which the access control rule needs to be applied. The default option is **Immediate**. Available options: ■ Immediate – Applies the rules directly. ■ Consolidated - Applies the rules after the commit is issued.
Commit ACLs Now	The commit action to be taken for the access list. The default option is **False**. Available options: ■ False - Does not set the commit action. ■ True - Sets the commit action.

For more information about additional menu items in the **ACL &QoS** tab, see QoS WEB Fields.

Layer2 Management Tab

The following menu items are available in the **Layer 2 Management** tab:

Port Manager

The Port Interfaces can be administratively enabled or disabled. Port settings such as speed, duplex, auto-negotiation mode can be viewed and configured here.

The following fields are available in the **Port Basic Settings** page:

Field	Description
Select	The port for which the configuration needs to be done.
Port	Displays the port, which is a combination of interface type and interface ID.
Link Status	Displays the status of the link using graphics.
Administrative State	The desired state of the port.
Default User Priority	The default ingress user priority for the port.
Switch Port Mode	The mode of operation for the switch port.
MTU	The maximum transmission unit frame size MTU for the interface.
Link Up/Down Trap	Select whether the linkUp / linkDown trap should be generated for the interface.
Port Type	The port type to operate the port as an L2 port or as an L3 port.
MAC Address	The unicast MAC address of the interface.
Description *Starting with version 2.0.5*	Free flow text entry box to store port description.

The following fields are available in the **Port Control** page:

Field	Description
Select Port	The port for which the configuration needs to be done. Port Displays the port, which is a combination of interface type and interface ID.
Mode	The mode of negotiation for the port.

Duplex	The duplex mode that represents the flow of data through the port.
Speed	The speed of the interface.
FlowControl Admin Status	The default administrative PAUSE mode for the interface.
FlowControl Oper Status	Displays the PAUSE mode currently used in the interface.
HOL-Block Prevention	Select whether the Head-Of-Line (HOL) blocking should be prevented on a port.
Pause High Water Mark (kbps)	The ingress rate equal to or above which PAUSE frames are transmitted.
Pause Low Water Mark (kbps)	The ingress rate below which transmission of PAUSE frames are stopped.
Auto MDI/MDIX Capability *Starting with version 2.1*, the **Auto MDI/MDIX Capability** field has been removed.	The Auto - MDIX mode for the interface.
Description *Starting with version 2.0.5*	Displays port description.

VLAN

The VLAN interfaces can be created and removed. Per-port VLAN settings such as PVIDm Ingress/Egress VLAN TPIDs can also be configured. You can decide on a per-port basis which frame type the port should accept: **All, Tagged or UnTagged**, depending on the role the port has in the network. VLAN Port configurations includes:

- VLAN Basic Settings
- VLAN Port Settings
- Static VLAN Configuration
- VLAN Protocol Group Settings
- Port VLAN Protocol Settings
- FDB Flush

For more information, see VLAN Web Fields.

Protocol VLANs are also supported in the Layer2 Management Tab.

MSTP, PVRST and RSTP

The respective spanning tree protocols can be configured. RSTP is enabled by default. To enable a different spanning tree protocol, configure “System Control” for the other two as “Shutdown”, and for the desired one as “Start”. MSTP, PVRST and RSTP configuration options include:

- Global Configuration
- Instance Bridge Configuration
- Instance Port Configurations
- Instance Port Status

For more information see MSTP Web Fields, RSTP Web Fields, PVRST Web Fields.

Link Aggregation

The LACP protocol on the switch can be configured: you can create or destroy Aggregators and configure LACP-related settings on a per-port or per-LAG basis. Load balancing mode can also be configured here.

To configure an aggregator, first configure a “Port Channel ID” as UP, then assign ports to it in the “Port Channels Settings” page (gi0/1, gi0/2, etc.) and choose a mode (LACP or manual). In the port group page you can configure the per-port LACP settings such as Timeout and LACP mode (Active or Passive). Link Aggregation configuration options include:

- LA Basic Settings
- PortChannel Interface Basic Settings
- LA Port Channel Settings
- LA Port Settings
- LA Port StateMachine Information

For more information ,see Link Aggregation Web Fields.

LLDP

Link-Layer Discovery protocol is globally enabled by default and set to transmit/receive frames on all ports. Various global timers can be configured. Transmitting and receiving LLDPDUs are configurable on a per-port basis. LLDP Configuration options include:

- LLDP Global Configuration
- LLDP Basic Settings
- Interface Settings
- Neighbor Information

For more information, see LLDP Web Fields.

Mirroring *(Starting with version 2.1)*

The **Mirroring** feature is enabled by default and it has been added on the switch to send a copy of network packets available on one switch port (or anentire VLAN) to a network monitoring connection on another switch port or local sniffer device.

The following fields are available in the **Mirroring Control Settings** page:

Field	Description
Session Index	The index of the mirroring session. This value ranges from 1 to 7.
Mirror Type	The type of mirroring that the session supports. The default option is **None.** Available options: ■ **Port** ■ **MAC ACL** ■ **VLAN** ■ **IP ACL**
Source Entity	The source ID which participates in a mirroring session. Note: This field is not available if you selected the **VLAN** option in the **Mirror Type** field.
Destination Entity	The destination port ID from which the packets will be transmitted.
Mirror Mode	The mode of mirroring. The default option is **Both.** **Available options:** ■ Ingress - Mirrors only traffic that is ingressing on the source ports. ■ Egress - Mirrors only traffic that is egressing on the source ports. ■ Both - Mirrors both traffic that is ingressing on the source ports and

	egressing out of source ports. Note: If you selected the **VLAN** option in the **Mirror Type** field, you will have available only the **Ingress** option.
VLAN	The VLAN identifier from which the packets will be transmitted. Note: This field is available only if you selected the **VLAN** option in the **Mirror Type** field.

Dynamic ARP Inspection *(Starting with version 2.1)*

The **Dynamic ARP Inspection** feature is disabled by default on all VLANs. The **DAI** feature has been added in the WEB interface so that the ARP response packets can be validated in the network. Without Dynamic ARP Inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet.

The following fields are available in the **Per-VLAN DAI Status** page:

Field	Description
Select	Selects the VLAN ID for which the configuration needs to be done.
VLAN ID	The VLAN ID for which the configuration needs to be done.
Dynamic ARP Inspection Status	Enables/Disables Dynamic ARP Inspection.

The following fields are available in the **DAI Trust State** page:

Field	Description
Select	Selects the port for which the configuration needs to be done.
Port	Displays the port, which is a combination of interface type and interfaceID.
Link Status	Displays the status of the link using graphics
Administrative State	The desired state of the port.
Trust State	Configures the DAI trust state of the interface.
Description	Displays port description.

The following fields are available in the **Per-VLAN DAI Statistics** page:

Field	Description
VLAN ID	Selects the VLAN ID for which the configuration needs to be done.
Get stats (button)	Get the DAI statistics per-VLAN
Clear stats (button)	Clear the DAI statistics per-VLAN

Layer3 Management Tab

The following menu items are available in the **Layer 3 Management** tab:

IP

IP interfaces can be configured on VLANs. The “Get IP Address Mode” can be configured either as “manual” or “DHCP” for each interface.

The following fields are available in the **VLAN Interface Basic Settings** page:

Field	Description
VLAN Interface	The VLAN/VFI Id for the Interface to be created. The value ranges from 1 to 65535.

Admin State	The Admin Status of the VLAN interface. The default option is Down.
IPv4 Enabled State	The status of IPv4 on the interface. The default option is UP.
Proxy ARP	The Proxy ARP admin status for the interface. The default option is Disabled.
MTU	The Maximum Transmission Unit (MTU). The MTU for the interface as shown to the higher interface sub-layer (this value should not include the encapsulation or header added by the interface).

LLDP additional configuration options include:

- IPv4 Interface Settings
- IP Route Configuration
- IP Information
- ARP ENTRY

For more information, see IP Web Fields.

IPv6

The IPv6 Interface can be configured using this option. Before configuring the IPv6 interface, first you have to create a VLAN IP interface in the VLAN Interface Basic Settings page.

The following fields are available in the **Address Settings** page:

Field	Description
Interface	The index, which uniquely identifies the IPv6 interface on which the IPv6 address entry exists from the list already configured in the system.
Address	The IPv6 address to which the entry's addressing information pertains.
Prefix Length	The length of the prefix (in bits) associated with the entry's IPv6 address.
Address Type	The type of address. The default option is Unicast.
Address Profile ID	The index for the IPv6 Address Profile Table.

DHCP Server

The switch can run a DHCP server application that will offer IP addresses to DHCP clients.

To offer this service to a network, first create an IP interface on a VLAN by using the **VLAN Interface Basic Settings** page, then create a DHCP pool on the same subnet as the configured VLAN IP interface.

The following fields are available in the **DHCP Basic Settings** page:

Field	Description
DHCP Server	The DHCP server status in the router. The default option is Disabled.
Blocked IP Address Reuse Timer (seconds)	The reuse timeout value used by DHCP in seconds.
ICMP Echo	The status of ICMP (Internet Control Message Protocol) Echo feature for the DHCP server.

Various DHCP options can be configured for each pool in the **DHCP Pool Option Settings** page or for any particular host in the **DHCP Host Option** page. A specific hosts identified by its MAC address can be associated to a specific IP address in a pool in the **DHCP Host IP Settings** page.

For more on these additional options, see DHCP Server Web Fields.

DHCP Relay

DHCP Relay agent is used to forward the DHCP packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information like the network in which the packet is removed and then forwards it to the server. The server identifies the client's network from this information and allocates IP

accordingly, then sends the reply to the relay. The relay strips the information inserted and broadcasts the packets into the client's network.

The following fields are available in the **DHCP Relay Configuration** page:

Field	Description
DHCP Relay Service	The Service DHCP relay status in the switch. The default option is Disabled.
IP DHCP Relay Information Option	The controlling status of the processing related to the Relay Agent Information options.
DHCP Server Address	The IP address of the DHCP Server to which the Relay Agent needs to forward the packets from the client. A maximum of 5 servers can be configured.

For more on additional options, see DHCP Relay Web Fields.

DHCP Client

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

The following fields are available in the **DHCP Option Type Settings** page:

Field	Description
Interface Name	Used to select an interface for which DHCP option type settings to be configured from the list of vlan interfaces already created in the system.
Option Type	The DHCP Client Option Type for the specified interface created in the system.
Option Code	Displays the Option code for the specified interface created in the system.
Option Value	Enter a value to identify the octets of data, of length specified by length for that entry. This value will be taken from DHCP ACK message which is sent from server to client.

The following fields are available in the **DHCP Client Identifier Settings** page:

Field	Description
Interface Name	Used to select an interface for which DHCP option type settings to be configured from the list of vlan interfaces already created in the system.
Client Identifier	The unique identifier of DHCP client for the specified interface created in the system

RIP *(Starting with version 2.1)*

RIP sends routing-update messages at regular intervals and when the network topology changes.

The following fields are available in the **RIP Global Configuration** page:

Field	Description
Select	Enables/Disables the RIP Admin Status.
Auto-summary status	Enables/Disables auto summarization option in RIP.

For more information, see RIP Web Fields.

OSPF *(Starting with version 2.1)*

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System.

The following fields are available in the **OSPF Basic Settings** page:

Field	Description
Select	Select the Context Name for which the configuration needs to be modified or deleted.
Admin Status	Enables/Disables the OSPF feature.
Router ID	Enter a 32-bit integer uniquely identifies the originating router in the Autonomous System.
Autonomous System	The status of an ASBR (AS Border Router).
RFC 1583 Compatibility	The compatibility status of RFC 1583.
NSSA ASBR-Default-Route	The status of the P-Bit setting for the default Type-7 LSA (Link State Advertisement) generated by NSSA internal ASBR.
ABR-type	The type of ABRs supported. The default option is Standard.
Distance	The administrative distance (the metric to reach destination) of the routing protocol. The value tange: 1 to 255.
Default-Information	The default information that will be used for OSPF Basic Settings configurations.
SPF Delay	The interval by which the SPF calculation is delayed after a topology change reception.
SPF Hold Time	The minimum time between two consecutive SPF calculations.
Trace-Level	The level of trace required for OSPF.

For more information, see OSPF WEB Fields.

Router Redistribution (Starting with version 2.1)

The **Router Redistribution** feature enables the user to configure the redistribution of the routes that are learnt through other routing protocols to OSPF and RIP.

The following fields are available in the **Router Redistribution RIP Configuration** page:

Field	Description
RIP Status	Used to select the route redistribution status for RIP. The default value: Disabled.
Default Metric	The default metric for the imported routes.
Import Routes	Used to select the protocol from which the routes are to be imported to RIP.
Route Tag Type	Used to select whether the tag is manually configured or automatically generated.
Route Tag	Router tag. Note: This field is mandatory only for manual route type.

The following fields are available in the **Router Redistribution OSPF Configuration** page:

Field	Description
OSPF Status	Used to select the route redistribution status for OSPF.
Import Routes	The source protocols from which the direct/static/OSPF routes are

	imported into OSPF.
Metric Value	Sets the metric type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain.
Metric Type	The metric type applied to the route before it is advertised into the OSPF domain.

DHCPv6-Client

DHCPv6 client is a node that initiates requests on a link to obtain configuration parameters, such as the list of available DNS (Domain Name Server) servers, from DHCPv6 servers. It transmits and receives DHCP messages using link-local address or addresses determined through other mechanisms.

The following fields are available in the **DHCPv6 Client Basic Settings** page:

Field	Description
Trap Administrative Control	Specifies the transmission status of SNMP TRAP notification messages for the DHCPv6 client. The default option is None.
Source Port	The UDP (User Datagram Protocol) listen port number to be provided in UDP header of the information-request message. The default value is 546.
Destination Port	Specifies the UDP destination port number to be provided in UDP header of the information-request message. The default value is 547.

The following fields are available in the **DHCPv6 Client Interface Configuration** page:

Field	Description
Interface	Used to select the interface index of the entry in DHCPv6 Client Counter Interface table from the list which are already configured.

Multicast Tab

The following menu items are available in the **Multicast** tab:

IGMP Snooping

You can enable IGMP snooping globally, and then you can enable it on any existing VLAN. Per-VLAN settings include “Operating Version”, “Querier Status”, and various timers. Router Ports can also be configured in this tab including:

- IGMP Snooping Configuration
- IGMP Snooping Timer Configuration
- IGMP Snooping Vlan Configuration
- IGMP Snooping Interface Configuration
- IGMP Snooping Vlan Router Port Configuration
- IGMP Snooping VLAN Router Ports
- IP Based Multicast Forwarding Table

For more information, see IGMP Snooping Web Fields.

TAC

Transmission and Admission Control module allows the network administrator to filter IGMP reports based on their group or source IP addresses. Filtered groups are not registered on the switch.

The following fields are available in the **TAC Profile Configuration** page:

Field	Description
Profile ID	The unique identifier for a multicast profile entry.

The following fields are available in the **TAC Profile Filter Configuration** page:

Field	Description
Profile ID	The unique identifier for each multicast profile entry.
Group Start Address	The multicast group address, which is the start of multicast group address range.
Group End Address	The multicast group address, which is the end of multicast group address range.
Source Start Address	The multicast source address, which is the start of multicast group address range.
Source End Address	The multicast source address, which is the end of multicast group address.

RMON Tab

The following menu items are available in the **RMON** tab:

RMON

You can configure various alarms that are triggered when certain SNMP object values reach a threshold.

The following fields are available in the **RMON Basic Settings** page:

Field	Description
RMON Status	The status of RMON on the switch.

Additional configuration options include:

- RMON Alarm Configuration.
- Ethernet Statistics Configuration.
- Event Configuration.
- History Control Configuration.

For more information, see RMON Web Fields

Policy Based Automation Tab

The following menu items are available in the **Policy Based Automation** tab:

In the **Auto Attach Basic Settings** page, you can control global Auto-Attach settings, such as:

- Enabling/disabling the feature in the **Auto Attach Global Status** field.
- Setting the string comparison mode in the **String Comparison** field .

In the **Auto Attach Interface Settings** page, the current state of the Auto Attach feature on all system ports is displayed.

In the **Auto Attach Rule Settings** page, you can define new Auto Attach rules or delete rules that are not referenced by an Auto Attach policy.

In the **Auto Attach Action Settings** page, you can define Auto Attach Actions or delete existing actions.

In the **Auto Attach Policy Settings** page, you can define Auto Attach policies or delete existing policies that are not currently active.

In the **Auto Attach Script Settings** page, you can define Auto Attach scripts or delete existing scripts that are not currently active

The following fields are available in the **Auto Attach Basic Settings** page:

Field	Description
Auto Attach Global Status	The global status of the Auto Attach feature.
String Comparison	The string comparison method used fior device identification.

The following fields are displayed in the **Auto Attach Interface Settings** page:

Field	Description
Select	Select the port for which the Auto Attach parameters will be configured.
Port	Displays the port, which is a combination of interface type and interface ID.
Administrative State	Enables/Disables the administrative state of the port.
Message Authentication Status	Controls the current Auto Attach message authentication status for the associated interface.
Policies Applied	Displays the number of times a policy has been applied to the port.
Policies Expired	Displays the number of times a policy has expired on the port.
Policy Errors	Displays the number of times an error has been detected during application/expiration on the port.
Active Policy	The name of the policy specification that is currently applied to the port.
Description *Starting with version 2.0.5*	Displays port description.

The following fields are displayed in the **Auto Attach Rule Settings** page:

Field	Description
Rule Name	The name for the rule specification.
Rule Type	The Auto Attach rule type to determine how a device is identified using data associated with the device.
Device Data	The Auto Attach device data to specify the data that is used to identify a device.

The following fields are displayed in the **Auto Attach Action Settings** page:

Field	Description
Action Name	The name for the action specification.
VLAN Data	VLAN IDs to be associated with an interface.
Native VLAN	The native VLAN ID for an interface.
Switch Port Mode	The port mode for an interface.

The following fields are displayed in the **Auto Attach Policy Settings** page:

Field	Description
Policy Name	The name for the policy specification.

Status	Select the status of the policy to be applied.
Precedence	Enter the precedence value. Note: A policy with a lower precendence value is applied before a policy with a higher value.
Rule Name	The name of the rule specification that is referenced by the policy.
Rule Type	Select he rule type to determine how a device is associated with the device (e.g. using exported LLDP TLV data).
Rule Device Data	Specifies the data used to identify a device (depends on the associated rule type).
Action Name	The name of the action specification that is referenced by the policy.
Action VLAN Data	Specifies the VLAN IDs (maximum 20) to be associated with an interface.
Action Native VLAN	The native VLAN ID for an interface.
Action Switch Port Mode	The switch port mode for an interface.

The following fields are displayed in the **Auto Attach Script Settings** page:

Field	Description
Cambium Device Name	The Cambium product name used by Auto Attach feature to set up automatic device detection rules. Note: Only **cnPilot** Cambium product is currently supported.
VLAN Data	VLAN IDs to be associated with an interface.
Native VLAN	The native VLAN ID for an interface.

Clock Tab

The following menu items are available in the **Clock** tab:

Clock Interactions

This option enables you to set the time source of the system clock and maintains the information about the clock quality such as clock accuracy, class, and variance.

The following fields are available in the **Clock Interaction Settings** page:

Field	Description
Clock Variance	The variance of the primary clock. This object reflects the value provisioned by the external source (NTP/SNTP) that synchronizes the system clock.
Clock Class	The class of the primary clock. This object reflects the value provisioned by the external source (NTP/SNTP) that synchronizes the system clock.
Clock Accuracy	The accuracy of the primary clock. Clock accuracy is the mean of the time or frequency error between the clock under test and a perfect reference clock, over an ensemble of measurements.
Clock Time Source	The time source of the primary clock. The system clock is synchronized only through the specified source. Note: Only the NTP option is supported.
Clock UTC Offset	The current UTC (Coordinated Universal Time) offset in scaled nanoseconds with respect to the system time.
Hold Over Mode	The option to specify whether the system clock is in Hold Over Mode.

Statistics Tab

The statistics for various applications are displayed.

1.1.2 cnMaestro

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

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

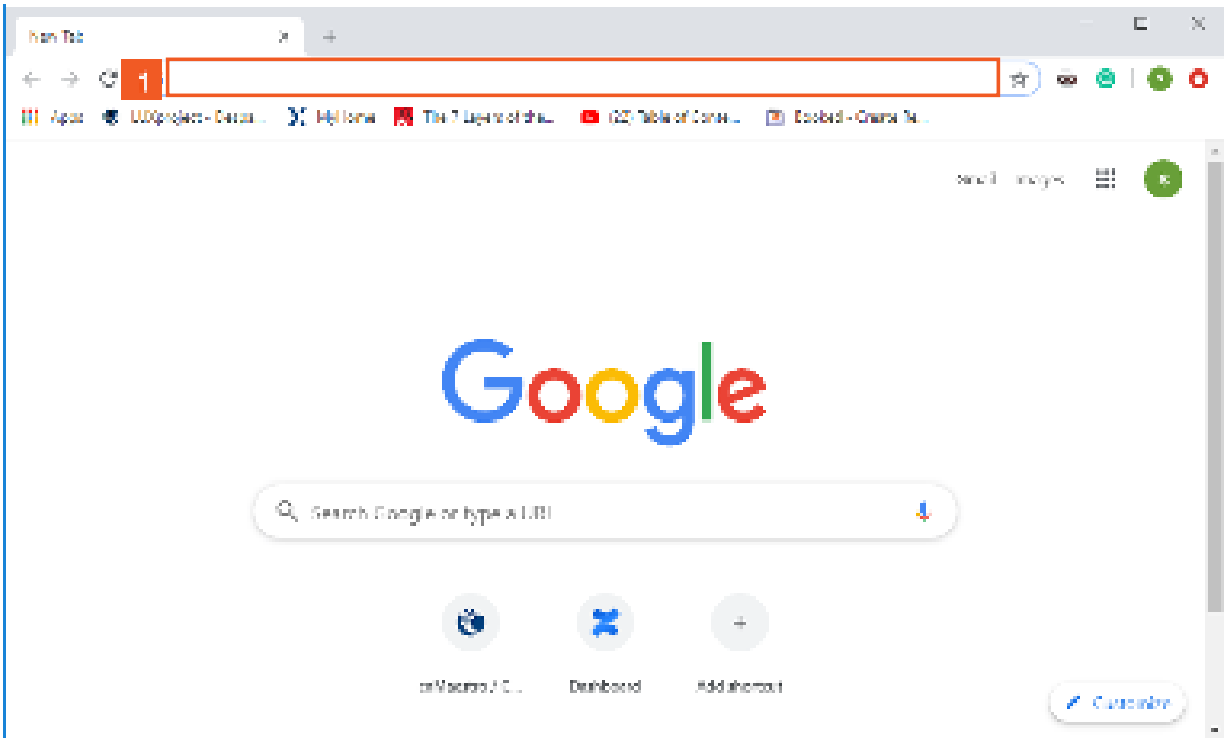
Starting with 2.0.3, cnMaestro Cloud supports cnMatrix devices with minimum 2.0.3-r4 build. You should manually upgrade your cnMatrix switch to version 2.0.3–r4.

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

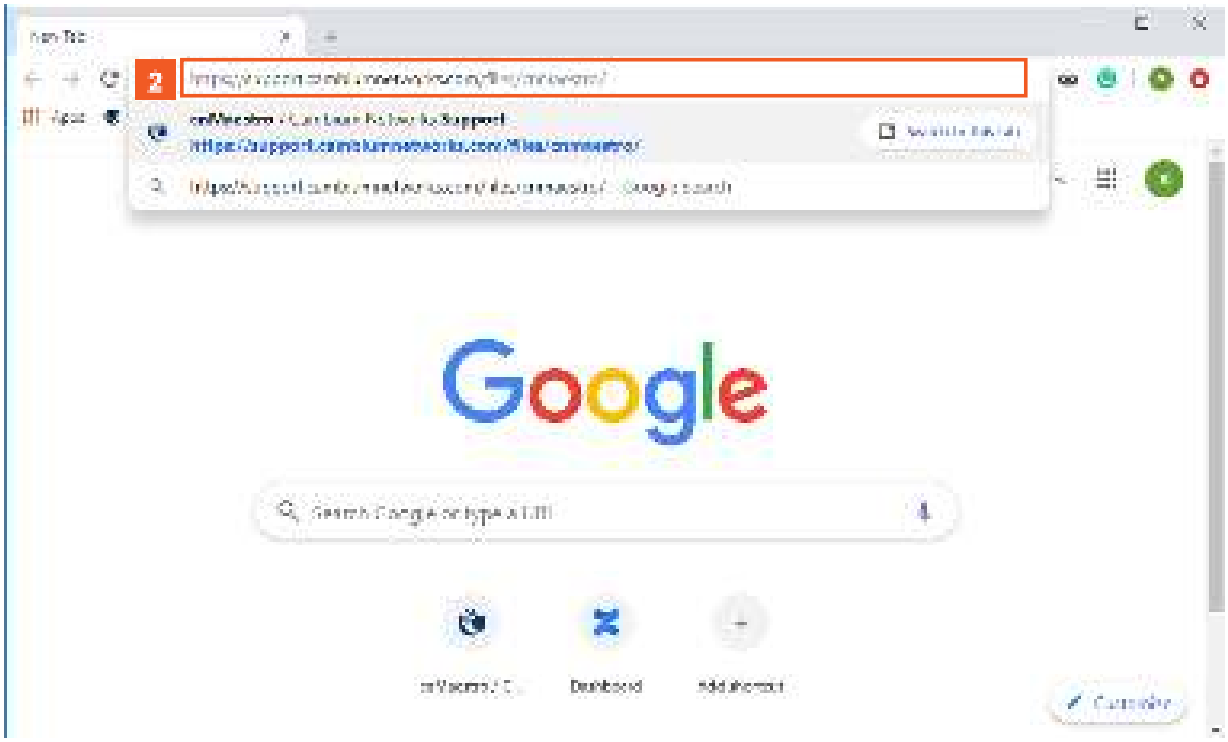
The cnMatrix switches with 2.0.1 version will be automatically upgraded during the onboarding process.

1.2 Configuring Web and cnMaestro

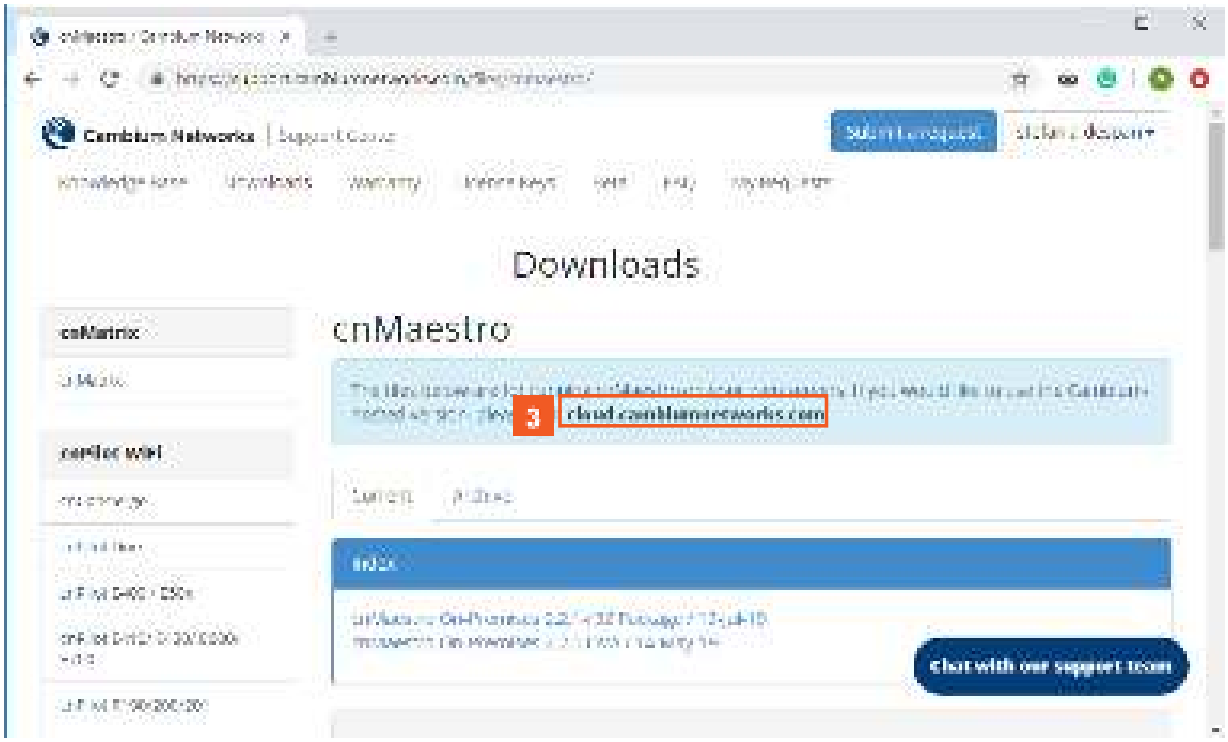
1.2.1 Accessing cnMaestro WEB



1 Enter **https://support.cambiumnetworks.com/files/cnmaestro/** into the **Address and search bar** field.



2 Press the key.



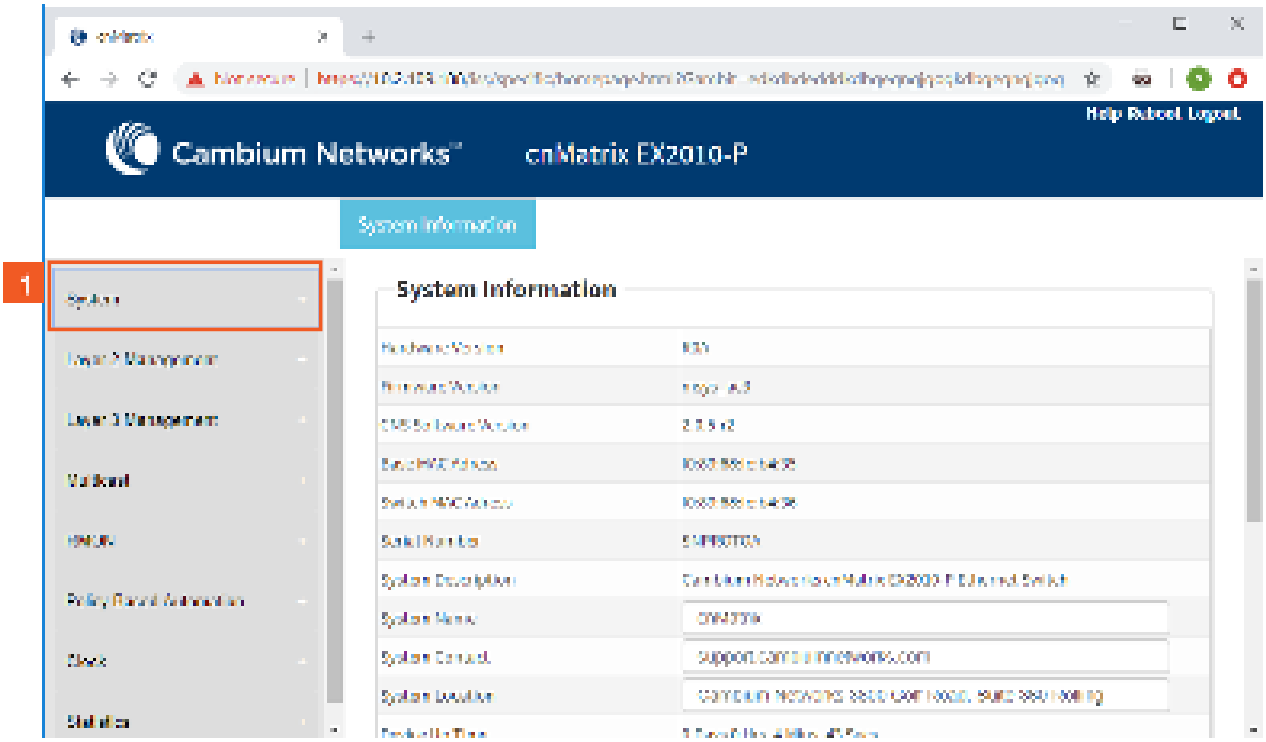
3 Click the **cloud.cambiumnetworks.com** hyperlink.

4 Click the **Sign In** button if you know your Cambium user login credentials.

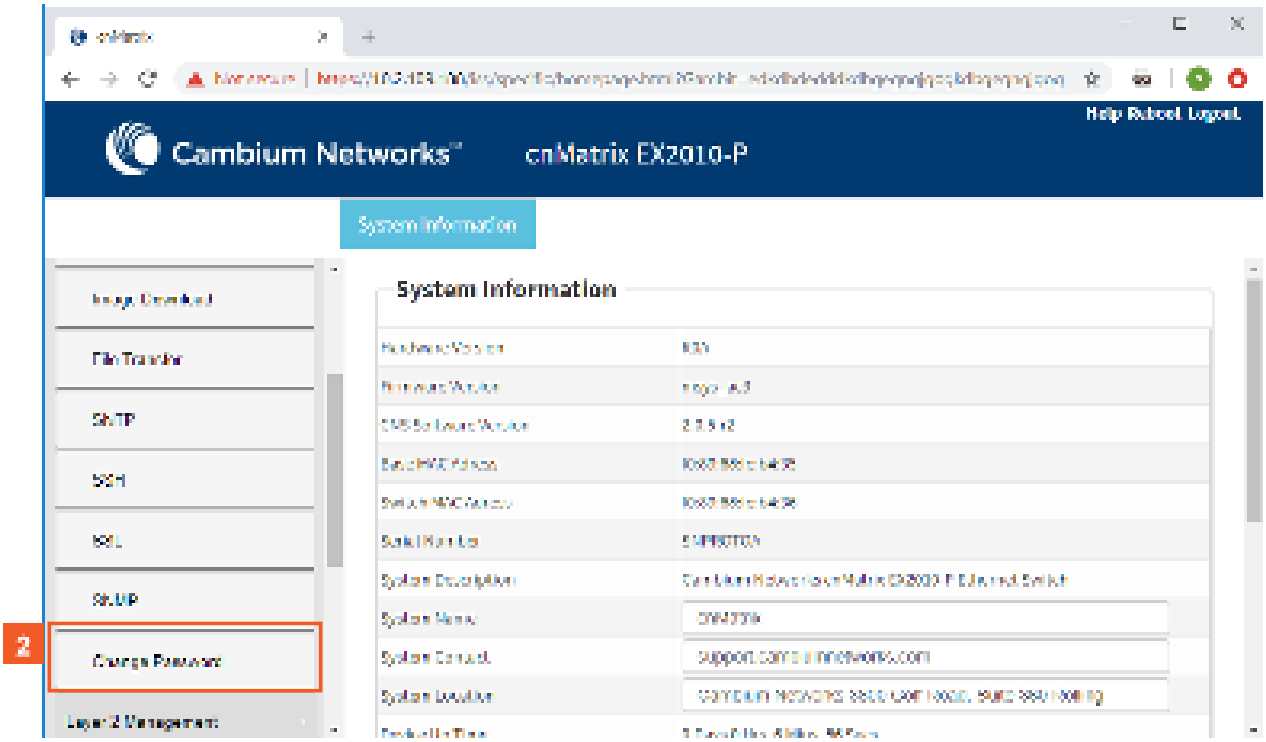
For more information, see How to Create a Cloud Account.

1.3 How to Change the Password in WEB Interface

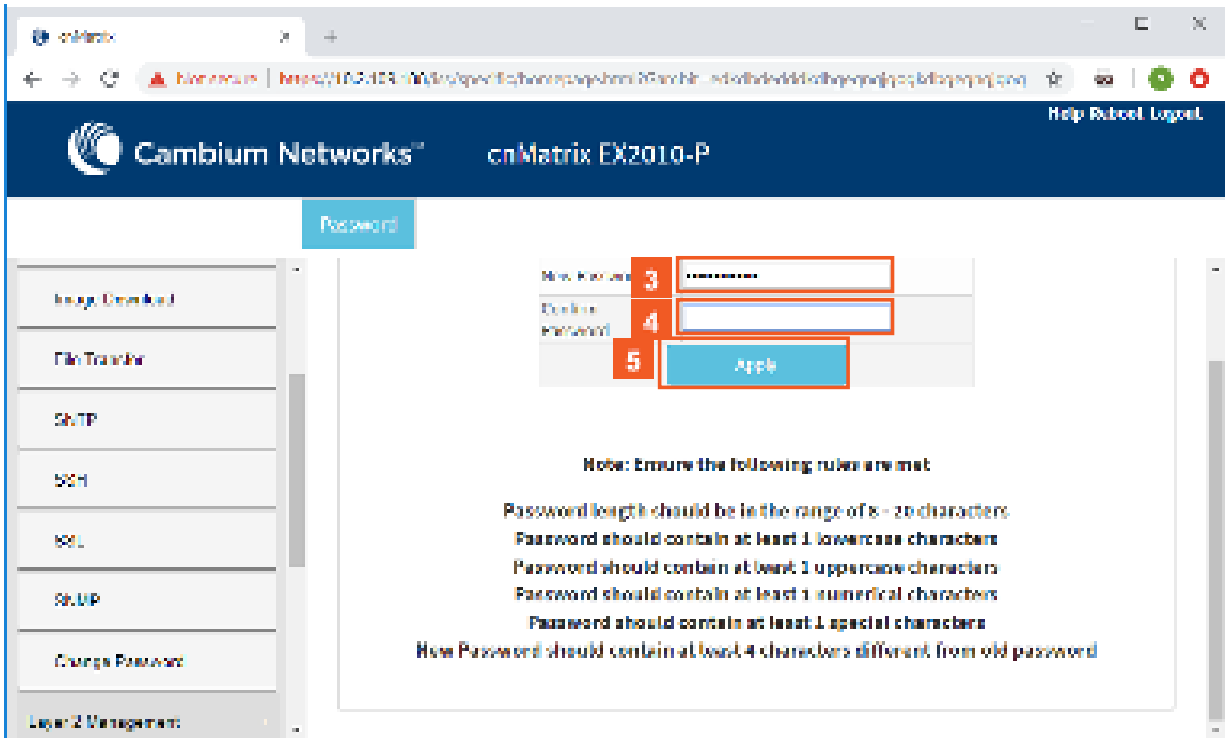
1.3.1 How to Change the Password in WEB Interface



1 Click the **System** tab.



2 Click the **Change Password** menu item.



3 Type **cnMatrix2019*** into the **New Password** field.

After your password is successfully changed, you will use the same password for WEB and CLI interfaces.

The password is case sensitive.

4 Type **cnMatrix2019*** into the **Confirm Password** field to confirm your new password.

5 Click the **Apply** button.

2 L2 Features

2.1 VLAN

2.1.1 VLAN in WEB interface

2.1.1.1 Managing VLAN

1.1.1.1.1 Feature Description

Feature Overview

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

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

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

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

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

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

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

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

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

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

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

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

Standards

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

Scaling Numbers

- A maximum of 4066 series can be created.

Limitations

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

Default Values

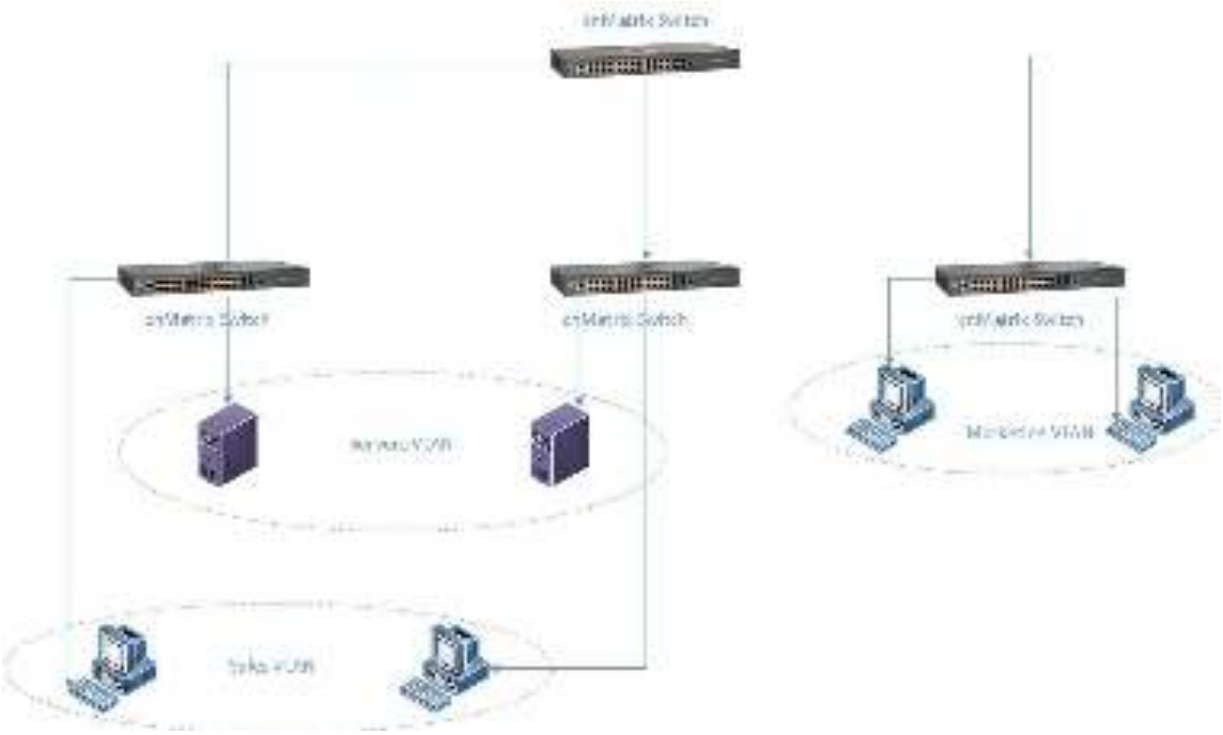
- VLAN is enabled by default.
- VLAN 1 is created by default.
- All available ports are configured as member ports and untagged ports of the default VLAN (VLAN 1).
- The default operation mode for all ports: hybrid.

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

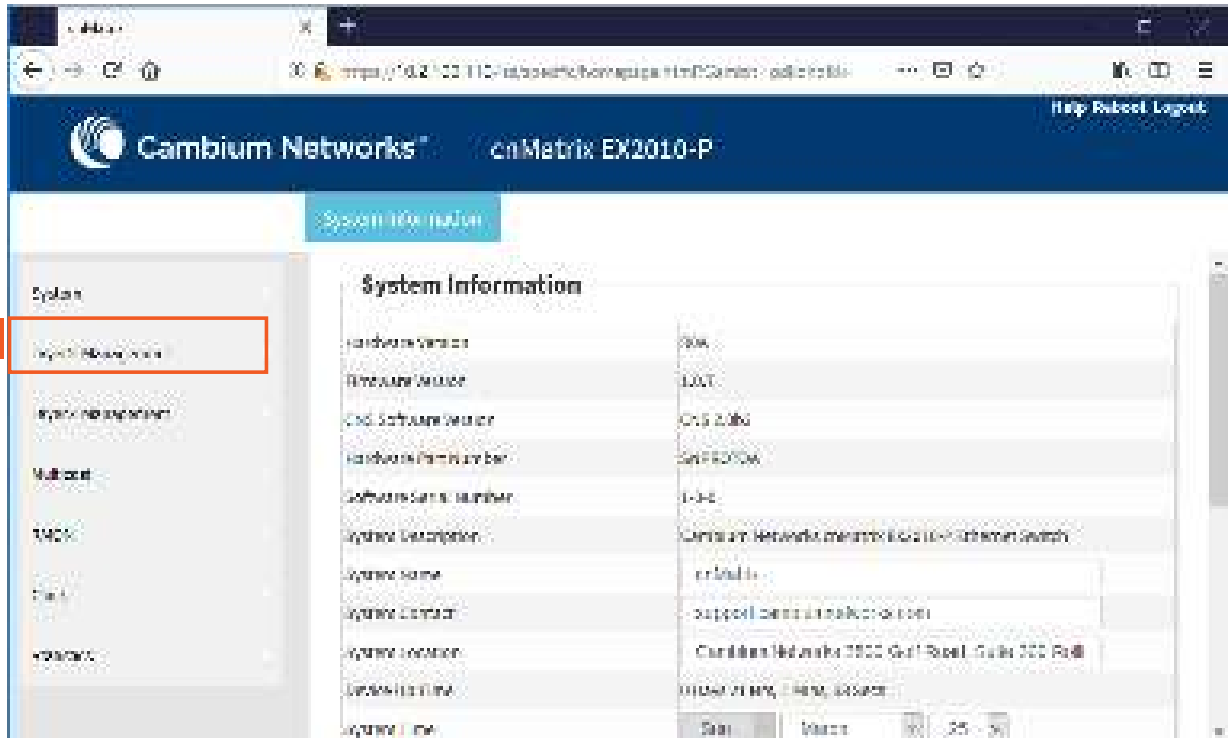
The static ARP will be removed after deleting the VLAN interface.

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

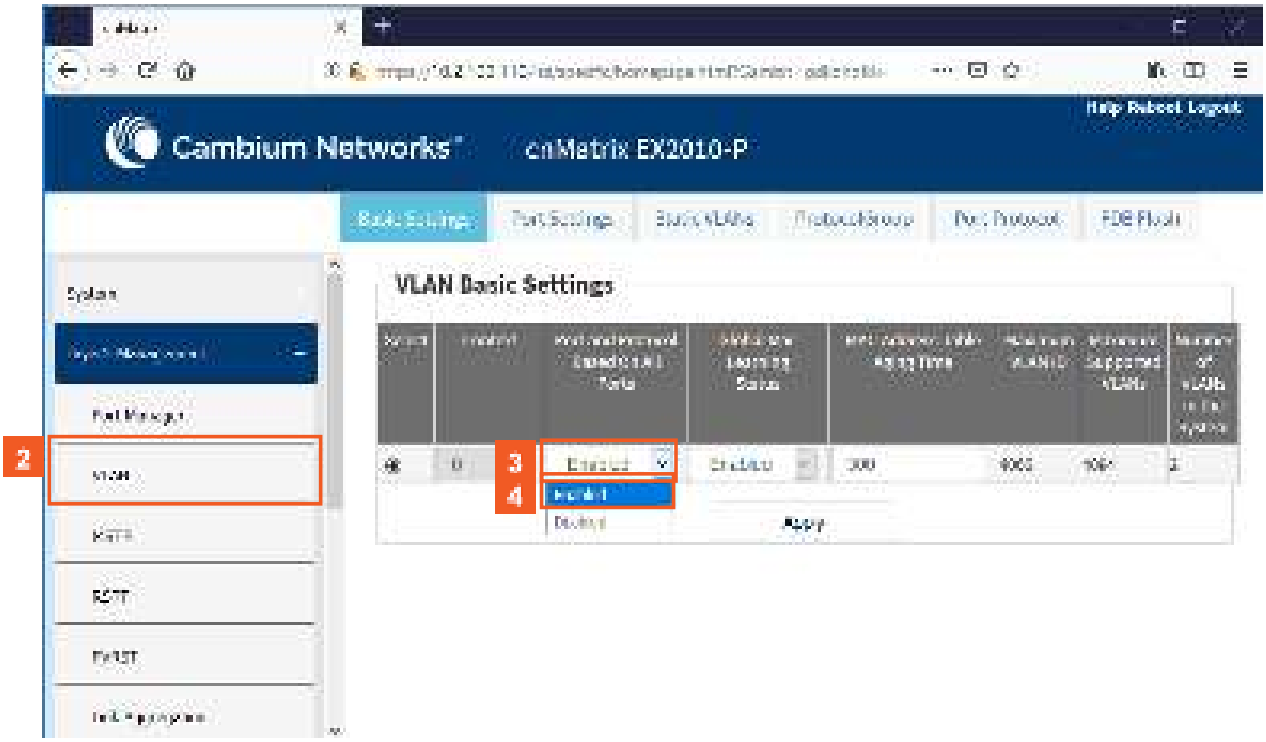
1.1.1.1.2 Network Diagram



2.1.1.2 How to Enable and Configure VLAN in WEB Interface



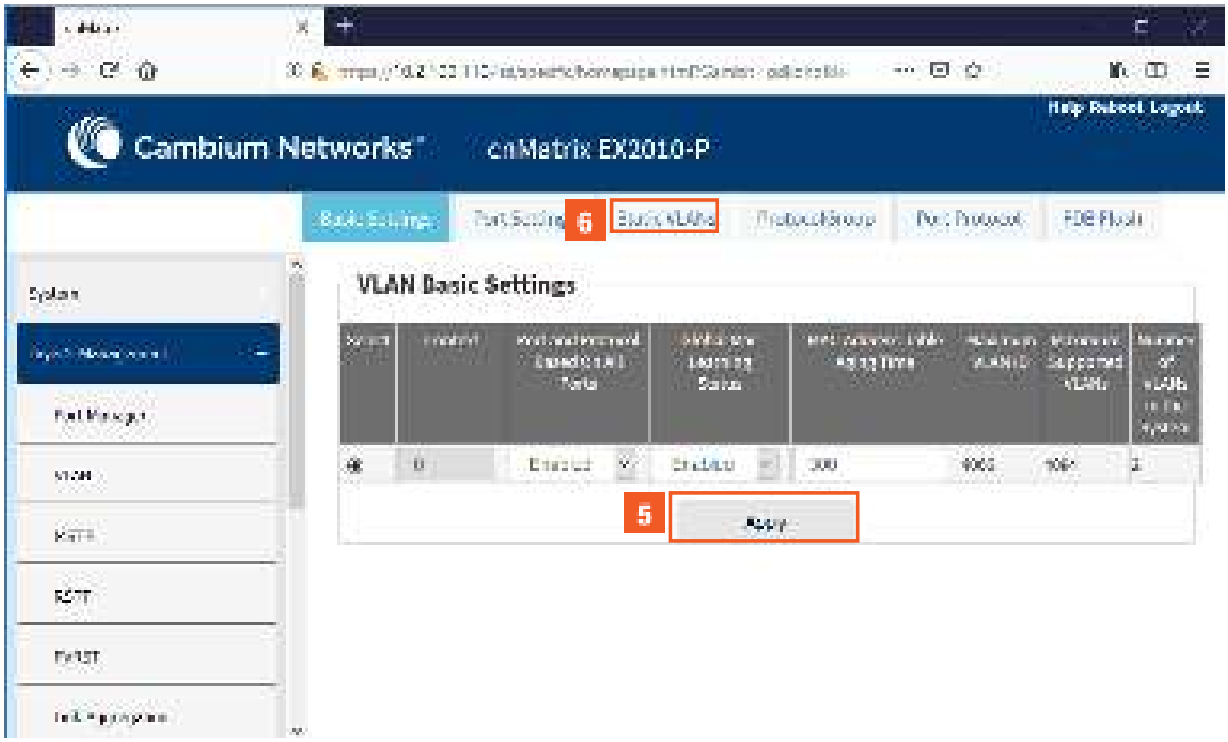
1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.



2 Click the **VLAN** menu item.

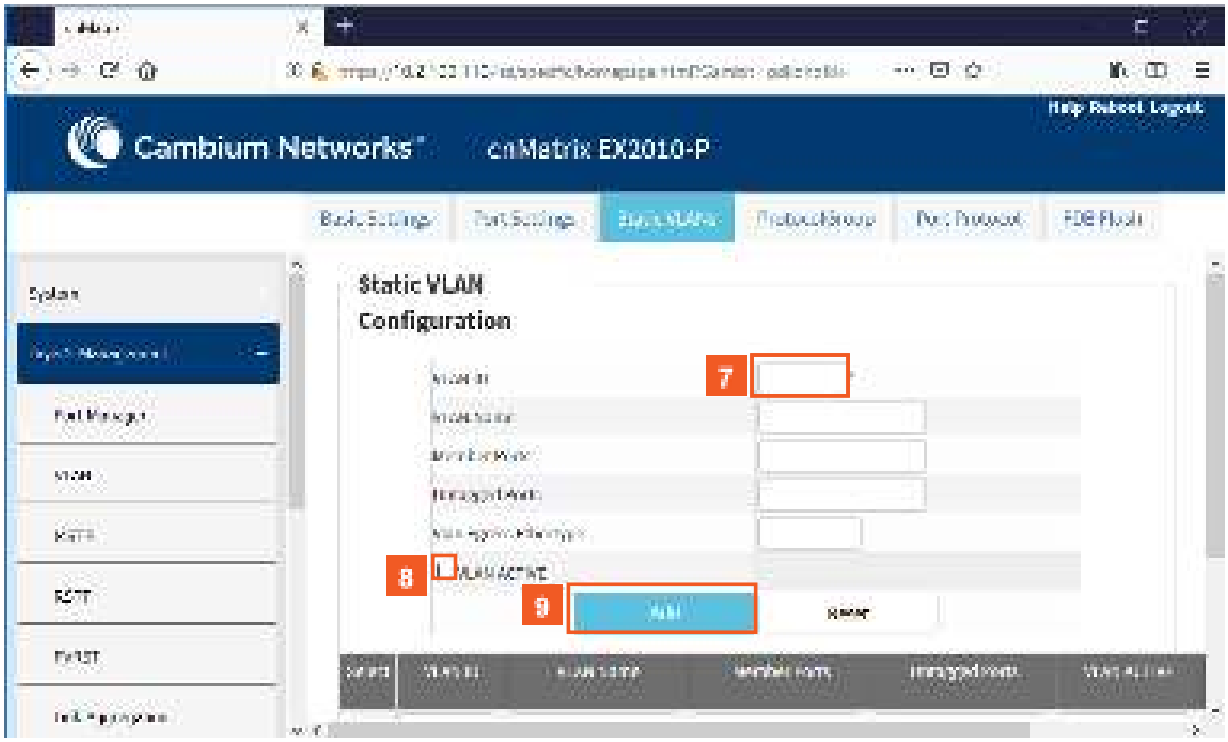
3 Click the **Port and Protocol Based on All Ports** drop-down button to select whether the classification of VLAN membership should be done based on port and protocol on the selected port.

4 Select the **Enabled** list item.



5 Click the **Apply** button.

6 Click the **Static VLANs** tab. The **Static VLAN Configuration** window is displayed.



7 Type the value **3** into the **VLAN ID** field.

Number **3** represents the VLAN ID that uniquely identifies a specific VLAN. The maximum value for VLAN ID is: 4066.

8 Select the **VLAN ACTIVE** checkbox. The configured VLAN becomes active on your switch.

9 Click the **Add** button.

2.2 STP

2.2.1 STP in WEB interface

2.2.1.1 STP

Feature Overview

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

STP in cnMatrix

Standards

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

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

Scaling Numbers

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

Limitations

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

Default Values

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

Prerequisites

N/A

2.2.1.2 Managing RSTP

Feature Overview

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

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

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

RSTP has three port states:

- Discarding
- Learning
- Forwarding

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

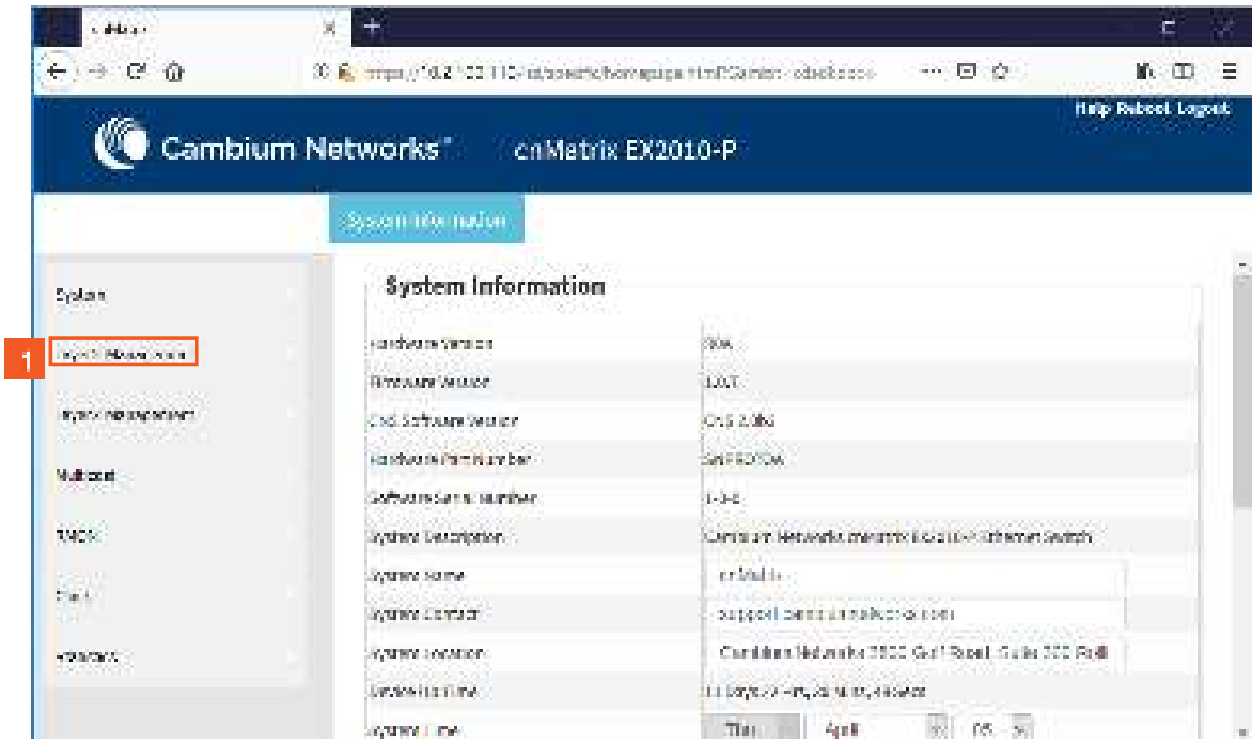
Standards

- 802.1w

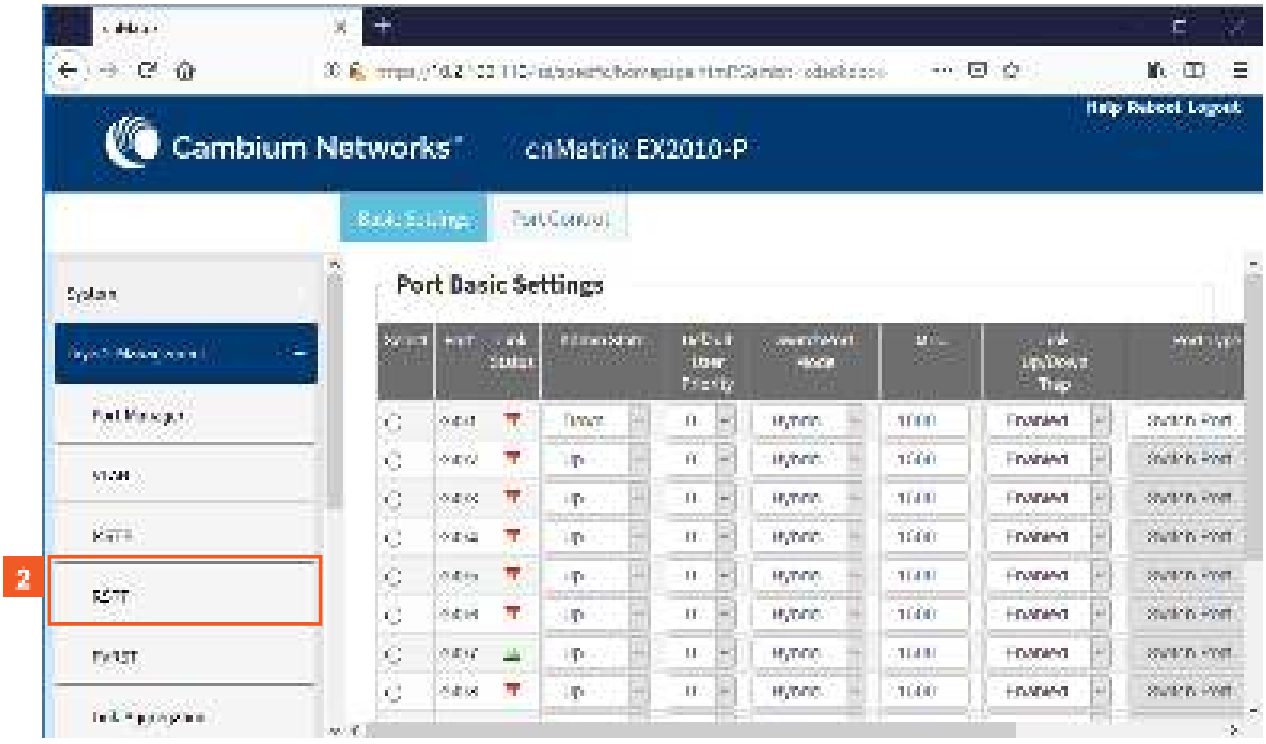
Default Values

- Hello time - 2 seconds.

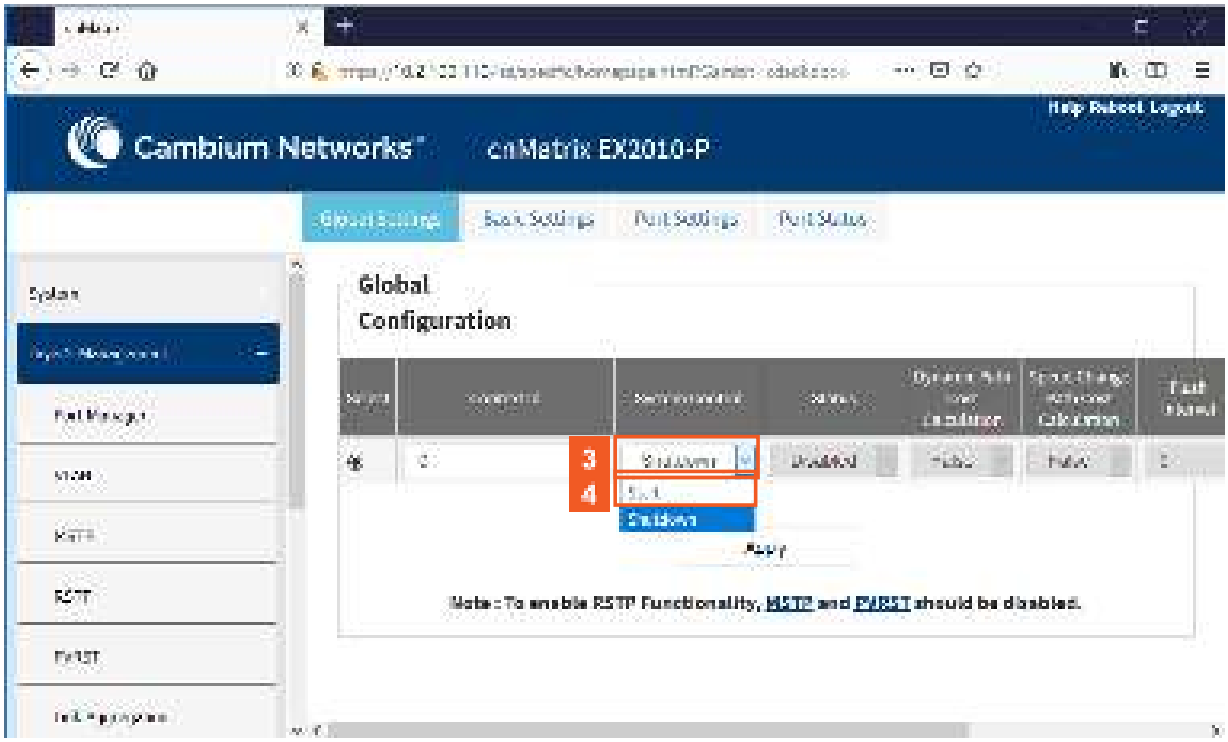
2.2.1.3 How to Enable and Configure RSTP in WEB Interface



1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.

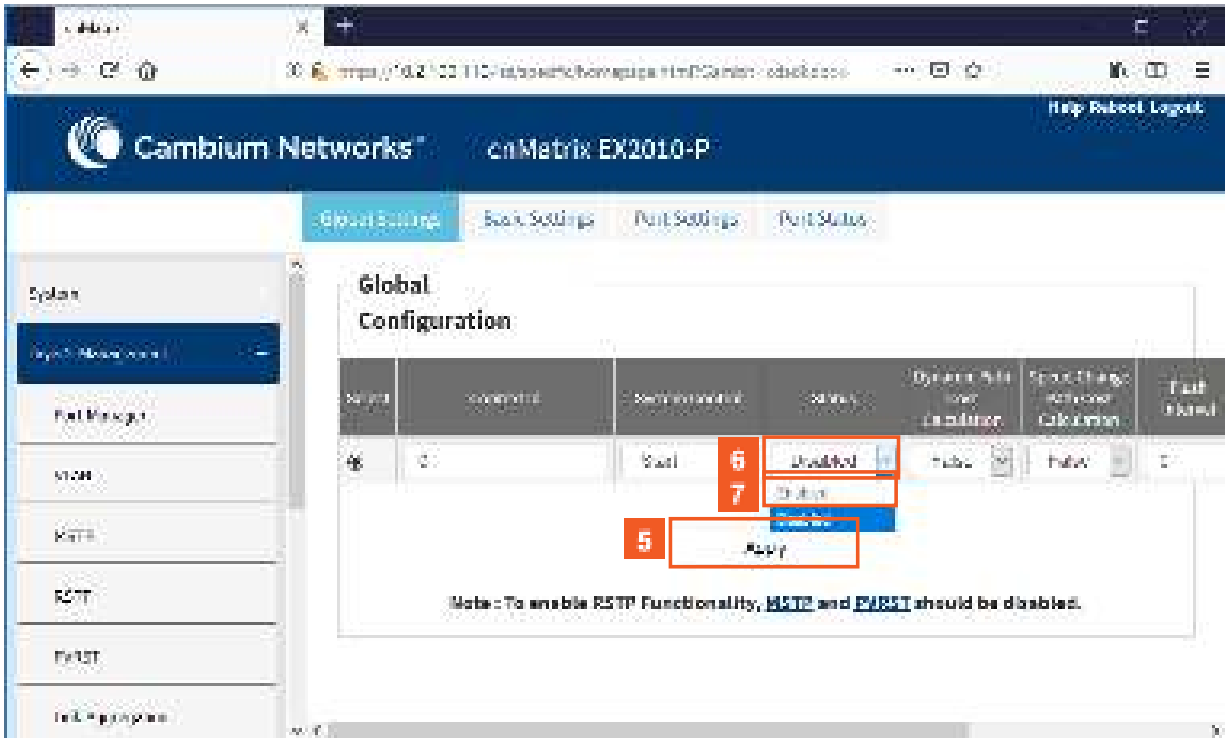


2 Click the **RSTP** menu item.



3 Click the **System Control** drop-down list to select the administrative system control status for the RSTP feature.

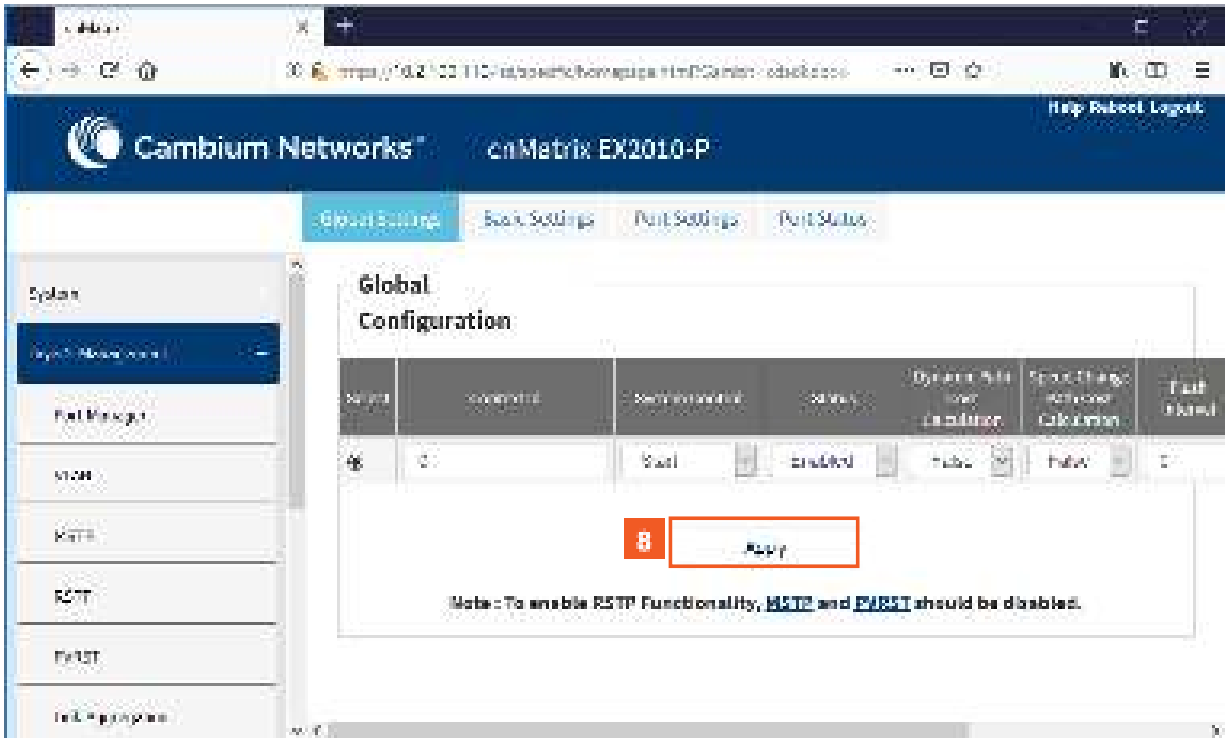
4 Select the **Start** list item.



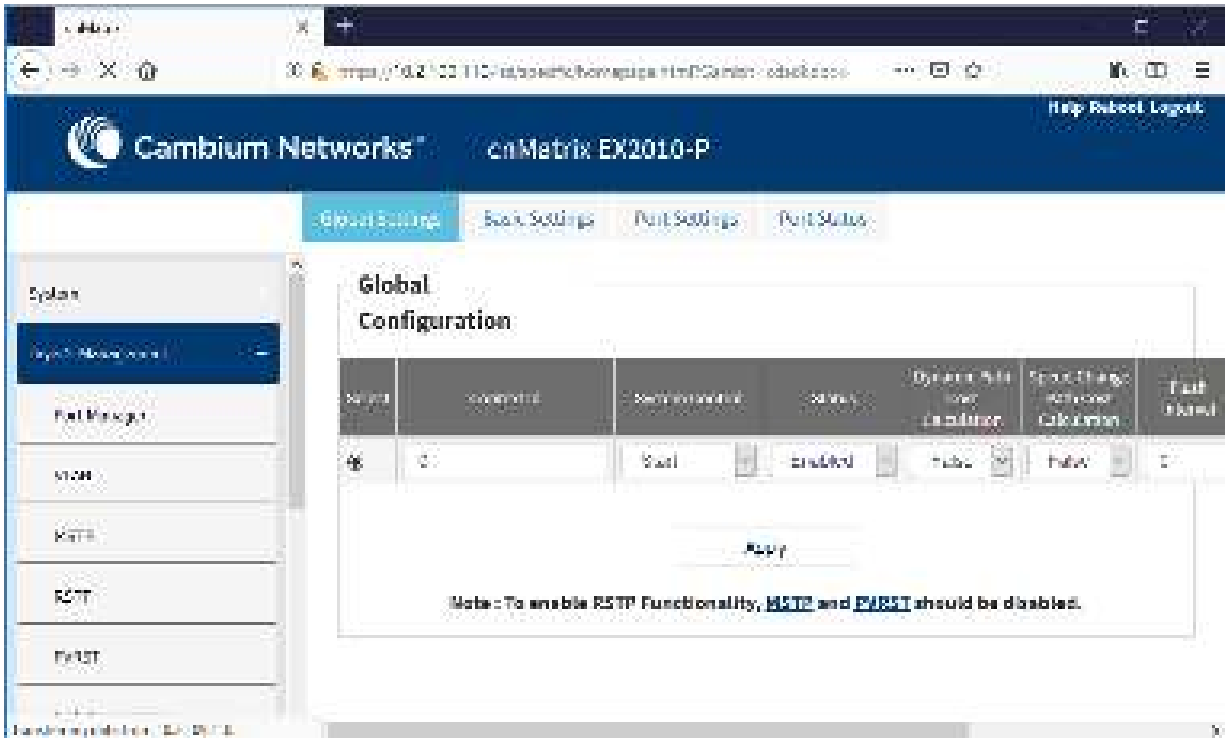
5 Click the **Apply** button.

6 Click the **Status** drop-down list to select the administrative module status for the RSTP feature.

7 Select the **Enabled** list item.



8 Click the **Apply** button.



To enable the RSTP feature, make sure that the MSTP and PVRST features are disabled.

2.2.1.4 Managing MSTP

1.1.1.1.3 Feature Description

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

Feature Overview

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

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

Standards

- 802.1s

Scaling Numbers

- Up to 8 MSTP instances.

Limitations

N/A

Default Values

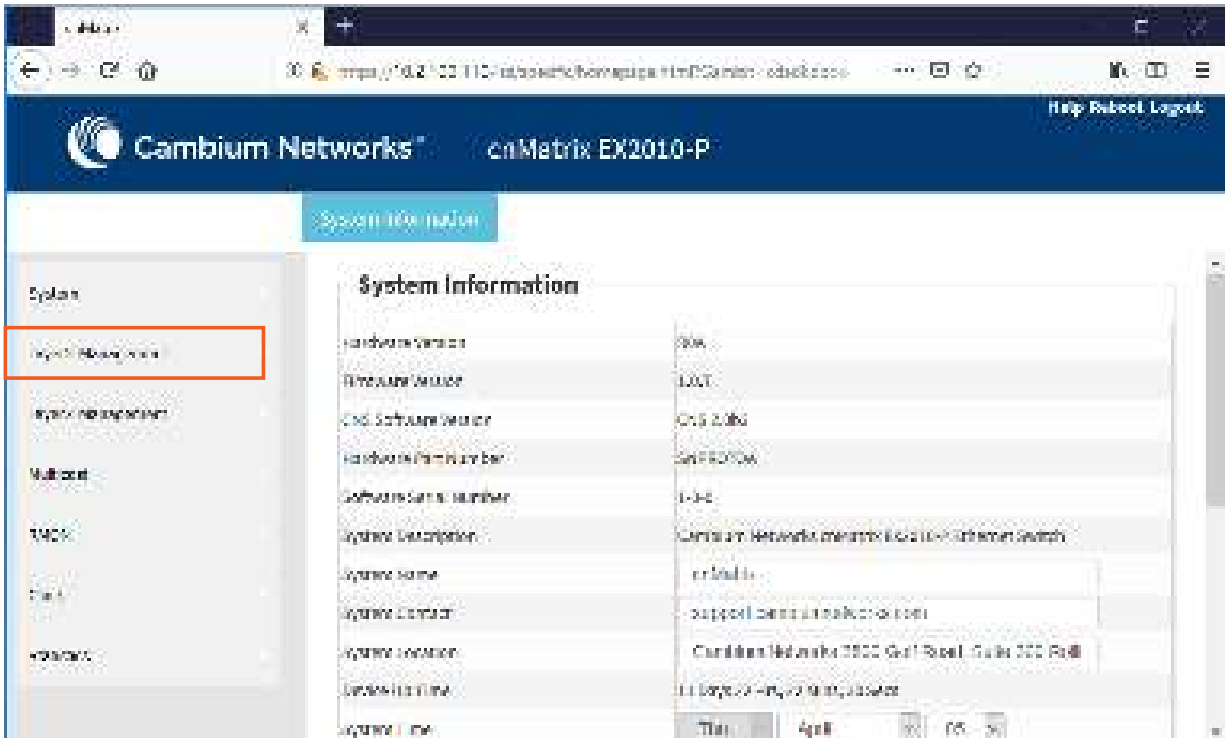
- The default value for the forward time of the spanning tree: 15 seconds.
- The default value for the max-age timer of the spanning tree: 20 seconds.
- The default value for the revision number for the MST region: 0.
- The MST instance 0 is created and mapped with all VLANs.
- The default spanning tree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

Prerequisites

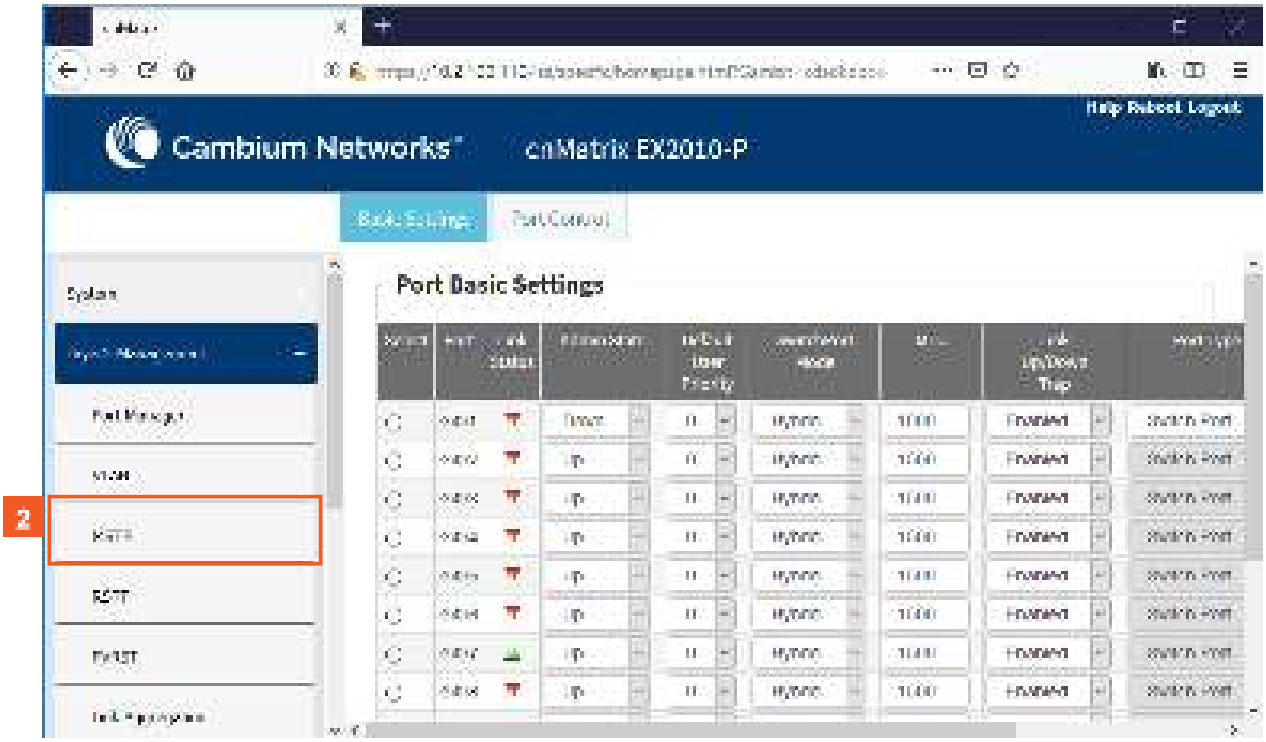
- N/A

1.1.1.1.4 Network Diagram

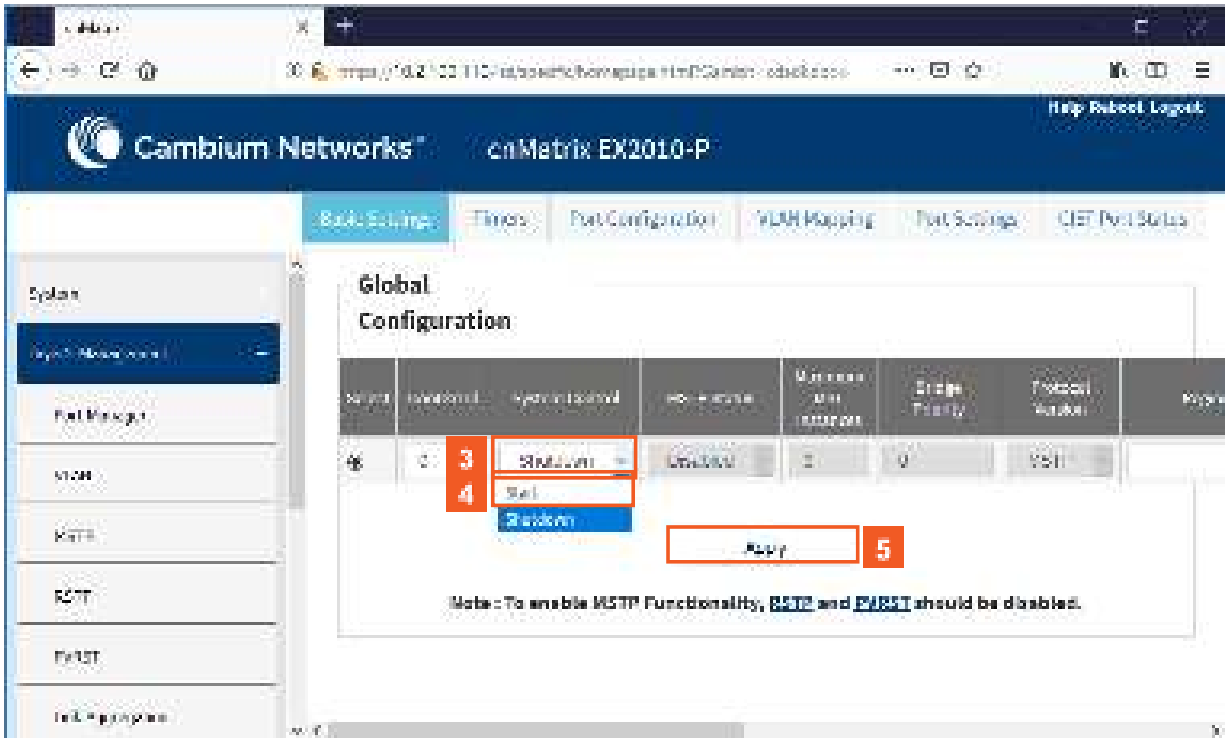
2.2.1.5 How to Enable and Configure MSTP in WEB Interface



1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.



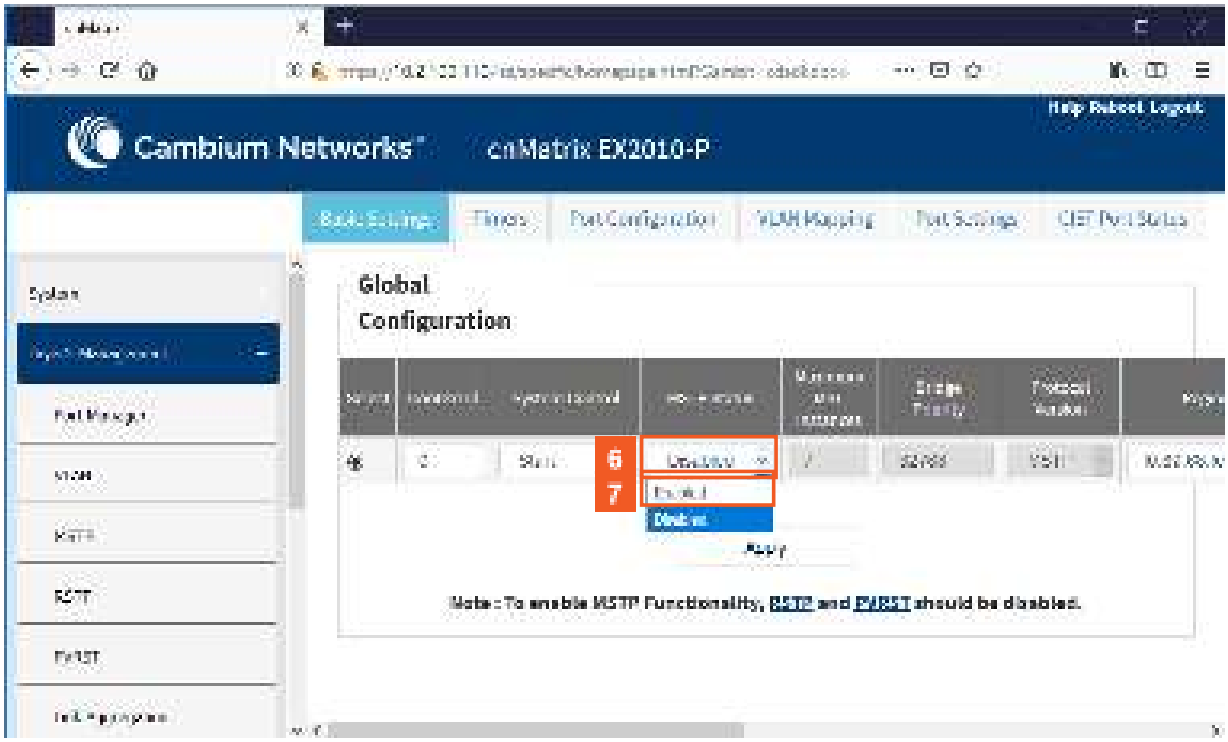
2 Click the **MSTP** menu item.



3 Click the **System Control** drop-down list to select the administrative shutdown status for the MSTP module.

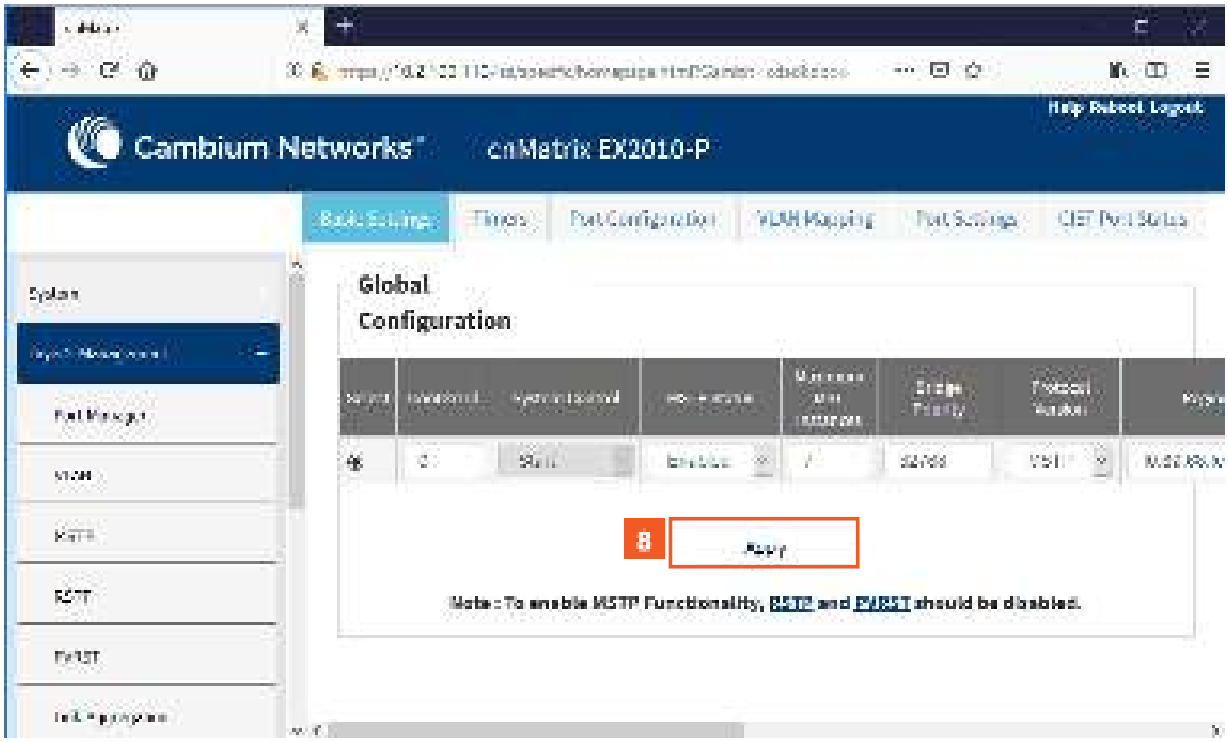
4 Select the **Start** list item.

5 Click the **Apply** button.



6 Click the **MSTP Status** drop-down list to select the administrative status for the MSTP feature.

7 Select the **Enabled** list item.



8 Click the **Apply** button.

To enable the MSTP feature, make sure that the RSTP and PVRST features are disabled.

2.2.1.6 Managing PVRST

1.1.1.1.5 Feature Description

Feature Overview

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

Standards

- 802.1w

Scaling Numbers

- Up to 32 PVRST instances.

Default Values

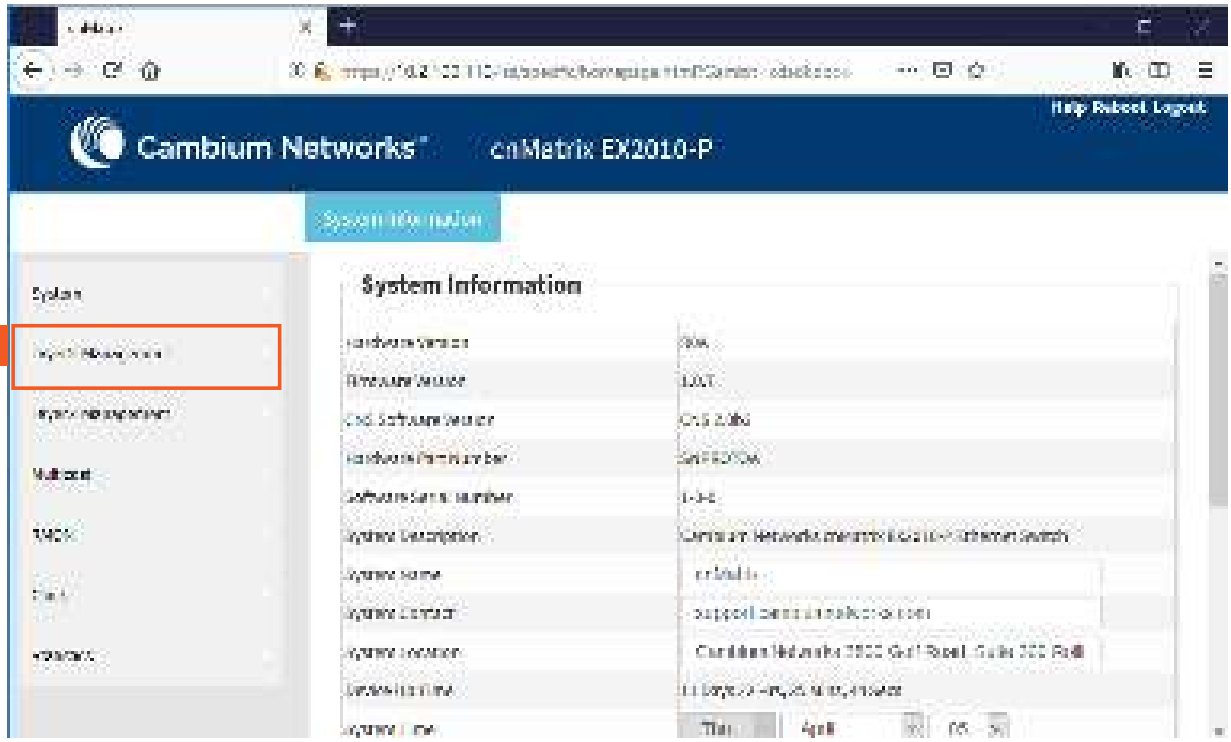
- The default value for the forward time of the spanning tree: 15 seconds.
- The default value for the max-age timer of the spanning tree: 20 seconds.
- The default value for the revision number for the PVRST region: 0.
- The PVRST instance 0 is created and mapped with all VLANs.
- The default spanning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

Prerequisites

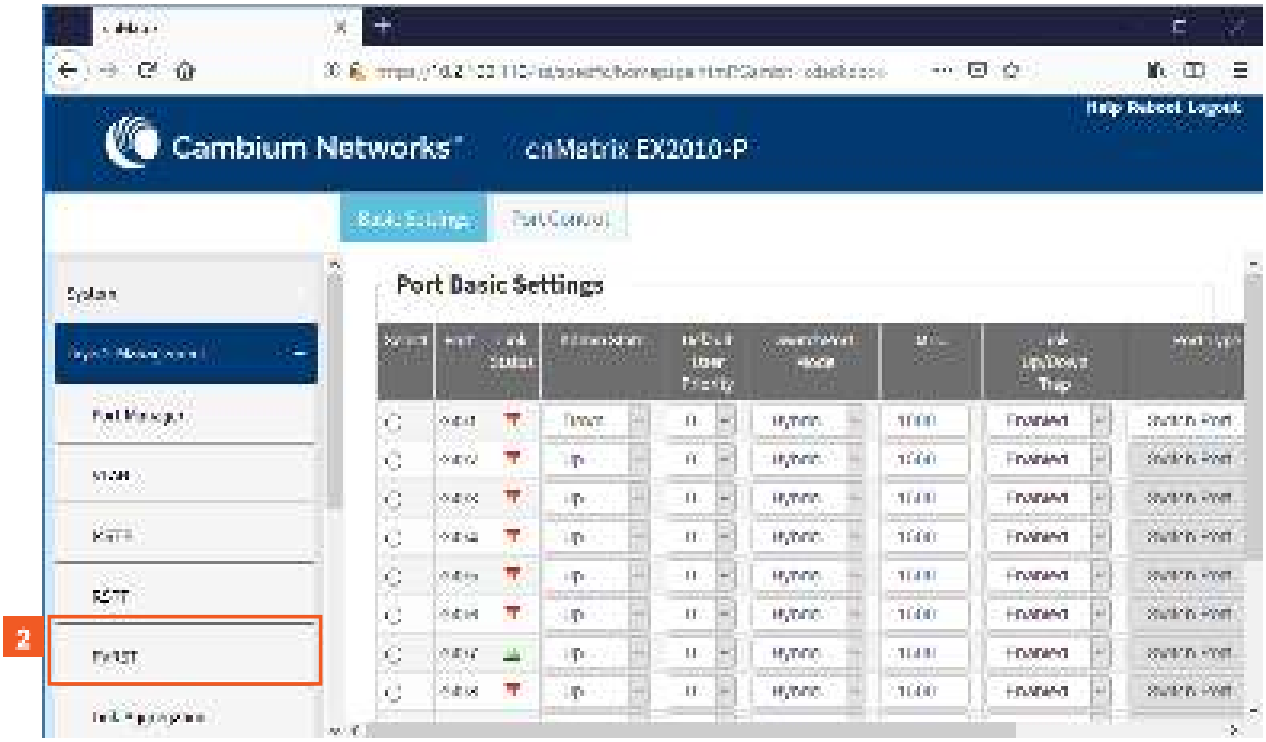
- To enable the PVRST Functionality, MSTP and RSTP should be disabled.

1.1.1.1.6 Network Diagram

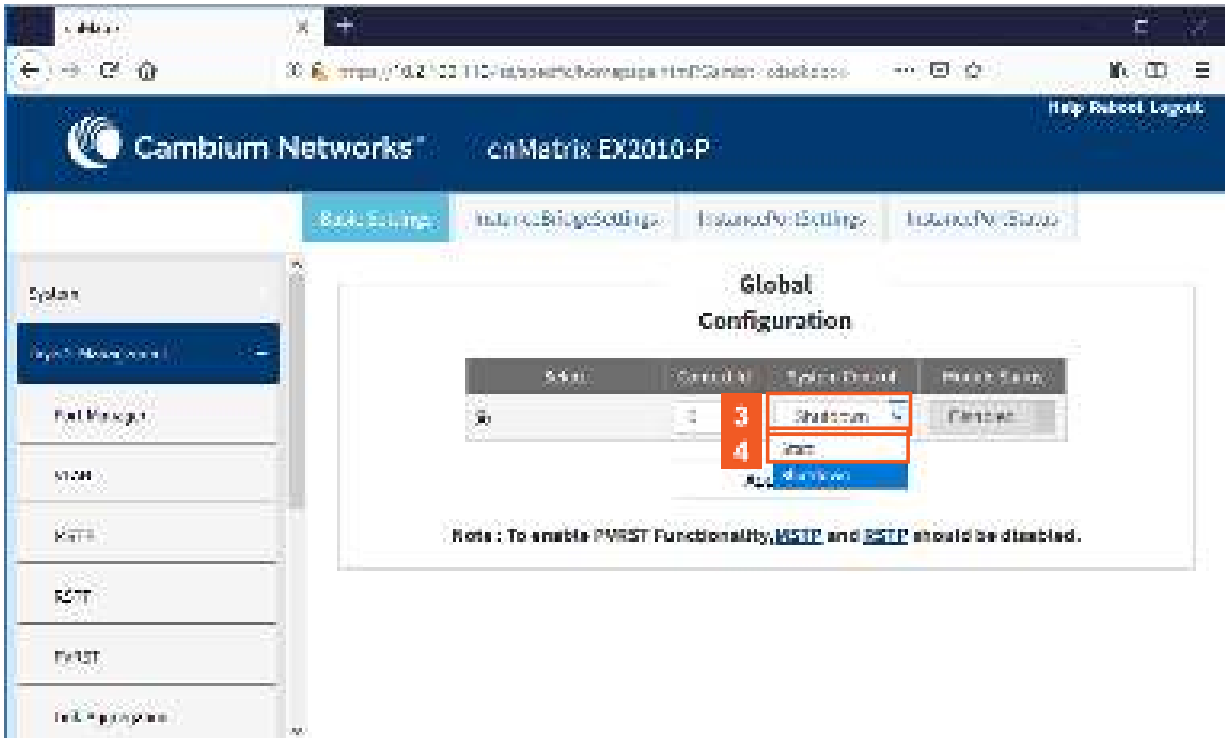
2.2.1.7 How to Enable and Configure PVRST in WEB Interface



1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.

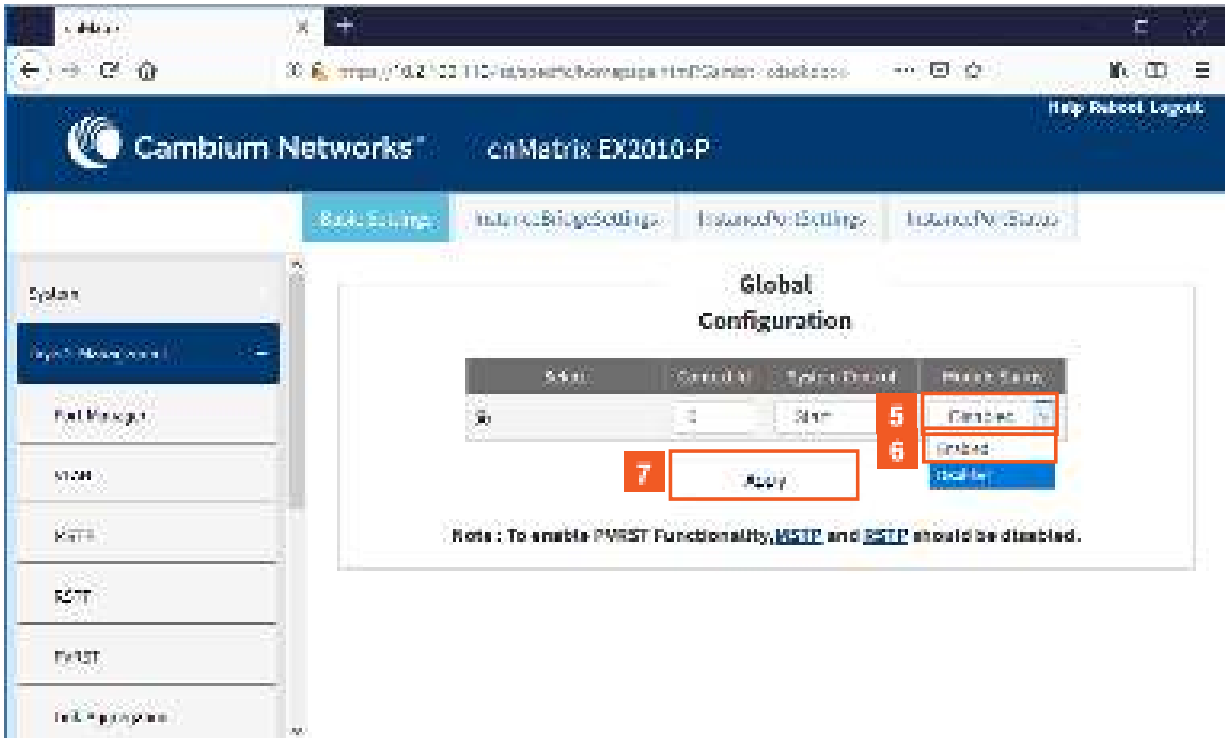


2 Click the **PVRST** menu item.



3 Click the **System Control** drop-down list to select the administrative system control status for the PVRST feature.

4 Select the **Start** list item.



5 Click the **Module Status** drop-down list to select from the drop-down the administrative module status for the PVRST feature.

6 Select the **Enabled** list item.

7 Click the **Apply** button.

Section complete. Click X to close.

2.3 LLDP

2.3.1 LLDP in WEB interface

2.3.1.1 Managing LLDP

Feature Overview

The LLDP feature enables you to discover the neighbor devices.

LLDP (Link Layer Discovery Protocol) is a link-layer protocol used by devices to advertise their identity and capabilities to their neighbors on a LAN.

Standards

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

Scaling Numbers

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

Limitations

- N/A

Default Values

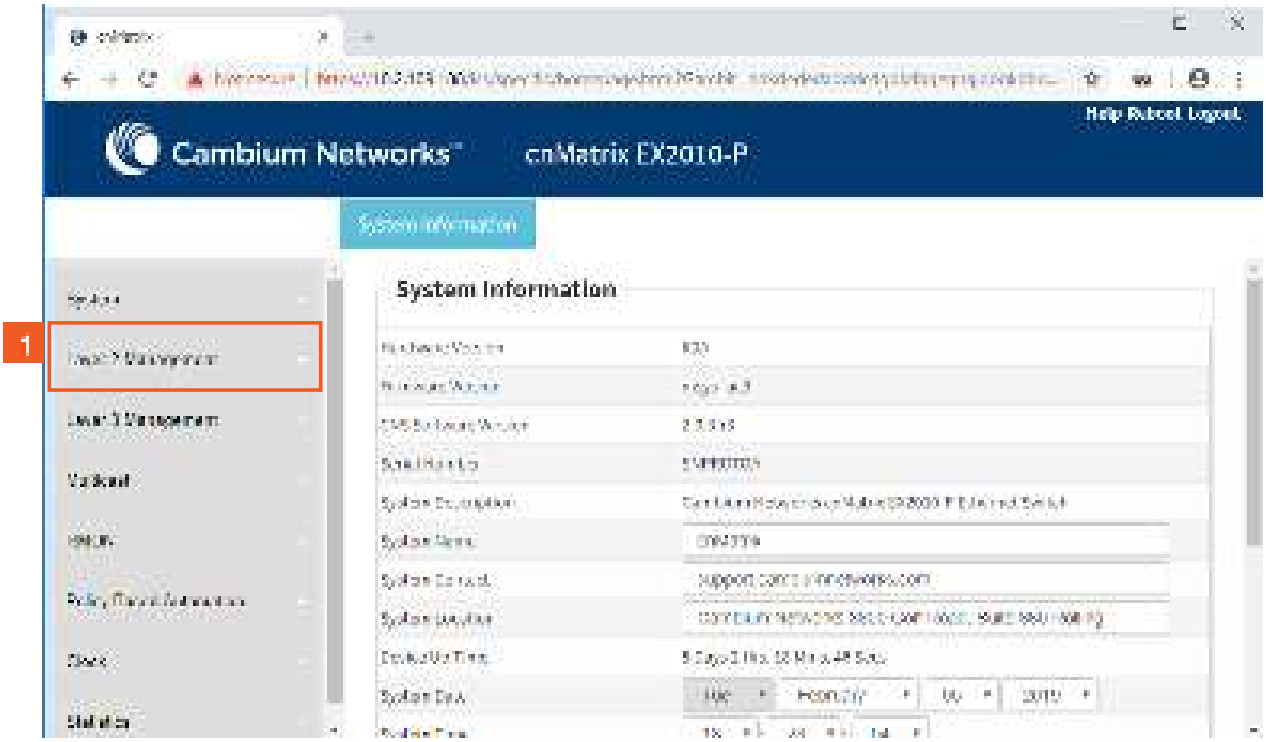
- The default transmission interval: 30 seconds.
- The default value for holdtime-multiplier: 4.
- The default value for reinitialization delay time: 2.

- Transmission / reception of LLDPU are enabled by default.
- The default LLDP version is v2.
- Port description, system name, system description and system capabilities TLVs are enabled on all ports.

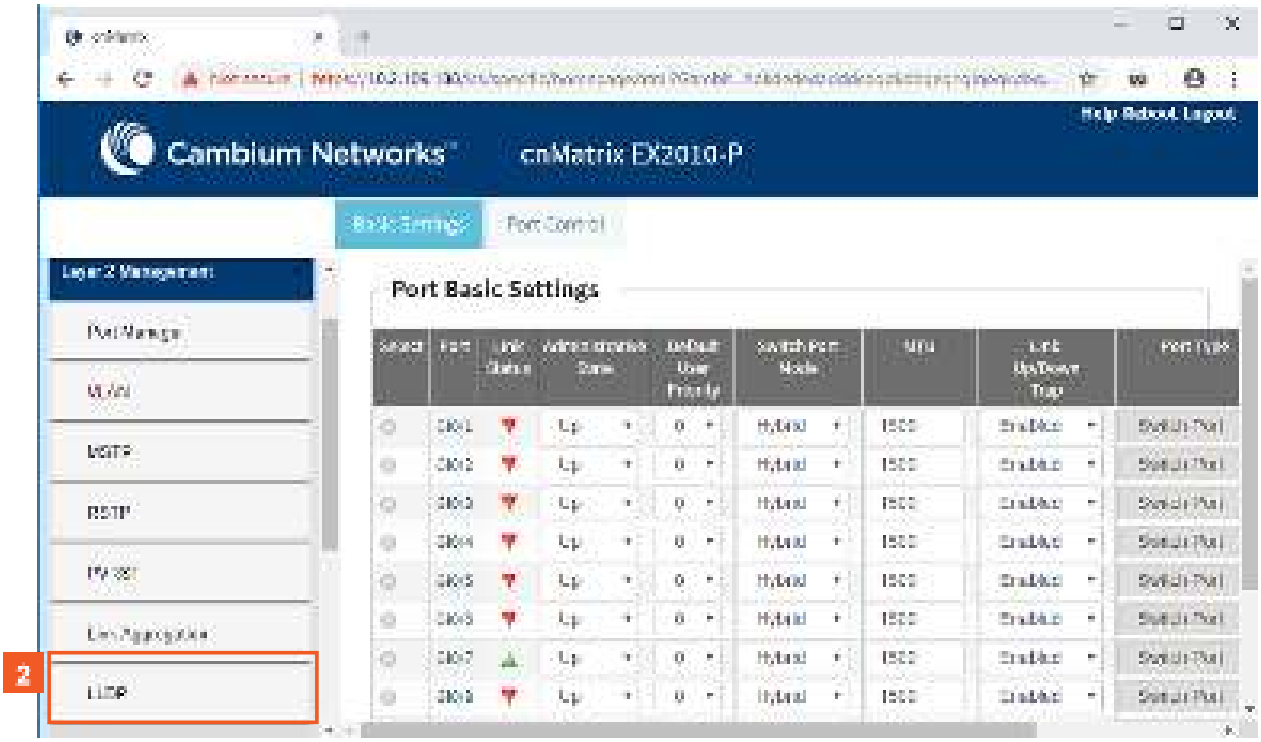
Prerequisites

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

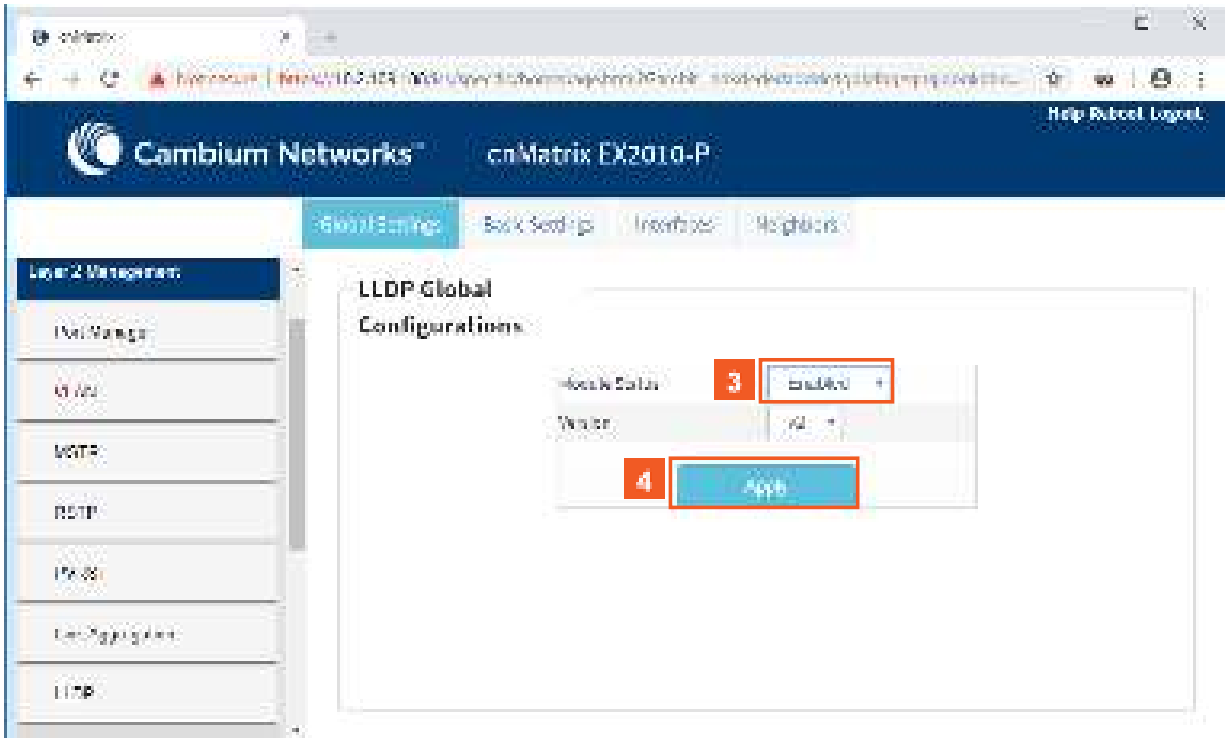
2.3.1.2 How to Enable and Configure LLDP in WEB Interface



1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.



2 Click the **LLDP** menu item.



3 Click the **Module Status** drop-down list to select the administrative module status of the LLDP feature. Select the **Enabled** list item.

4 Click the **Apply** button.

2.4 RMON

2.4.1 RMON in WEB interface

2.4.1.1 Managing RMON

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

Standards

- The RMON feature is documented in RFC 2819.

Scaling Numbers

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

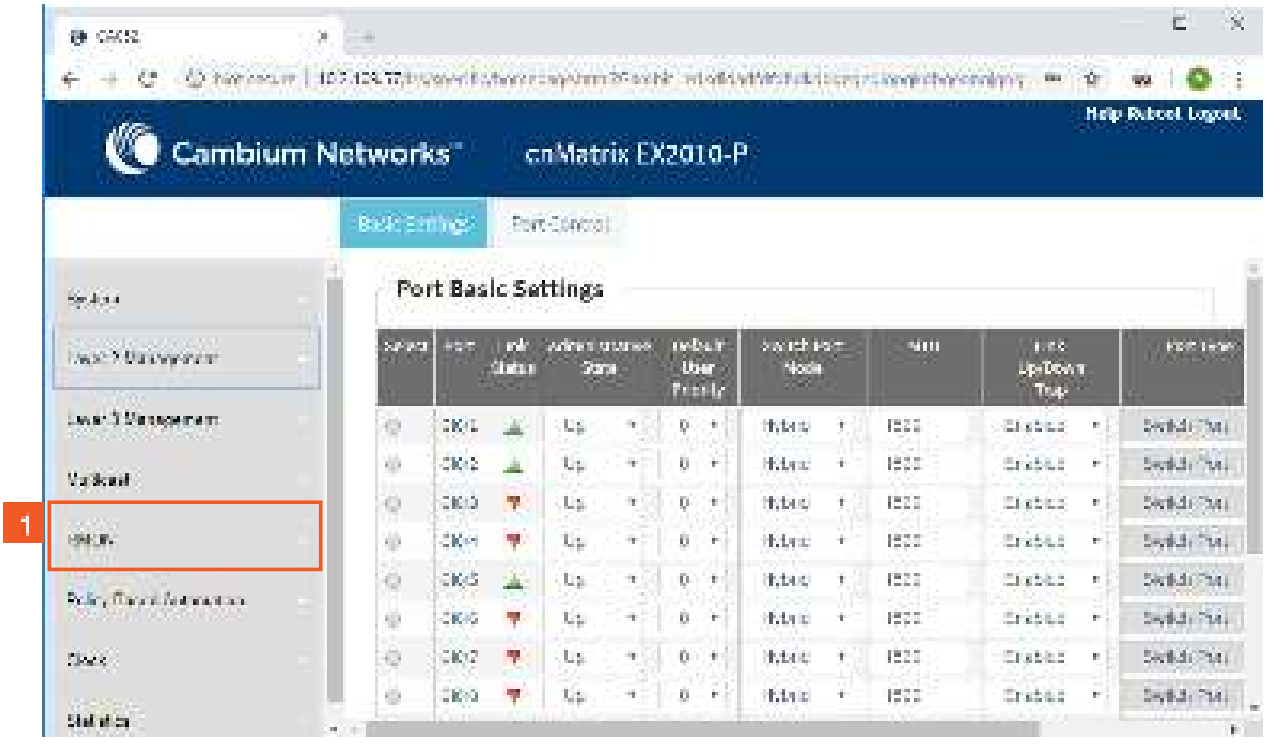
Limitations

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

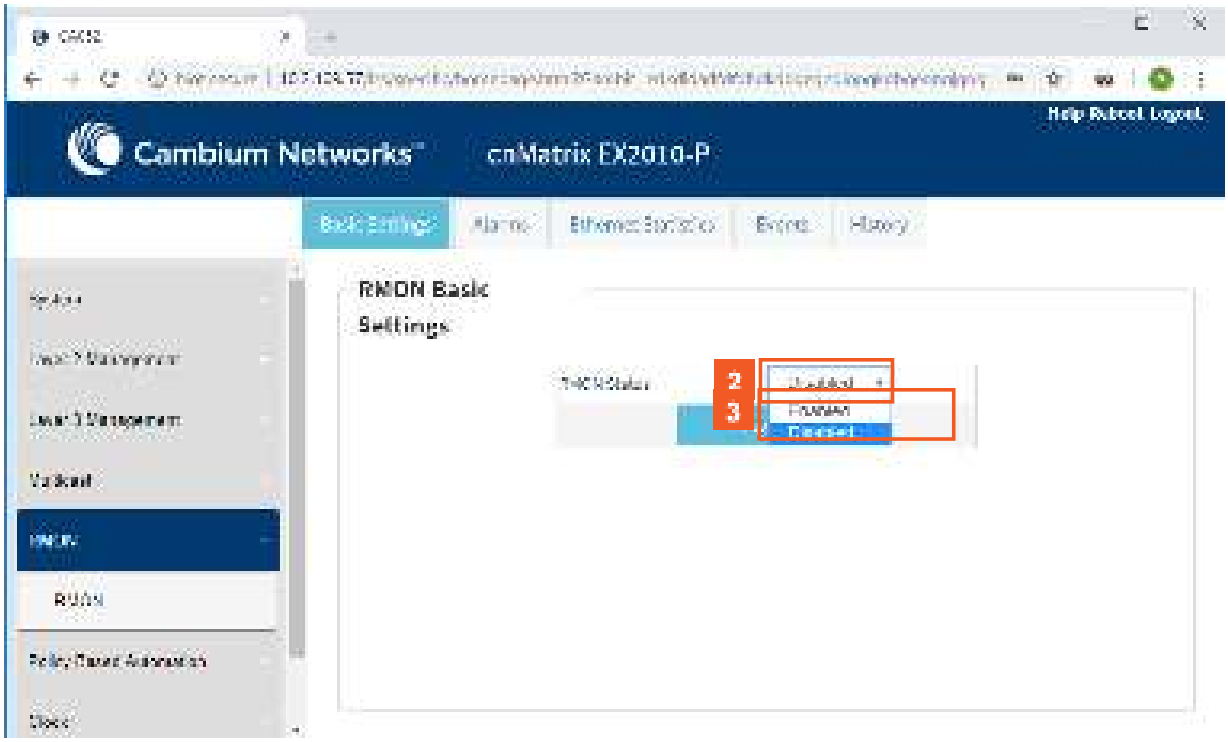
Default Values

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

2.4.1.2 How to Enable RMON in WEB Interface

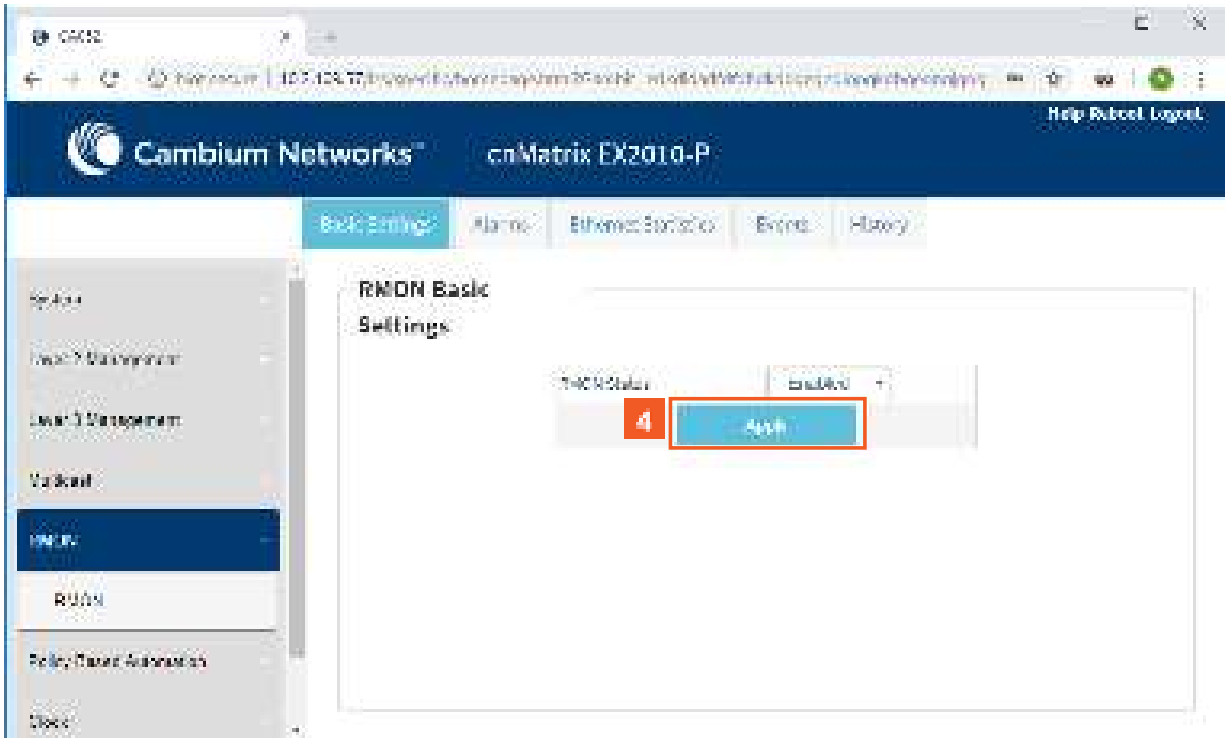


1 Click the **RMON** tab. The **RMON Basic Settings** window is displayed.



2 Click the **RMON Status** drop-down list and select the status of the RMON feature on the switch.

3 Select the **Enabled** list item.



4 Click the **Apply** button.

2.5 SNTP

2.5.1 SNTP in WEB interface

2.5.1.1 Managing SNTP

1.1.1.1.7 Feature Description

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

Standards

- cnMatrix SNTP client is RFC 4330 compliant.

Scaling Numbers

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

Limitations

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

- Discovers the version number of the server dynamically.
- Sets the transmit time field in the request packet which allows to determine roundtrip delay and system clock offset relative to the server.
- Sends client request messages periodically.
- Avoids sending client request messages with less than 1-minute periodic interval.
- Stops sending request packets to a particular server when receives a reply with stratum field set to zero.
- Retransmits a request packet using an exponential-backoff algorithm, after receiving reply packet with start field set as zero.

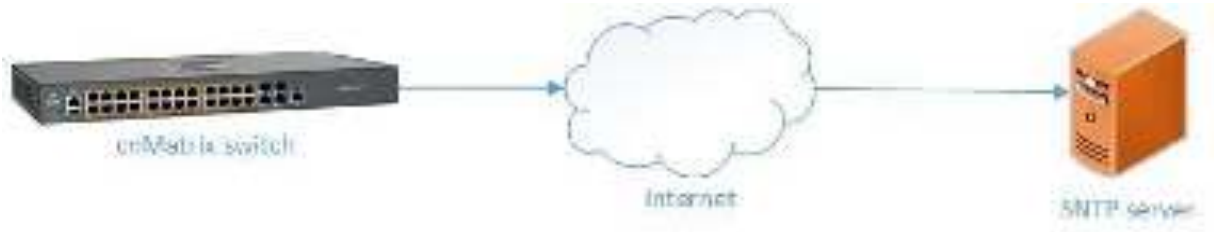
Default Values

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

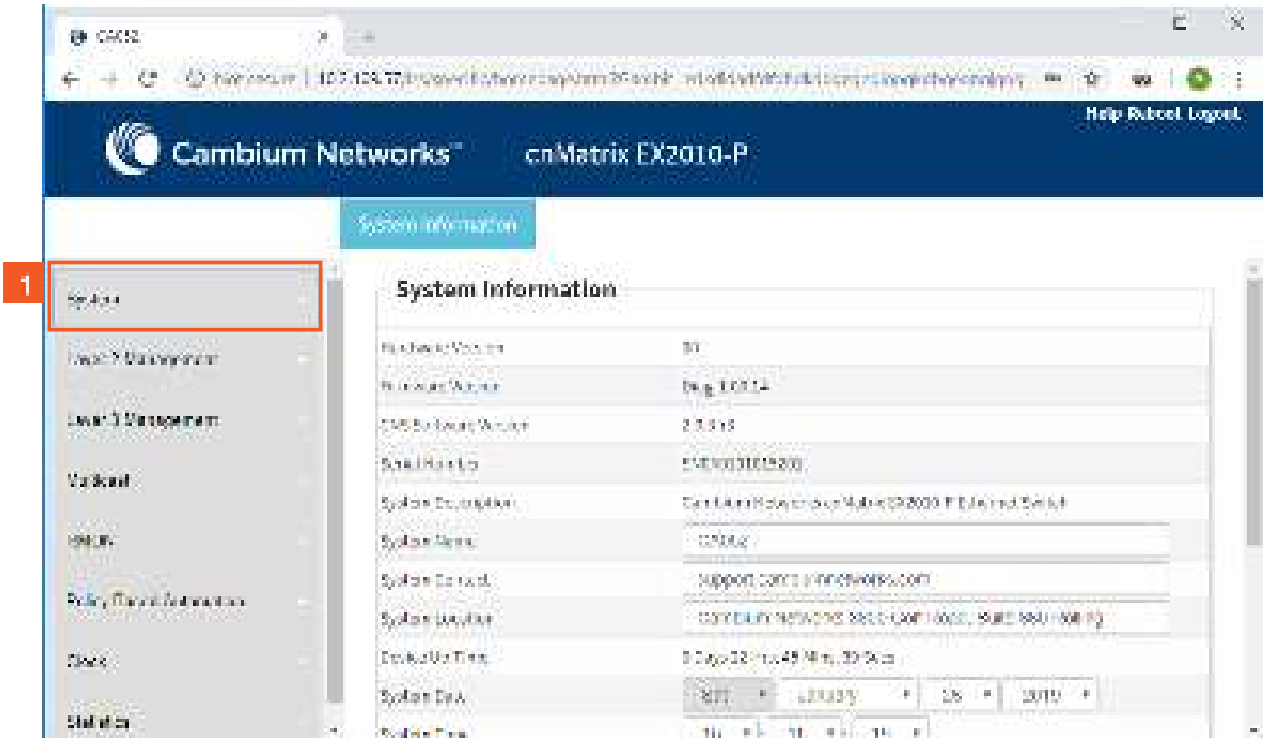
Prerequisites

- Network connectivity to a SNTP server.

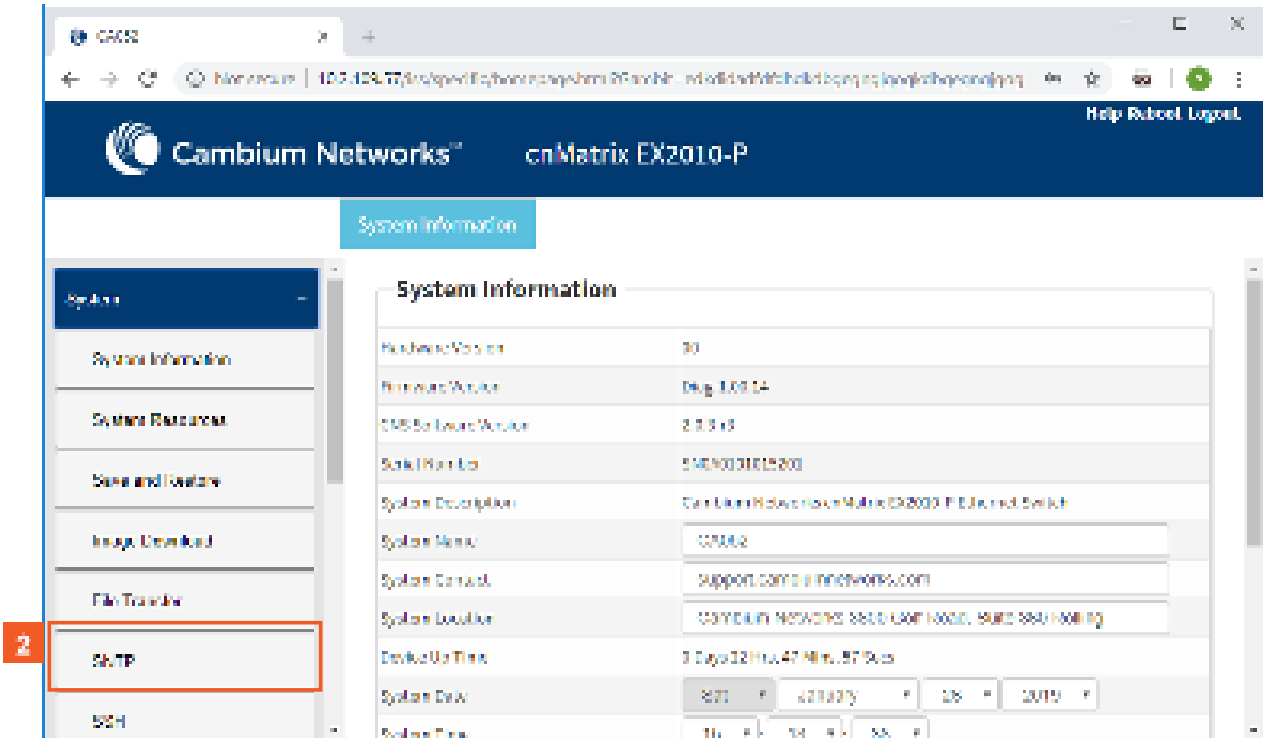
1.1.1.1.8 Network Diagram



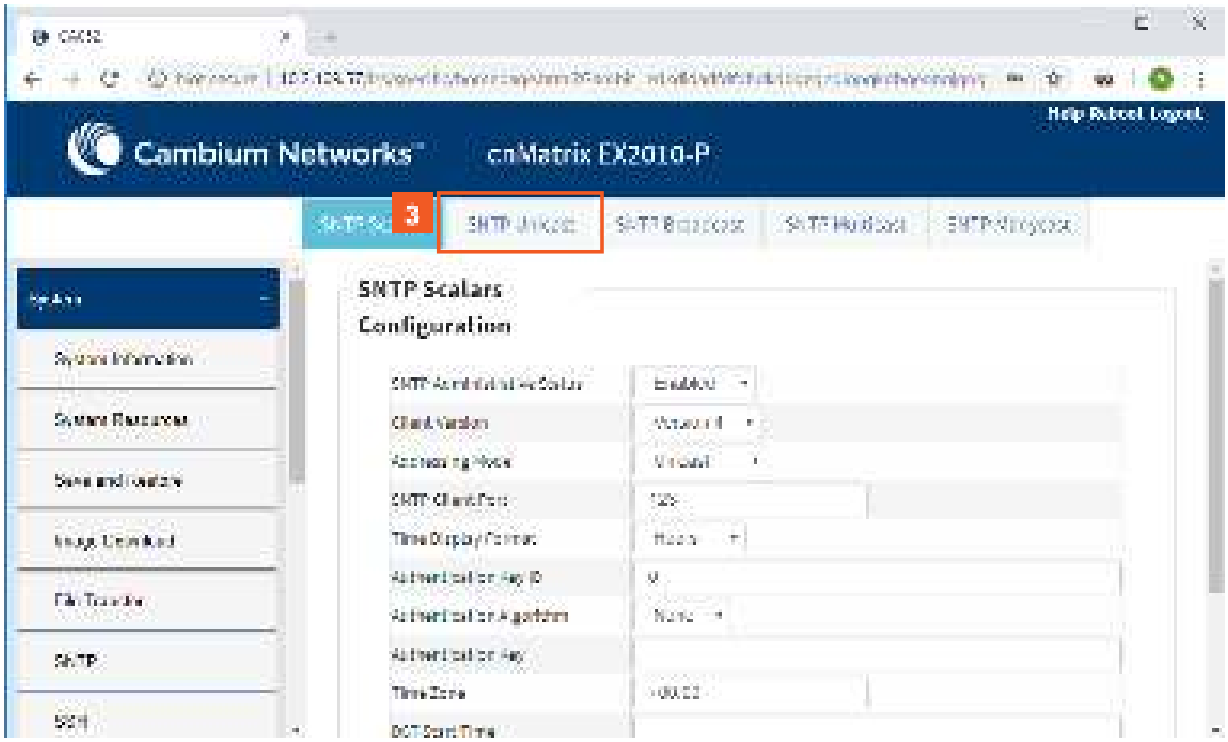
2.5.1.2 How to Enable and Configure SNTP in WEB Interface



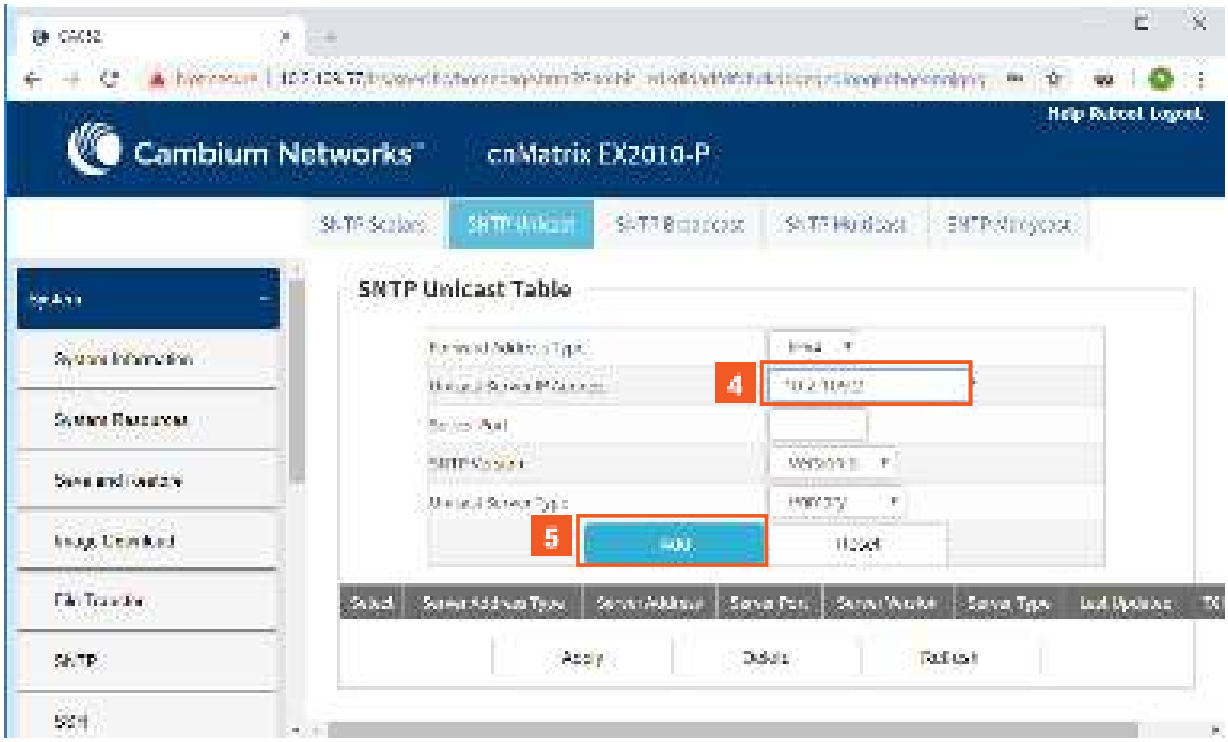
1 Click the **System** tab.



2 Click the **SNTP** menu item. The **SNTP Scalaras Configuration** window is displayed.



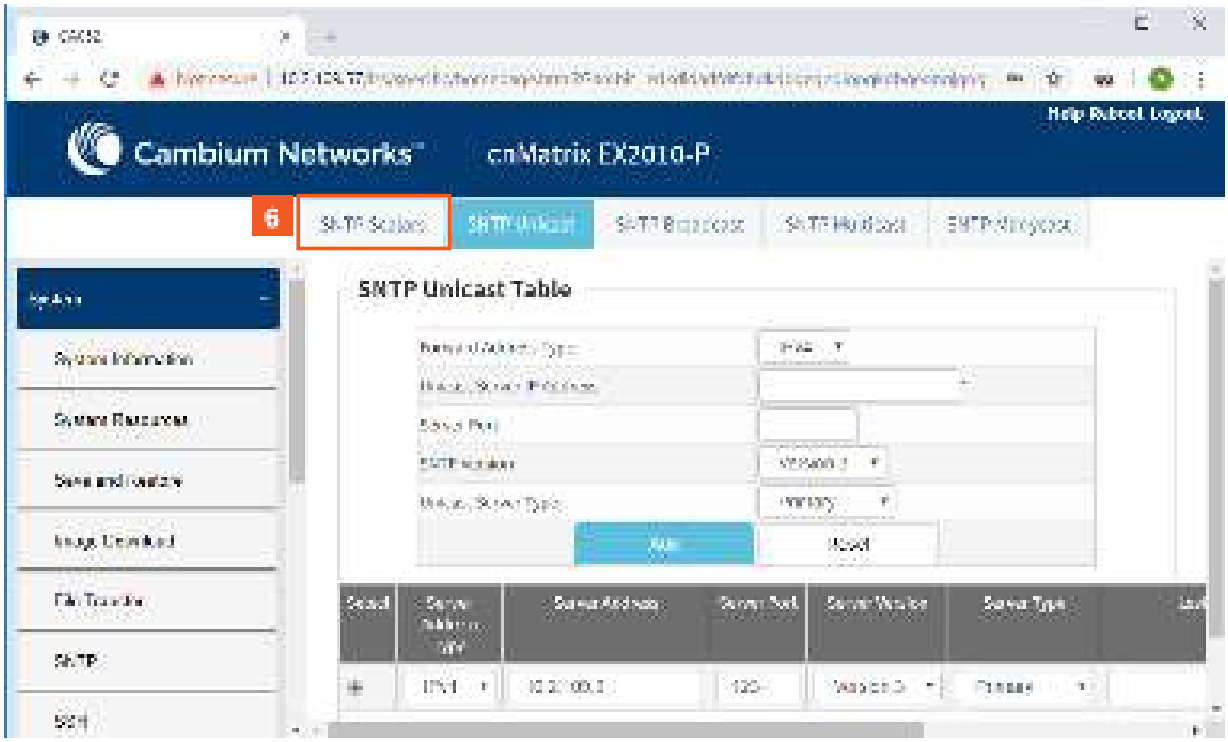
3 Click the **SNTP Unicast** tab. The **SNTP Unicast Table** window is displayed.



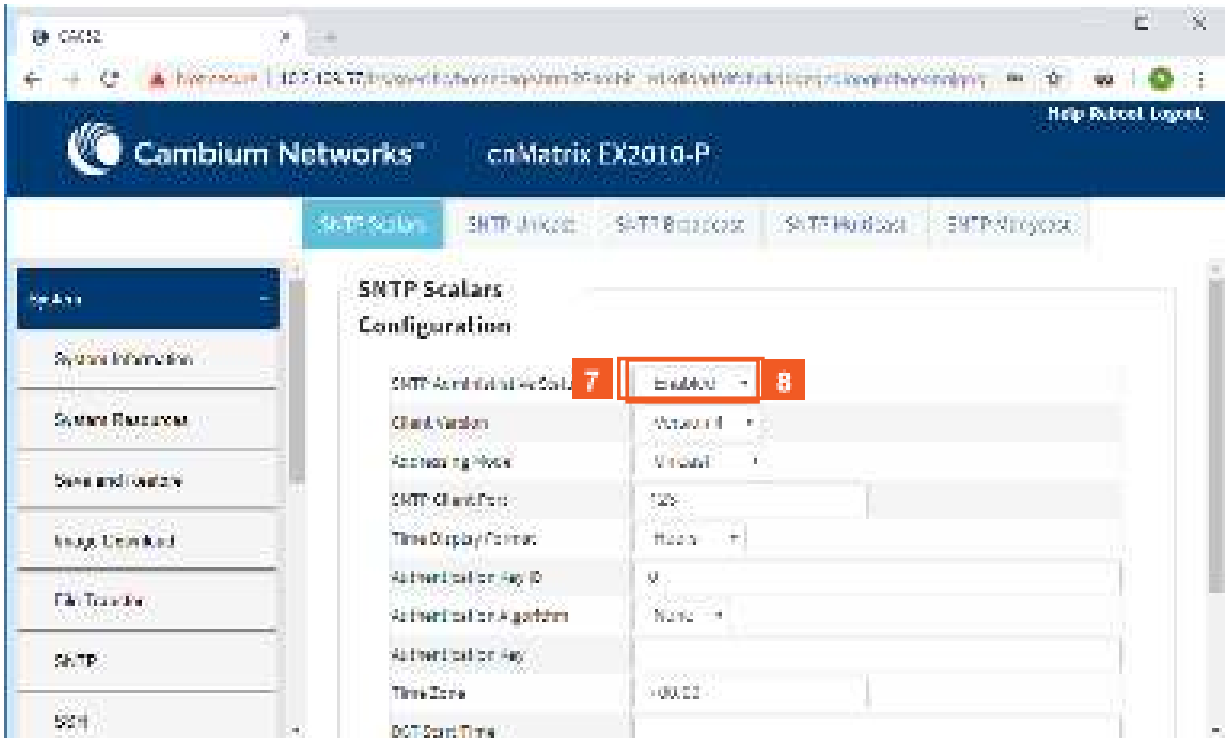
4 Type the value **10.2.109.2** into the **Unicast Server IP Address** field.

10.2.109.2 represents the unicast IPv4 server address.

5 Click the **Add** button.

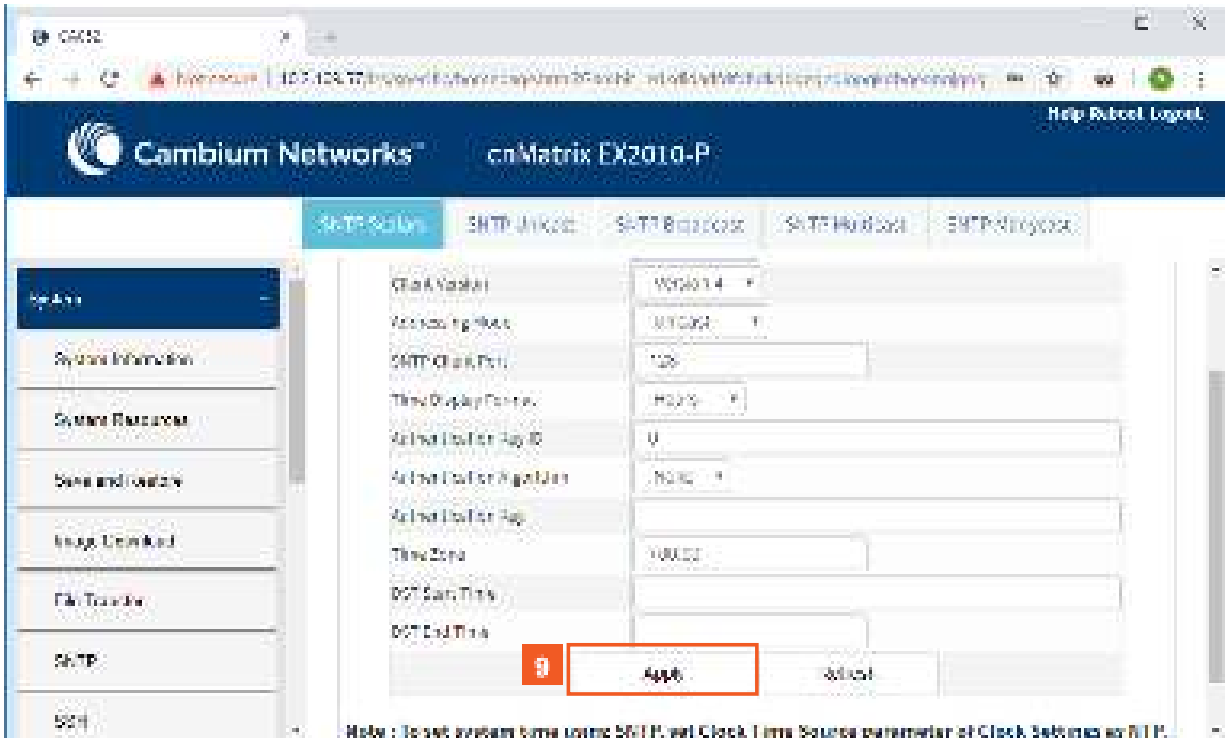


6 Click the **SNTP Scalars** tab. The **SNTP Scalars Configuration** window is displayed.

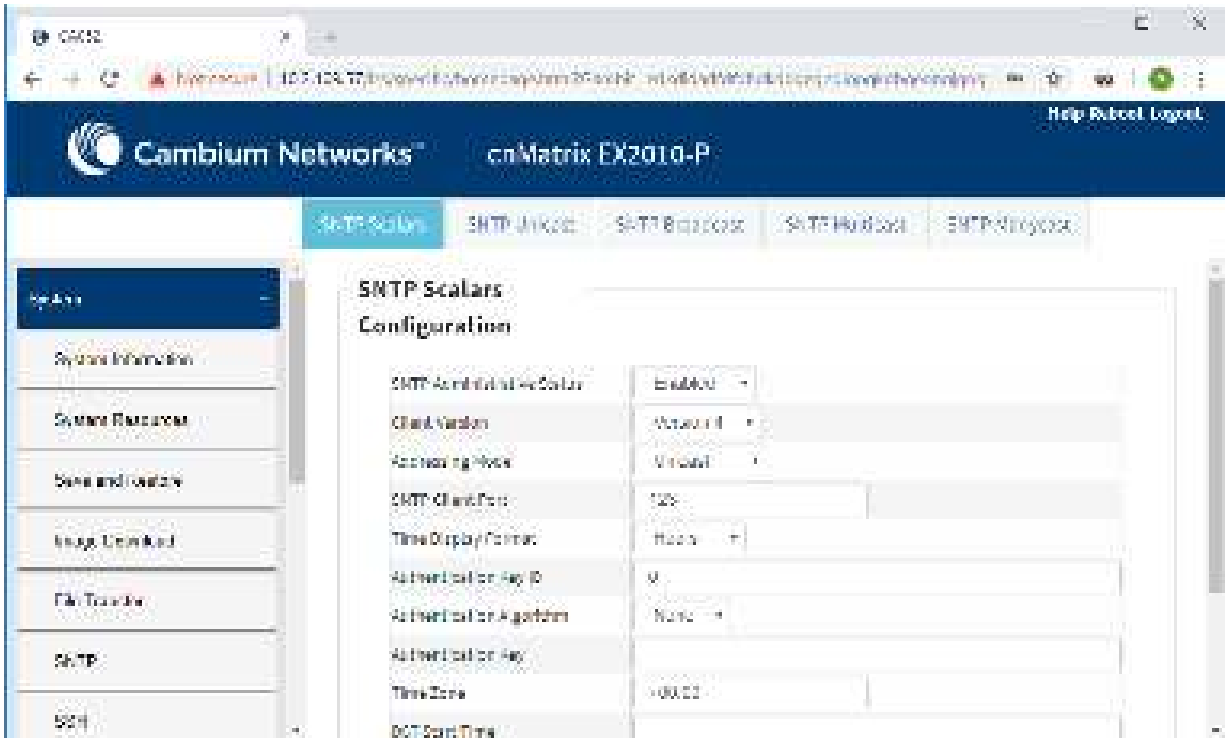


7 Click the **SNTP Administrative Status** drop-down list to select the SNTP client module status.

8 Select the **Enabled** list item.



9 Click the **Apply** button.



2.6 Port Settings Feature

2.6.1 Managing Negotiation

Feature Overview

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

Standards

N/A

Scaling Numbers

N/A

Limitations

- Fiber ports do not support auto-negotiation.

Default Values

- The negotiation setting is enabled by default.

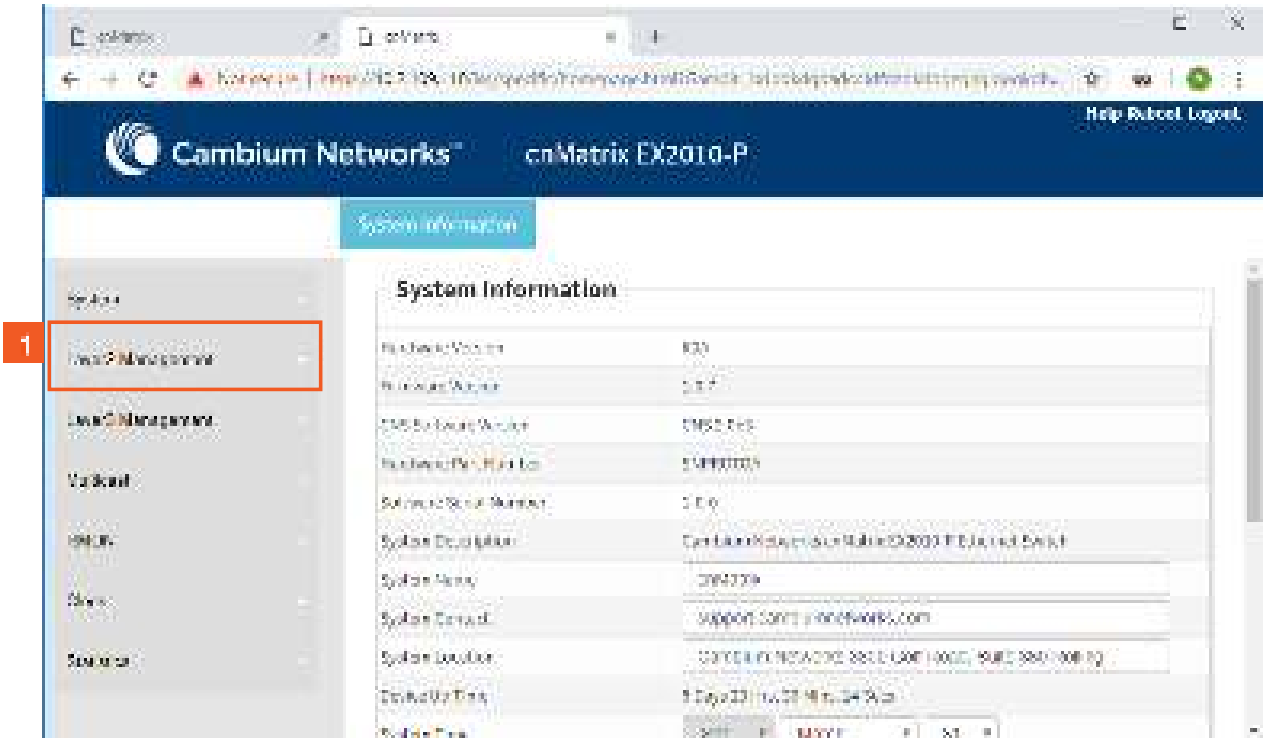
Prerequisites

- N/A

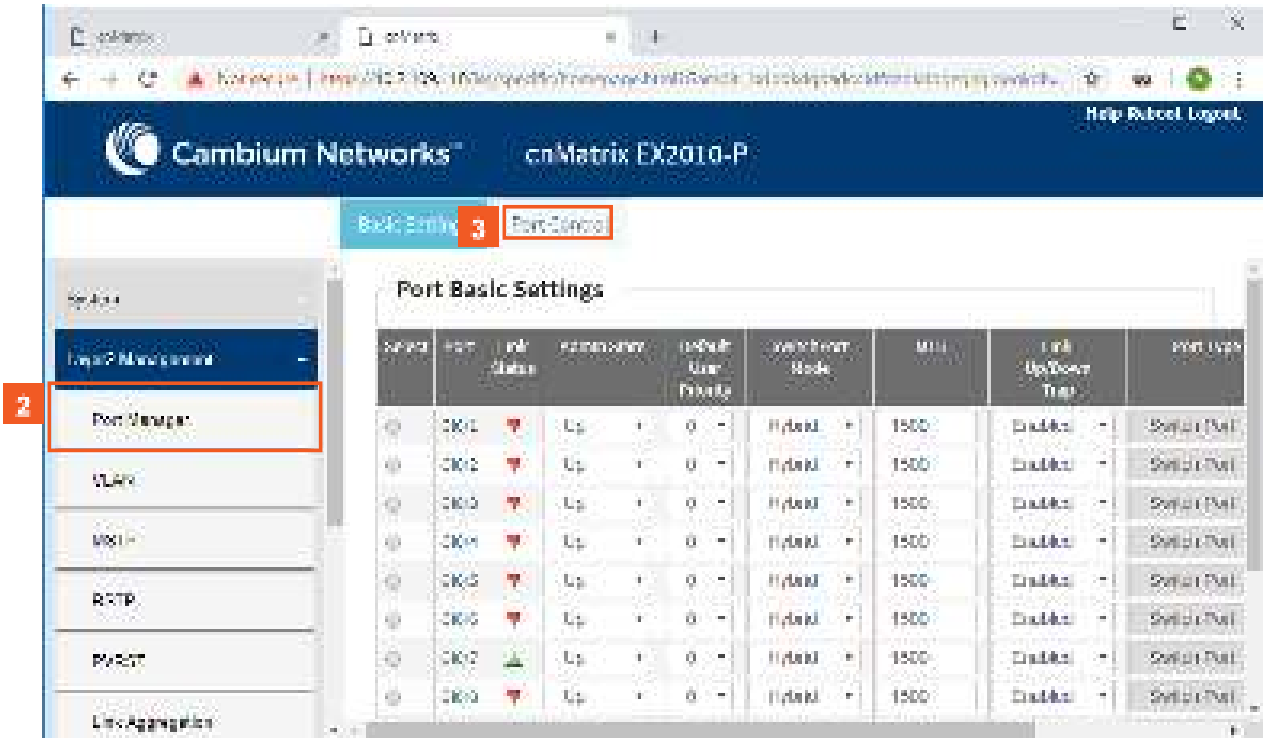
SNMP

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

2.6.2 How to Enable and Configure Negotiation in WEB Interface

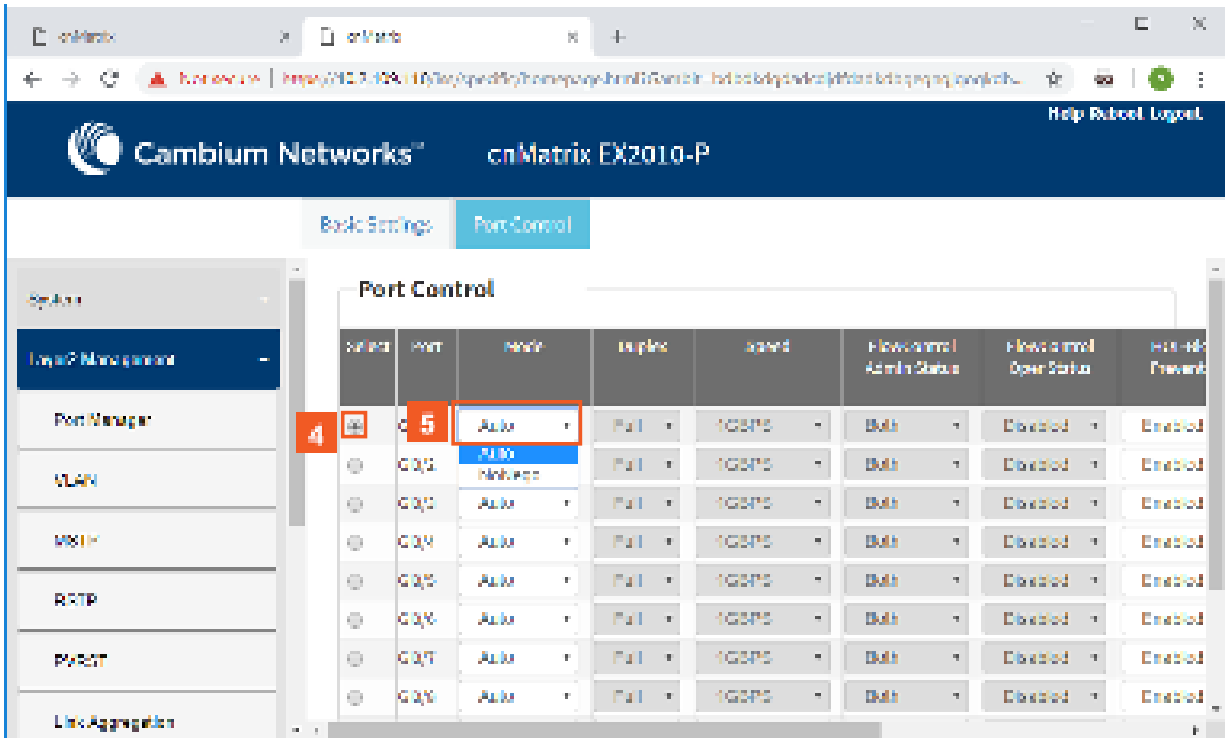


1 Click the **Layer2 Management** tab. The L2 Features are displayed.



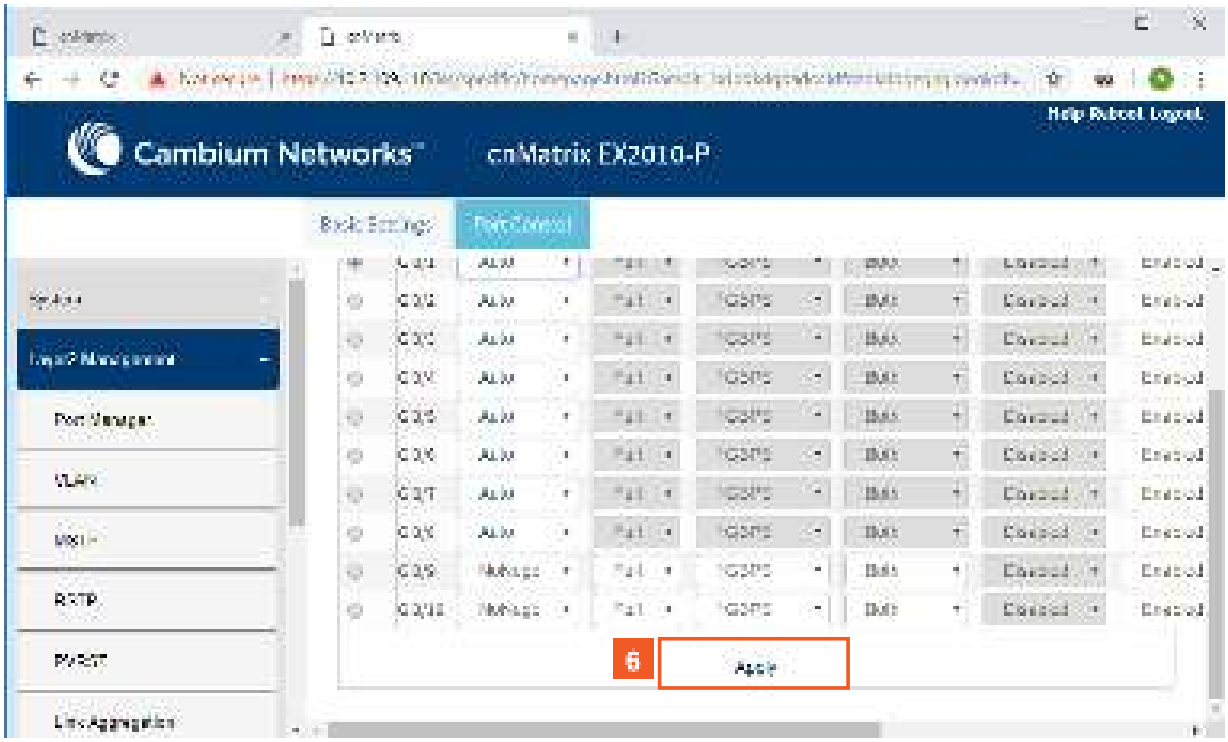
2 Click the **Port Manager** menu item.

3 Click the **Port Control** tab. The **Port Control** window is displayed.



4 Click the **Select** radio button and select the port for which the configuration needs to be done.

5 Click the **Mode** drop-down list to select the mode for negotiation of the port.Select the **Auto** list item.



6 Click the **Apply** button.

Section complete. Click X to close.

2.6.3 Managing Speed

Feature Overview

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

Standards

- N/A

Scaling Numbers

- N/A

Limitations

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

Default Values

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

Prerequisites

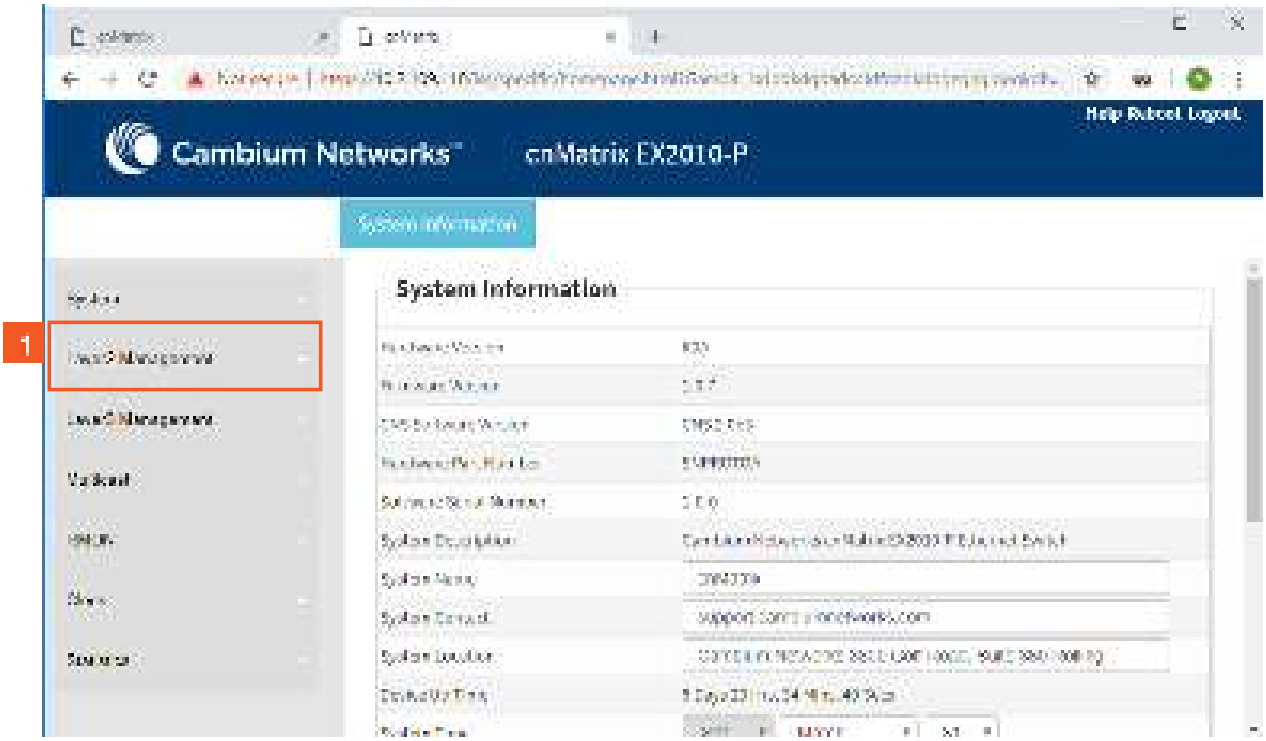
- N/A

SNMP

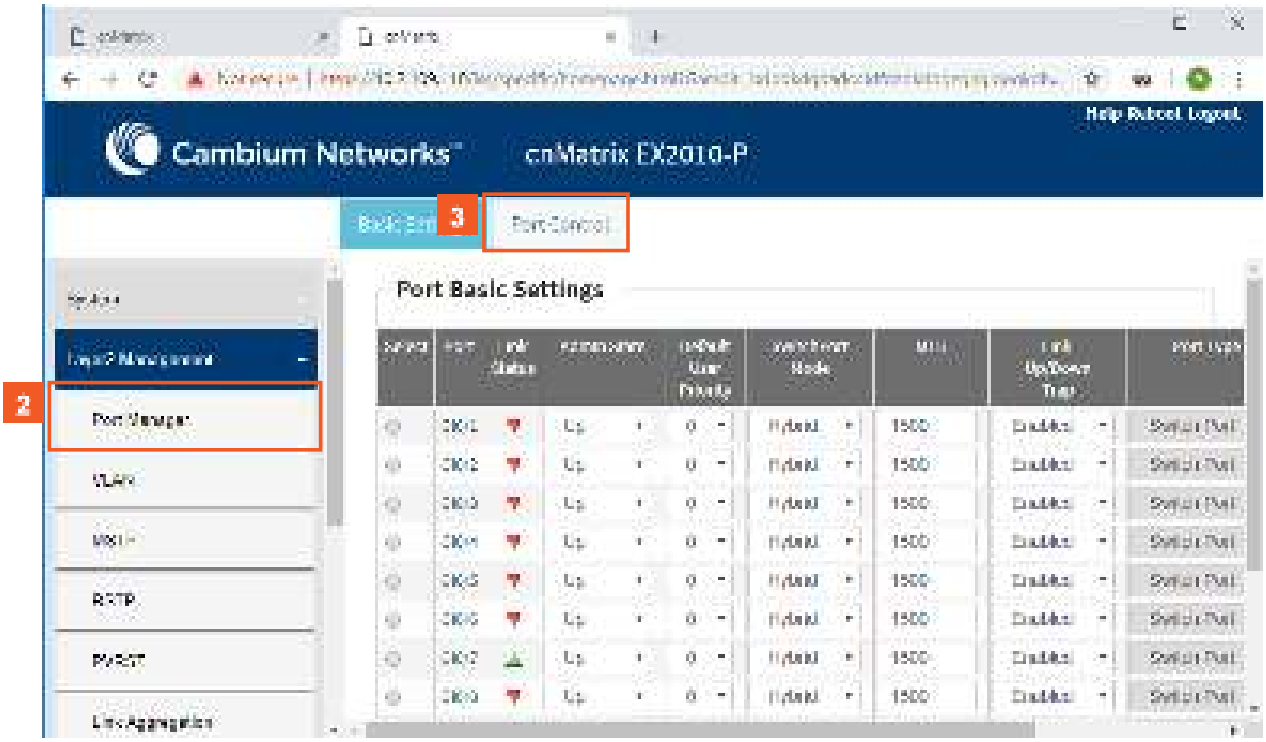
The object is called issPortCtrlSpeed and it is accompanied by an index which represents the port number. It is part of the issPortCtrlTable table.

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

2.6.4 How to Enable and Configure Speed in WEB Interface

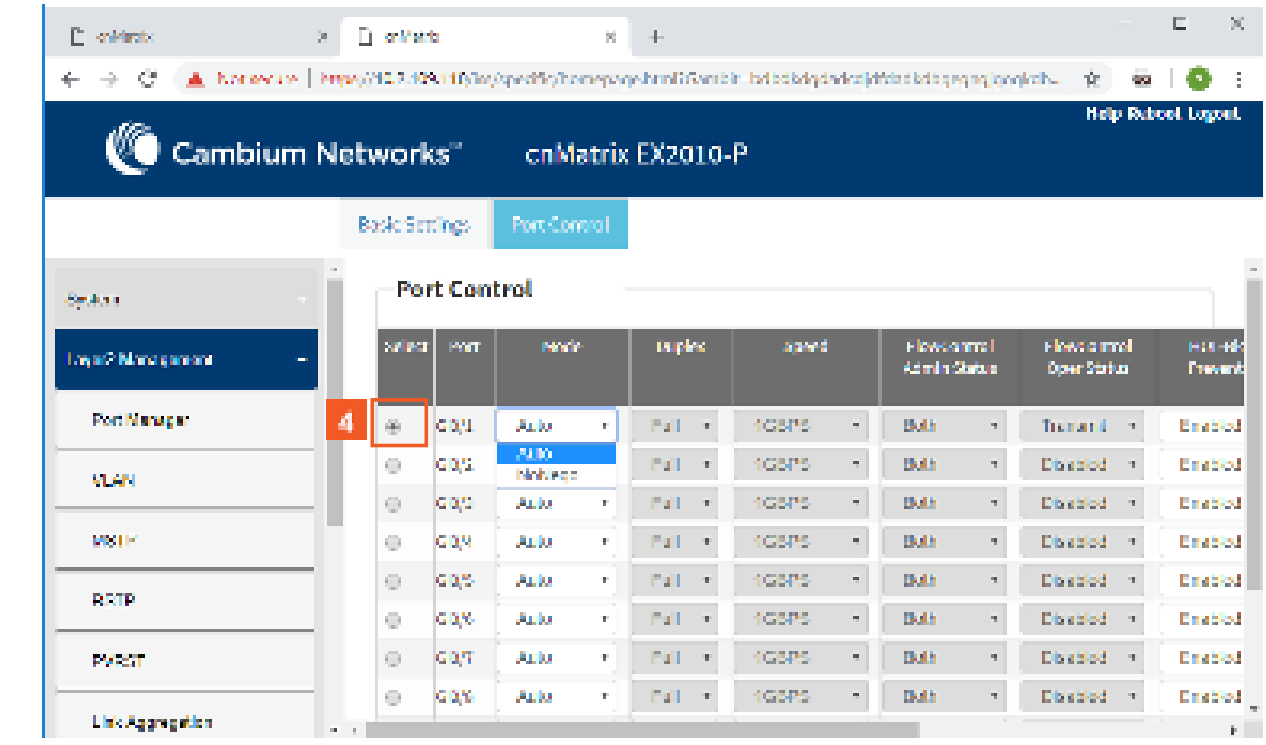


1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.

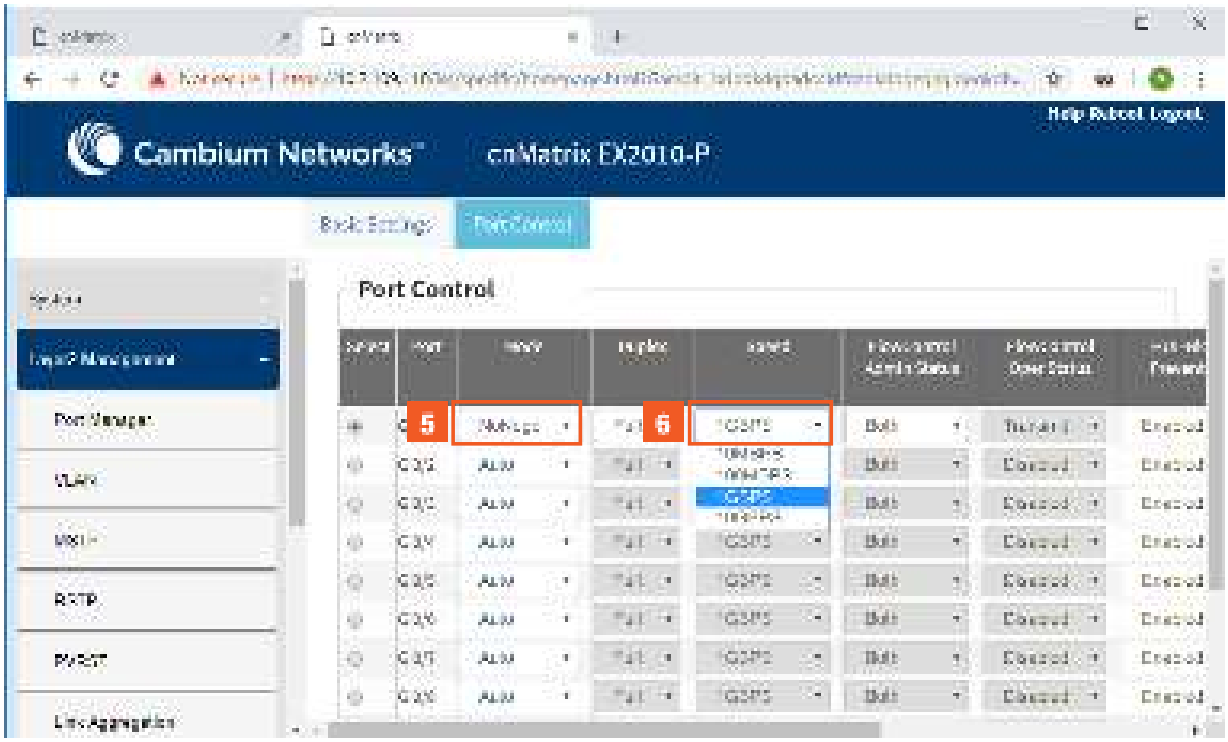


2 Click the **Port Manager** menu item.

3 Click the **Port Control** tab. The **Port Control** window is displayed.

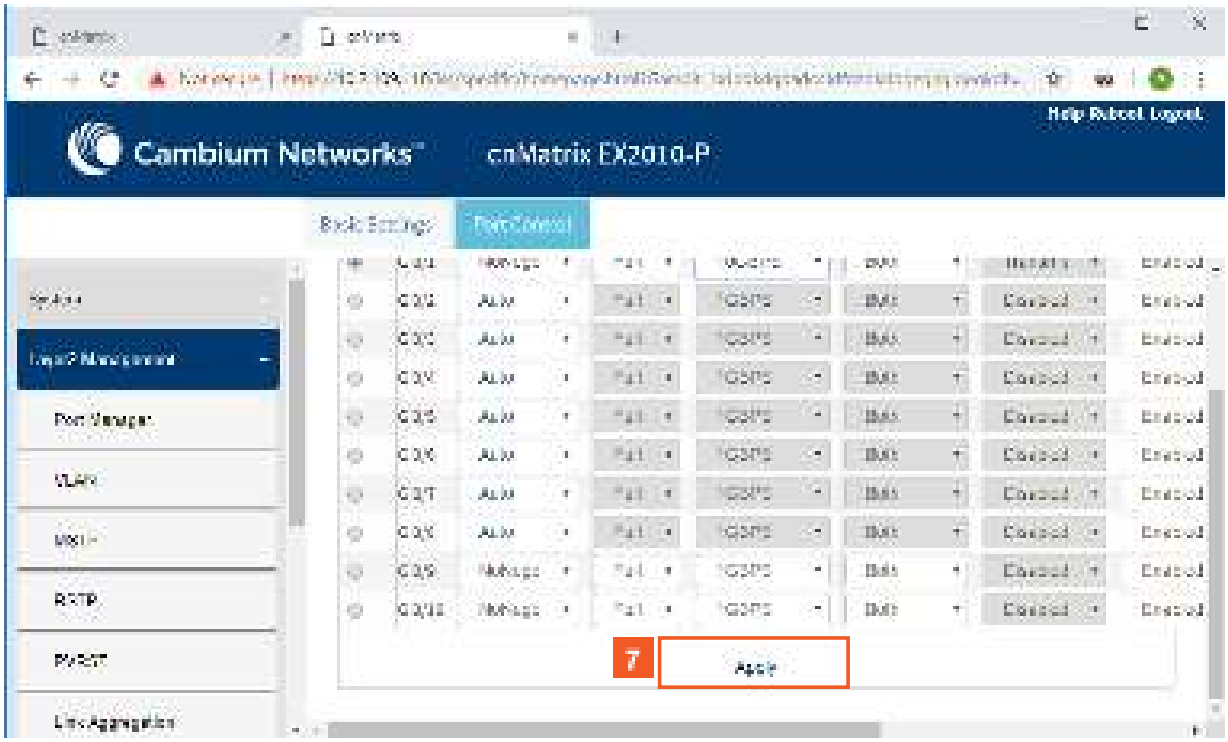


4 Click the **Select** radiobutton and select the port for which the configuration needs to be done. For example,**Gi0/1** radiobutton.



5 Click the **Mode** drop-down list to select the mode for the negotiation of the selected port. Select the **NoNego** list item.

6 Click the **Speed** drop-down list to select the speed of the interface. Select the **1GBPS** list item.



7 Click the **Apply** button.

2.6.5 Managing Duplex

Feature Overview

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

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

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

Limitations

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

Default Values

- The default value: full.

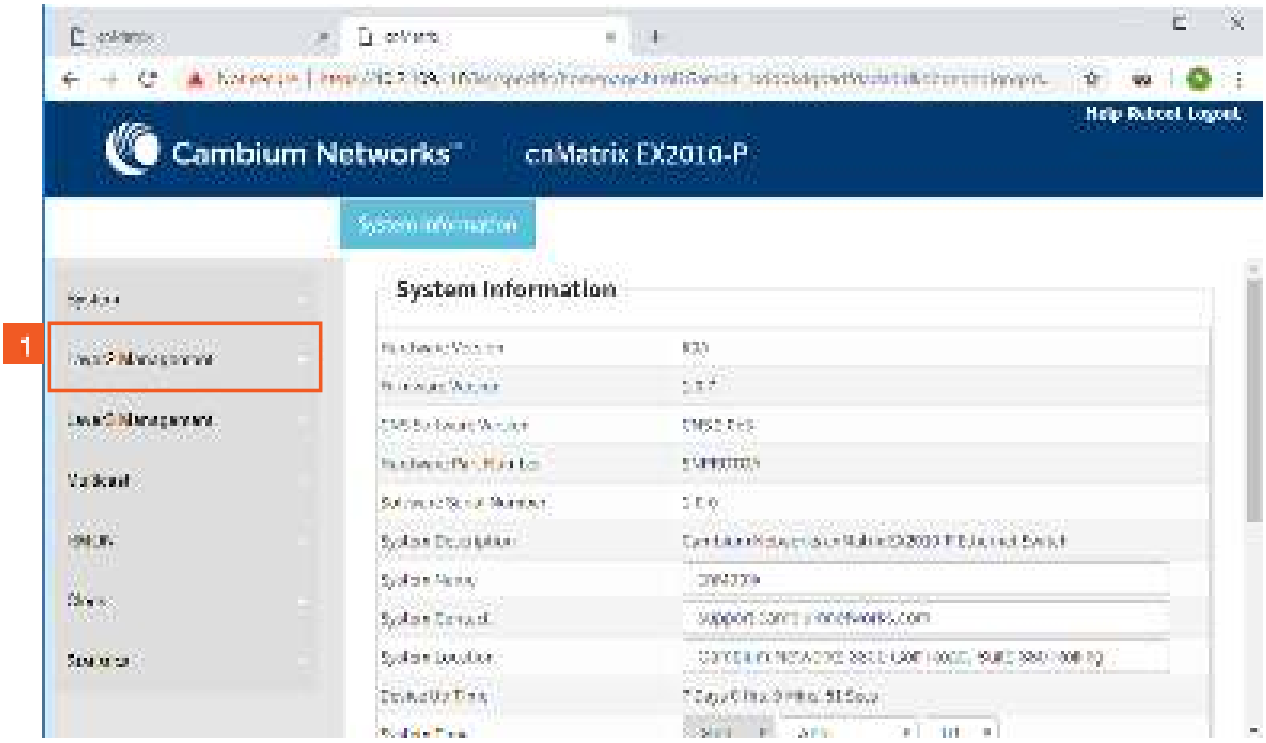
Prerequisites

- N/A

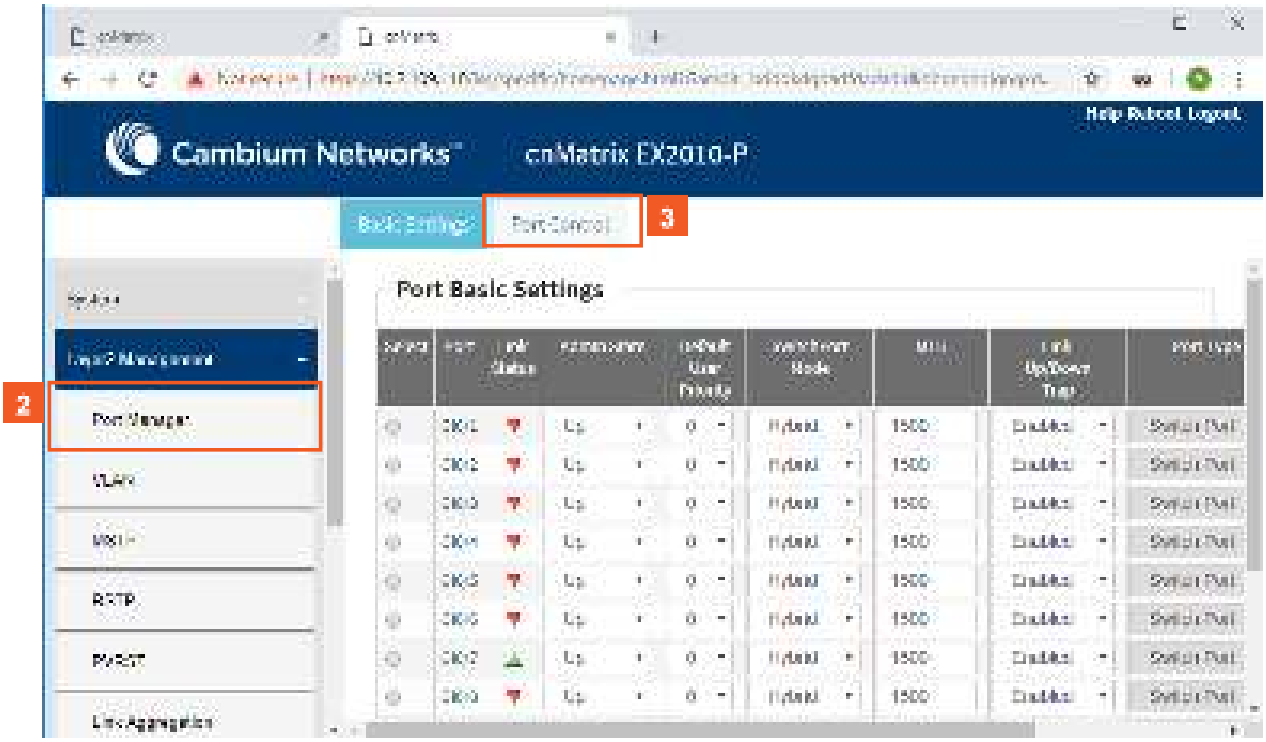
SNMP

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

2.6.6 How to Enable and Configure Duplex in WEB Interface

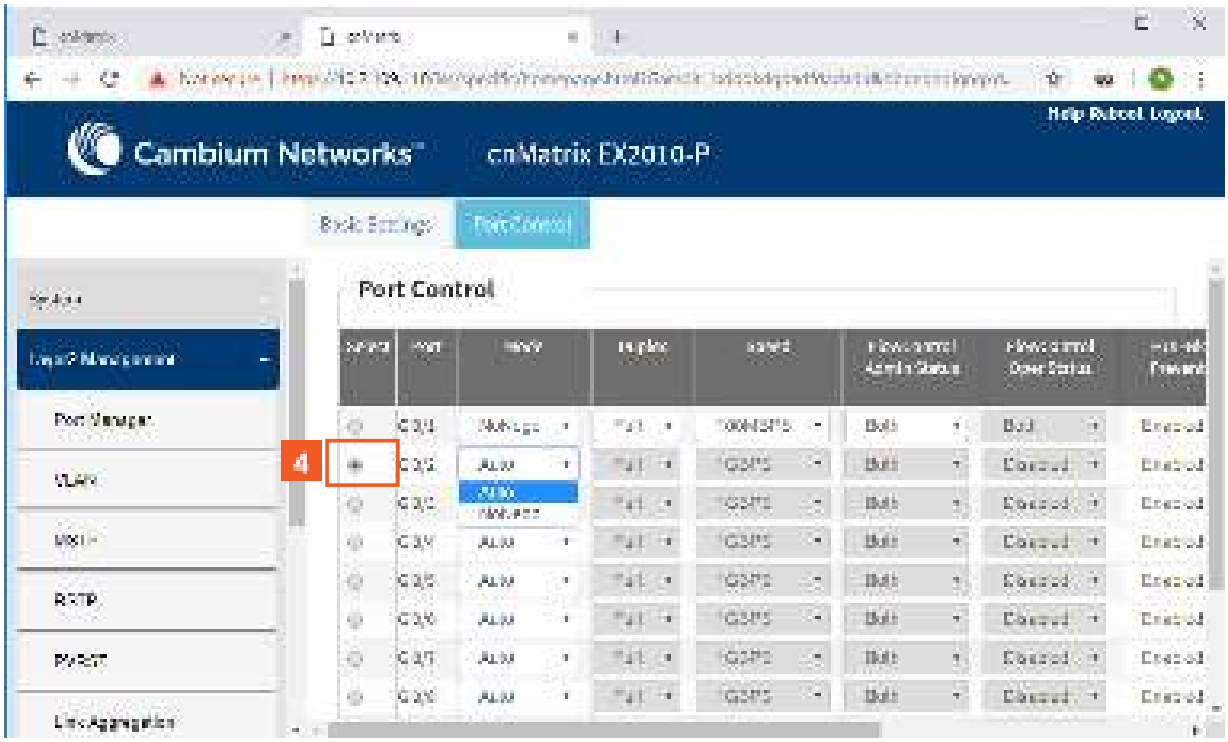


1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.

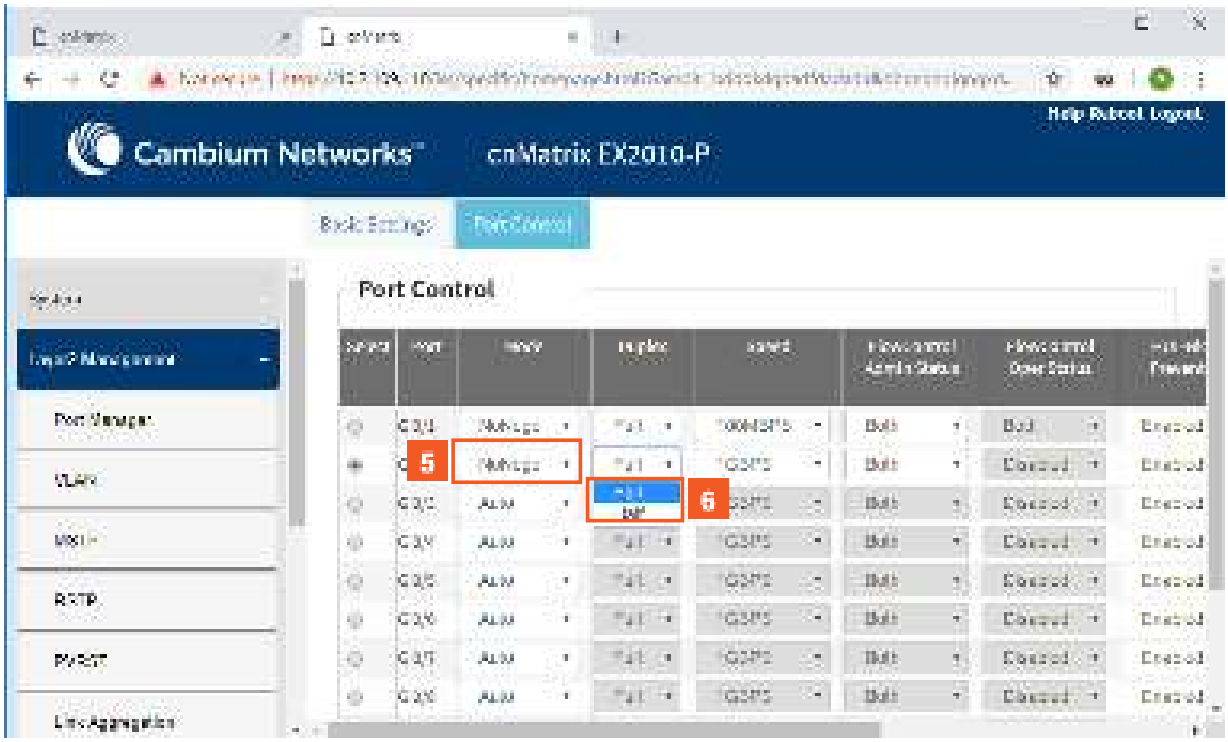


2 Click the **Port Manager** menu item.

3 Click the **Port Control** tab. The **Port Control** window is displayed.

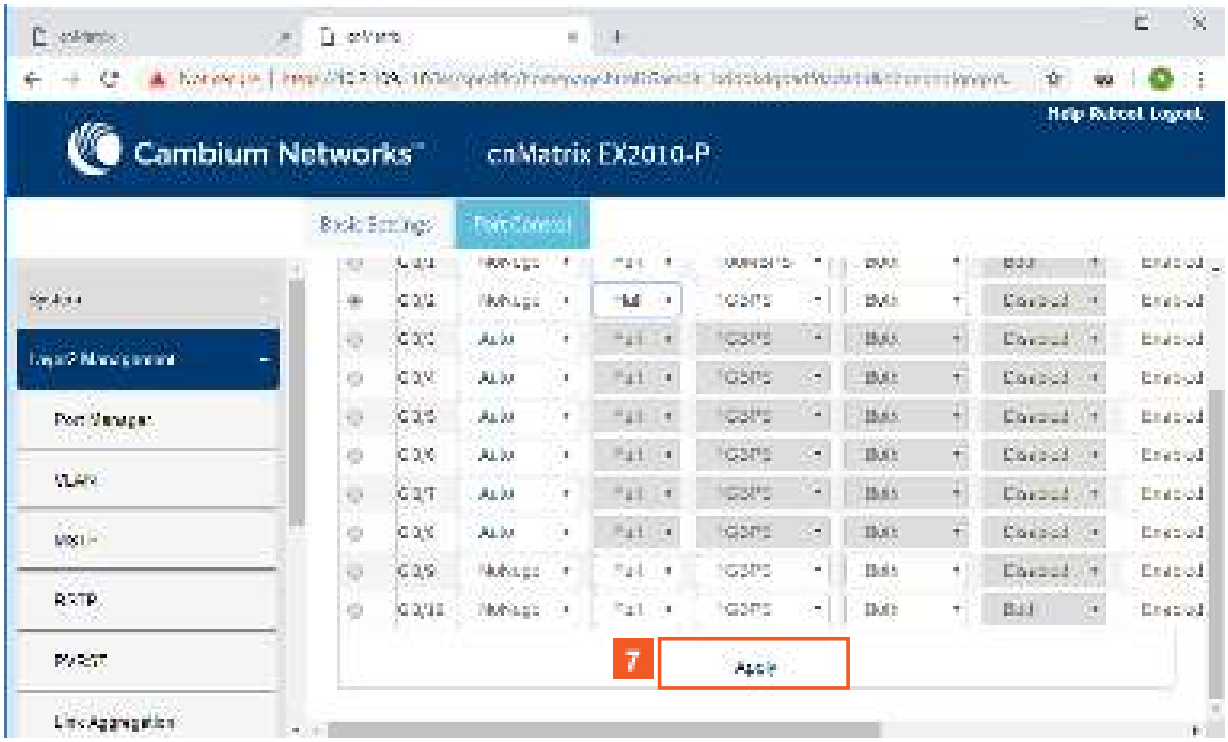


4 Click the **Select** radiobutton and select the port for which the configuration needs to be done.



5 Click the **Mode** drop-down list to select the mode for the negotiation of the port. Select the **NoNego** list item.

6 Click the **Duplex** drop-down list to select the flow of data through the port. Select the **Full** list item.



7 Click the **Apply** button.

2.6.7 Managing MTU

Feature Overview

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

Standards

- N/A

Scaling numbers

- N/A

Limitations

- N/A

Default Values

- The default MTU value: 1500 bytes.

Prerequisites

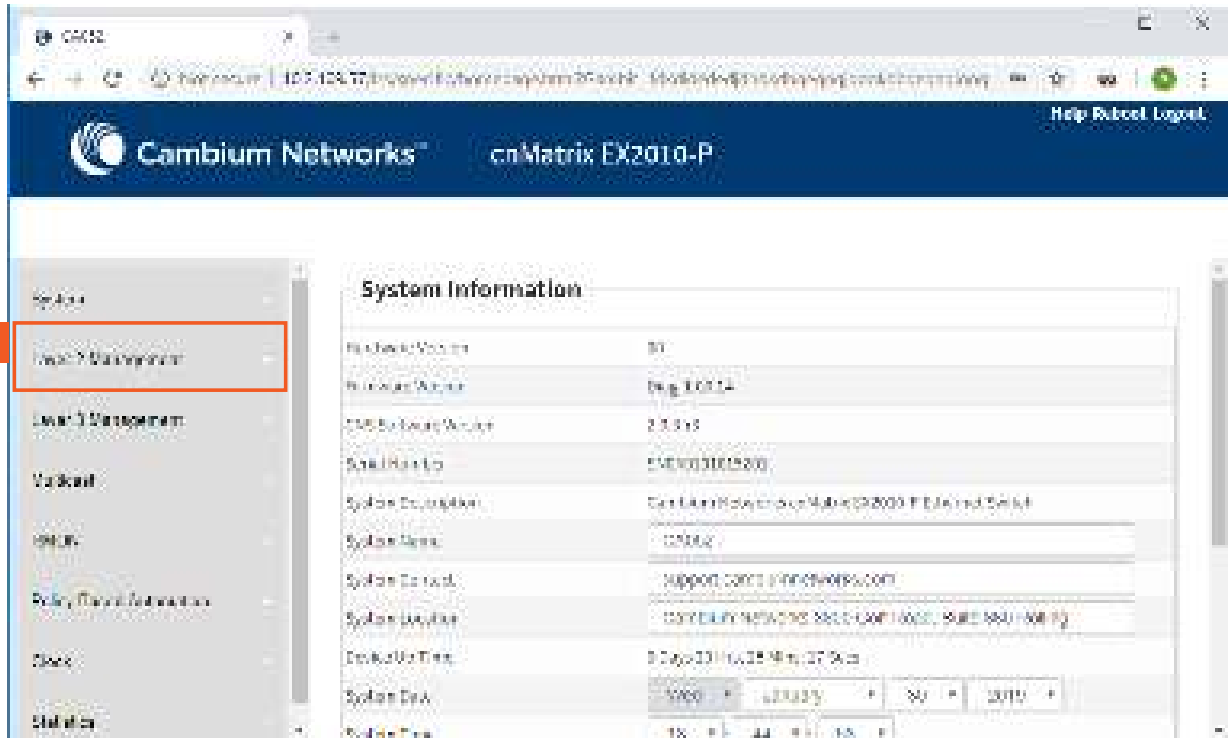
- N/A

SNMP

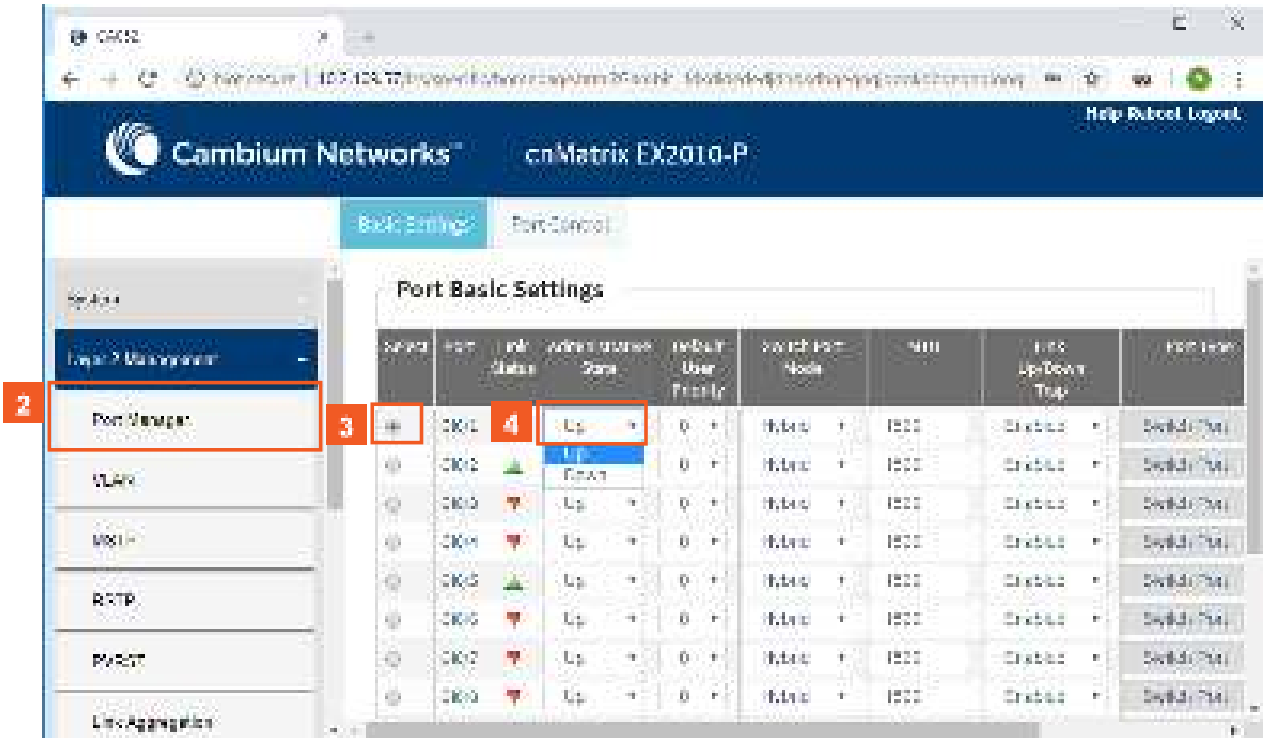
The object is called ifMainMtu, and it is accompanied by an index which represents the port number. It is part of the ifMainTable table.

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

2.6.8 How to Enable and Configure MTU (Maximum Transmission Unit) in WEB Interface



1 Click the **Layer2 Management** tab. The **L2 Features** are displayed

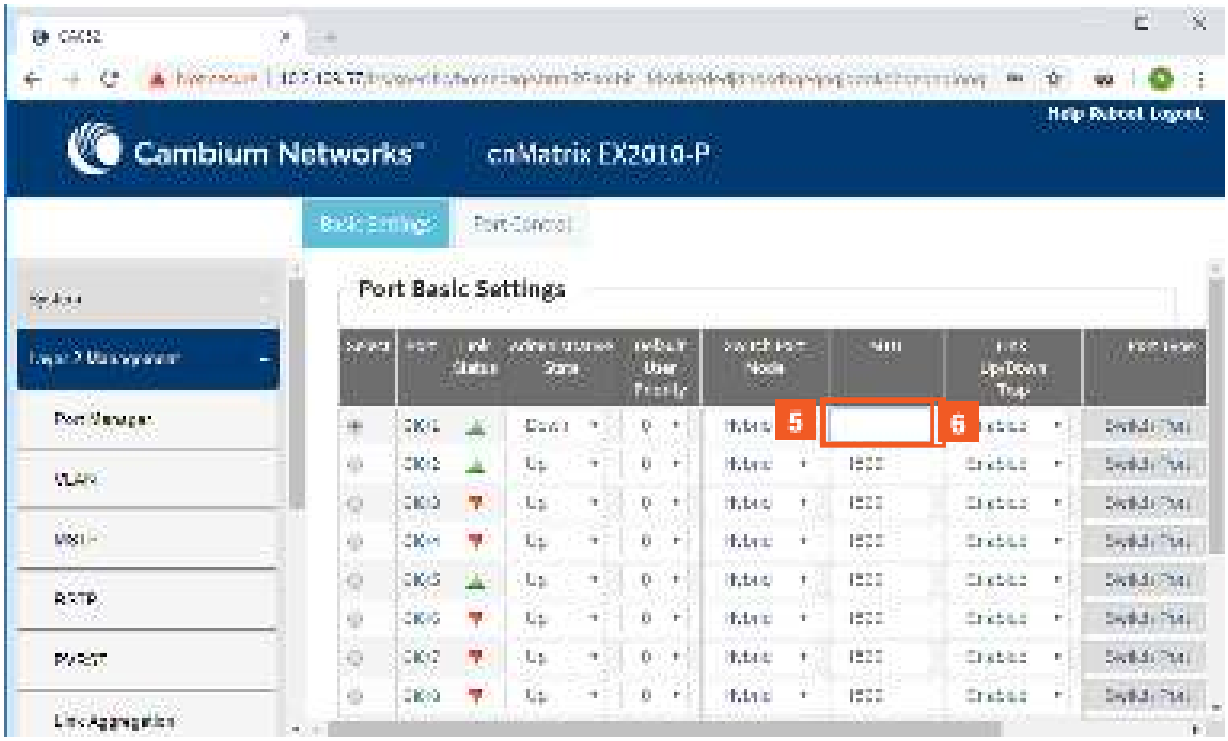


2 Click the **Port Manager** menu item.

3 Click the **Select** radio button and select the port for which the configuration needs to be done.

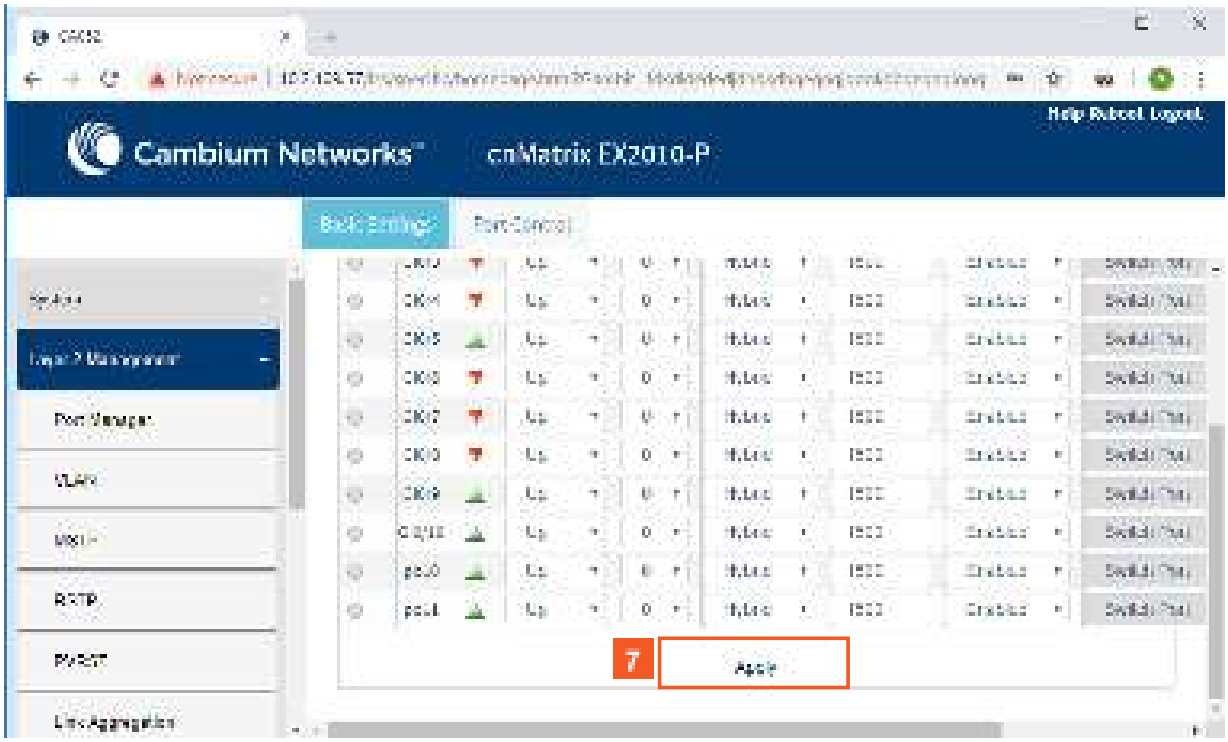
Make sure that the selected port is not part of the port channel group.

4 Click the **Administrative State** drop-down list to select the desired state of the port. Select the **Down** list item.



5 In the **MTU** column, type the maximum transmission unit frame size MTU for the interface.

6 Type the value **1000** into the **MTU** field.



7 Click the **Apply** button.

2.6.9 Managing Flow Control

Feature Overview

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

Standards

- IEEE 802.3x

Scaling Numbers

- N/A

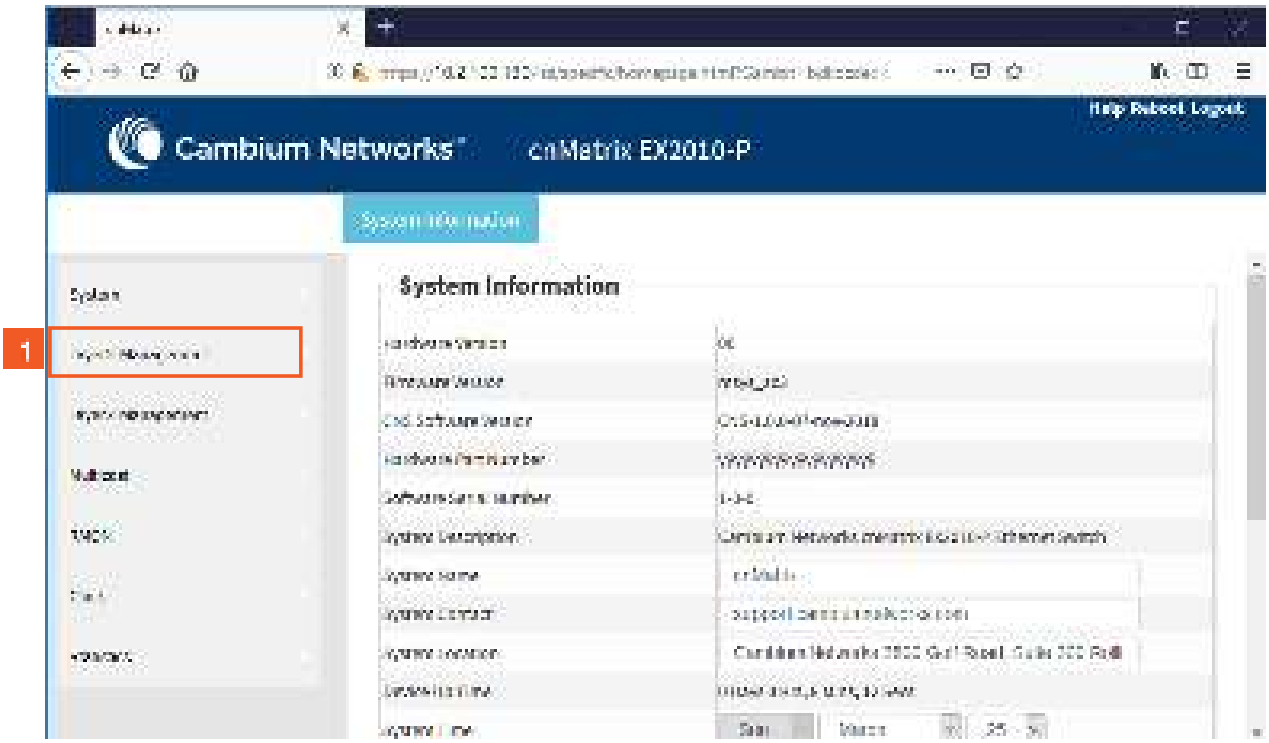
Limitations

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

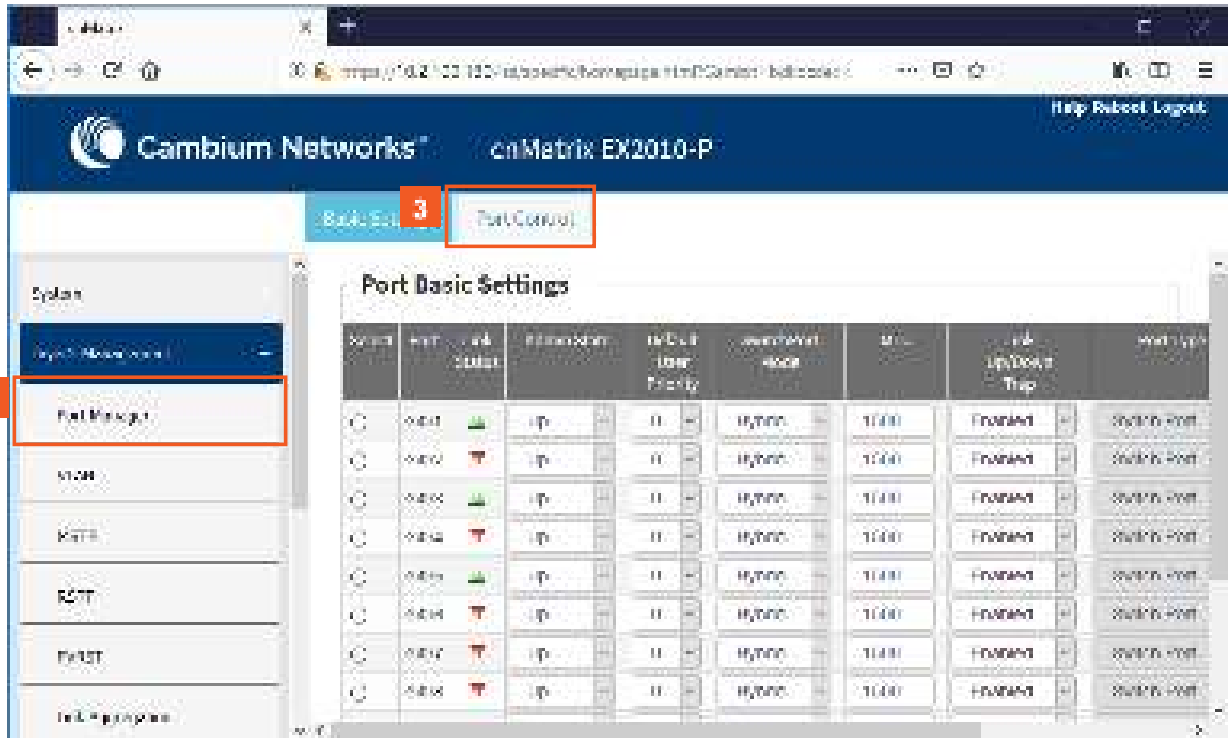
Default Values

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

2.6.10How to Enable and Configure Flow Control in WEB Interface

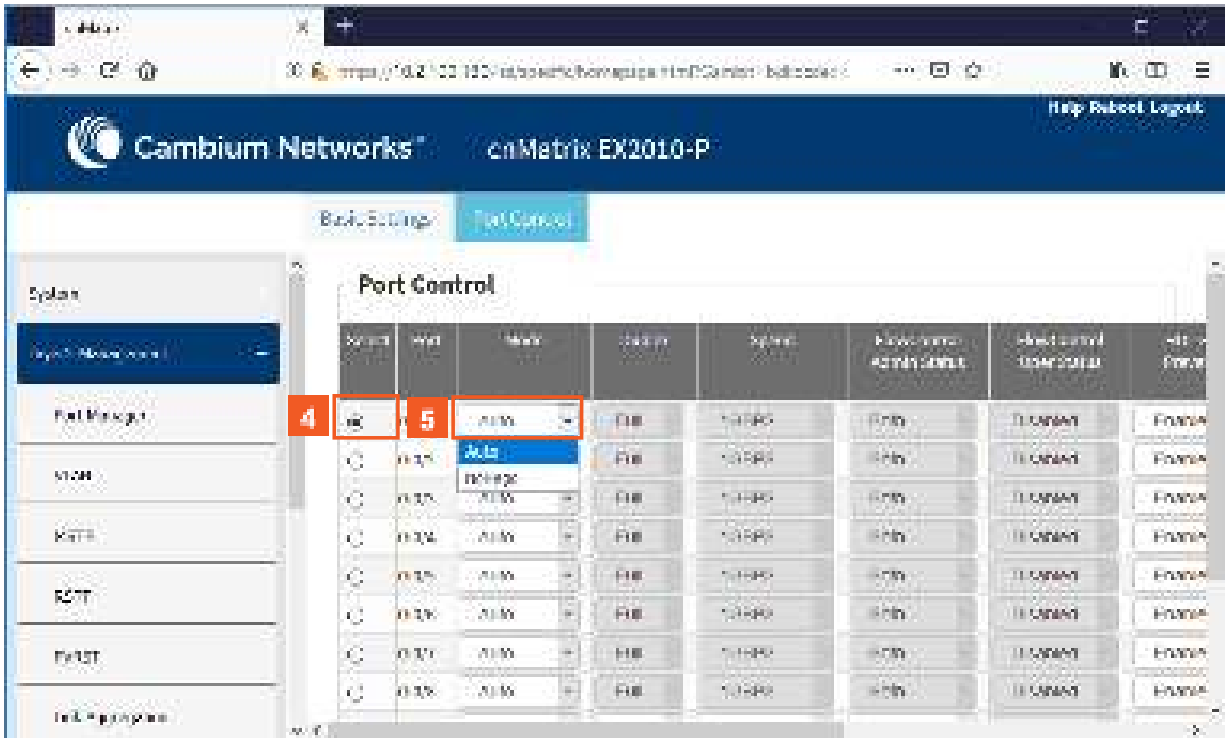


1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.



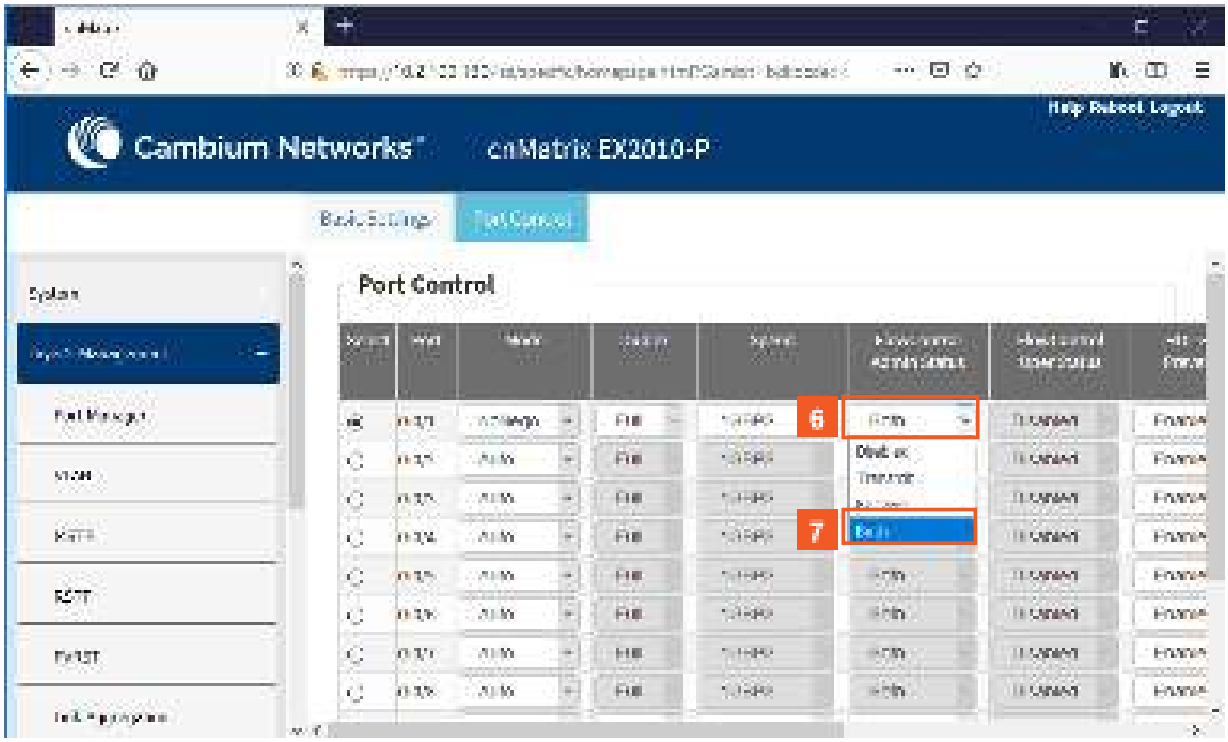
2 Click the **Port Manager** menu item.

3 Click the **Port Control** tab. The **Port Control** window is displayed.



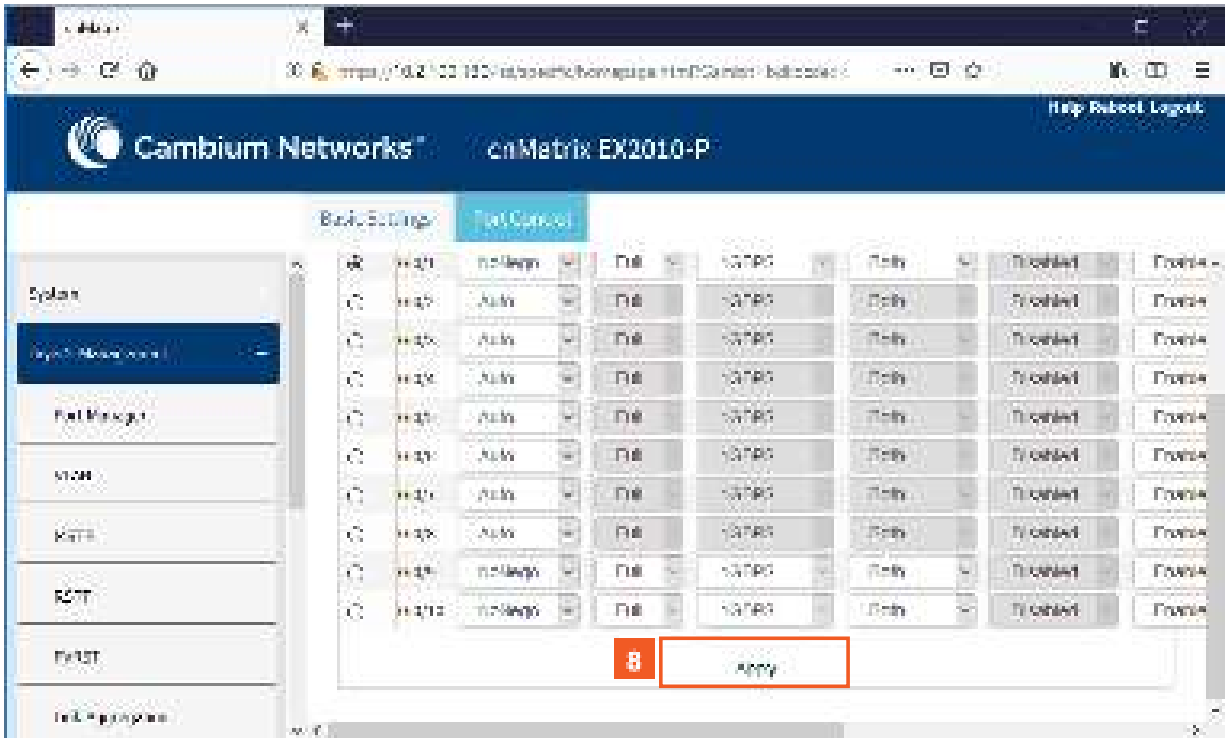
4 Click the Select radiobutton and select the port for which the configuration needs to be done. For example, Click the **Gi0/1** radiobutton.

5 Click the **Mode** drop-down list to sleect the mode for the negotiation of the port. Select the **Auto** list item.



6 Click the **FlowControl Admin Status** drop-down list to select from the default administrative pause mode for the interface.

7 Select the **Both** list item.



8 Click the **Apply** button.

Section complete. Click X to close

2.7 Link Aggregation

2.7.1 Managing Link Aggregation

2.7.1.1 Feature Description

Feature Overview

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

Standards

- IEEE 802.3ad

Scaling Numbers

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

Limitations

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

Default Values

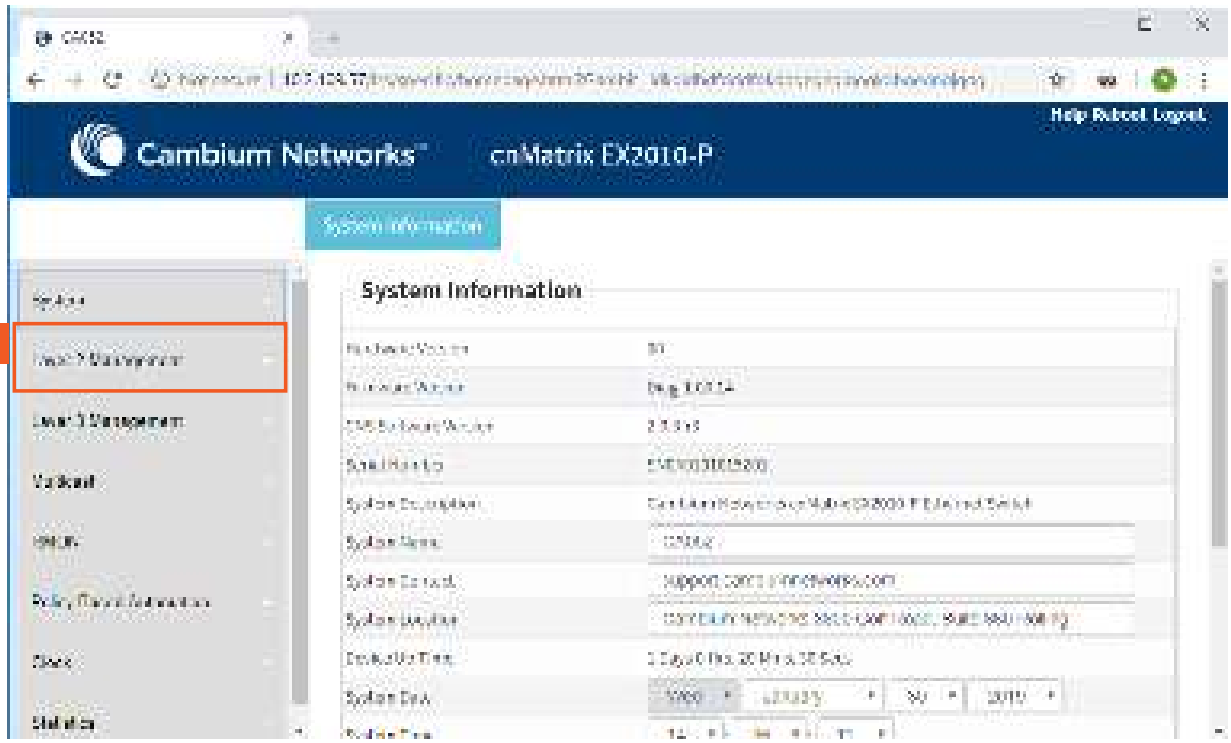
- The Link Aggregation feature is enabled by default.
- The admin status of the Link Aggregation Status in the switch is disabled by default.
- The default LACP wait-time: 2.
- The default LACP timeout period: long.
- The default LACP rate: normal.

Prerequisites

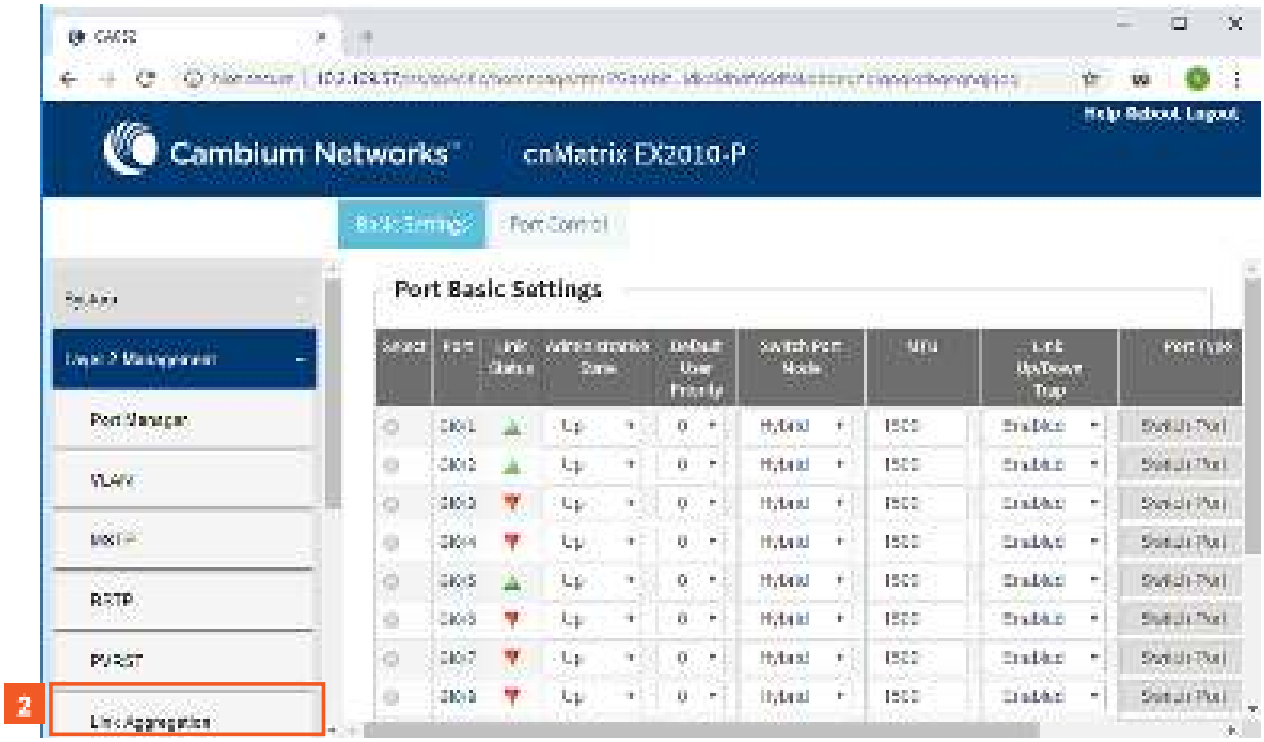
N/A

2.7.1.2 Network Diagram

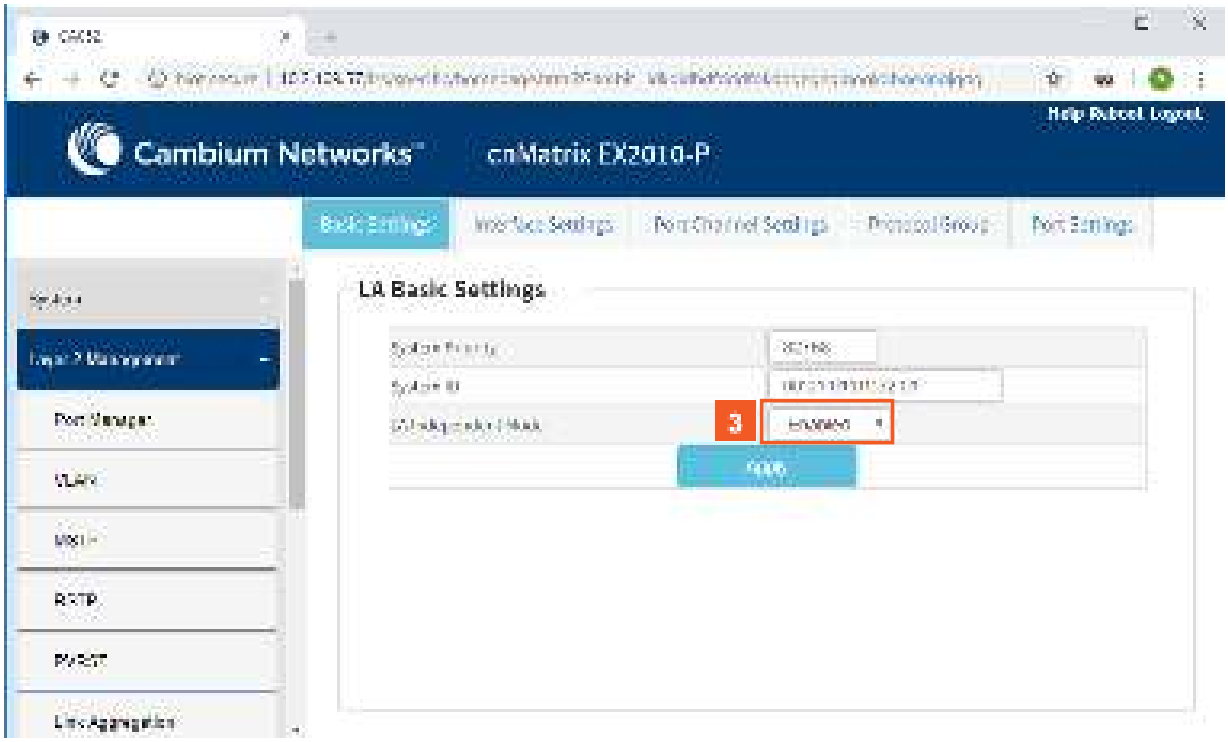
2.7.2 How to Enable Link Aggregation in WEB Interface



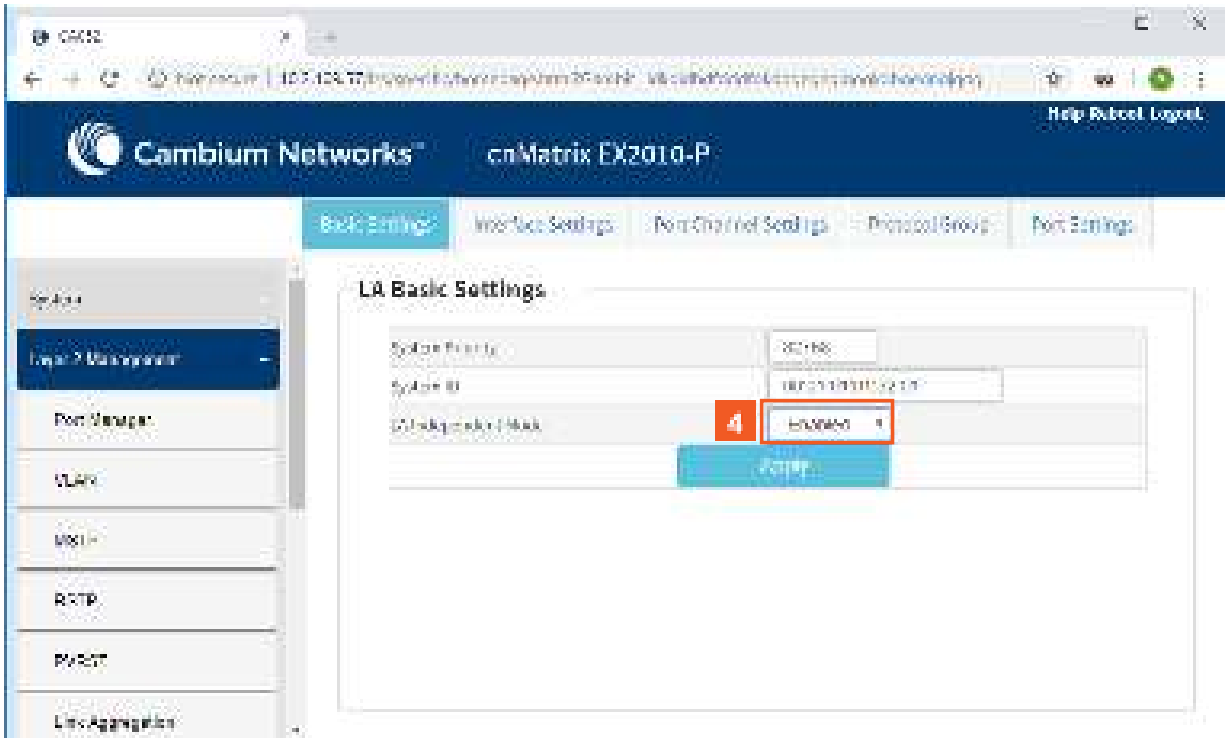
1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.



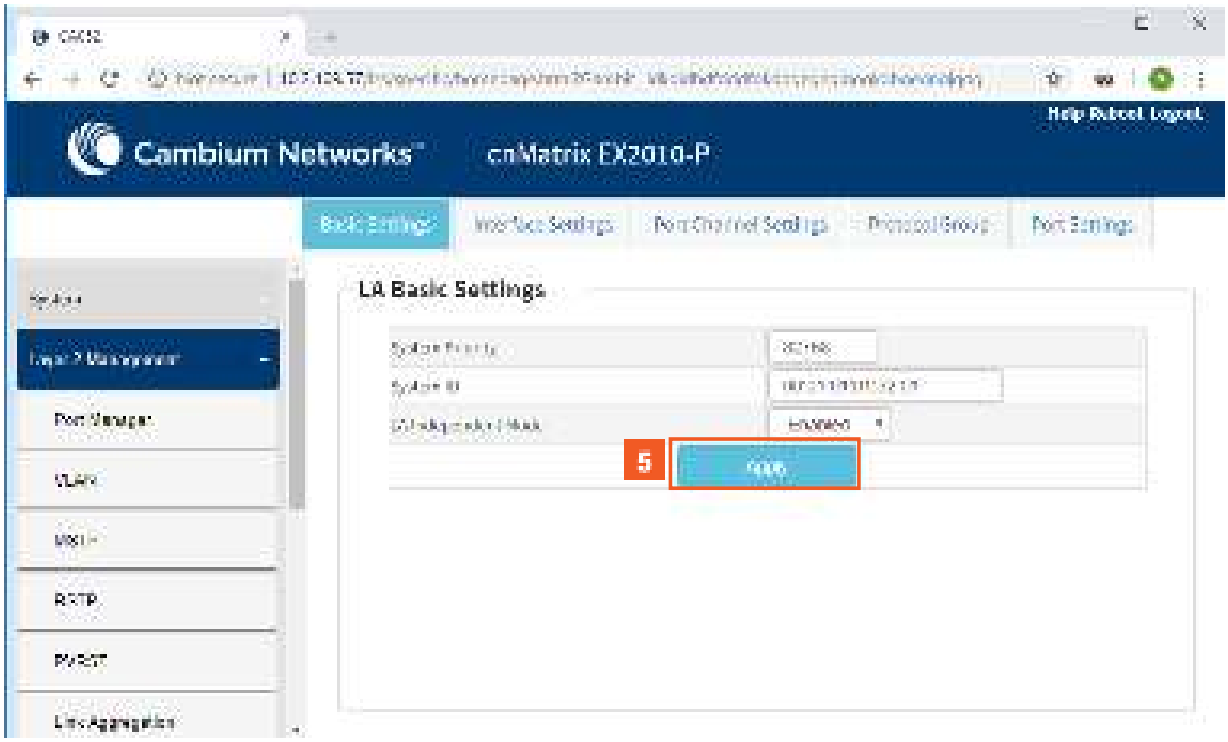
2 Click the **Link Aggregation** menu item.



3 Click the **LA Independent Mode** drop-down list and select the independent mode of the Link Aggregation module.



4 Select the **Enabled** list item.



5 Click the **Apply** button.

2.8 Private VLAN Edge

2.8.1 Managing Private VLAN Edge

2.8.1.1 Feature Description

When a port has protected status, it no longer forwards any L2 traffic (unicast, multicast, broadcast) to any other port that is also protected and on the same switch. The **Private VLAN Edge** feature enables you to control the flow of the Layer 2 traffic.

Standards

- N/A

Scaling Numbers

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

Limitations

- N/A

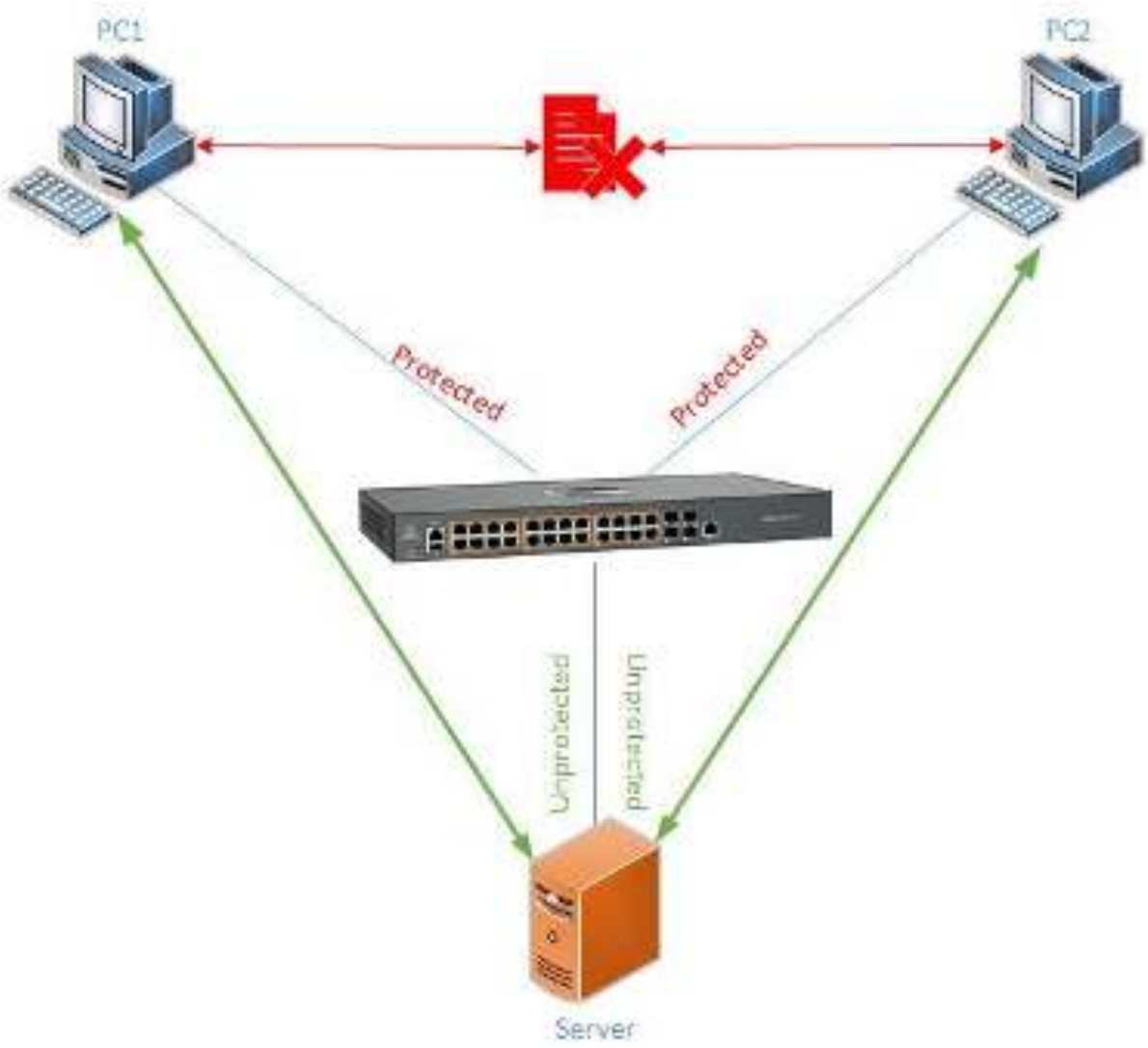
Default Values

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

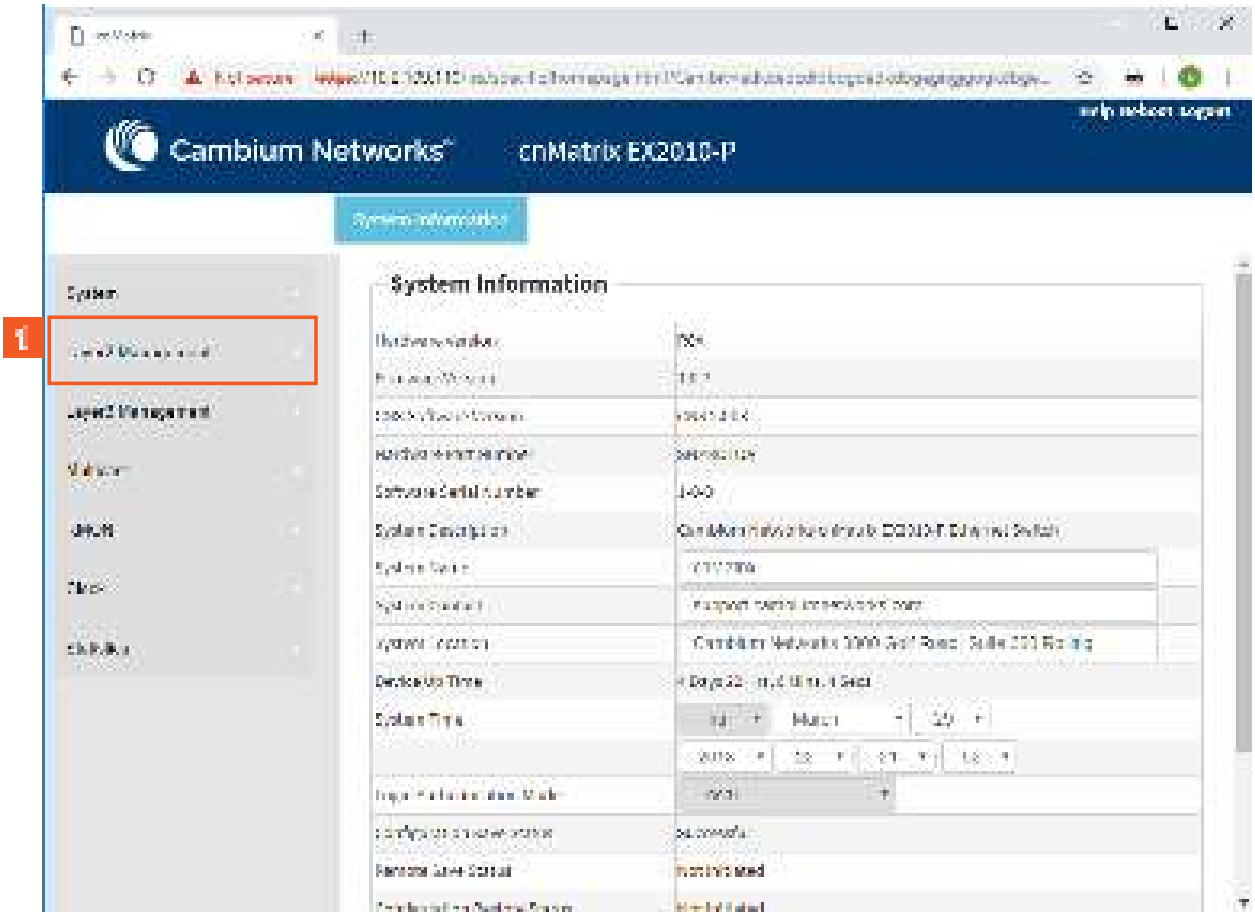
Prerequisites

- N/A

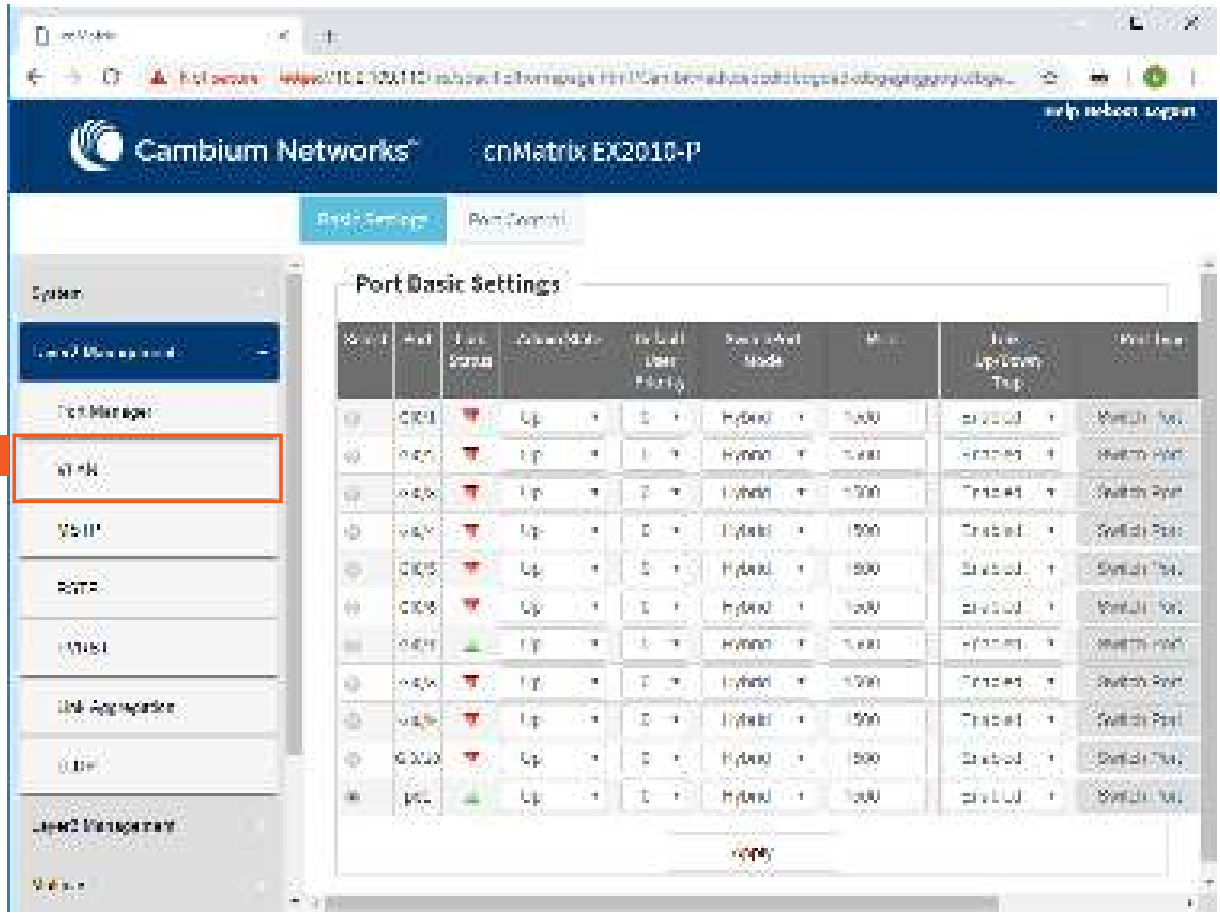
2.8.1.2 Feature Description



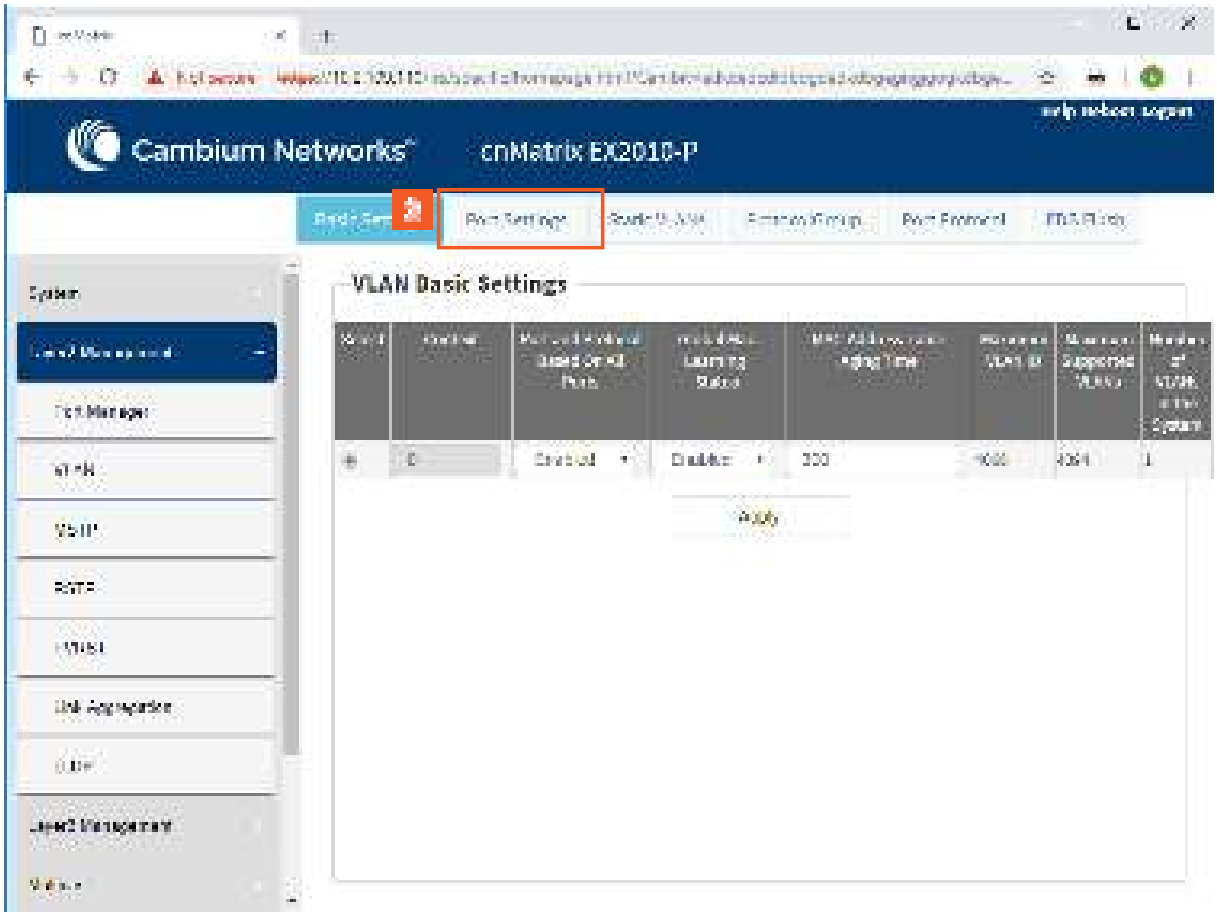
2.8.2 How to Enable Private VLAN Edge in WEB Interface



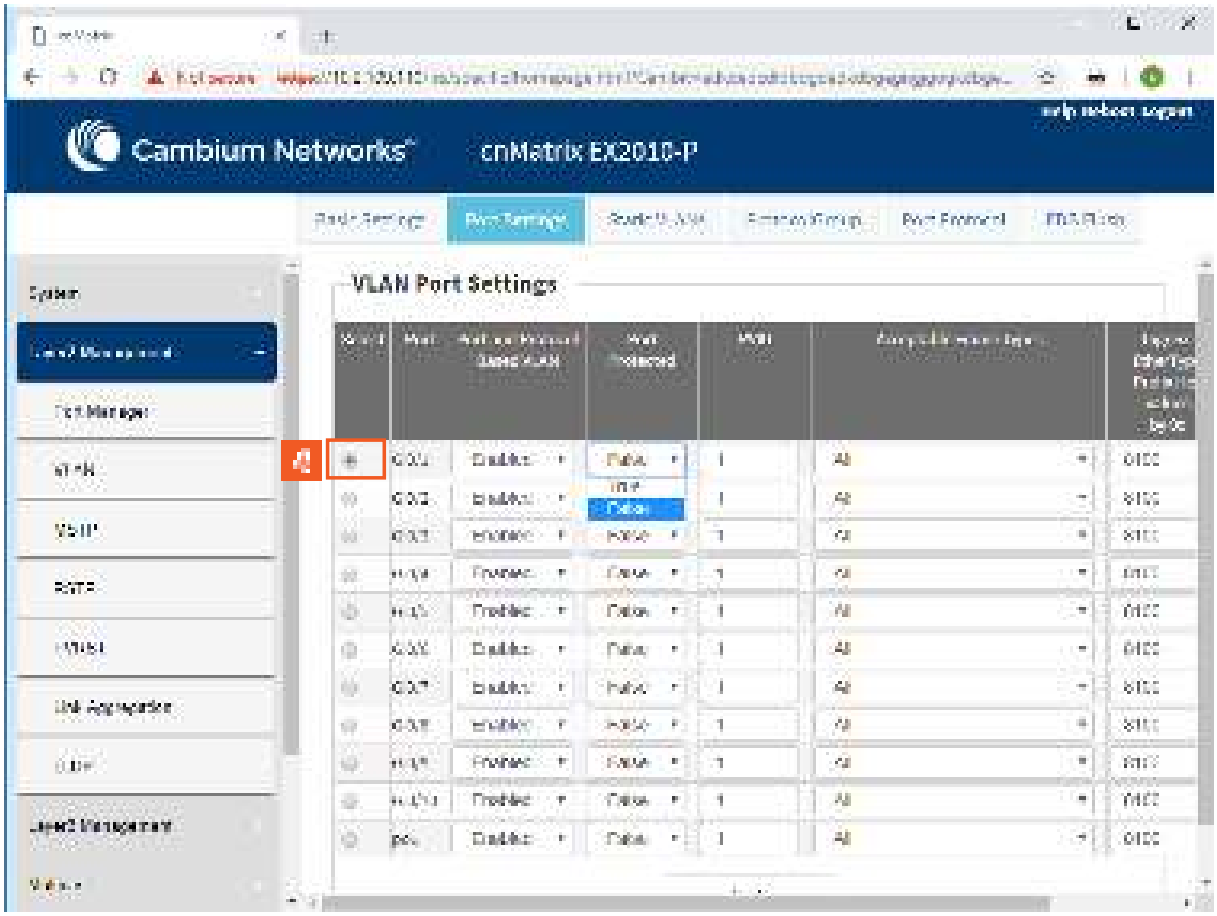
1 Click the **Layer2 Management** tab. The **L2 Features** are displayed



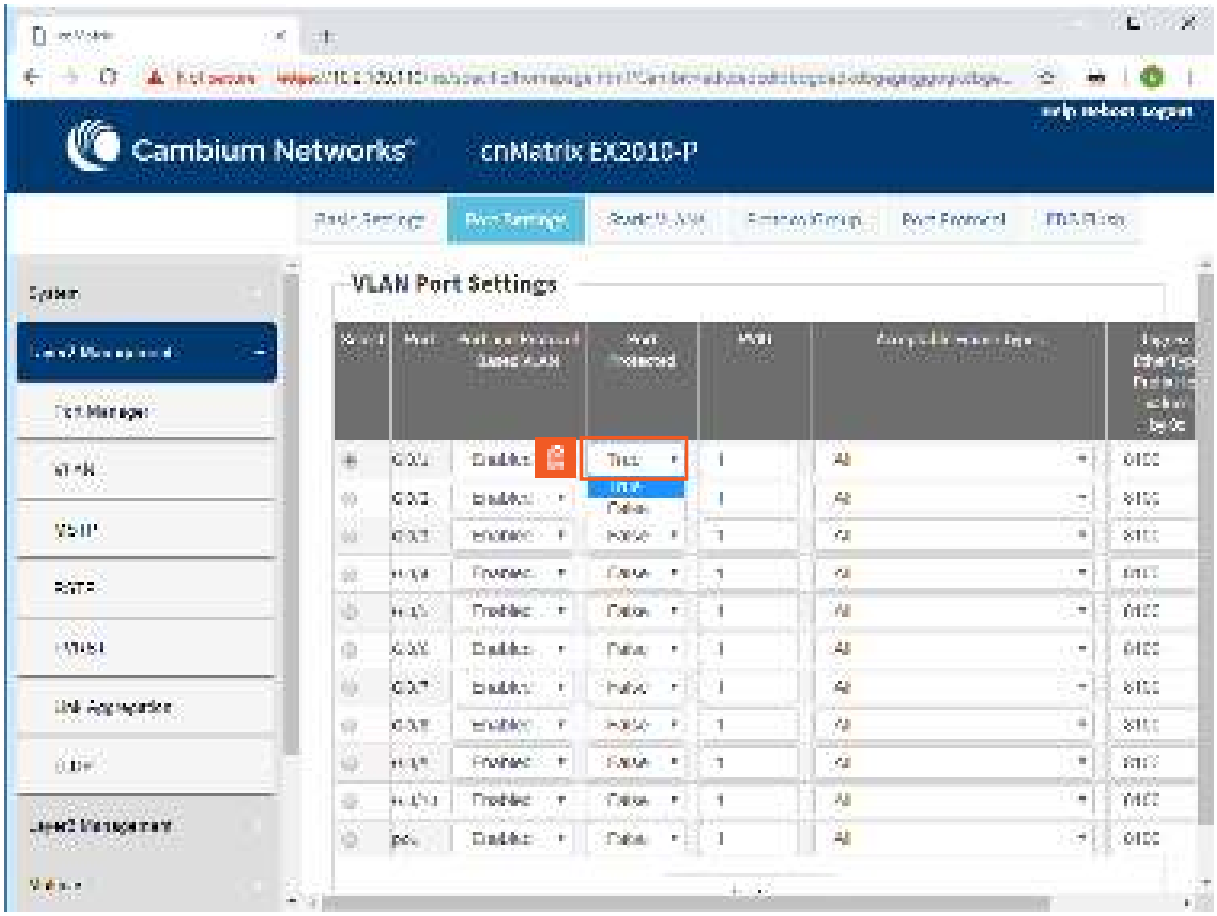
Click the **VLAN** menu item.



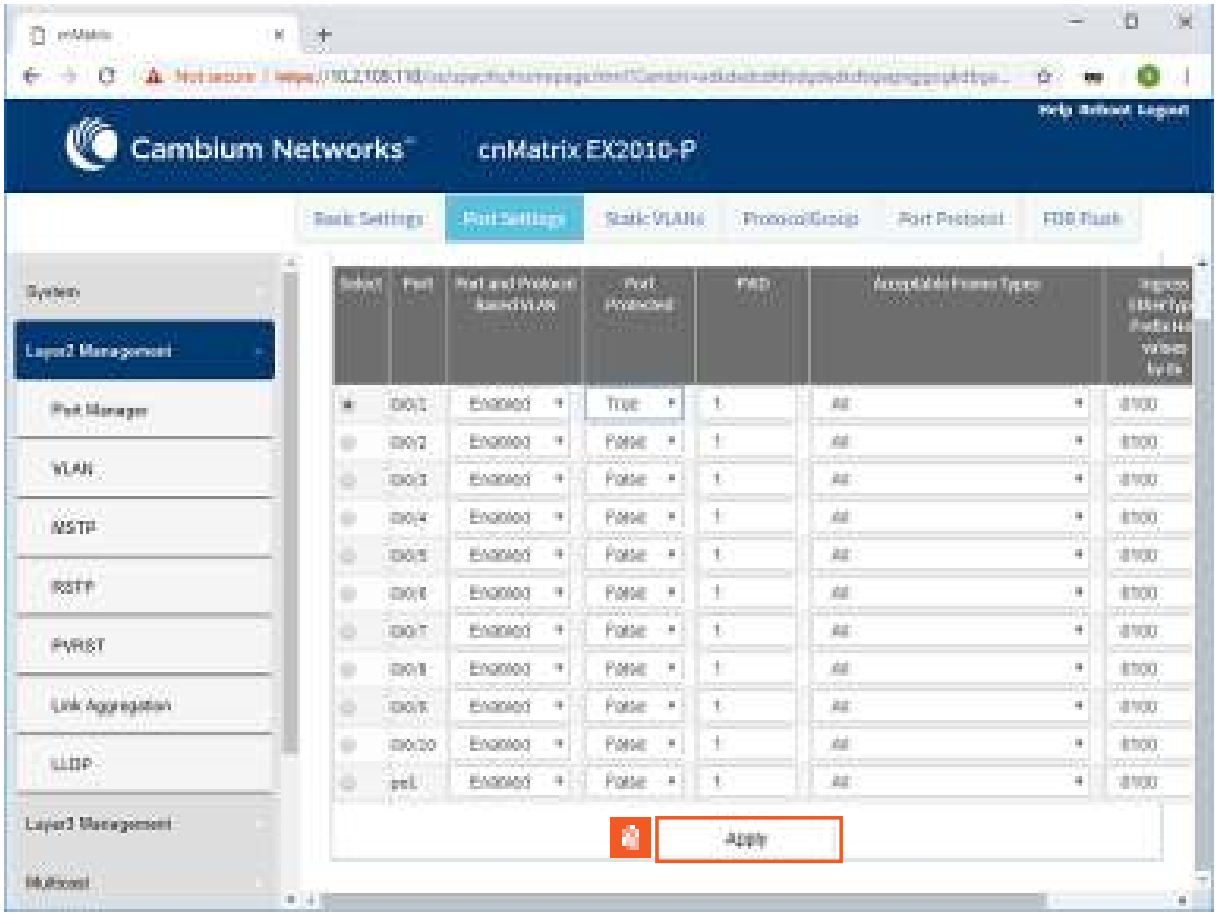
2 Click the **Port Settings** tab.



4 Click the **Select** radiobutton and select the port for which the configuration needs to be done. For example, click the **Gi0/1** radiobutton.



Click the **Port Protected** drop-down list to select whether the port should be configured as protected or not. Select the **True** list item.



Click the **Apply** button.

2.9 Power over Ethernet

2.9.1 Managing PoE (Power over Ethernet)

Feature Overview

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

Standards

- IEEE 802.3af
- IEEE802.3at

Scaling Numbers

N/A

Limitations

N/A

Default Values

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

2.10 Port Mirroring

2.10.1 Managing Port Mirroring

2.10.1.1 Feature Description

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

The following port mirroring modes are supported:

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

Standards

- N/A

Scaling Numbers

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

Limitations

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

Default Values

- The Port Mirroring feature is enabled by default.

Prerequisites

- N/A

2.10.1.2 Network Diagram

Destination port:

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

Source port:

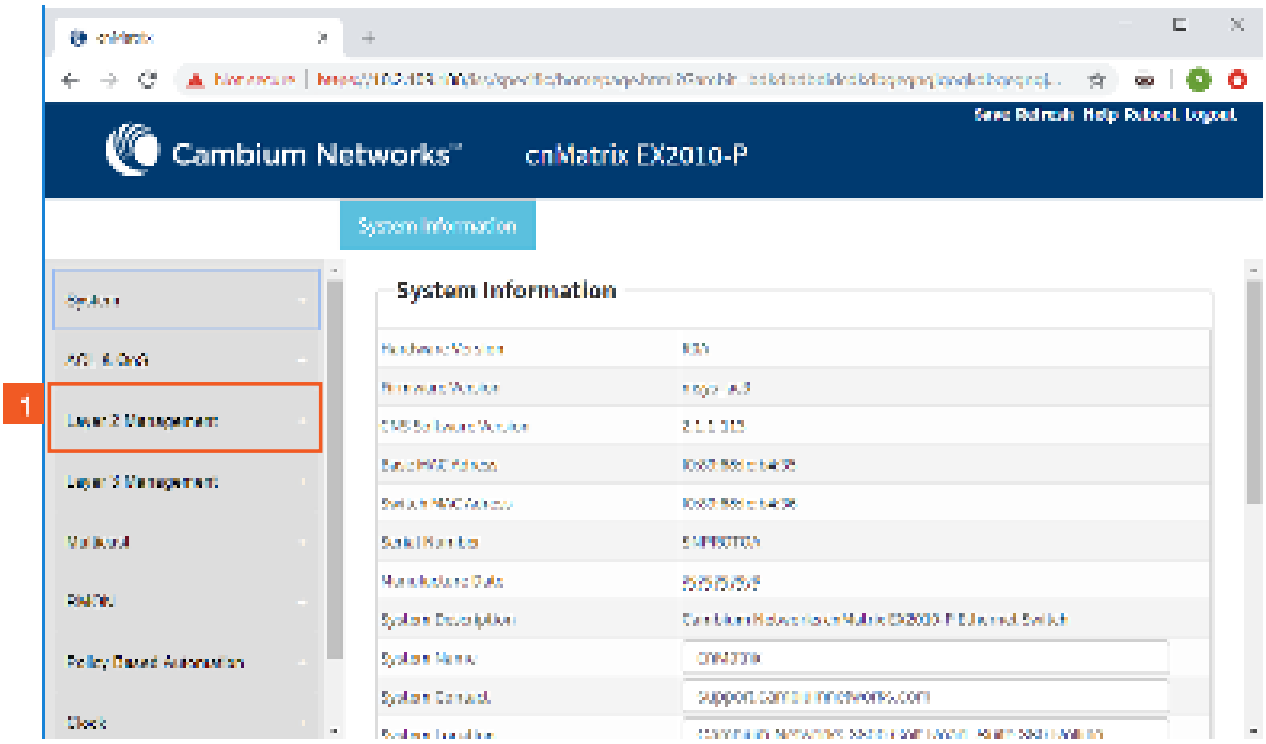
- Cannot be a destination port.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- Can be in the same or different VLANs.

2.10.2 Configuring Port Mirroring in WEB Interface

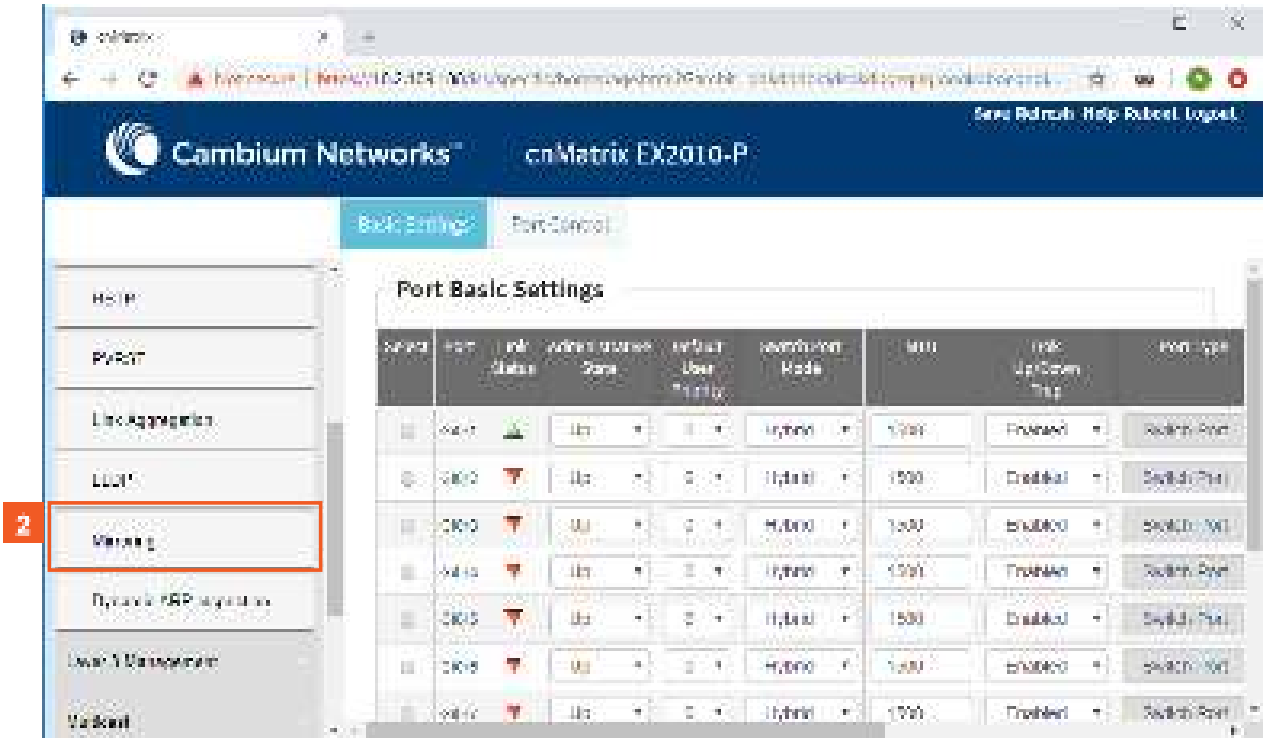
The **Port Mirroring** feature is not available in WEB interface.

Starting with version 2.1, the **Port Mirroring** feature is available in WEB Interface.

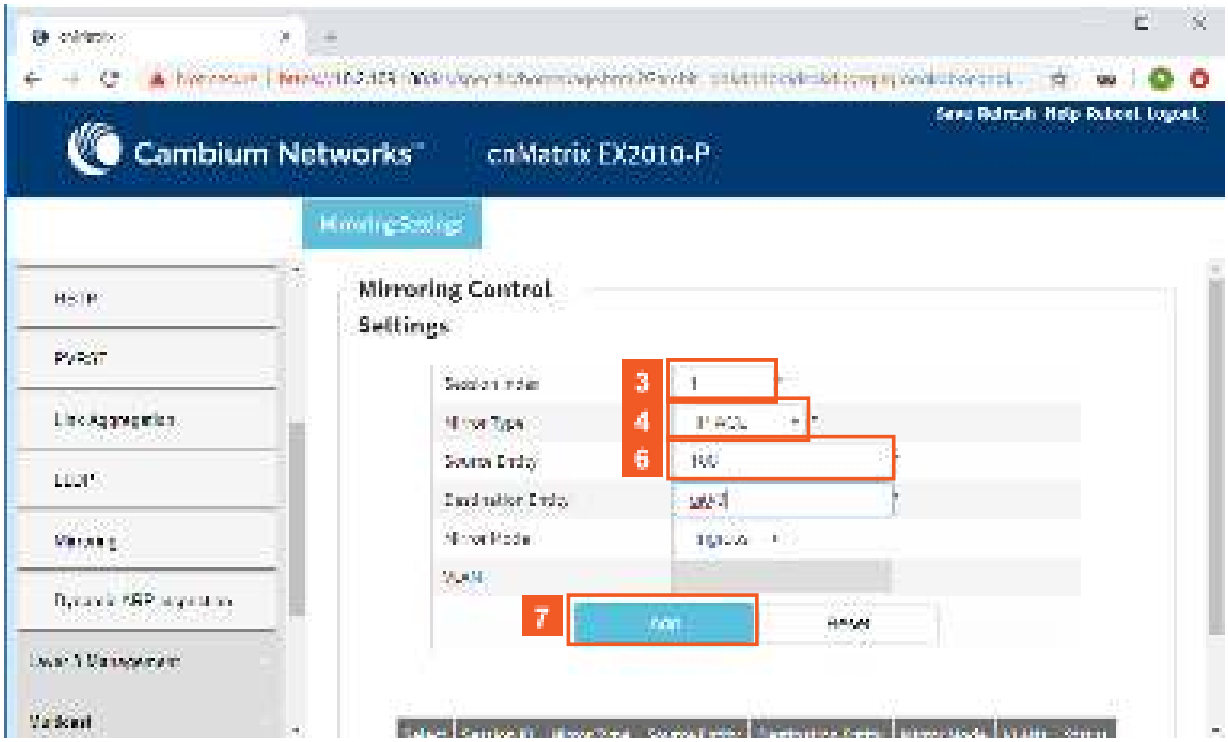
2.10.3 Configuring Port Mirroring - IP Based ACL in WEB Interface(Starting with version 2.1)



1 Click the **Layer 2 Management** tab. The **L2 Features** are displayed.



2 Click the **Mirroring** menu item. The **Mirroring Control Settings** window is displayed.



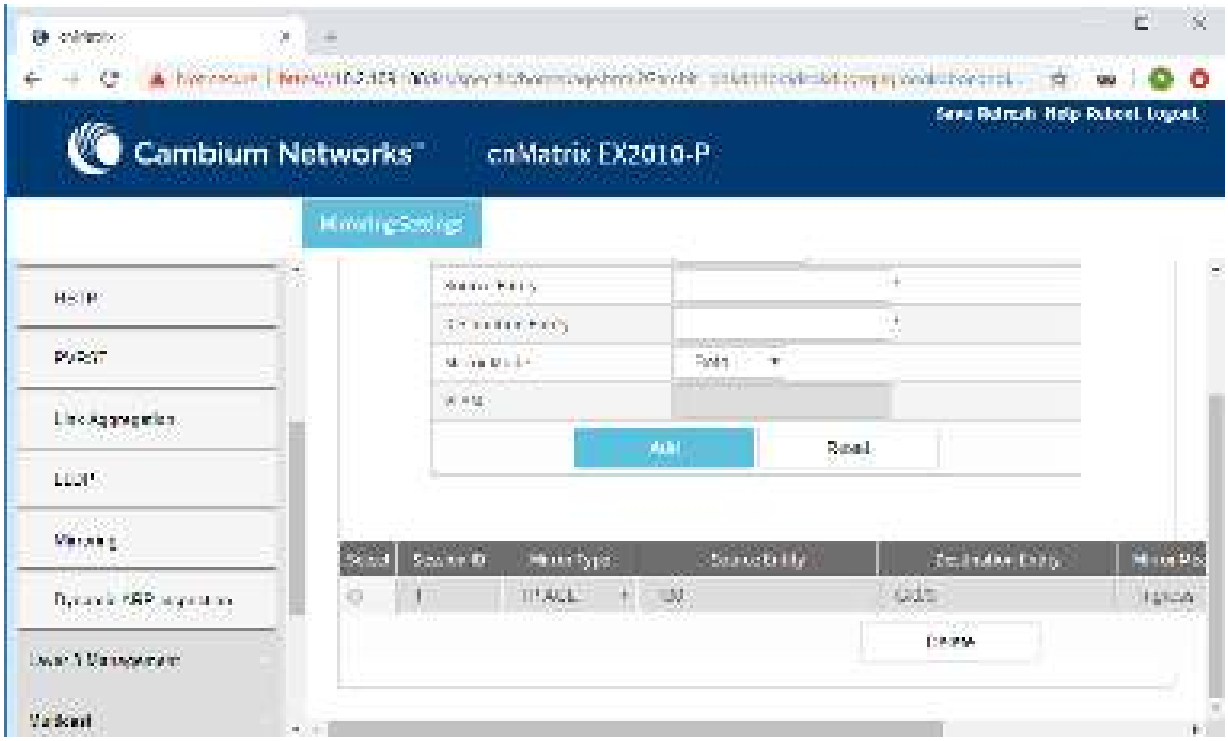
3 Type the value **1** into the **Session Index** field.

4 Click the **Mirror Type** drop-down list and select the **IP ACL** list item.

5 Type the value **100** into the **Source Entity** field.

6 Type the value **gi0/3** into the **Destination Entity** field.

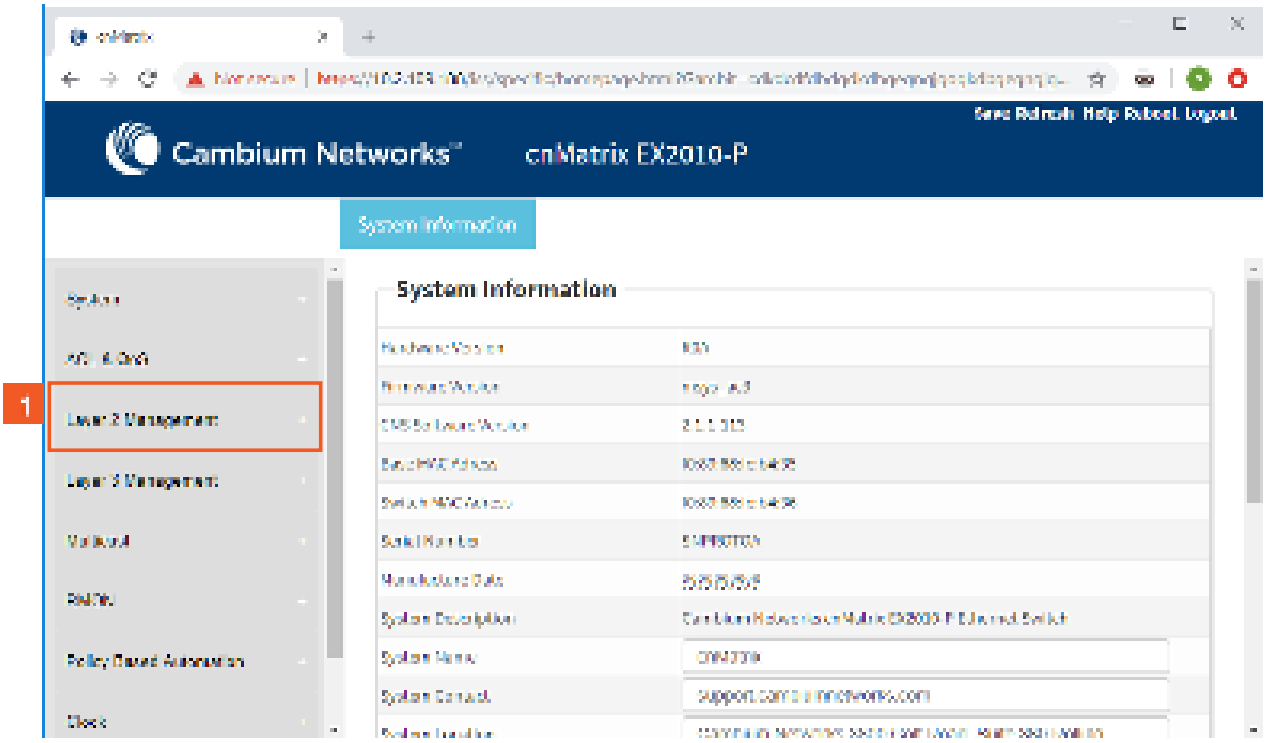
7 Click the **Add** button.



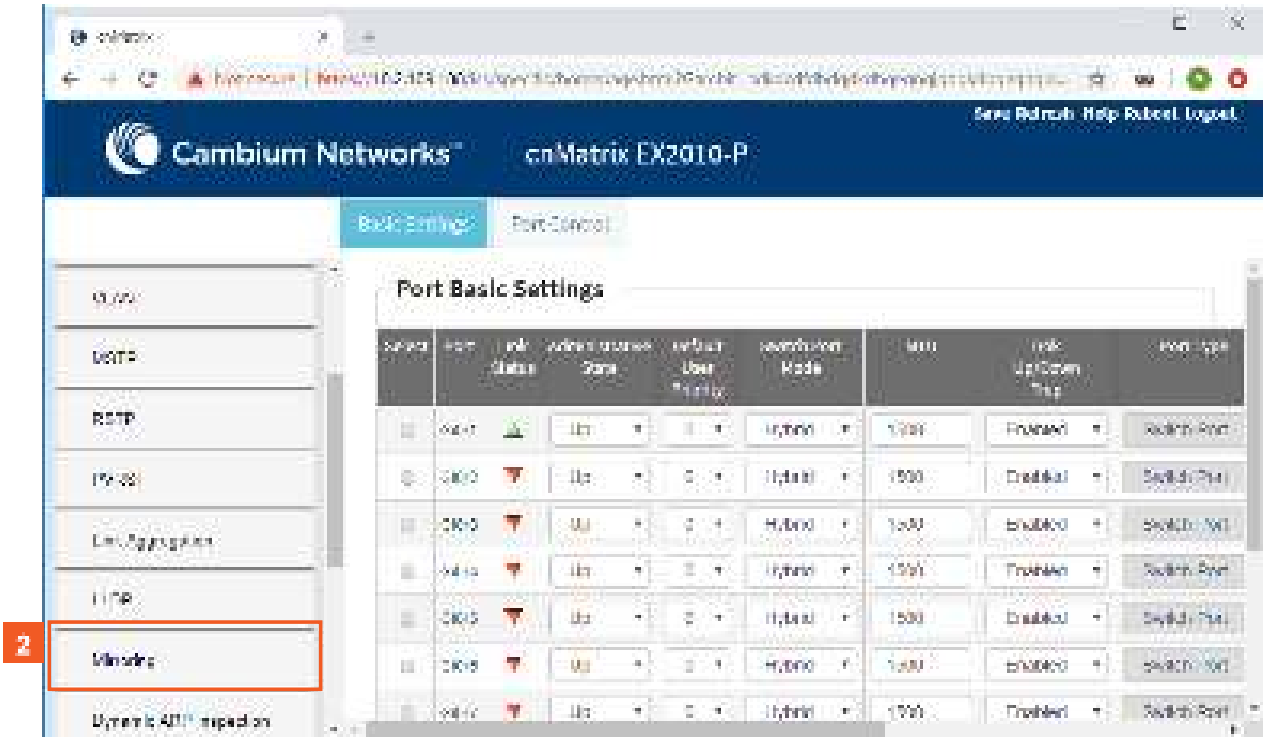
Make sure that ACL 100 was previously created.

Mirror Mode is not mandatory for IP Based ACL Mirroring.

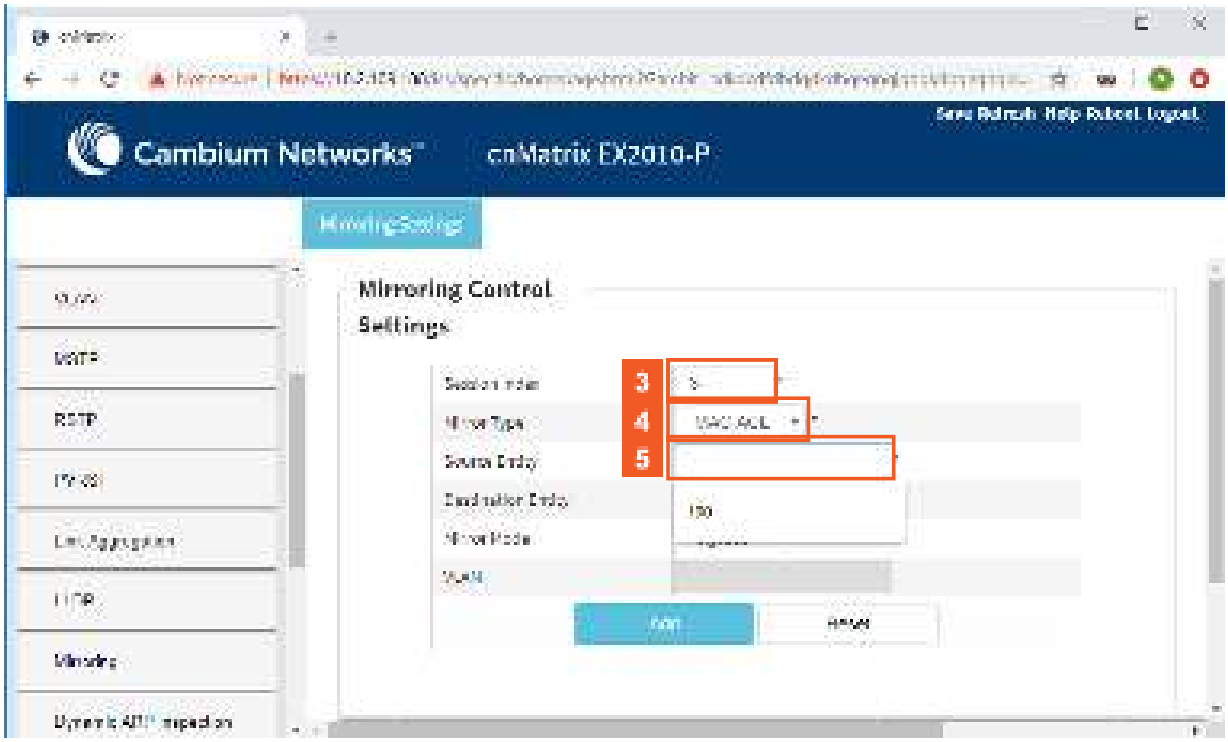
2.10.4 Configuring Port Mirroring - MAC Based ACL in WEB Interface (Starting with version 2.1)



1 Click the **Layer 2 Management** tab. The **L2 Features** are displayed.



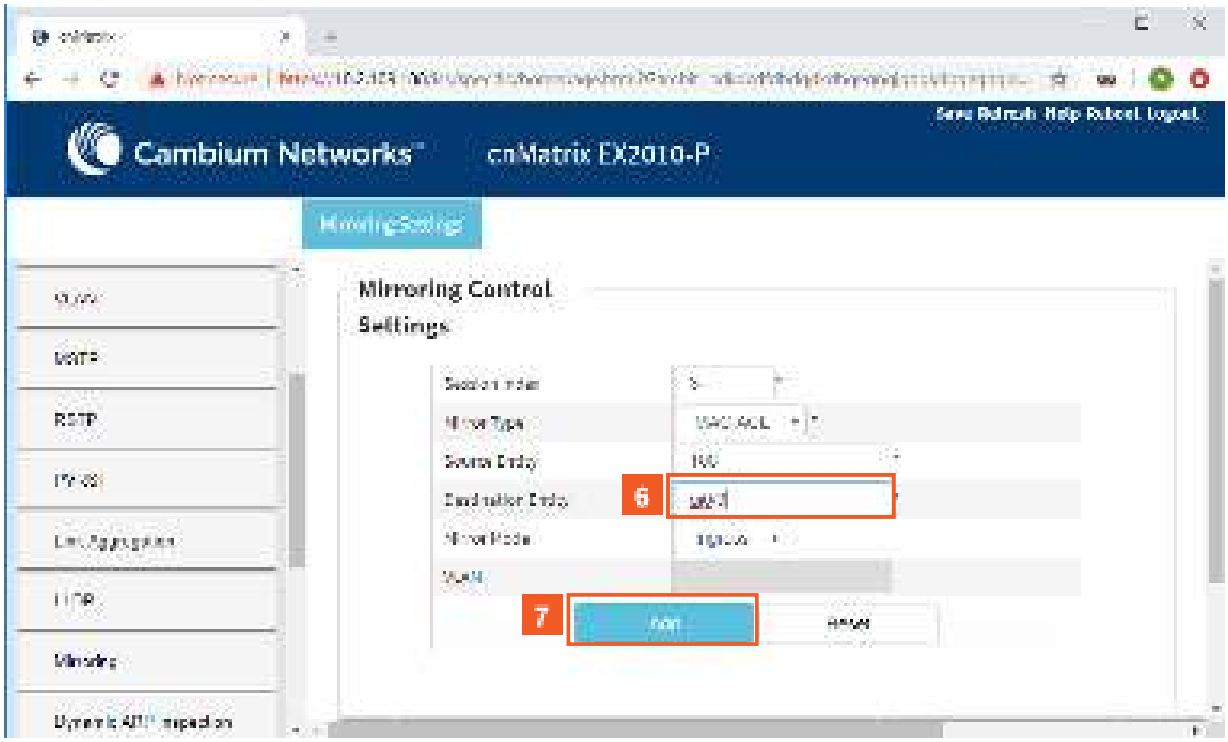
2 Click the **Mirroring** menu item. The **Mirroring Control Settings** window is displayed.



3 Type the value **3** into the **Session Index** field.

4 Click the **Mirror Type** drop-down list and select the **MAC ACL** list item.

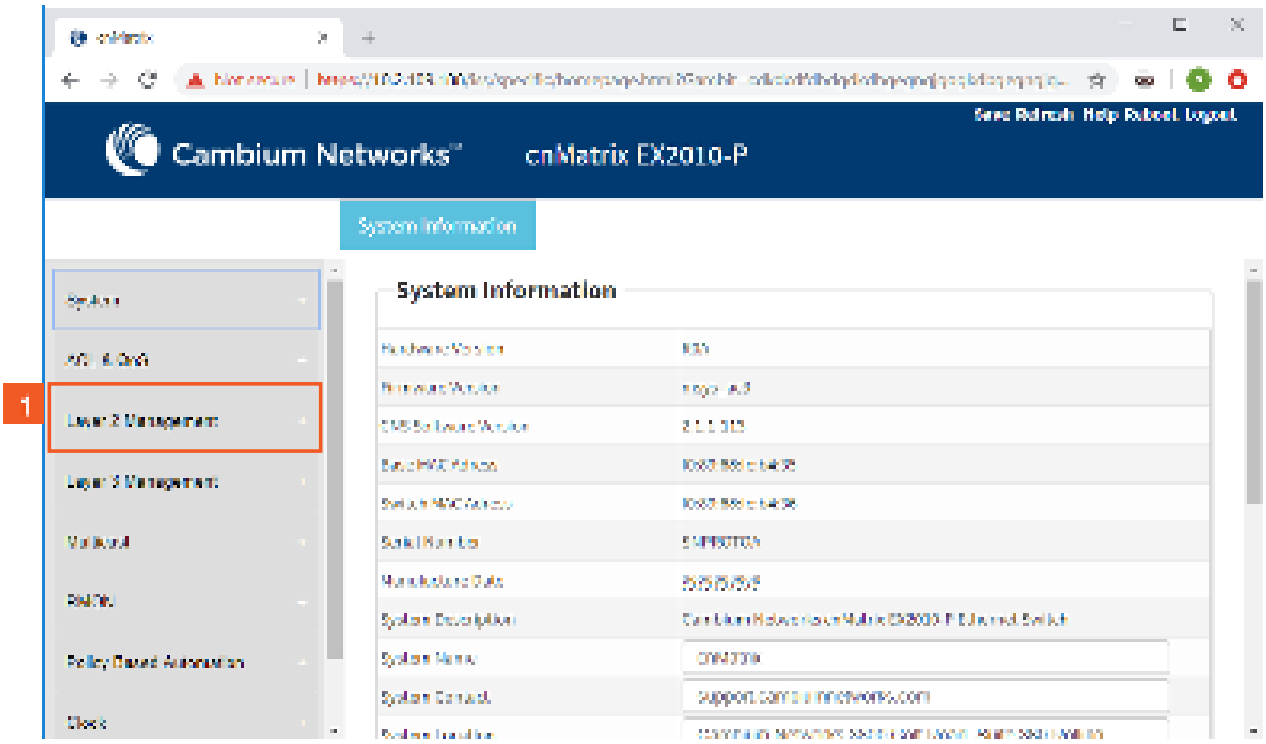
5 Type the value **100** into the **Source Entity** field.



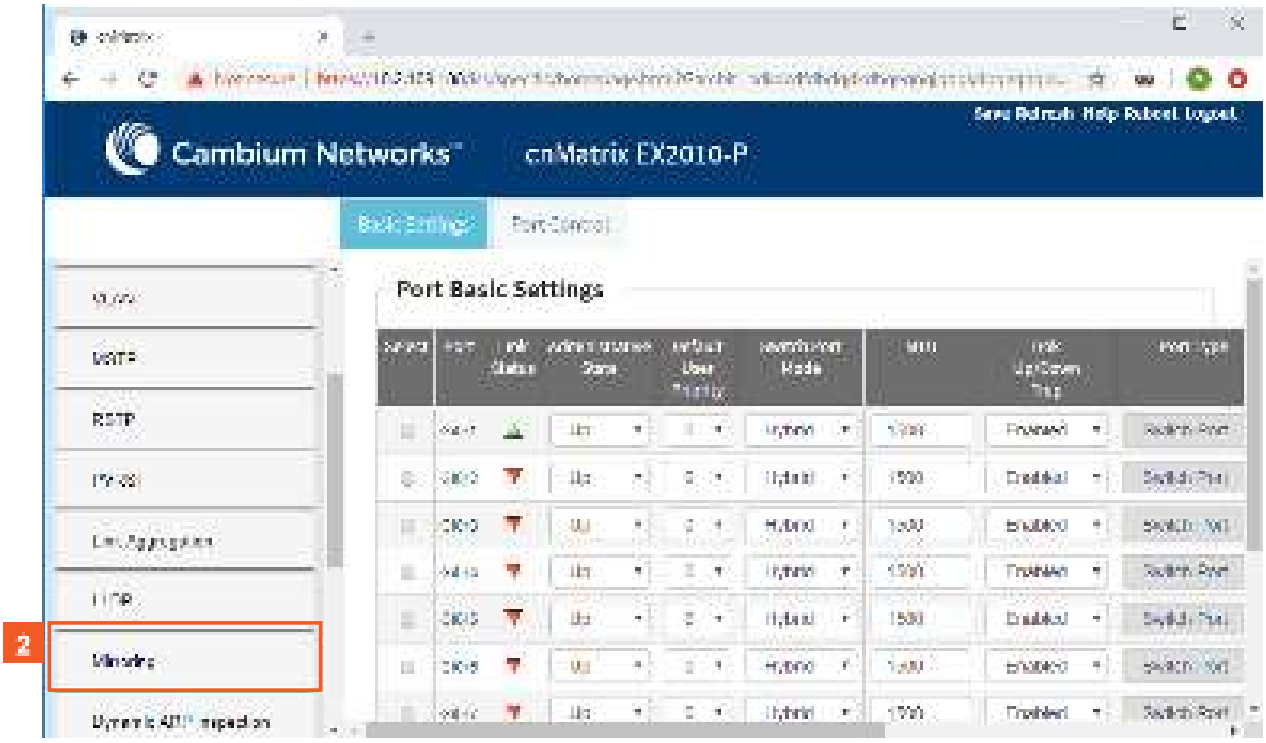
6 Type the value **gi0/3** into the **Destination Entity** field.

7 Click the **Add** button.

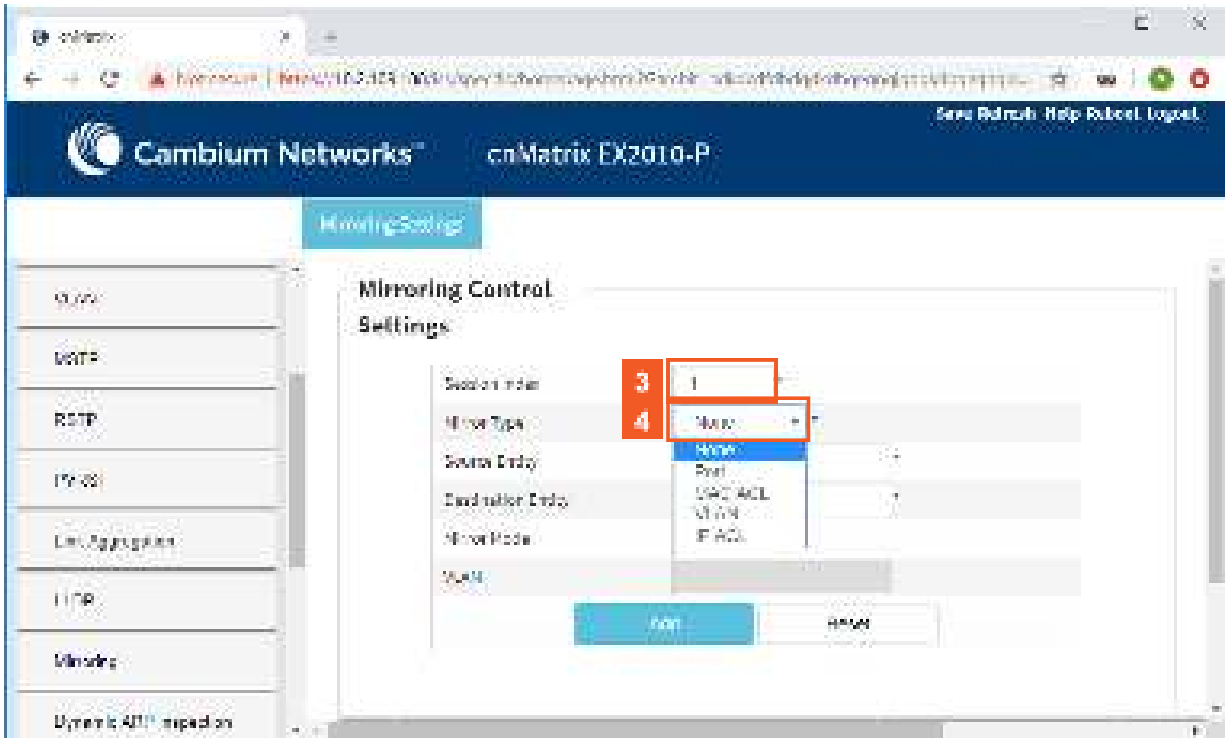
2.10.5 Configuring Port Mirroring - VLAN Based ACL in WEB Interface (Starting with version 2.1)



1 Click the **Layer 2 Management** tab. The **L2 Features** are displayed.

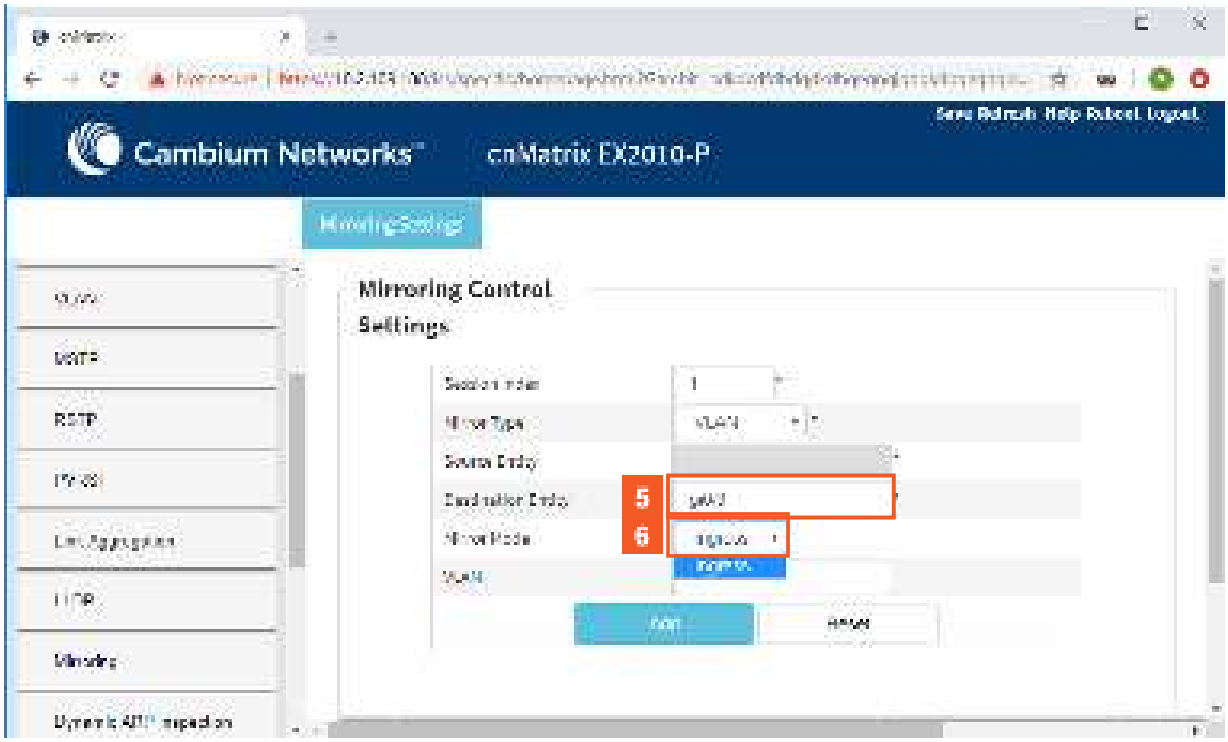


2 Click the **Mirroring** menu item. The **Mirroring Control Settings** window is displayed.



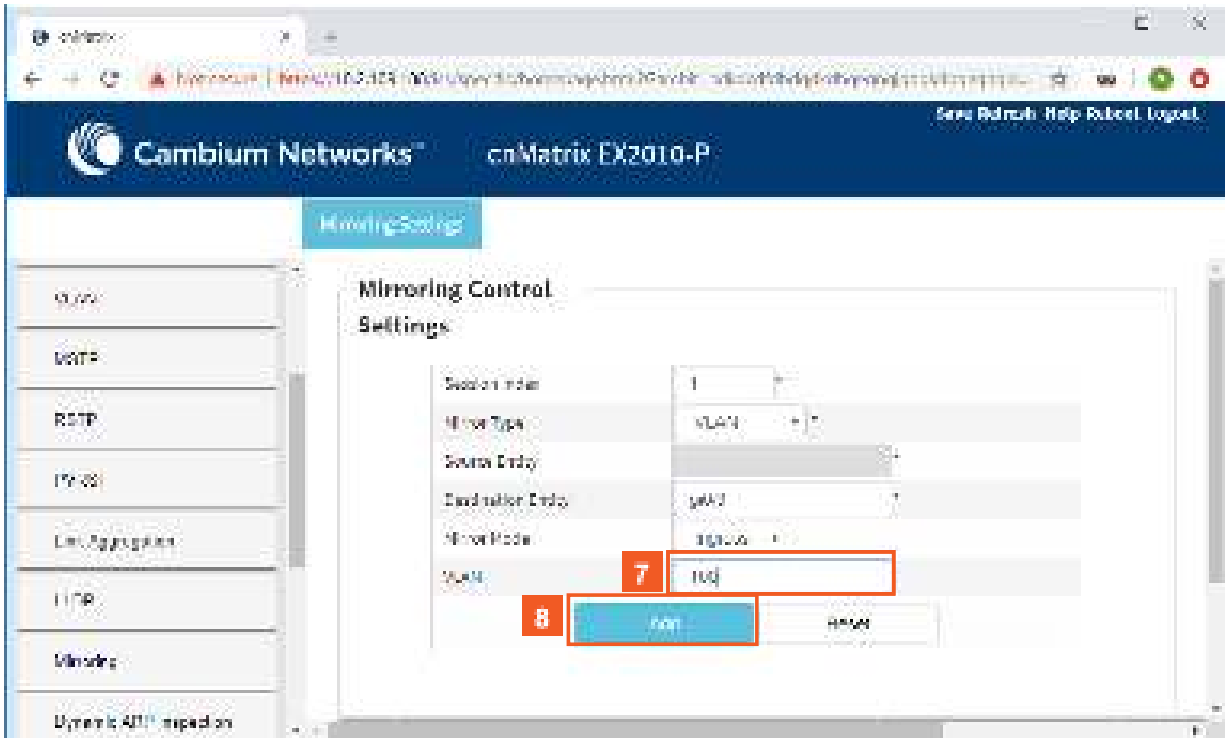
3 Type the value **1** into the **Session Index** field.

4 Click the **Mirror Type** drop-down list and select the **VLAN** list item.



5 Type the value **gi0/3** into the **Destination Entity** field.

6 Click the **Mirror Mode** drop-down list and select the **Ingress** list item.

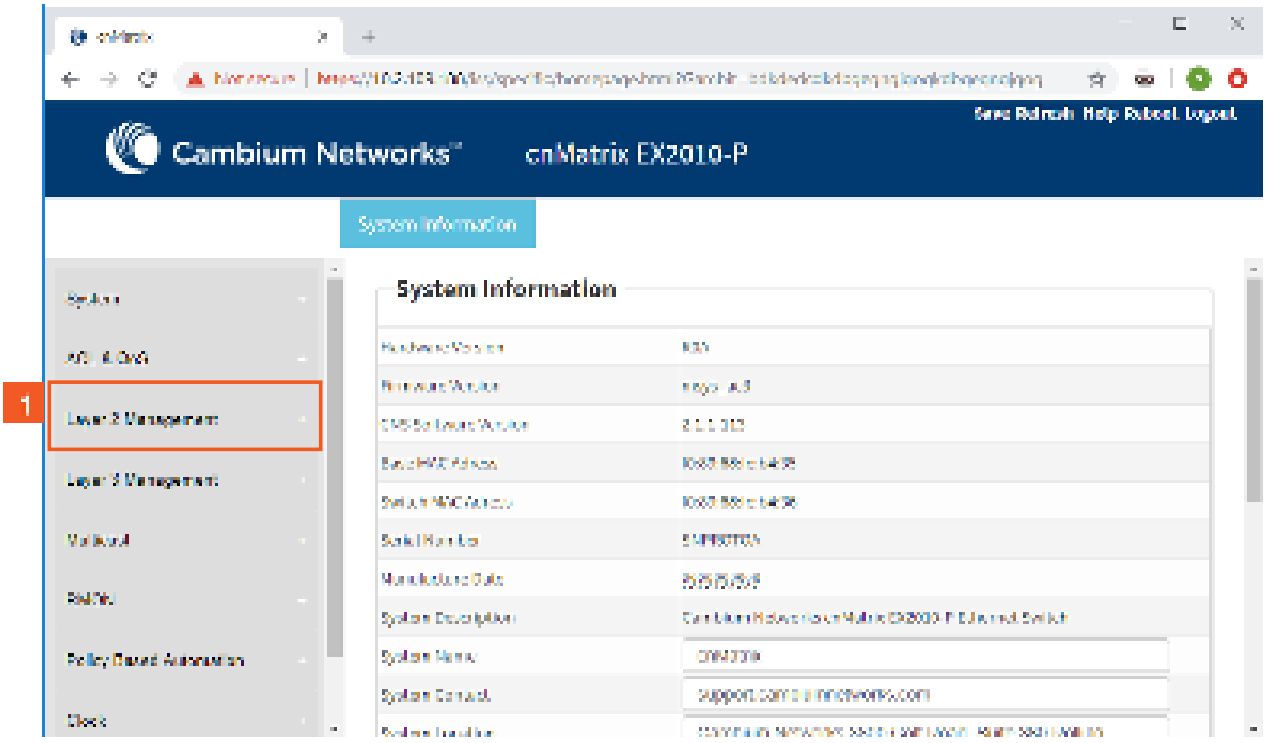


7 Type the value **100** into the **VLAN** field.

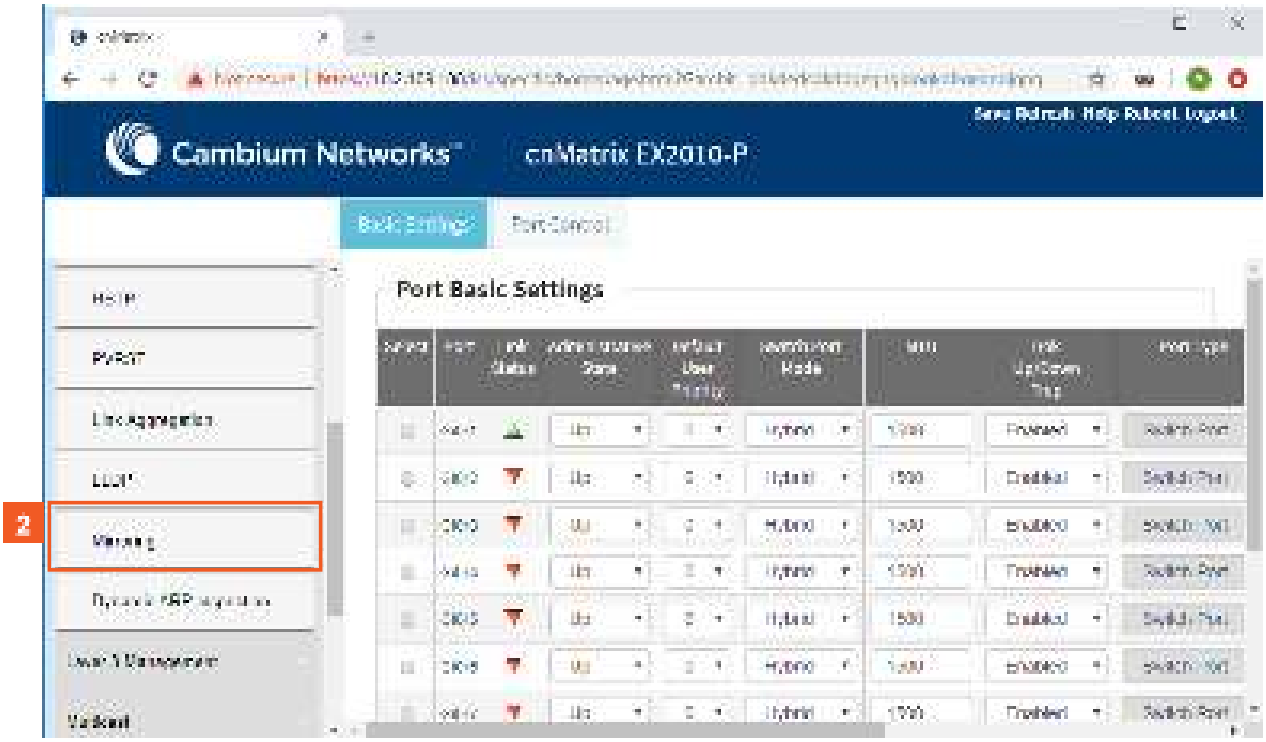
Make sure that VLAN 100 was previously configured.

8 Click the **Add** button.

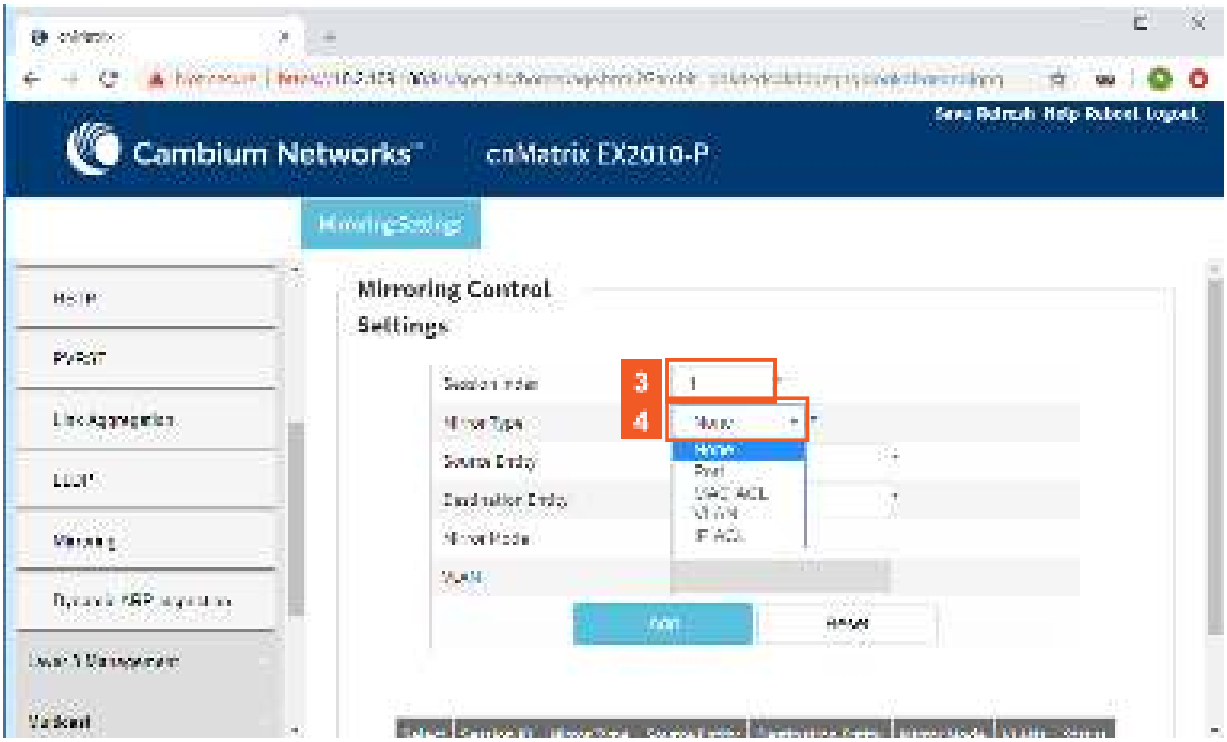
2.10.6 Configuring Port Mirroring - Port Based ACL in WEB Interface (Starting with version 2.1)



1 Click the **Layer 2 Management** tab. The **L2 Features** are displayed.

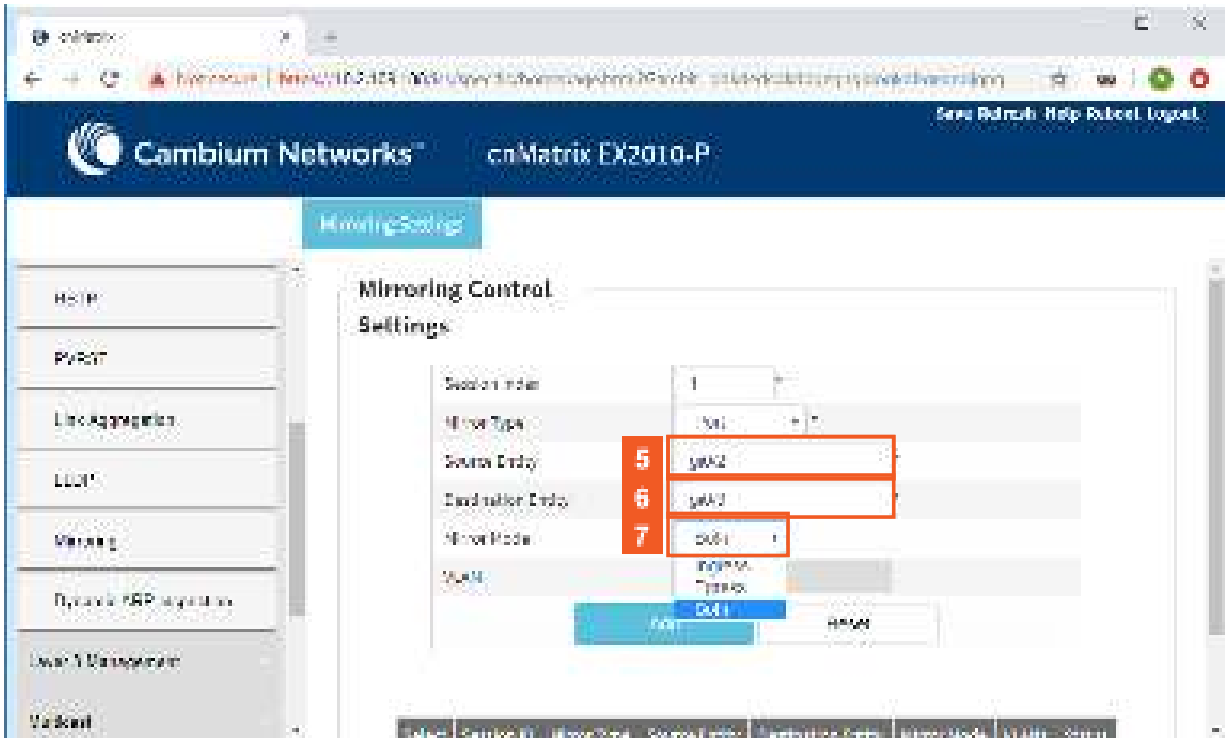


2 Click the **Mirroring** menu item. The **Mirroring Control Settings** window is displayed.



3 Type the value **1** into the **Session Index** field.

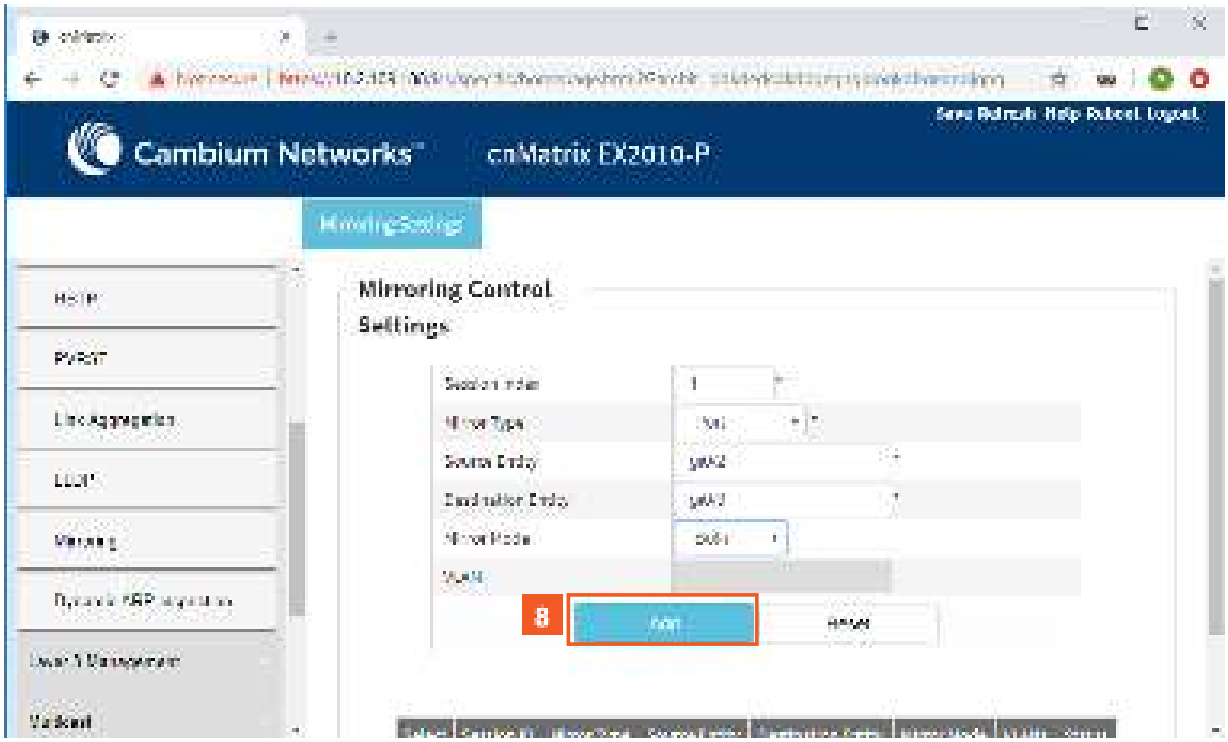
4 Click the **Mirror Type** drop-down list and select the **Port** list item.



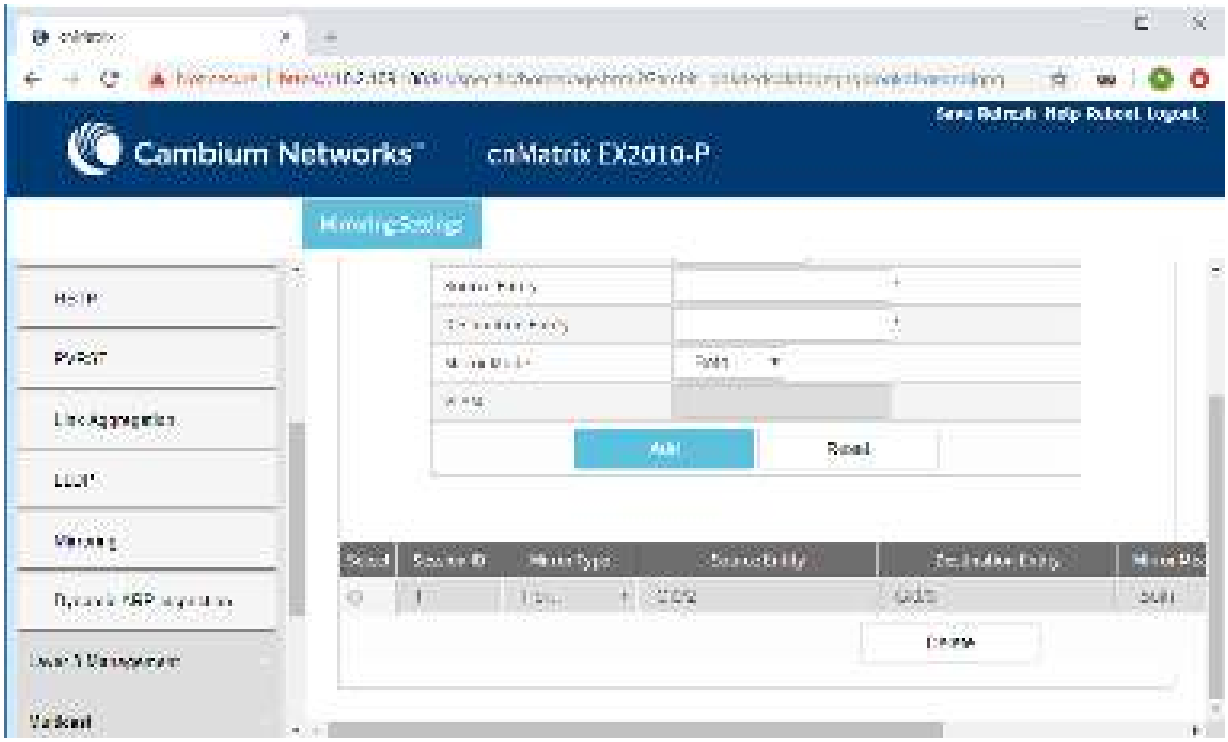
5 Type the value **gi0/2** into the **Source Entity** field.

6 Type the value **gi0/3** into the **Destination Entity** field.

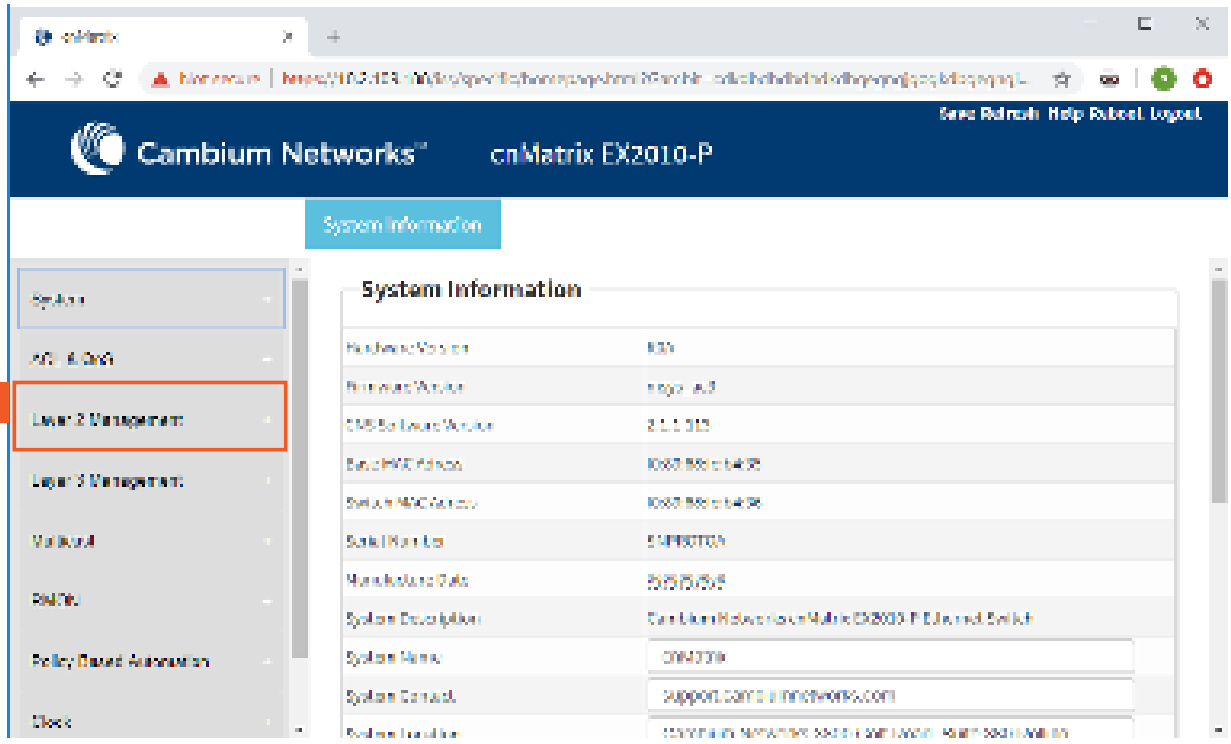
7 Click the **Mirror Type** drop-down list and select the **Both** list item.



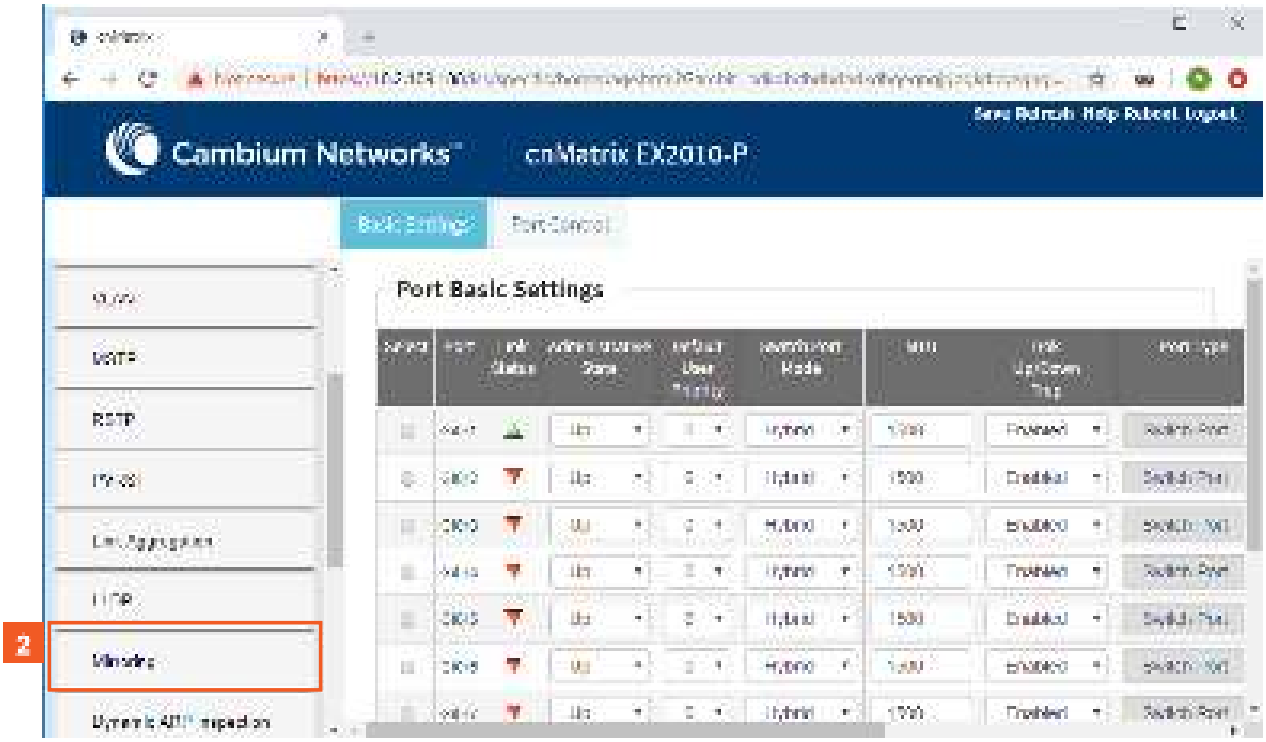
8 Click the **Add** button.



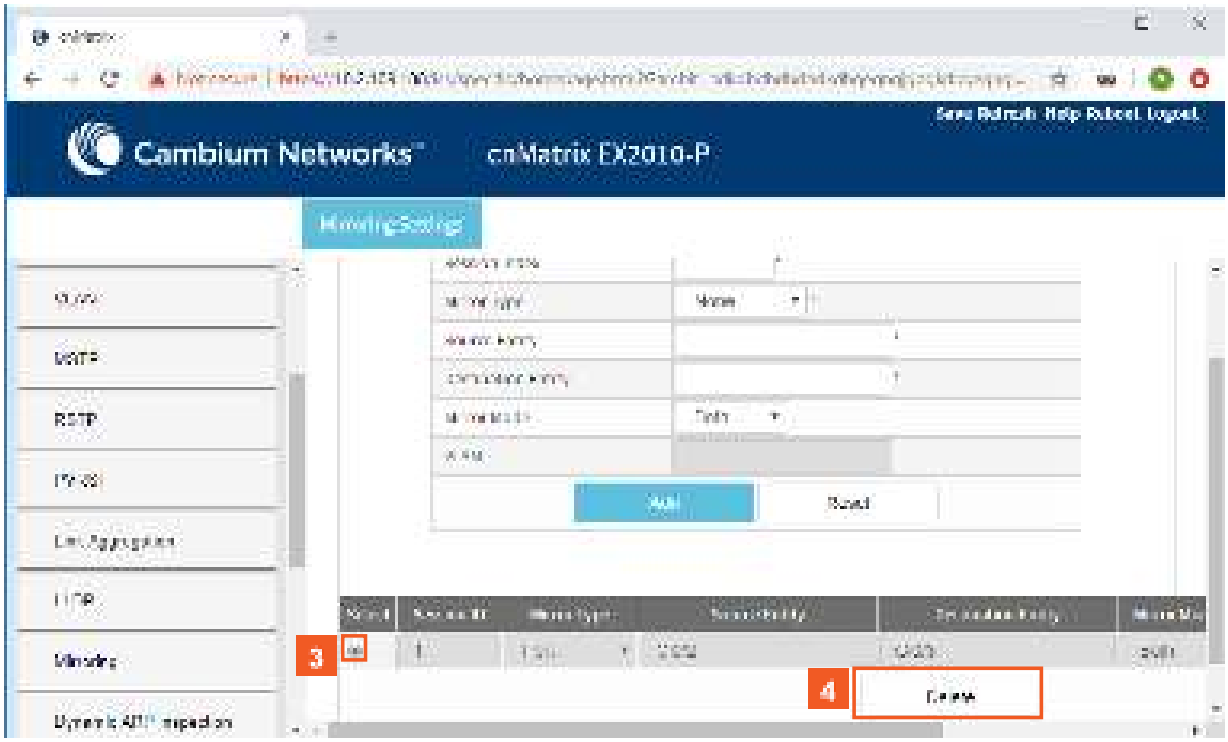
2.10.7 How to Remove a Mirroring Session in WEB Interface (Starting with version 2.1)



1 Click the **Layer 2 Management** tab. The **L2 Features** are displayed.



2 Click the **Mirroring** menu item. The **Mirroring Control Settings** window is displayed.



3 Select the radiobutton for a certain mirroring session(line) that you want to remove.

4 Click the **Delete** button.

2.11Storm Control

2.11.1Managing 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 640pkts/sec (for 100M speed), of 6400pkts/sec (for 1G speed) and for 64000pkts/sec (for 10G speed).

Default Values

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

2.12 Rate Limit Output

2.12.1 Managing Rate-Limit-Output

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.

2.12.2 Configuring Rate-Limit-Output in WEB Interface

The **Rate-Limit-Output** feature is not available in WEB interface.

2.13 Quality of Service

2.13.1 Managing QoS

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

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

QoS provides means of doing the following:

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

Feature Overview

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

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

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

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

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

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

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

- setting the trust mode to **dot1p** indicates that if a frame includes both 802.1p and a DSCP field, then the pbit field takes precedence. If the frame doesn't include a 802.1p field, the ingress port's priority is used to determine the packet's QoS properties.
- setting the trust mode to **DSCP** indicates that if a frame includes both 802.1p and a DSCP field, then the DSCP field takes precedence. For non-IP packets, the ingress port's priority is used to determine the packet's QoS properties.
- setting the trust mode to **None** indicates that the content of the frame is ignored, and the QoS properties of the packet are assigned by using the ingress port's default priority.

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

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

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

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

Standards

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

Scaling Numbers

- Up to 120 classes can be defined.

Limitations

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

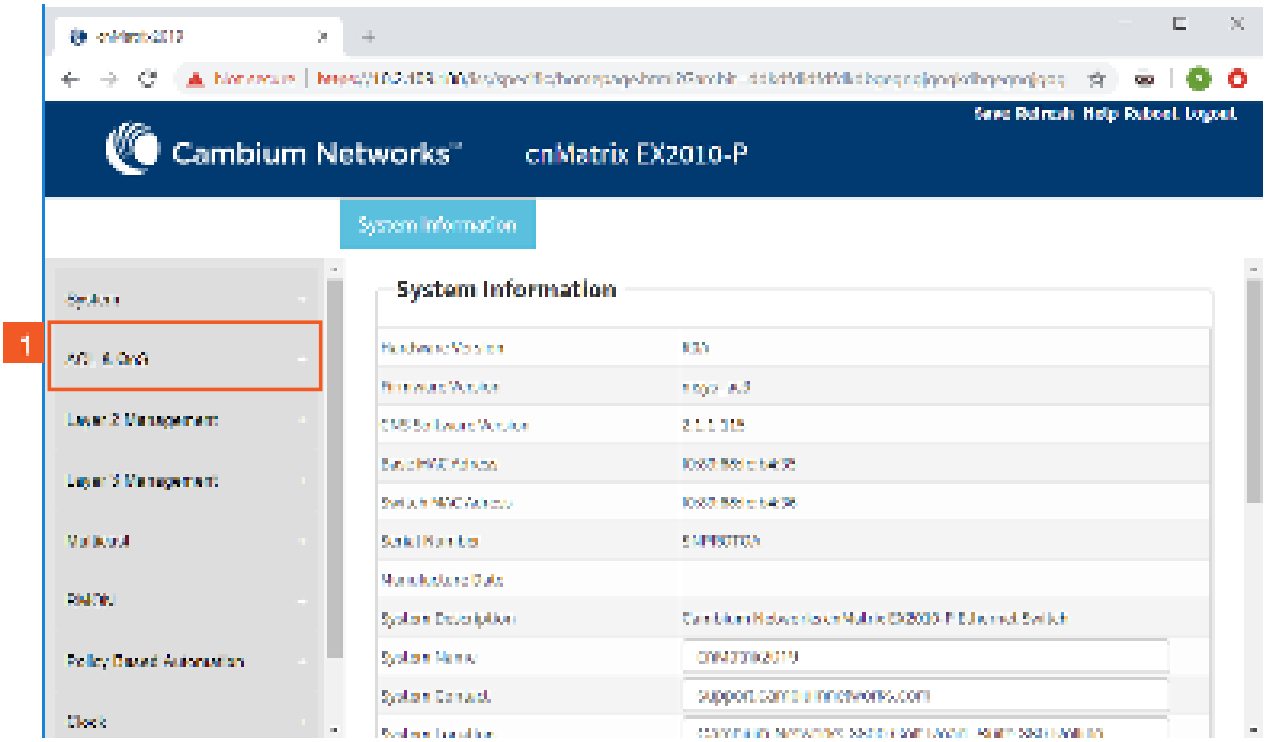
Default Values

- There are eight egress queues for every port, the default scheduling algorithm is strict-priority. Queue 1 is the top priority queue.

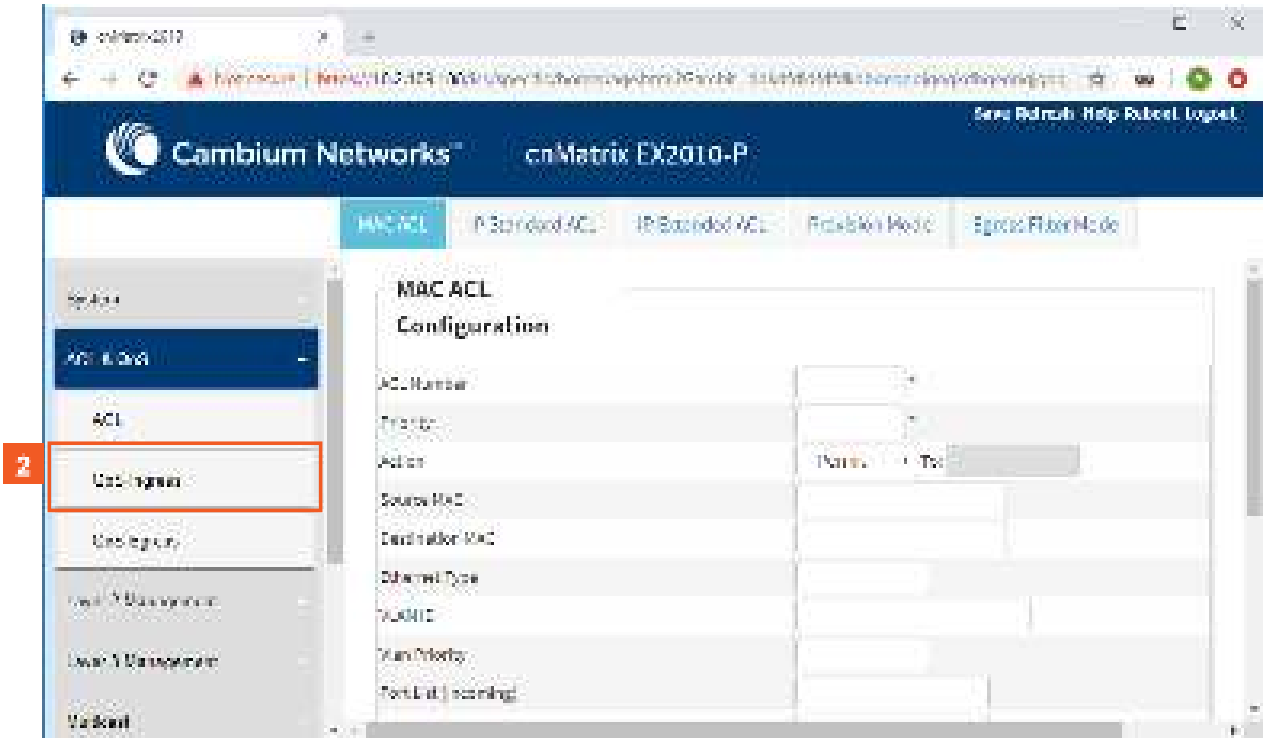
2.13.2 Configuring QoS in WEB Interface

The QoS feature is not available in WEB interface.

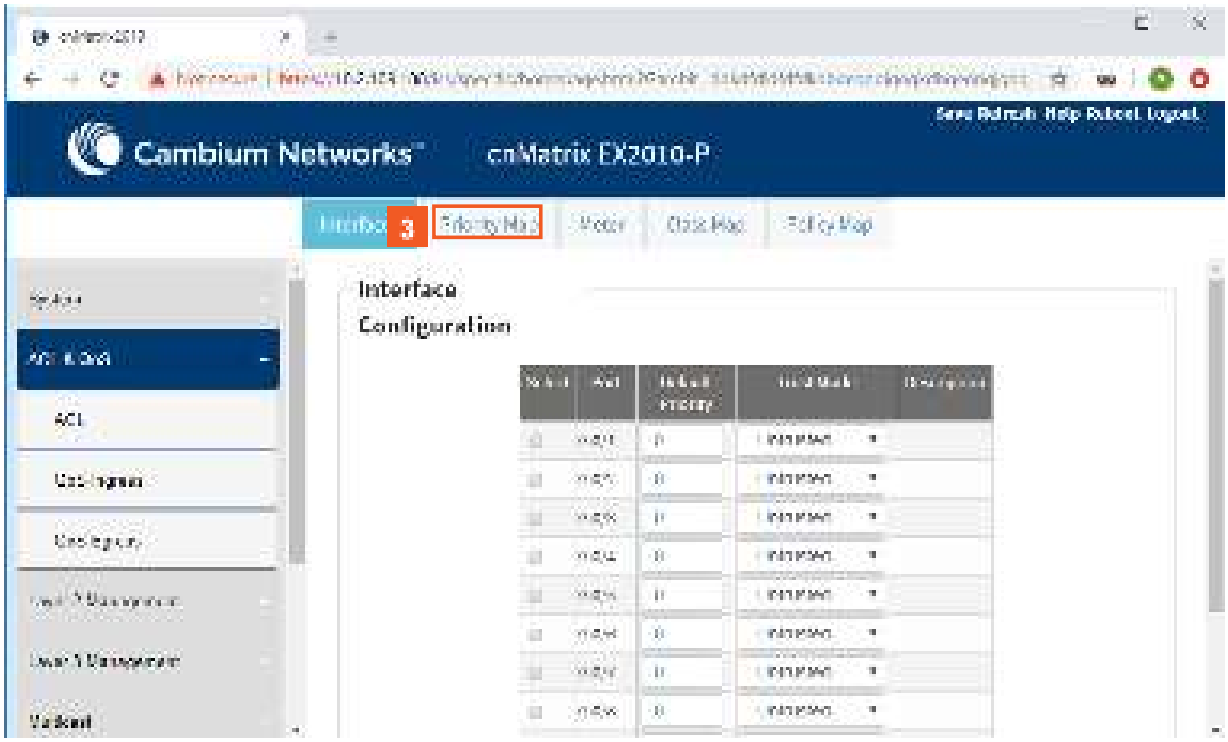
2.13.3 Remarking with Priority Maps - Example (Starting with version 2.1)



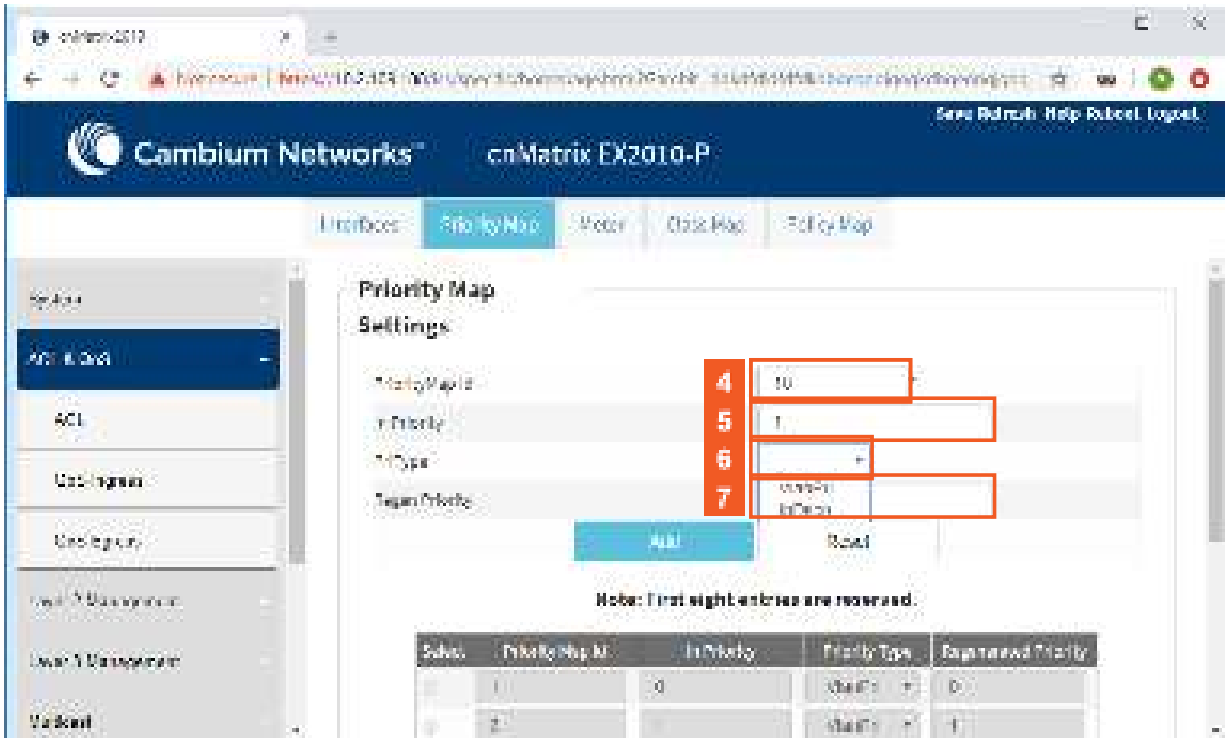
1 Click the **ACL & QoS** tab.



2 Click the **QoS Ingress** menu item.



3 Click the **Priority Map** tab.



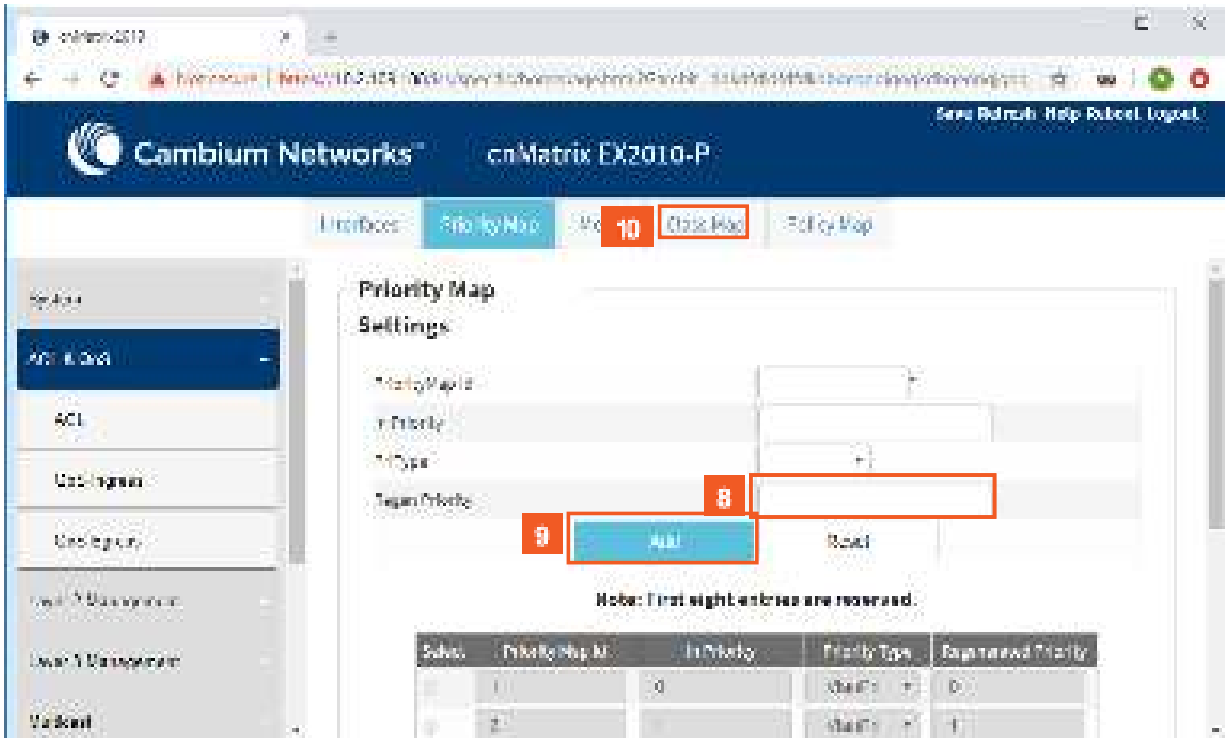
4 Type a value higher than **8**, for example **10** into the **PriorityMAP ID** field to set an unique ID for priority map.

5 Type the value **1** into the **In Priority** field to set the incoming priority value.

6 Click the **PriType** drop-down button to select the incoming priority type.

.

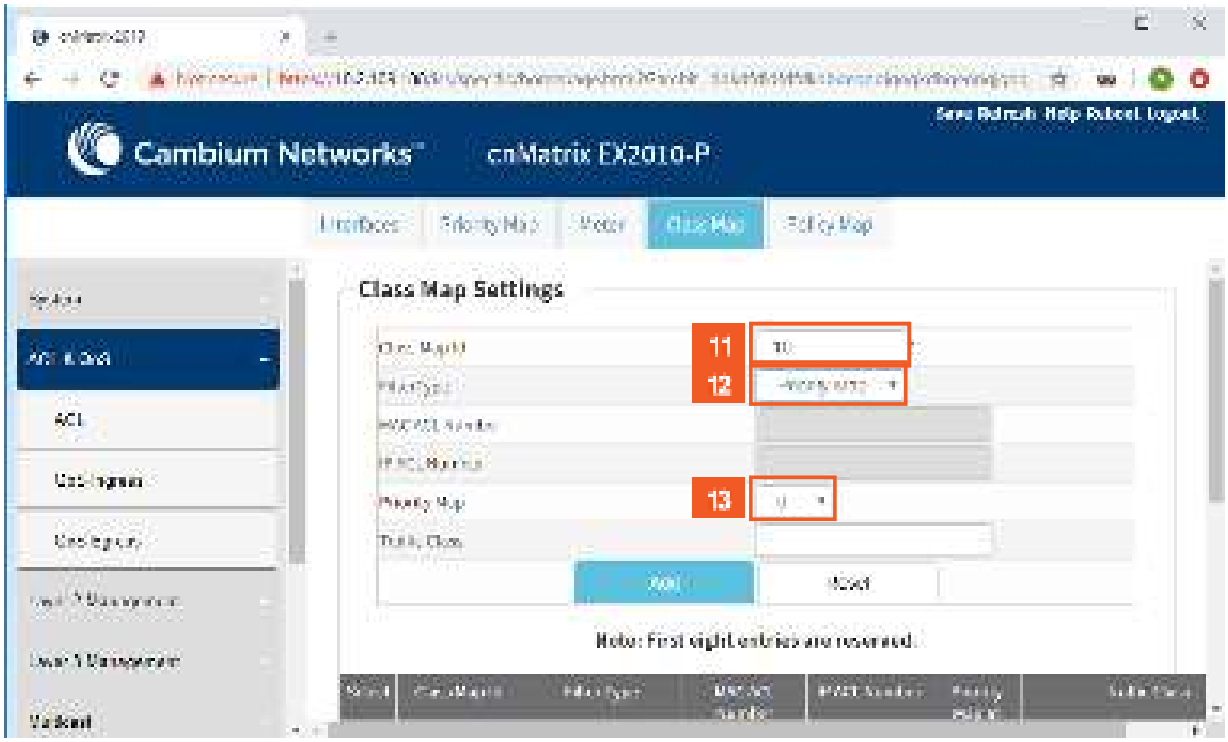
7 Select the **vlanPri** list item to set the incoming priority type as VLAN.



8 Type the value **6** into the **Regen Priority** field to set the regenerated priority.

9 Click the **Add** button to add and save the new configuration.

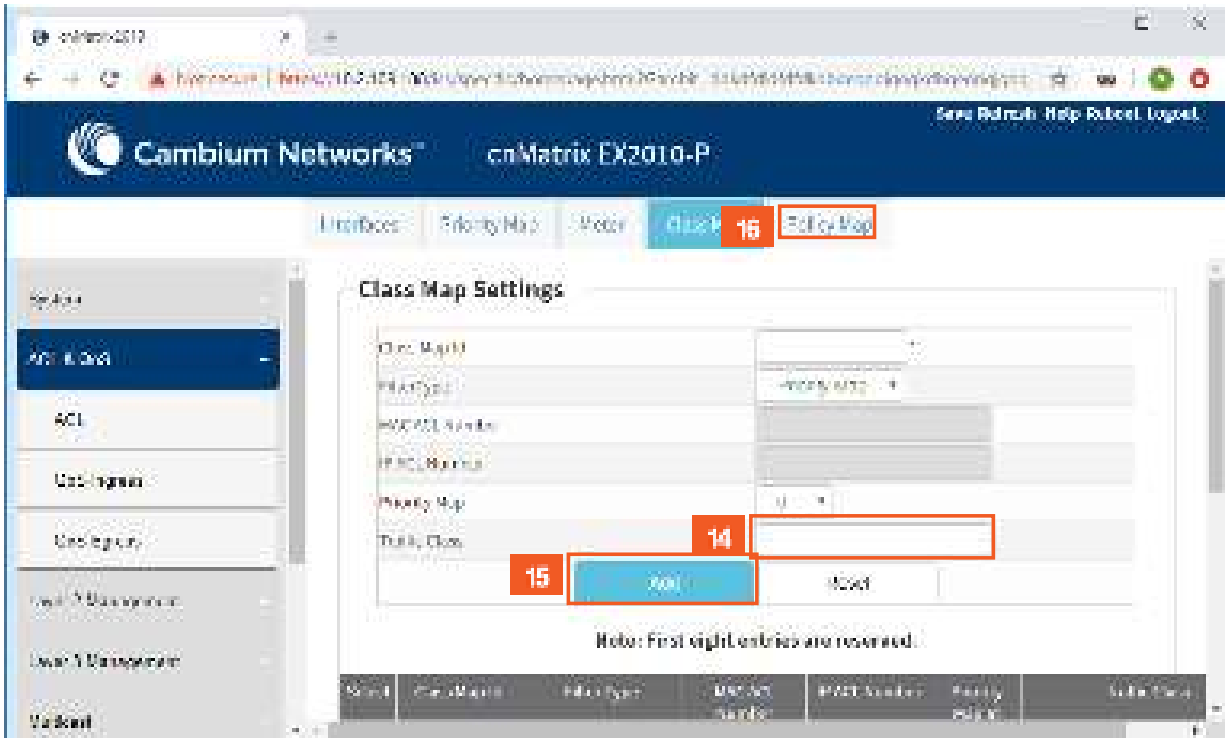
10 Click the **Class Map** tab.



11 Type the value **10** into the **Class Map ID** field to set an unique ID for class map.

12 Click the **Filter Type** drop-down list and select the **Priority Map** list item.

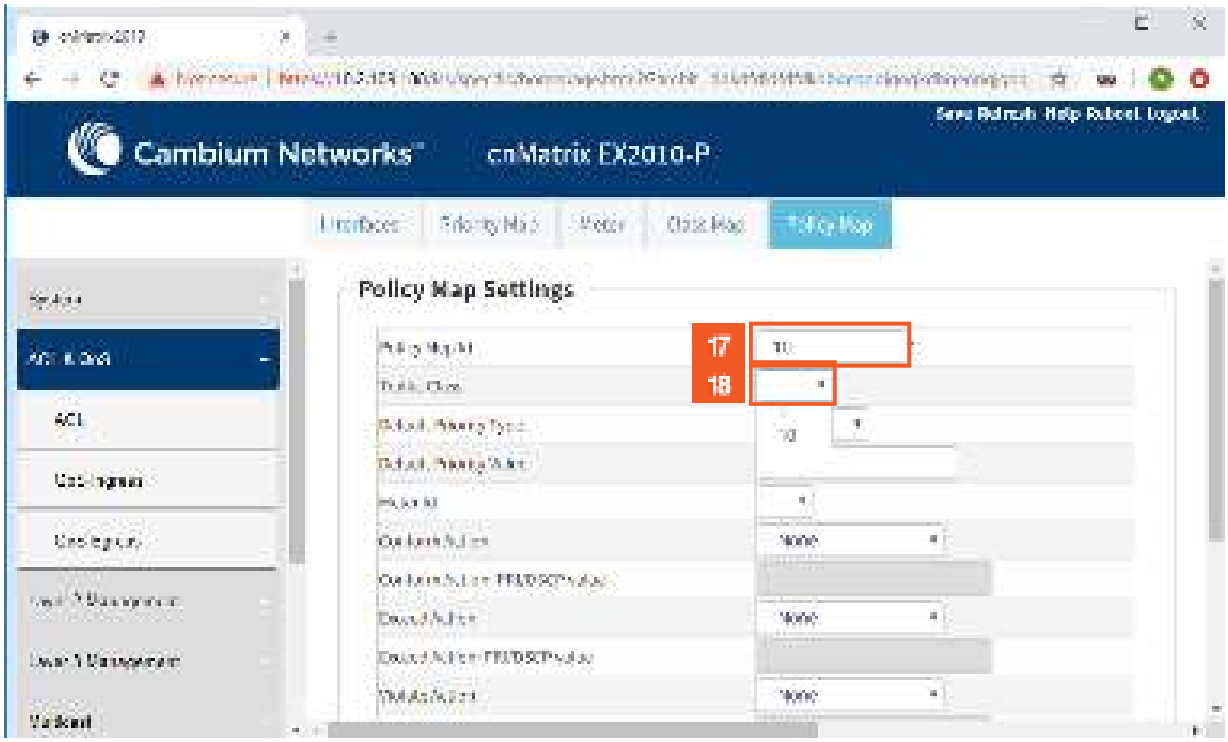
13 Click the **Priority Map** drop-down list and select the value **10** from the list items.



14 Type the value **10** into the **Traffic Class** field to set the traffic class associated with the class map.

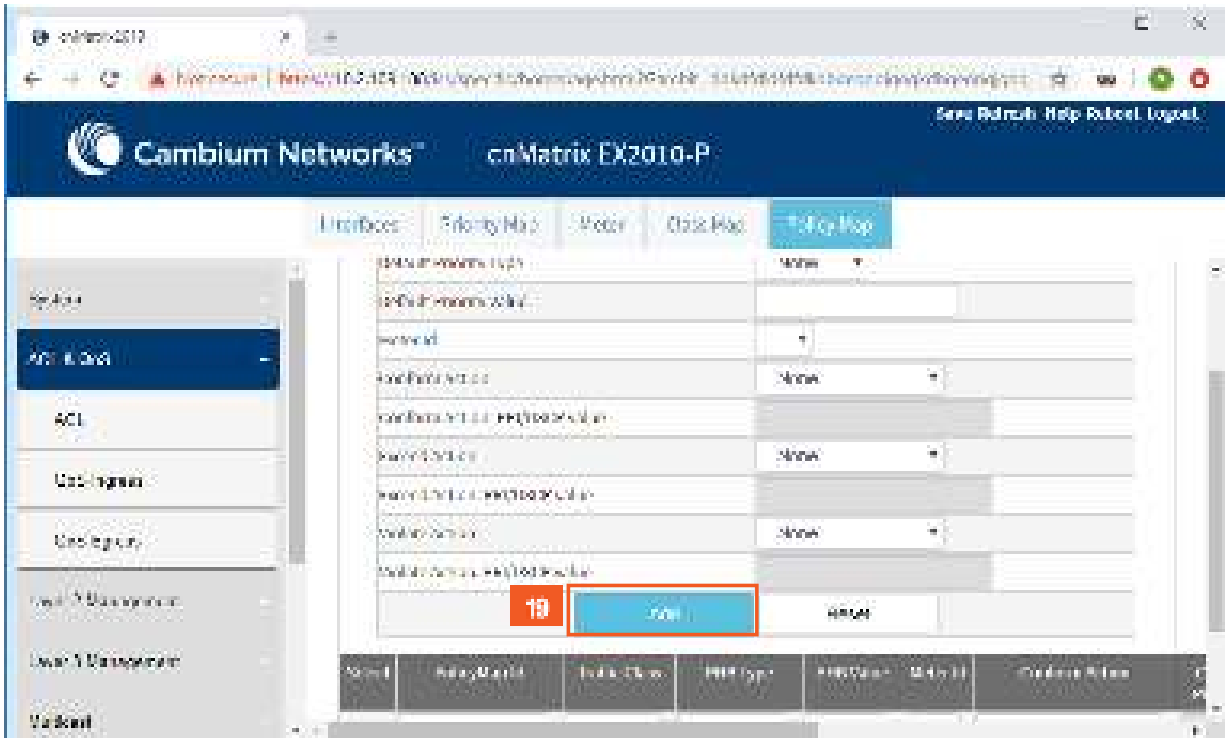
15 Click the **Add** button to add and save the new configuration.

16 Click the **Policy Map** tab.

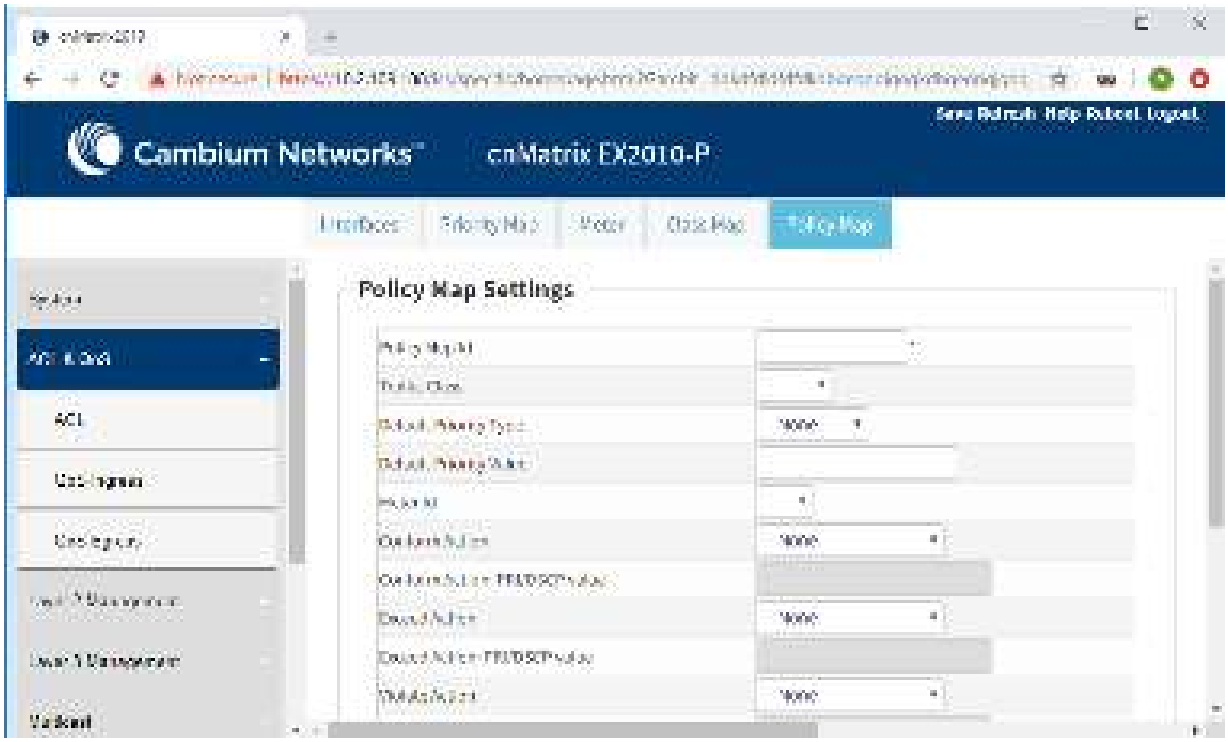


17 Type the value **10** into the **Policy Map ID** field to set the unique ID for policy map.

18 Click the **Traffic Class** drop-down list and select the value **10** from the list items.



19 Click the **Add** button to add and save the new configuration.



For more information about QoS WEB fields, see QoS WEB Fields.

2.14Policy-Based Automation with Dynamic Configuration

2.14.1Managing Policy Based Automation Using Auto Attach

2.14.1.1 Feature Description

Feature Overview

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

A typical deployment scenario would consist of the following components:

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

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

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

Settings that may be updated based on device discovery include:

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

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

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

Auto Attach Release 2.0.1 Capabilities

- Device Identification
  - LLDP Core TLVs (user-specified string matching of TLV data):
    - Chassis ID (TLV Type 1)
    - Port ID (TLV Type 2)
    - Port Description (TLV Type 4)
    - System Name (TLV Type 5)
    - System Description (TLV Type 6)
    - System Capabilities (TLV Type 7)
- Dynamic Actions
  - VLAN creation and port association.
  - Port PVID update.
  - Switch port mode (Hybrid only) update.
- AA Monitoring/Configuration
  - CLI
  - SNMP

Limitations

User Interface Limitations:

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

Feature Interaction Limitations:

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

Feature Limitations:

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

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

    ==>Trunk
  - Action data can include a VLAN list. A PVID can't be specified.
  - The QoS Trust mode (i.e., Trust 802.1p/Trust DSCP/Untrusted) for a port can be updated based on device discovery. The QoS Trust mode setting is restored to the previous statically configured value during the device cleanup phase.
  - The default port 802.1p user priority value (0 to 7) can be updated based on device discovery. The default port 802.1p user priority value setting is restored to the previous statically configured value during the device cleanup phase.
  - The administrator can identify up to four device ports to act as PBA uplinks. VLANs (newly created or existing) that are applied to the port on which the matching device was detected are also associated with the uplink ports. The VLAN membership update remains in effect while the related PBA policy is active. Uplink ports must be operating in hybrid switch port mode to be valid. Uplinks are identified using the interface type and

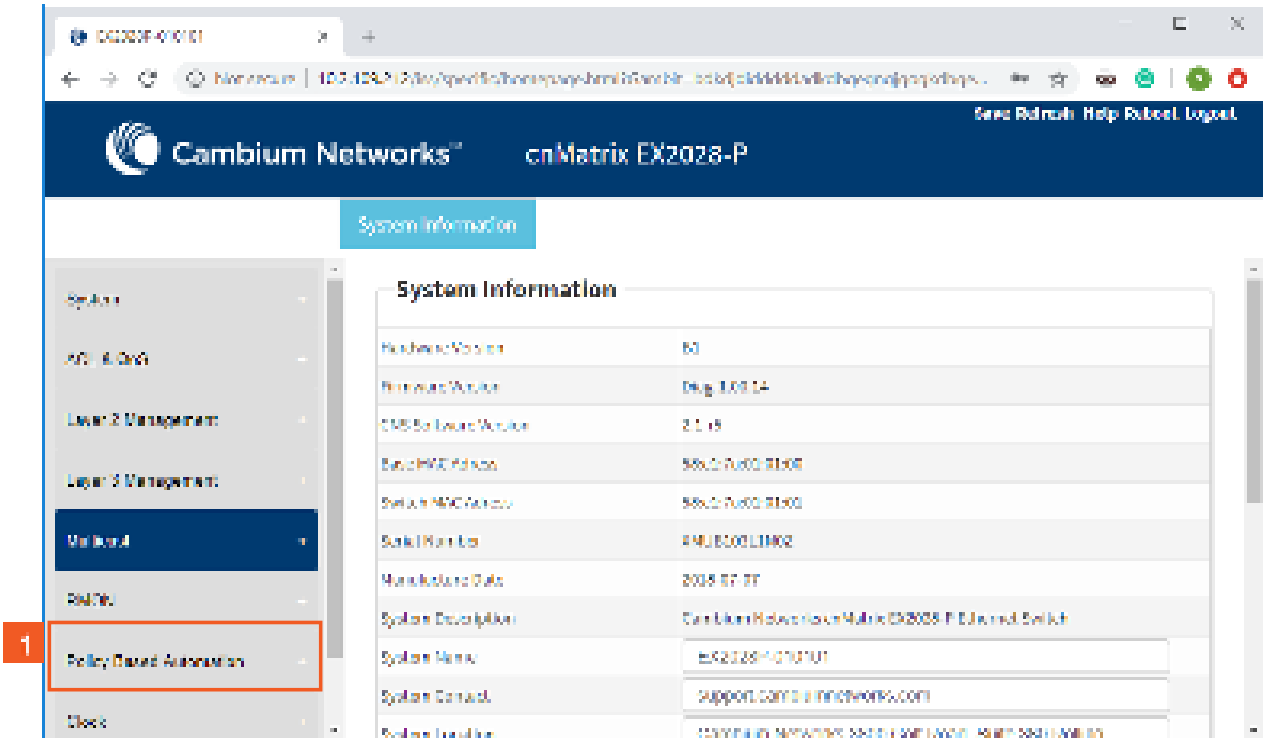
the slot/port naming convention (e.g., ‘Gi0/5,Ex0/1’). An action that includes uplink data must also include VLAN data for port membership updates.

- The PoE priority setting (i.e., Critical/High/Low) for a port can be updated based on device discovery. The PoE priority setting is restored to the previous statically configured value during the device cleanup phase. Requesting this action returns an error on devices that are not PoE-capable.

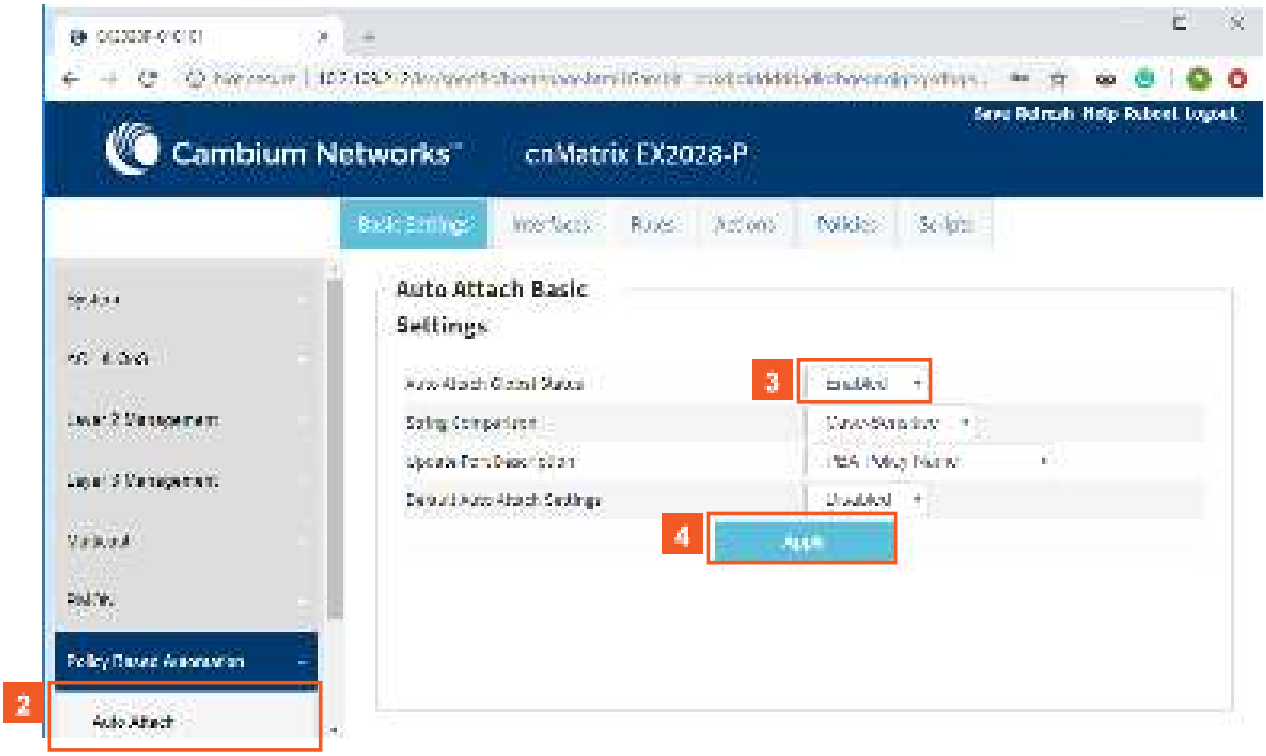
For more information, see Auto Attach Feature Description.

2.14.1.2 Network Diagram

2.14.2 How to Enable Auto Attach in WEB Interface



1 Click the **Policy Based Automation** tab.



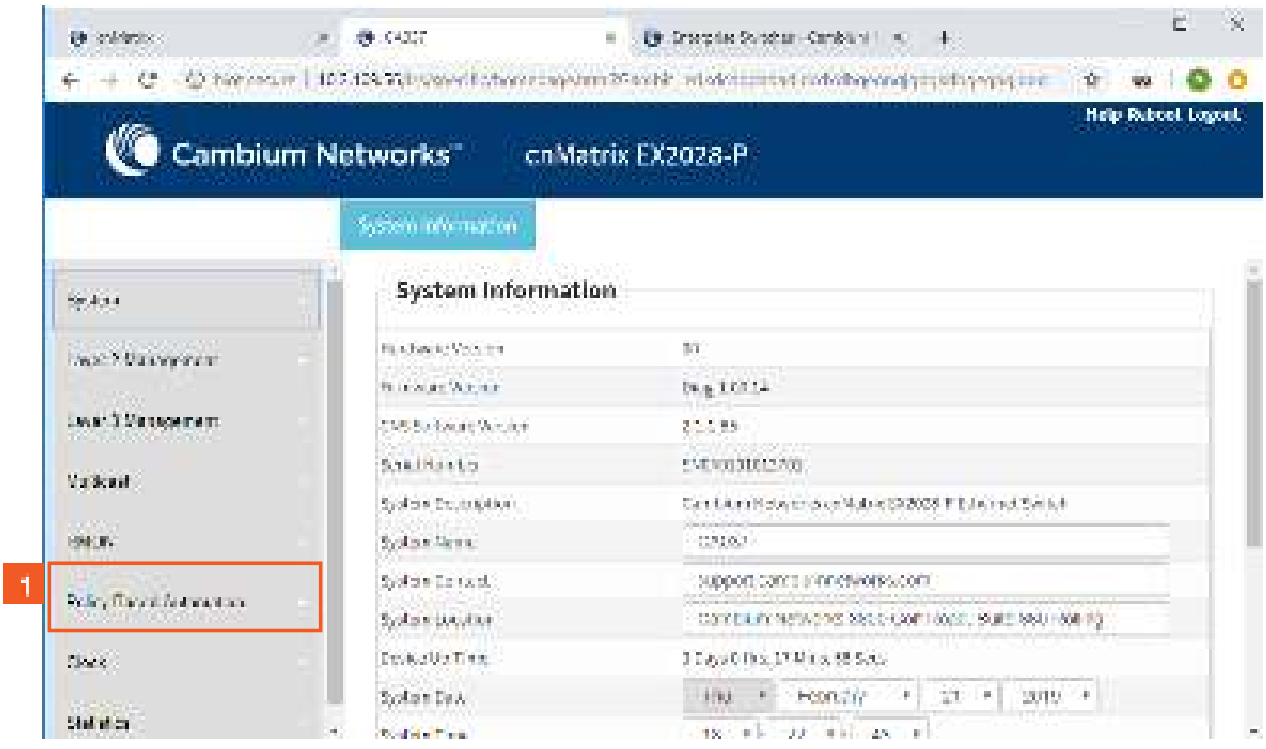
2 Click the **Auto Attach** menu item. The **Auto-Attach Basic Settings** page is displayed.

3 Click the **Auto Attach Global Status** drop-down list to select the **Auto Attach global status.** Select the **Enabled** list item.

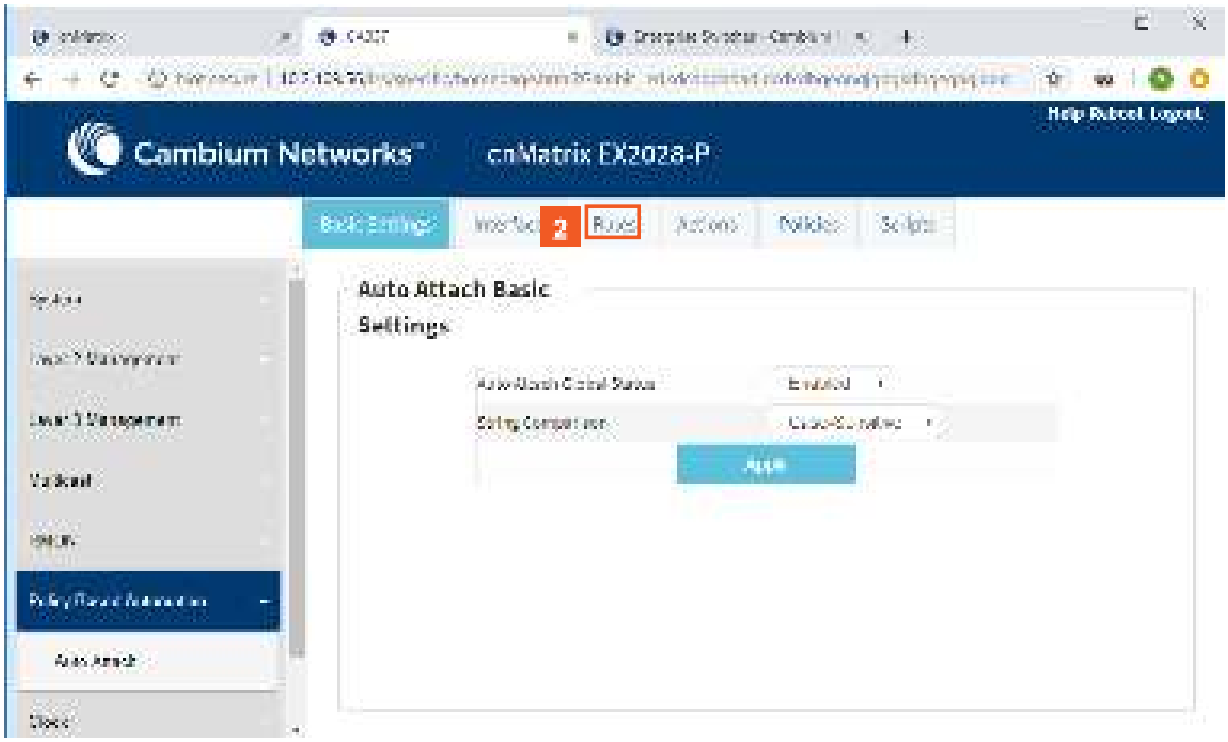
4 Click the **Apply** button.

The **Auto Attach** feature is enabled by default.

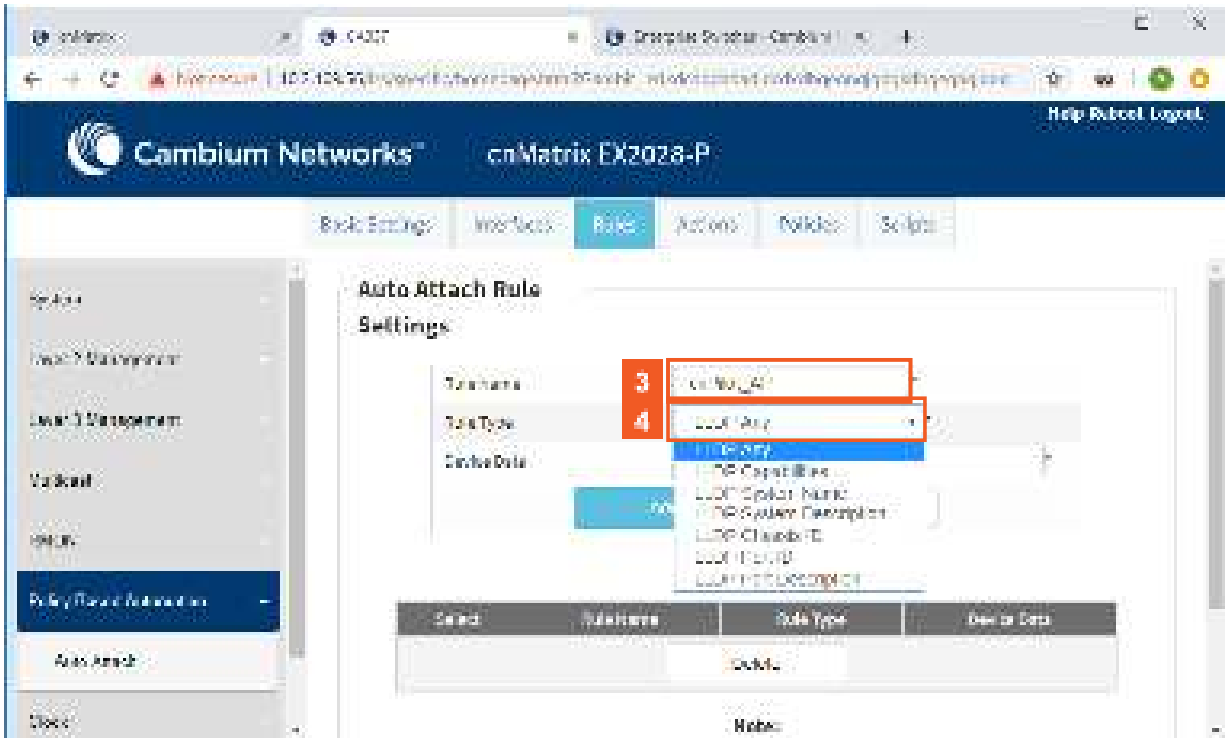
2.14.3Configuring Auto Attach Rules in WEB Interface



1 Click the **Policy Based Automation** menu item.

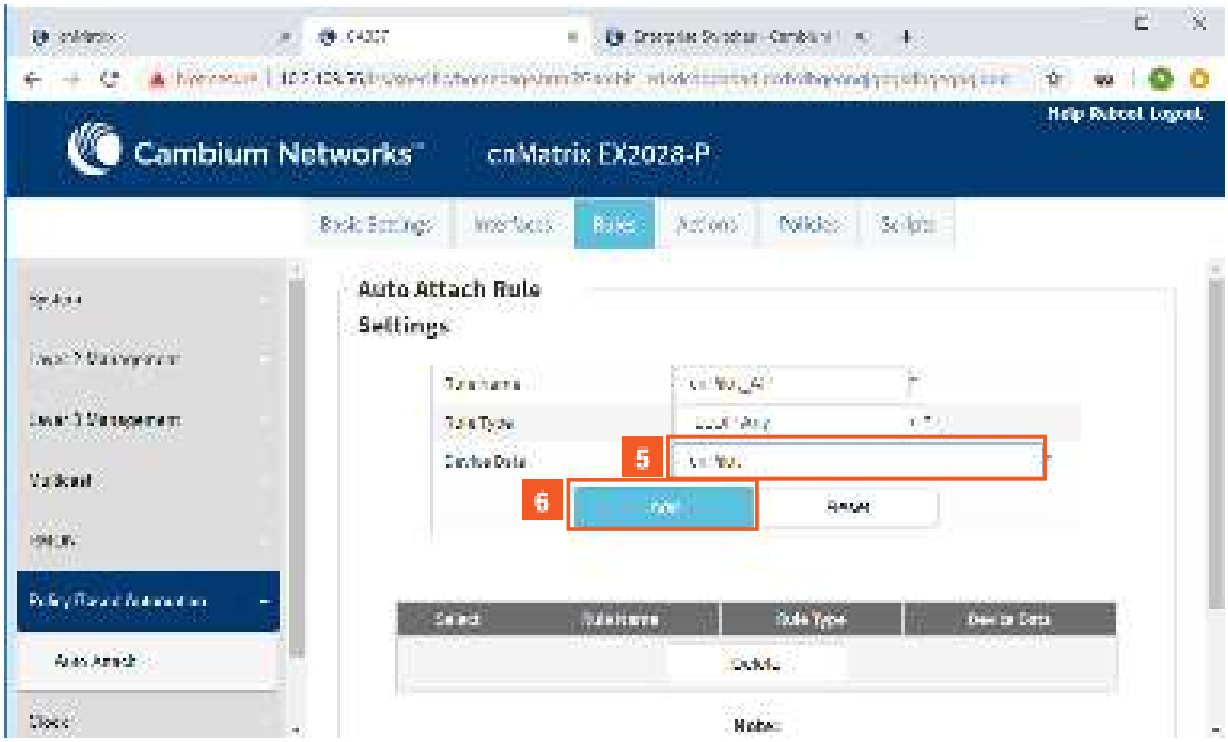


2 Click the **Rules** tab. The **Auto Attach Rule Settings** window is displayed.



3 Enter the **cnPilot_AP** (the Auto Attach rule name) name into the **Rule Name** field.

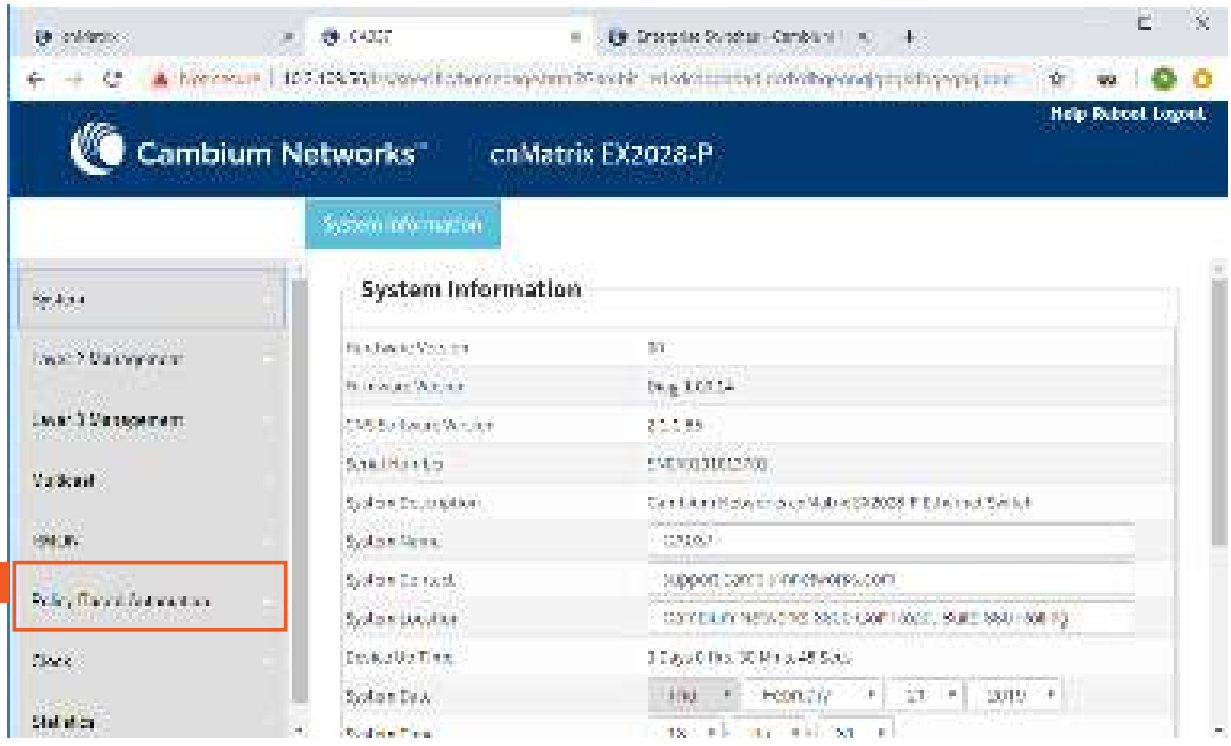
4 Click the **Rule Type** drop-down button and select the **LLDP Any** (matching criteria) list item.



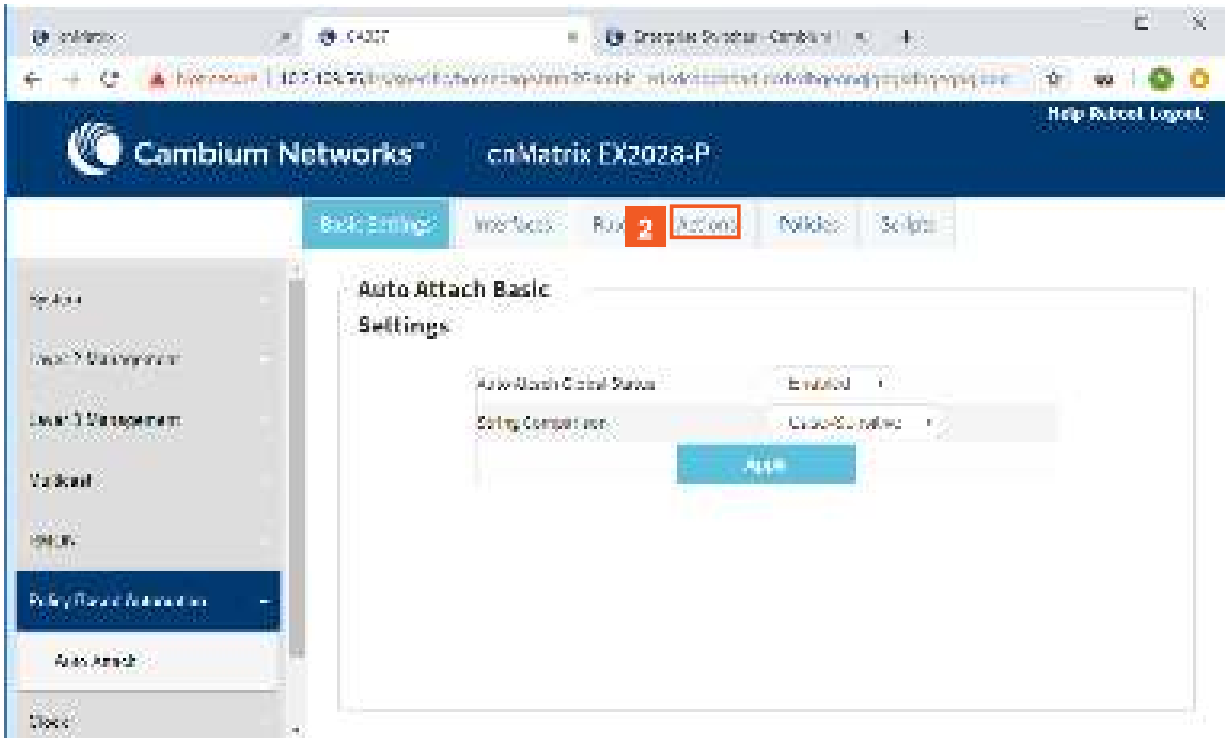
5 Enter the **cnPilot** (device data to be matched) device name into the **Device Data** field.

6 Click the **Add** button.

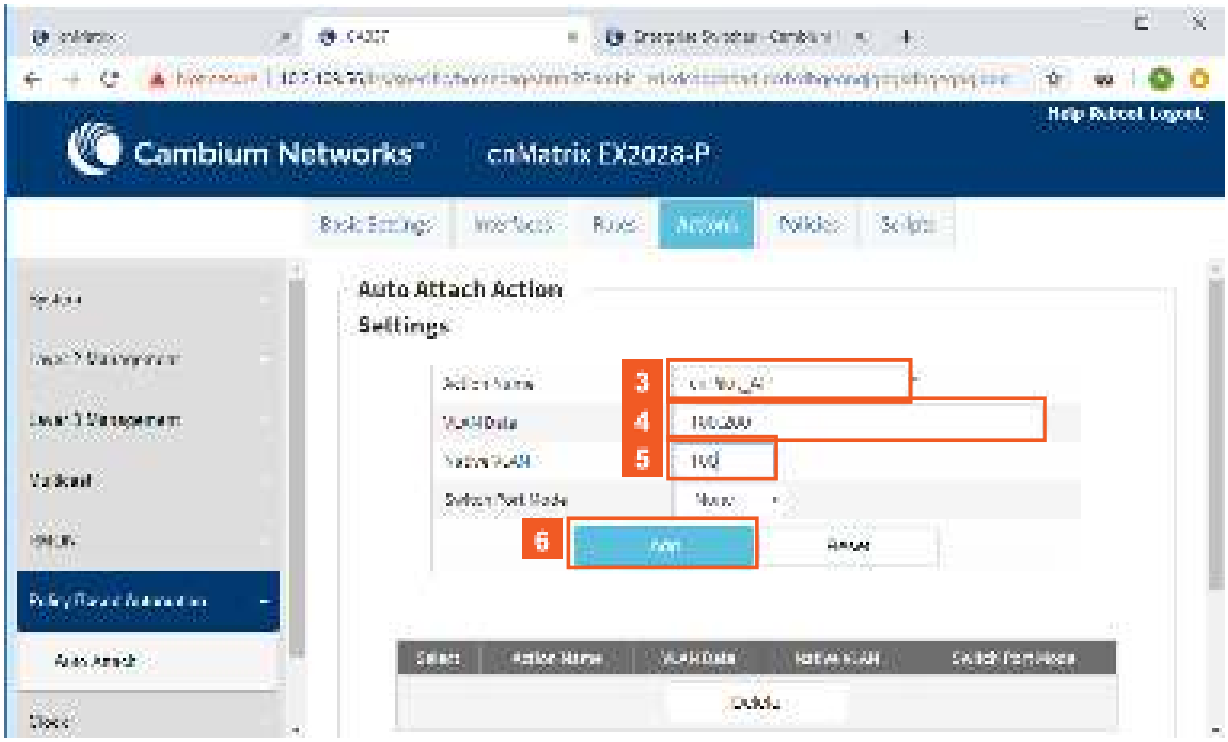
2.14.4Configuring Auto Attach Action in WEB Interface



1 Click the **Policy Based Automation** menu item.



2 Click the **Actions** tab. The **Auto Attach Action Settings** window is displayed.



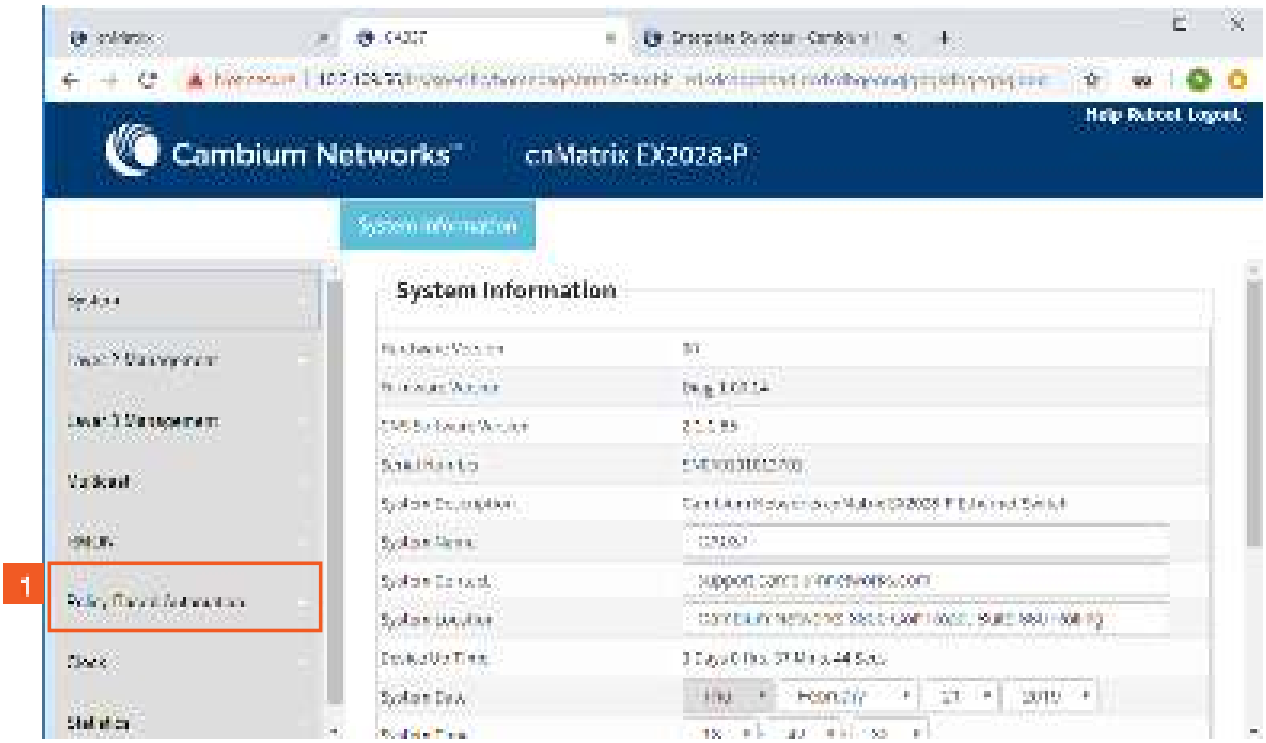
3 Enter the **cnPilot_AP** action name into the **Action Name** field.

4 Enter the **100,200** (VLAN IDs) values into the **VLAN Data** field.

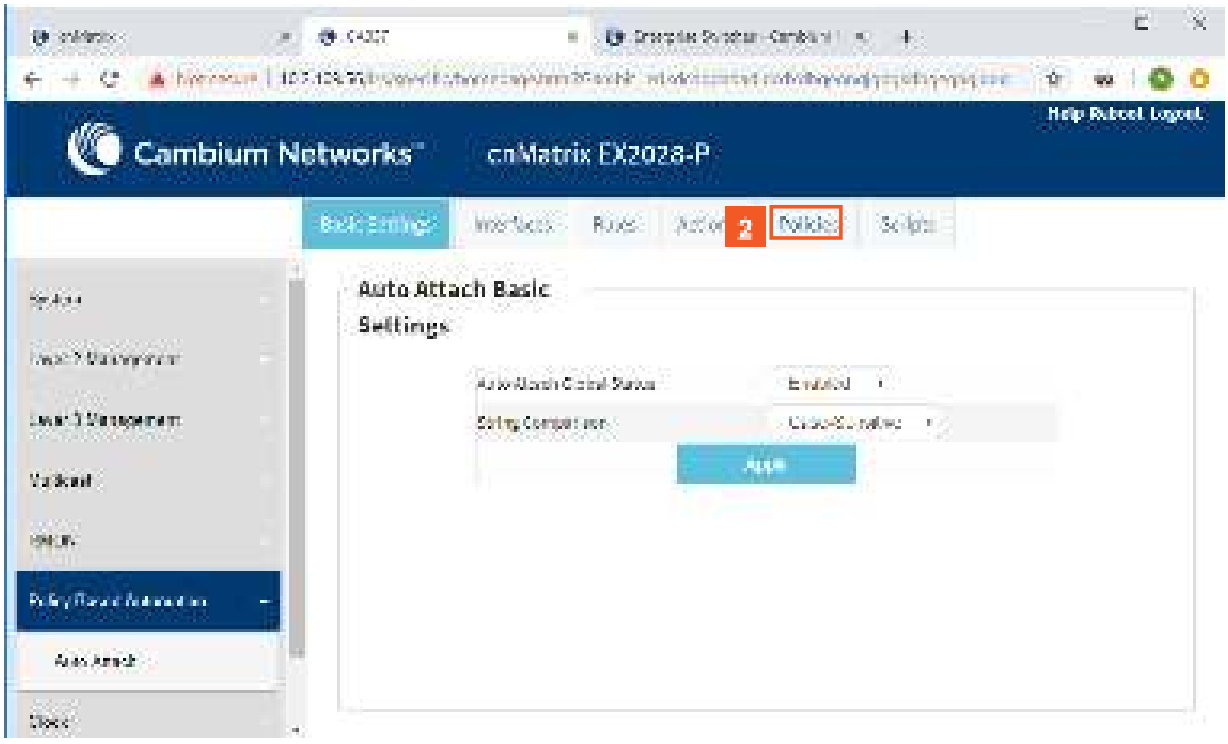
5 Enter the **100** (Native VLAN ID) value into the **Native VLAN** field.

6 Click the **Add** button to create the Auto Attach action.

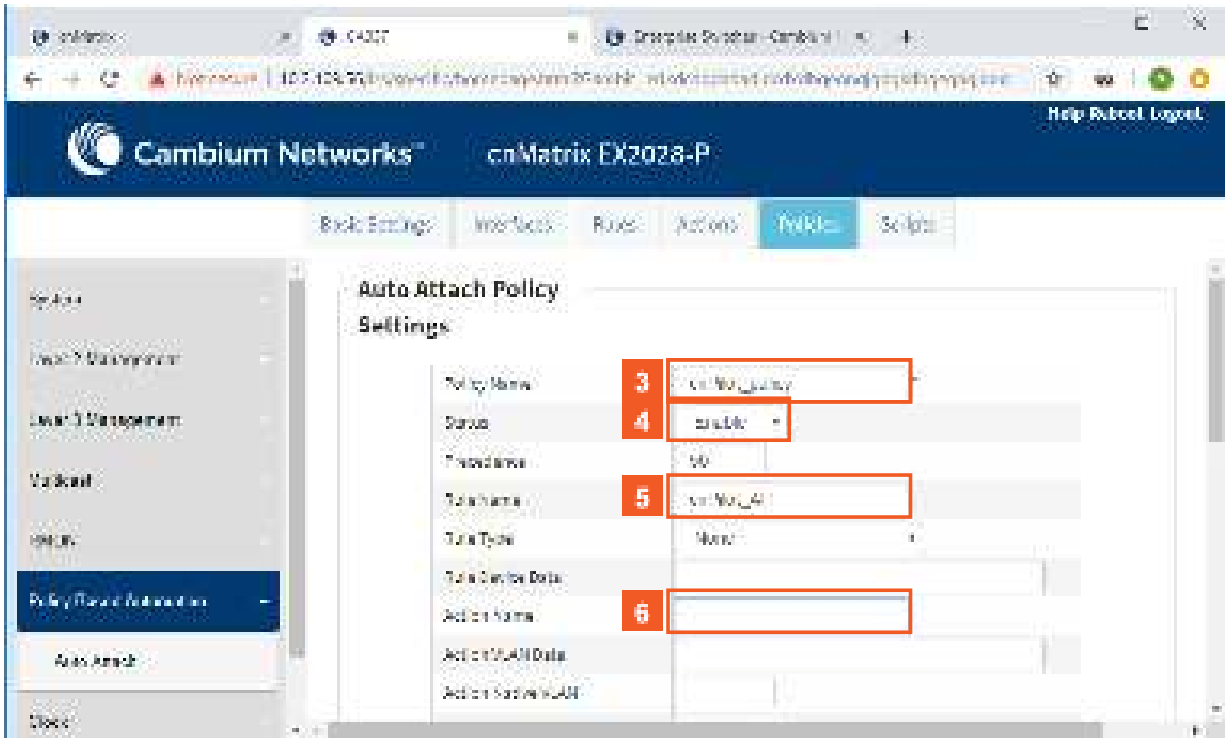
2.14.5Configuring Auto Attach Policy in WEB Interface



1 Click the **Policy Based Automation** menu item.



2 Click the **Policies** tab. The **Auto Attach Policy Settings** window is displayed.

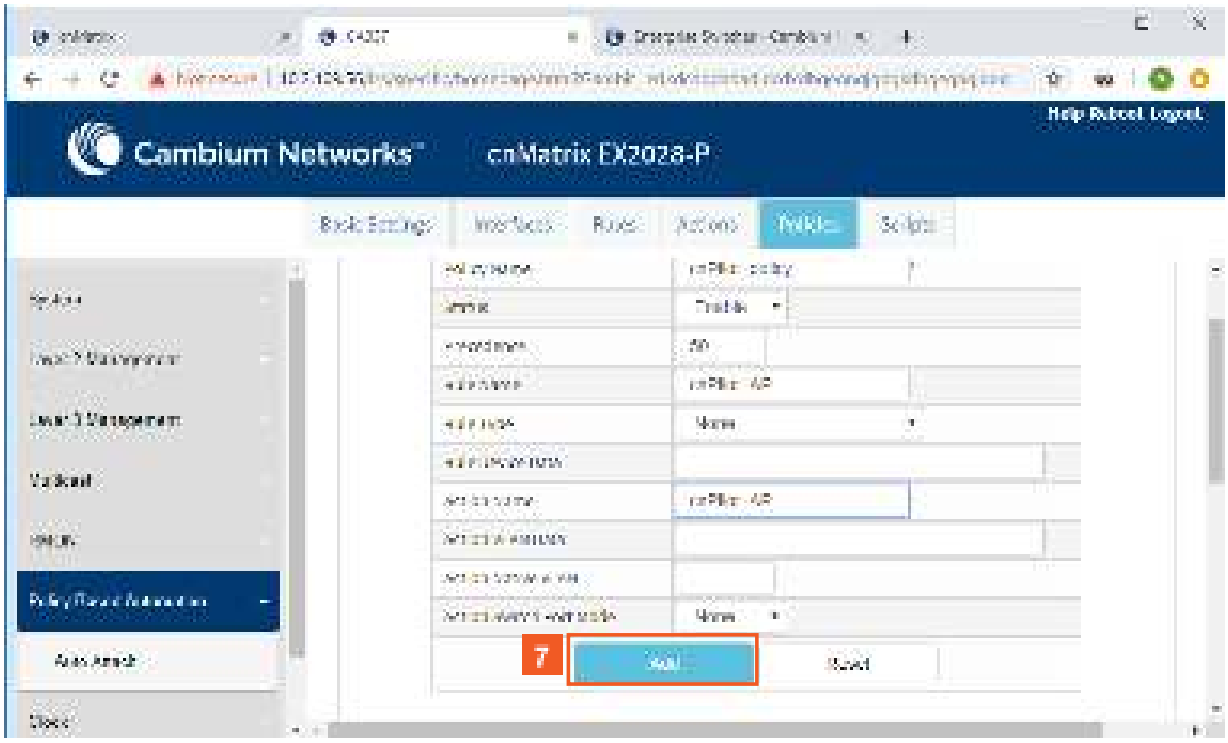


3 Enter the **cnPilot_policy** name into the **Policy Name** field.

4 Click the **Status** drop-down button and select the **Enable** list item.

5 Enter the **cnPilot_AP** name (previously configured rule) into the field.

6 Enter the **cnPilot_AP** name (previously configured action) into the **Action Name** field.



7 Click the **Add** button.

2.15 Dynamic ARP Inspection (Starting with version 2.1)

2.15.1 Managing Dynamic ARP Inspection

2.15.1.1 Feature Overview

Feature Overview

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

Scaling Numbers

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

Limitations

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

Default Values

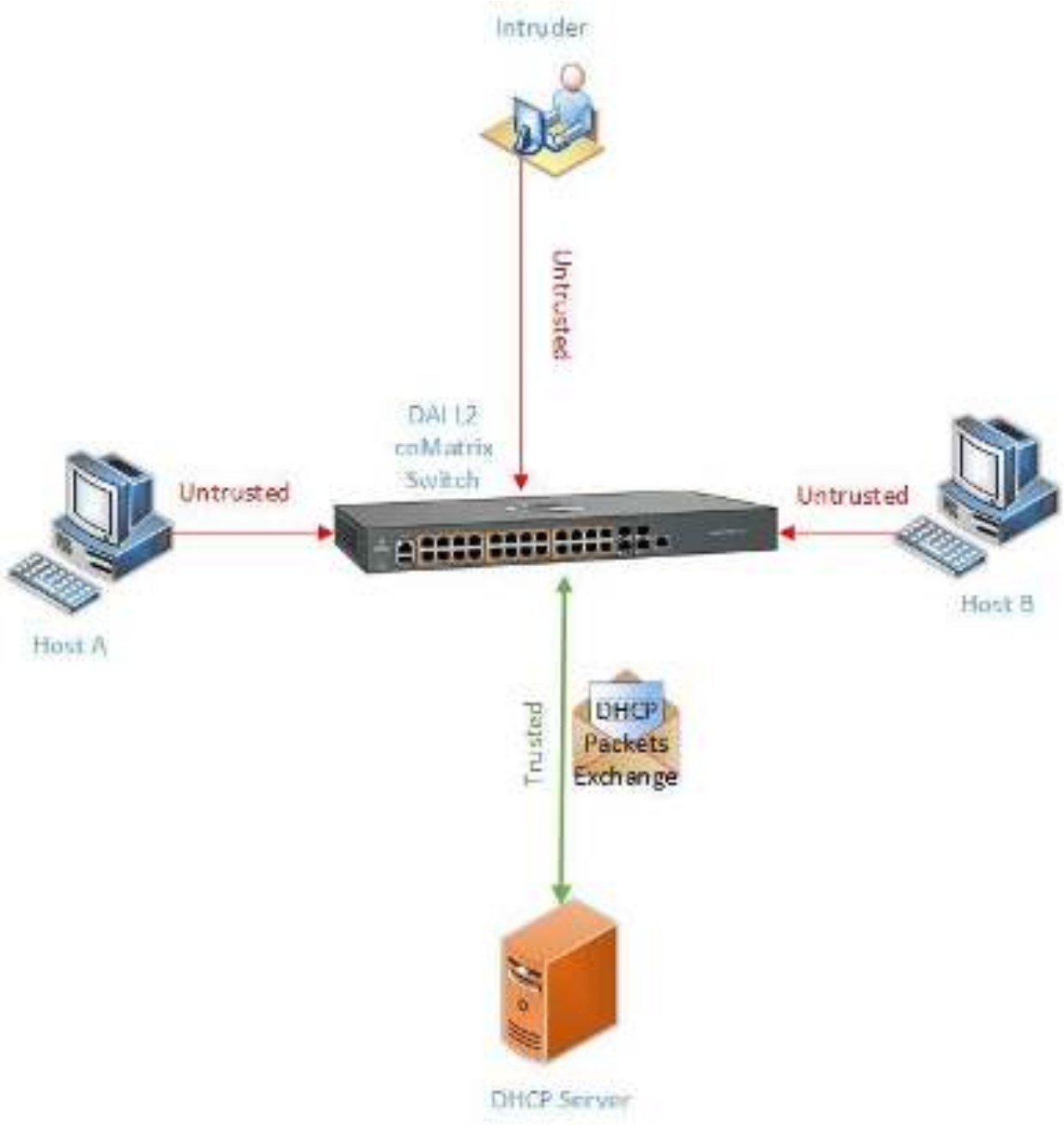
- The DAI feature is disabled on all VLANs.
- The DAI trust state is set as untrusted on all the physical interfaces.
- The DAI feature does not perform any validation checks.

Prerequisites

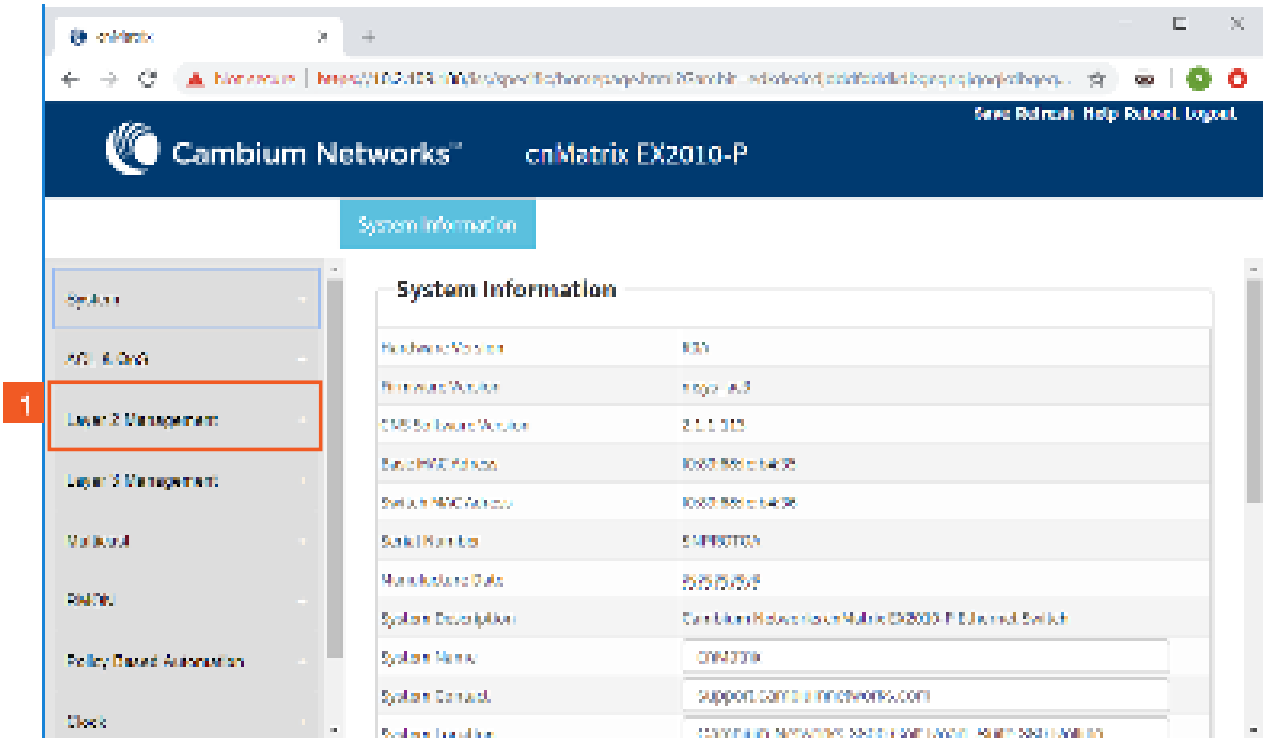
- In order for the DAI validation process to be initiated, the DAI has to be enabled on the VLAN on which the DAI is required to validate the ARP packets. DAI associates a trust state with each interface on the switch. ARP response packets received on trusted interfaces will skip the DAI validation process,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

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

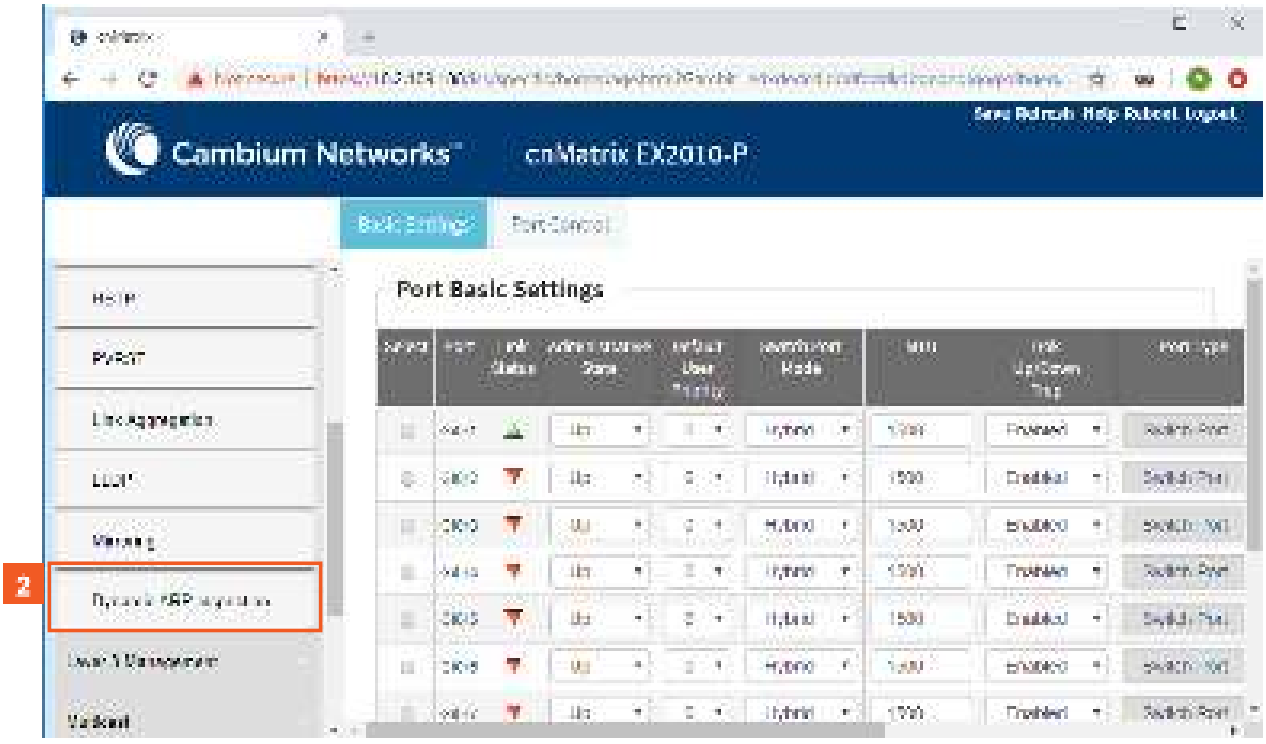
2.15.1.2 Network Diagram



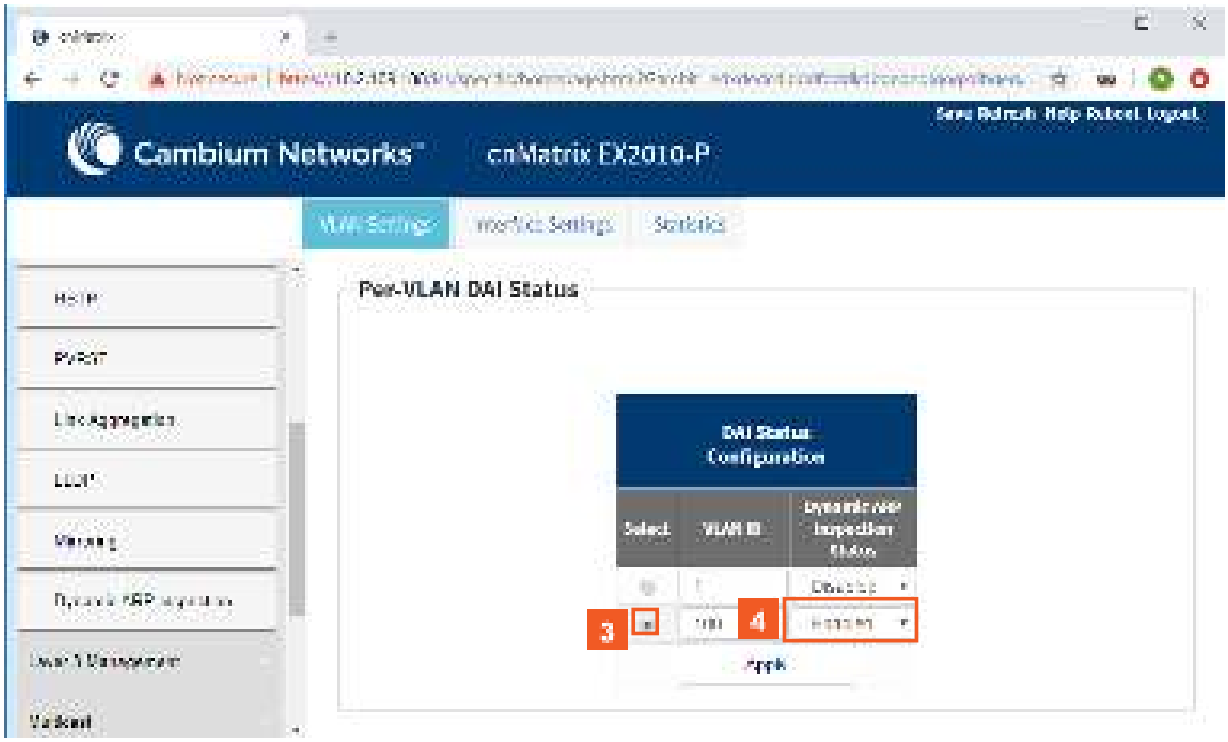
2.15.2 How to Enable Dynamic ARP Inspection in WEB Interface



1 Click the **Layer 2 Management** tab.



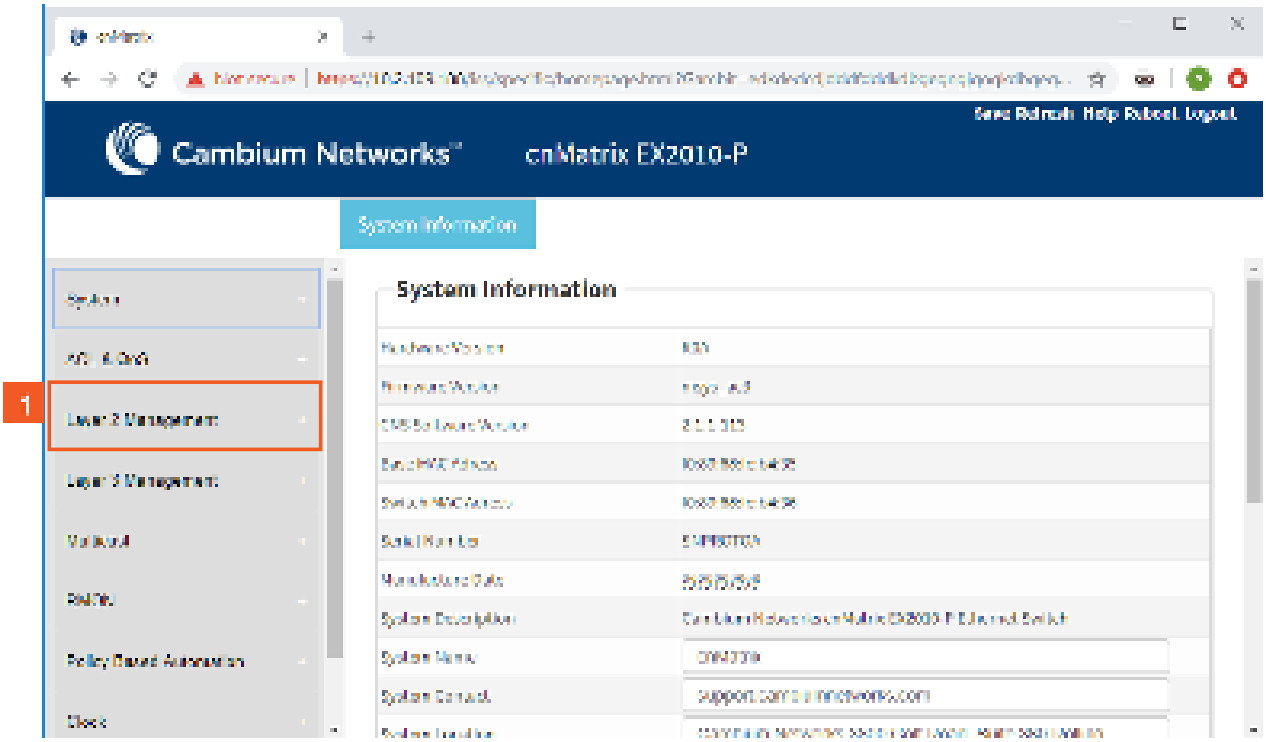
2 Click the **Dynamic ARP Inspection** menu item. The **Per-VLAN DAI Status** window is displayed.



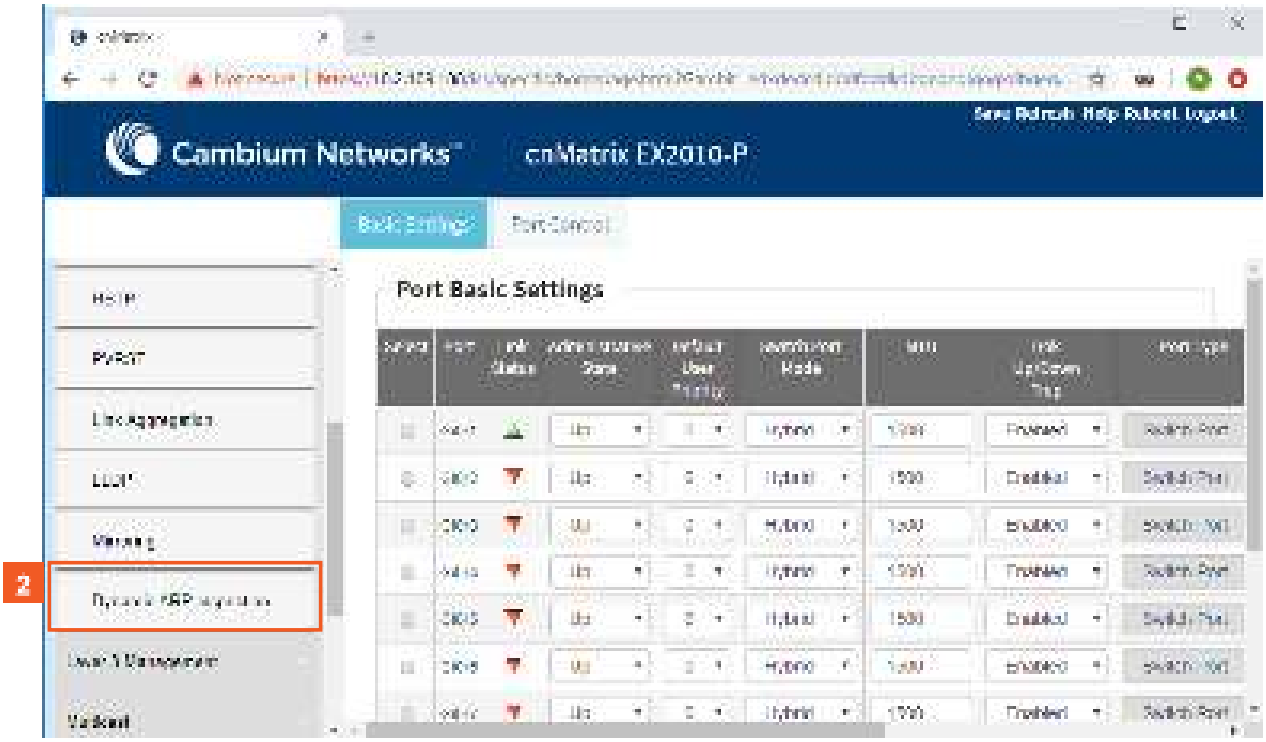
3 Select the radio button for the VLAN on which you want to enable the DAI feature.

4 Click the **Dynamic ARP Inspection Status** drop-down list and select the **Enabled** list item.

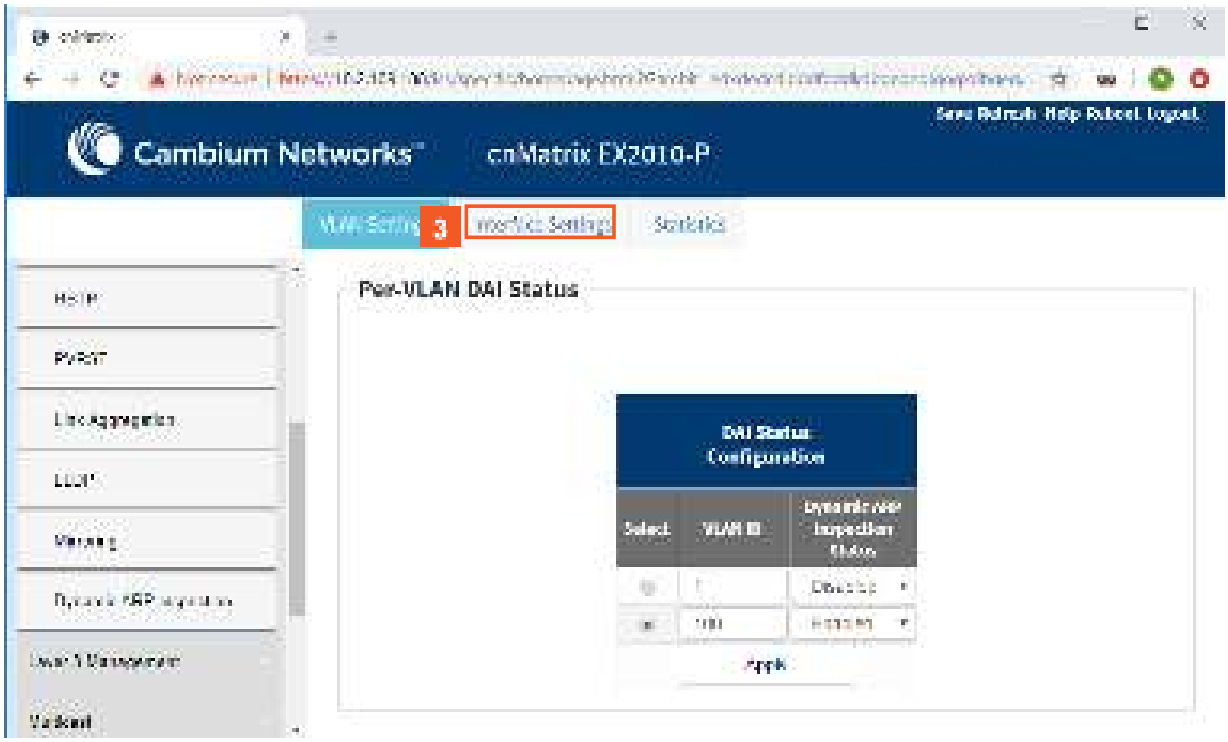
2.15.3 Configuring the Dynamic ARP Inspection Trust State on an Interface in WEB Interface



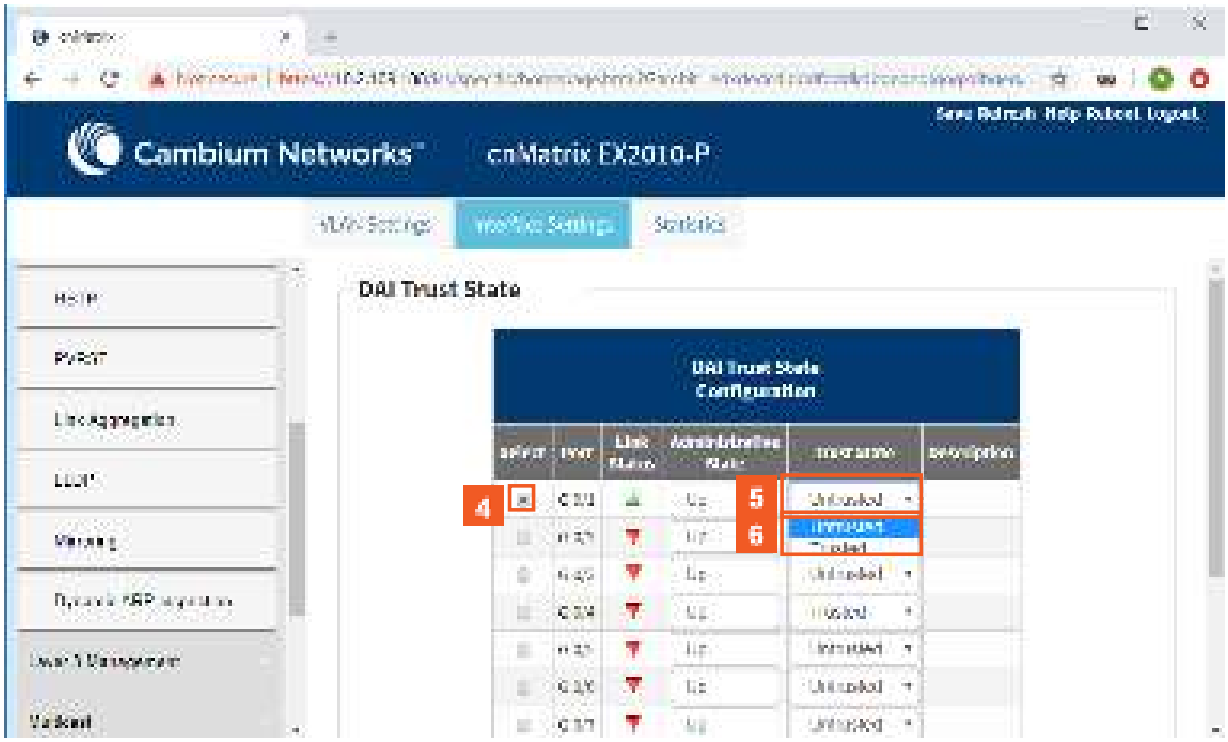
1 Click the **Layer 2 Management** tab.



2 Click the **Dynamic ARP Inspection** menu item.



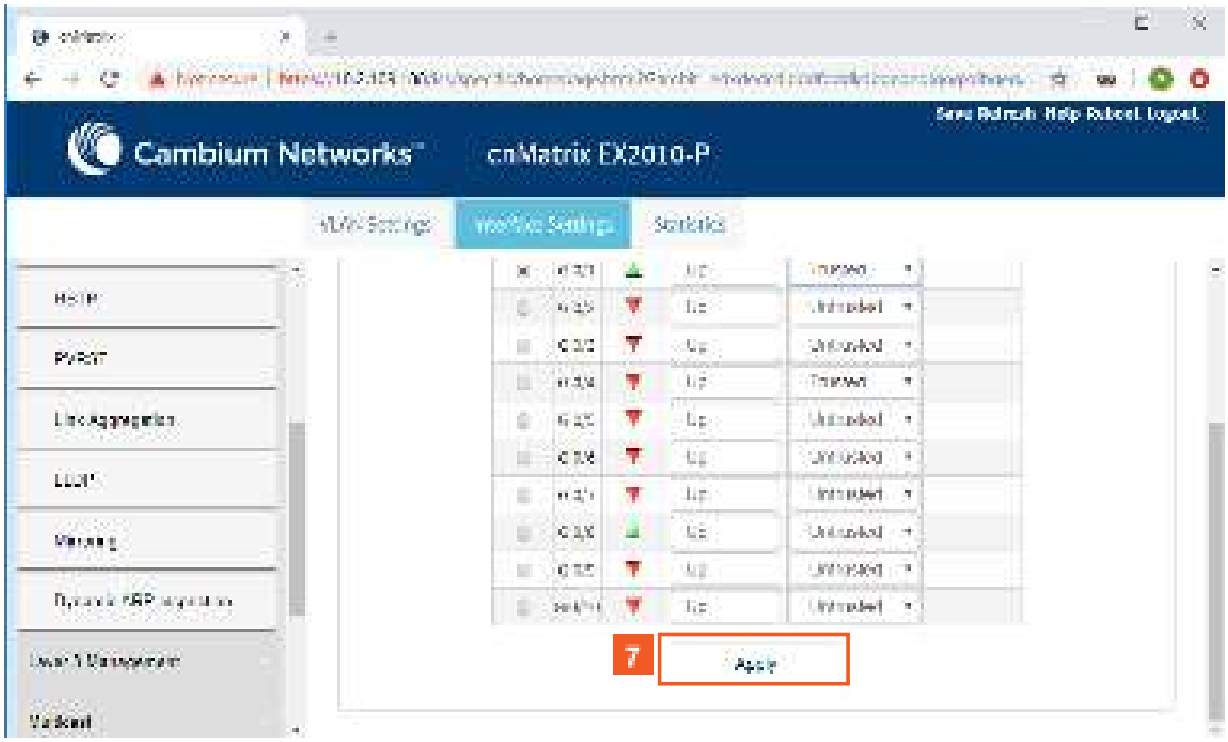
3 Click the **Interface Settings** tab. The **DAI Trust State** window is displayed.



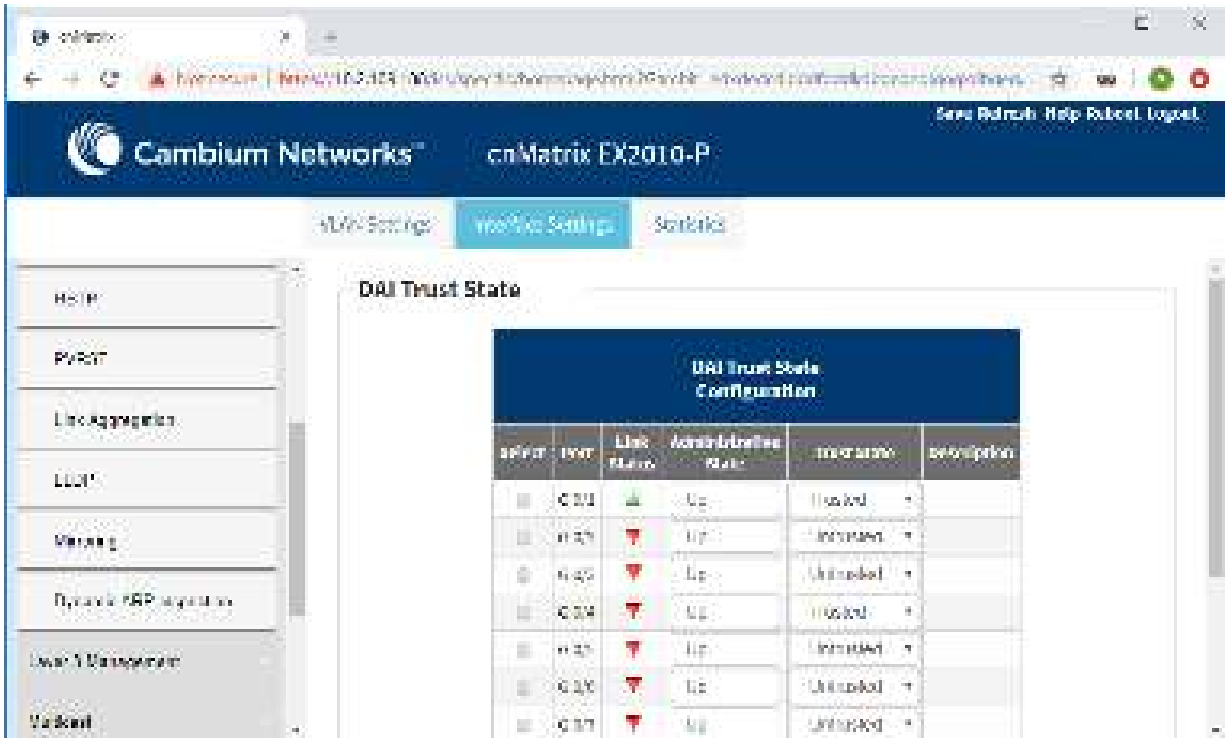
4 Select the radiobutton for the interface that you want to configure as trusted.

5 Click the **Trust State** drop-down (the line of the selected interface).

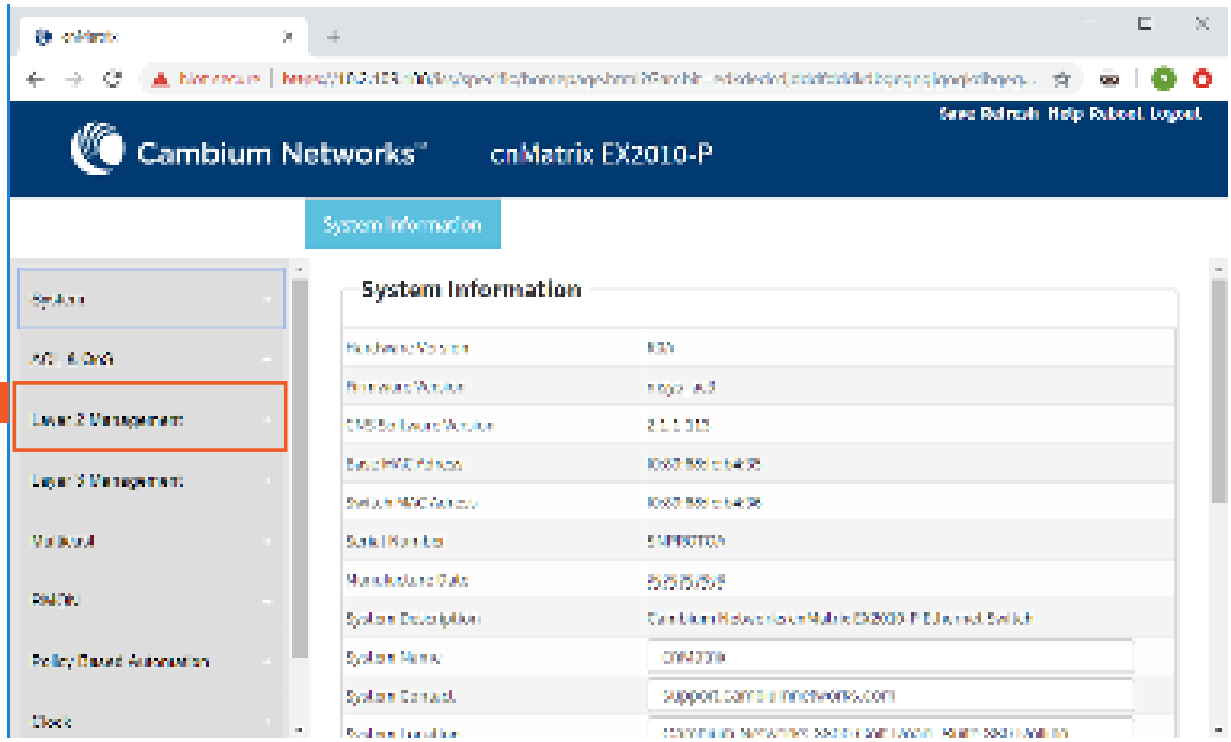
6 Select the **Trusted** list item.



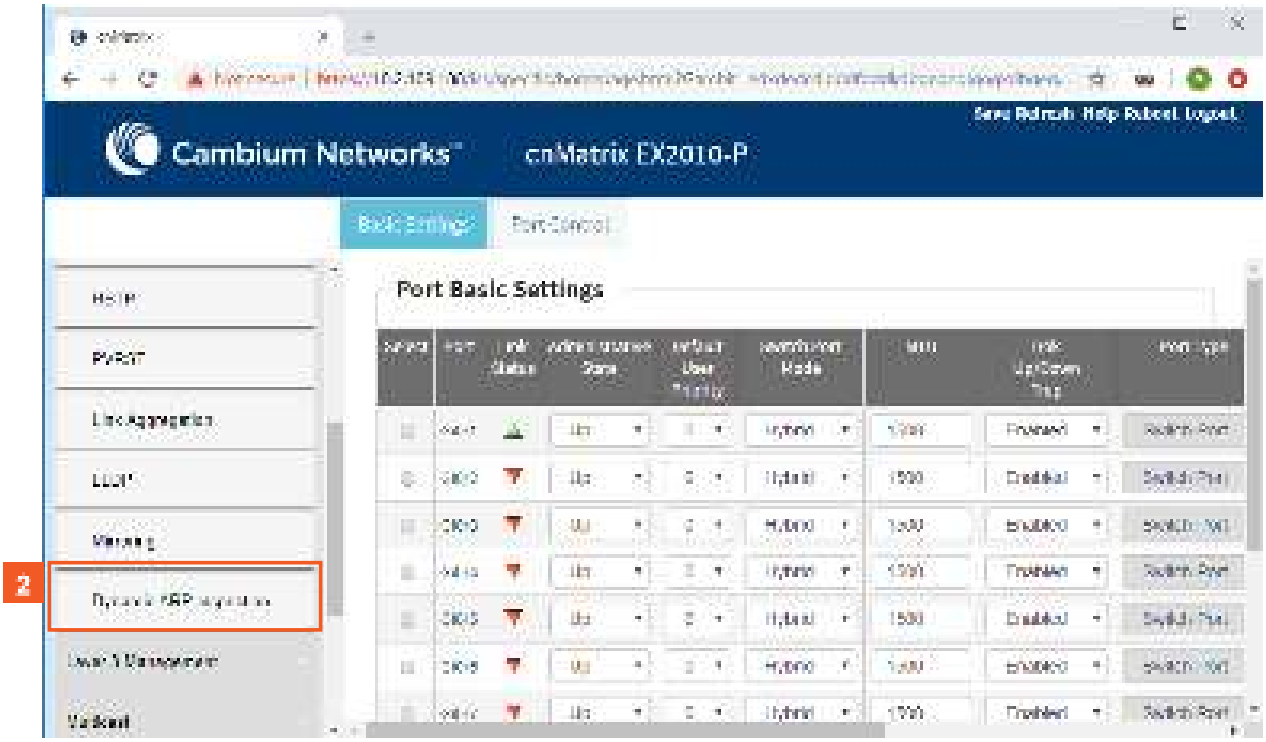
7 Click the **Apply** button.



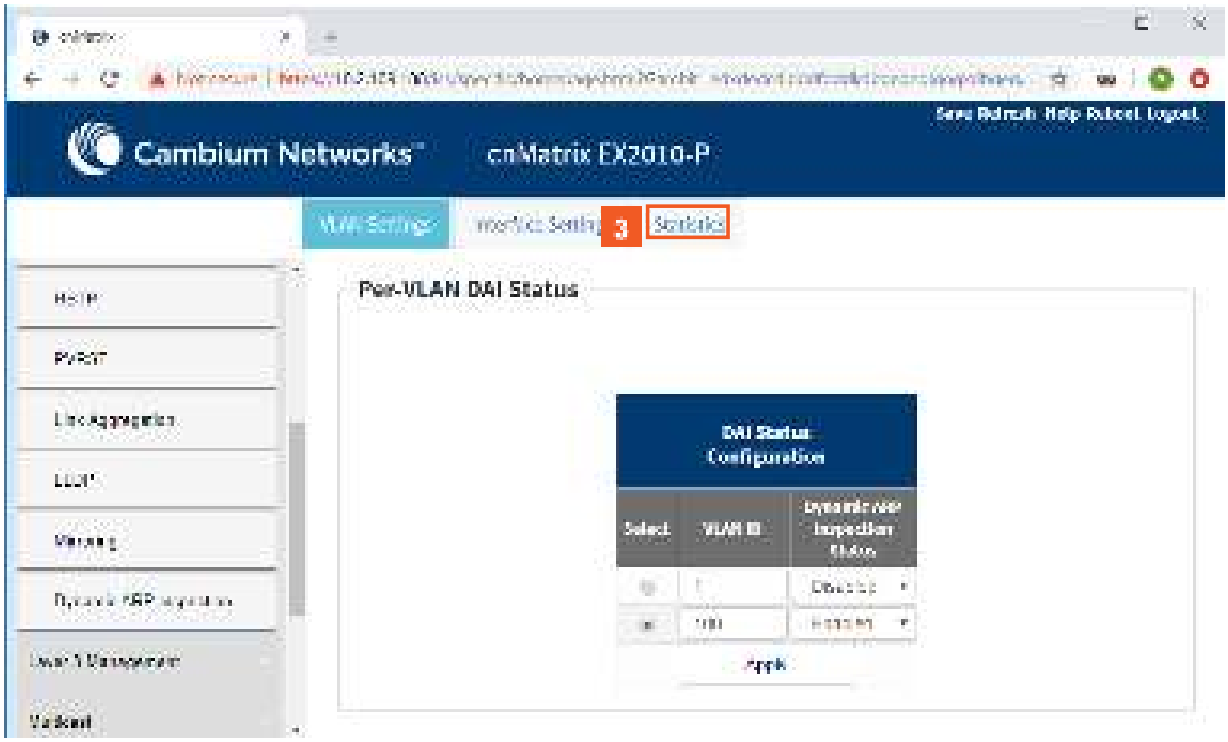
2.15.4How to Verify the Dynamic ARP Inspection per VLAN in WEB Interface



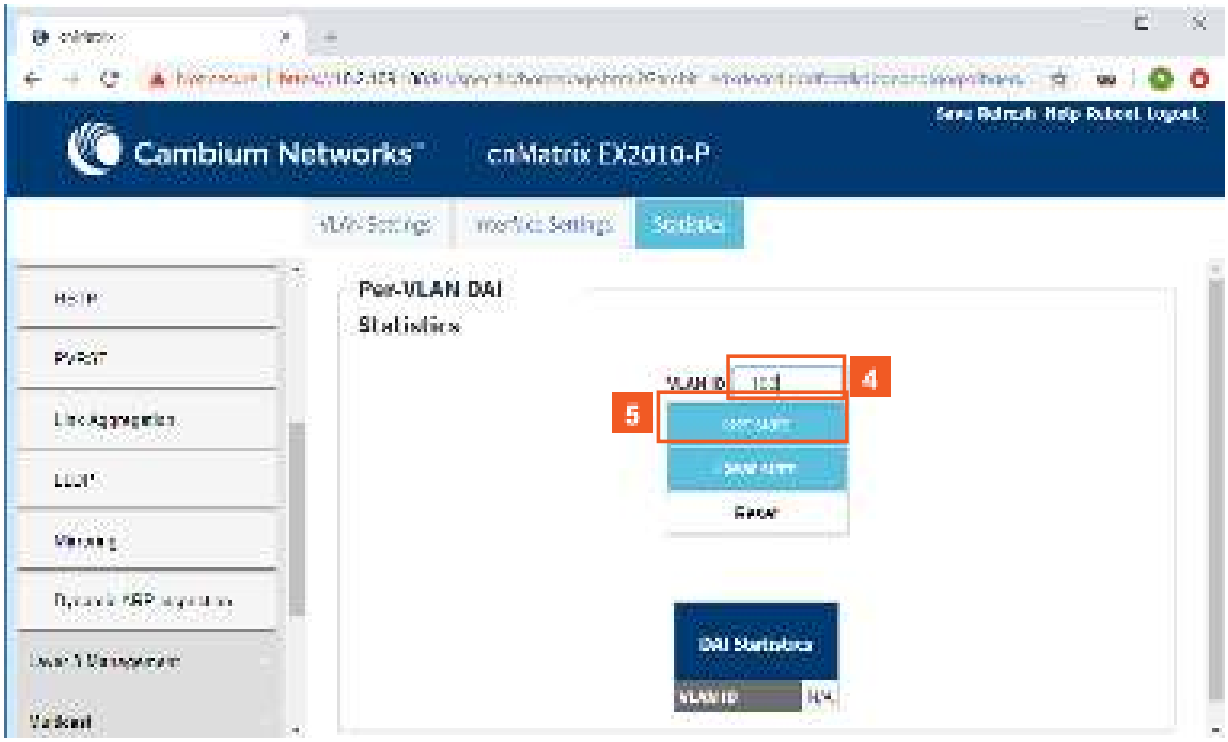
1 Click the **Layer 2 Management** tab.



2 Click the **Dynamic ARP Inspection** menu item.



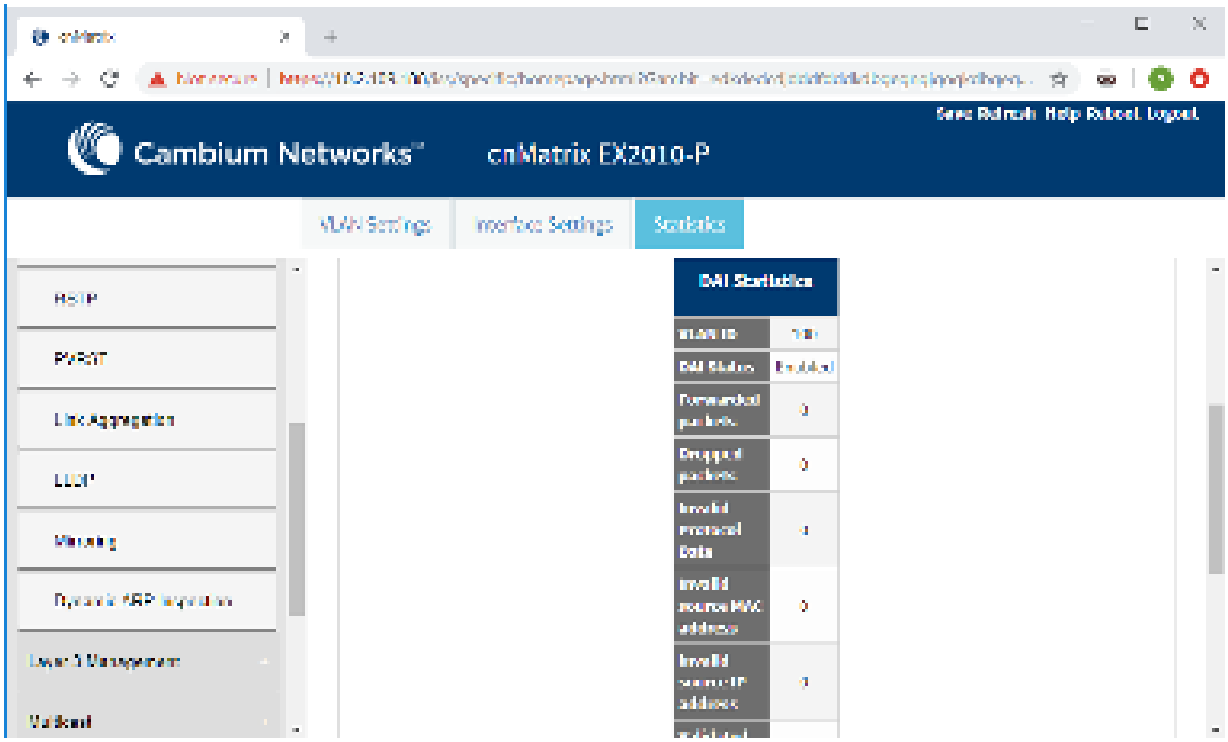
3 Click the **Statistics** tab.



4 Type the value **100** into the **VLAN ID** field (previously created VLAN).

100 = VLAN-ID

5 Click the **Get stats** button to display the Dynamic ARP Inspection statistics for the selected VLAN .



3 L3 Features

3.1 DHCP Relay

3.1.1 Managing DHCP Relay

3.1.1.1 Feature Description

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

Standards

- RFC 3046
- RFC 2131

Scaling Numbers

- Maximum 200 clients can use this feature simultaneously.

Limitations

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

Default Values

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

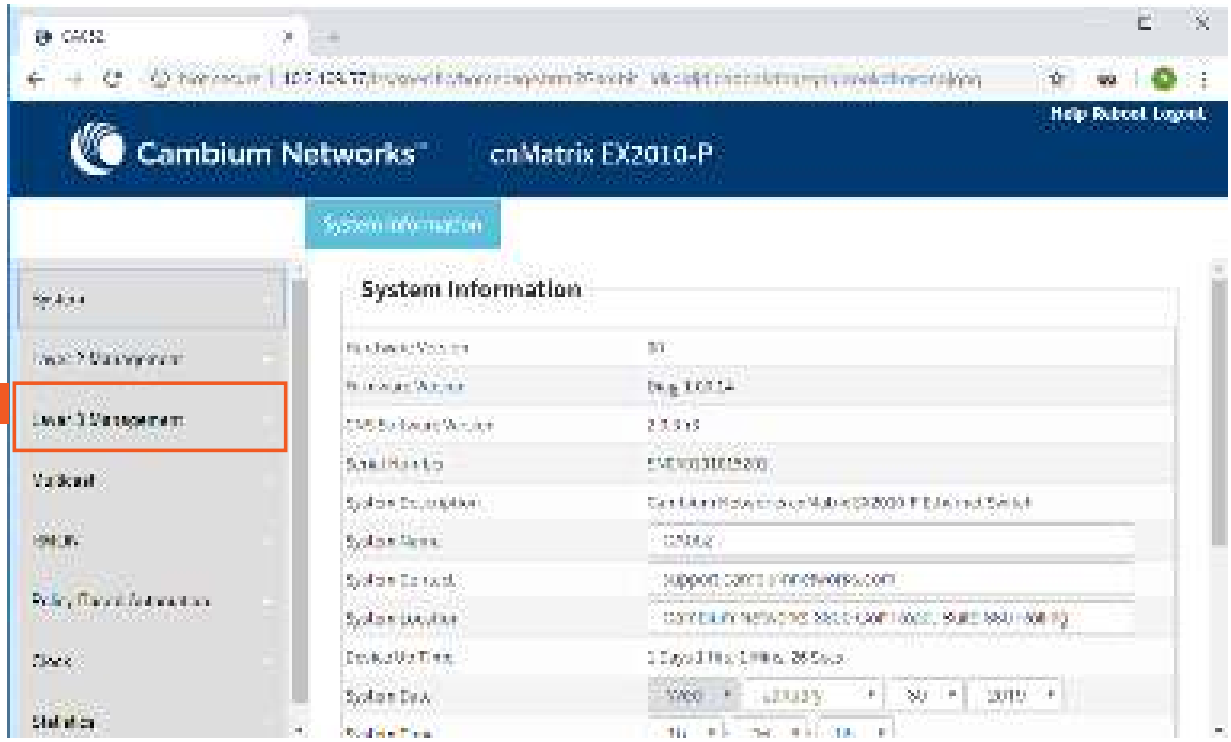
Prerequisites

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

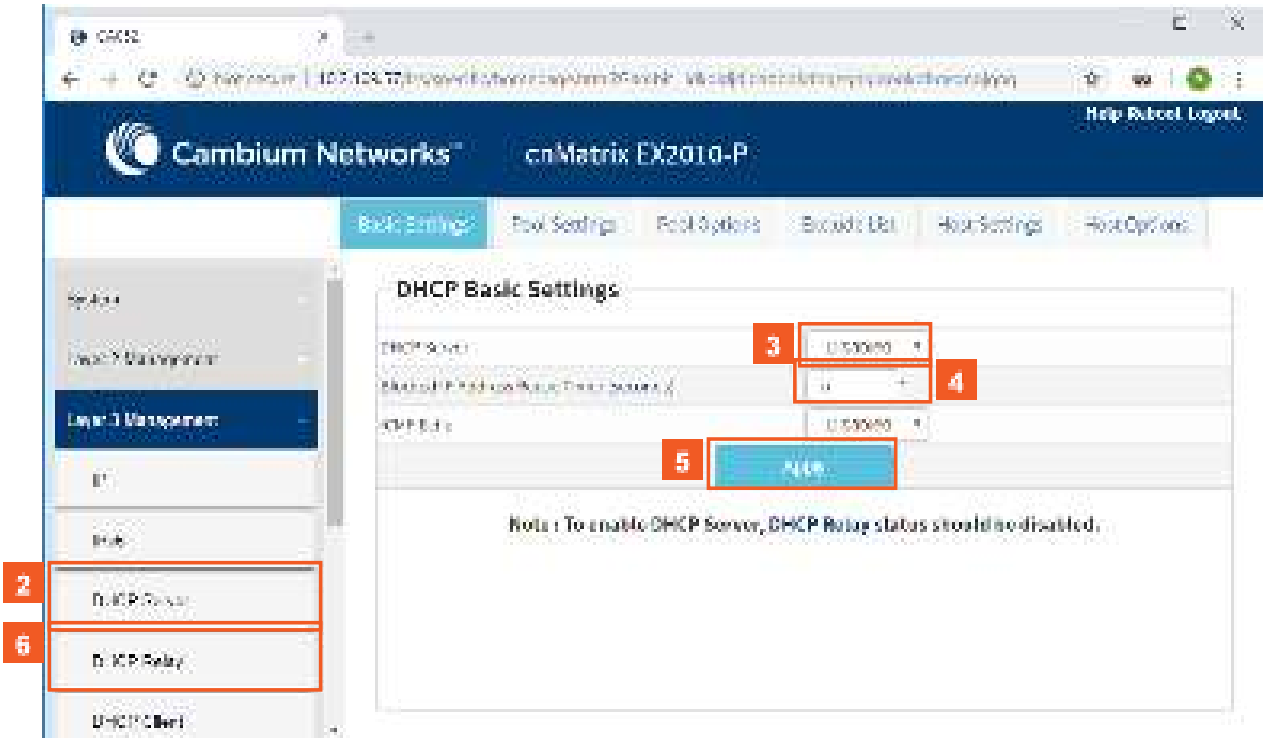
Even though the feature can be enabled on a VLAN or port, it will relay packets from all VLANs.

3.1.1.2 Network Diagram

3.1.2 How to Enable DHCP Relay in WEB Interface



1 Click the **Layer 3 Management** tab. The **L3 Features** are displayed.



2 Click the **DHCP Server** menu item.

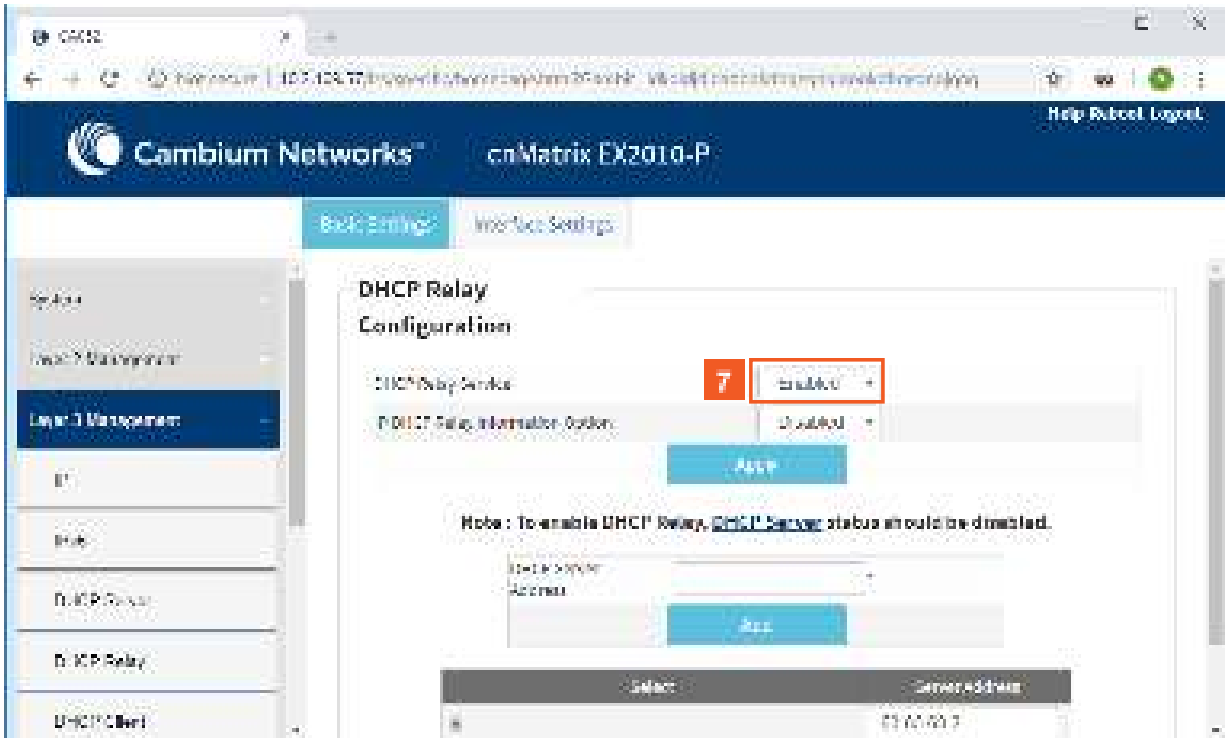
3 Click the **DHCP Server** drop-down list to select the DHCP server status in the router.

This is just an example so that you can see how to disable the DHCP Server feature (mandatory step when you want to enable the DHCP Relay feature). The DHCP Server feature is disabled by default.

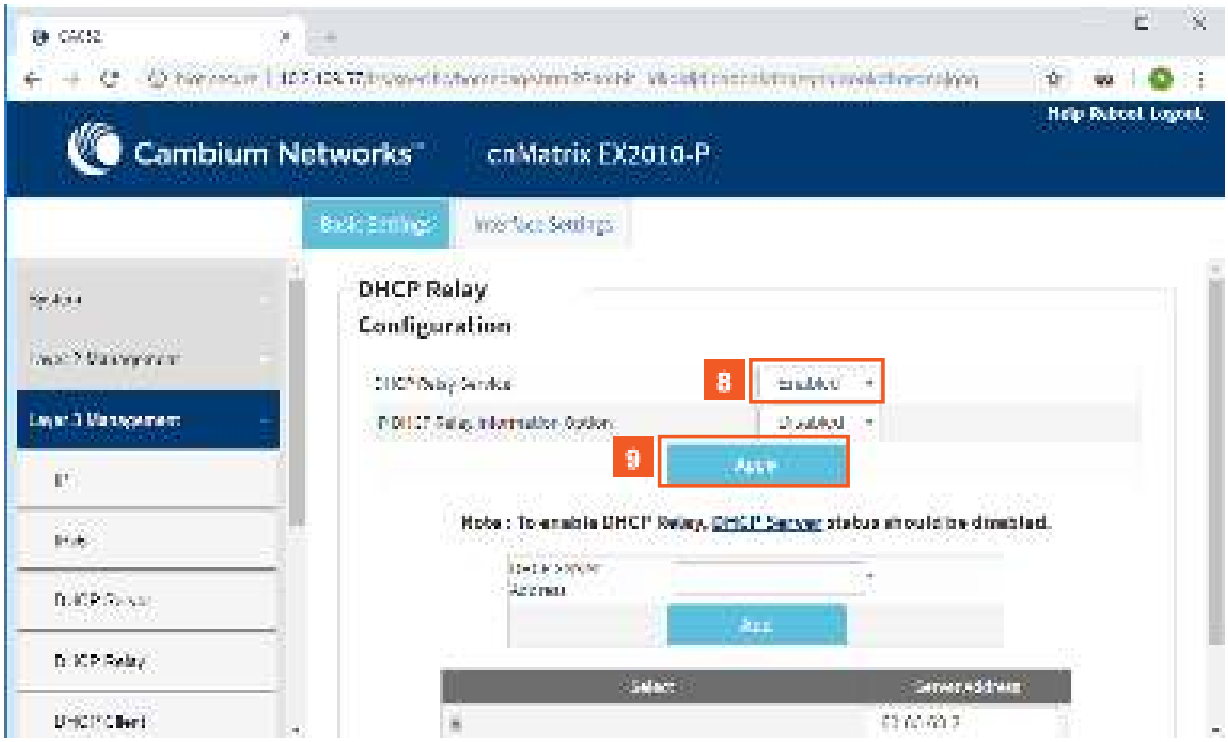
4 Select the **Disabled** list item.

5 Click the **Apply** button.

6 Click the **DHCP Relay** menu item.



7 Click the **DHCP Relay Service** drop-down list and select the DHCP Relay service status in the switch.



8 Select the **Enabled** list item.

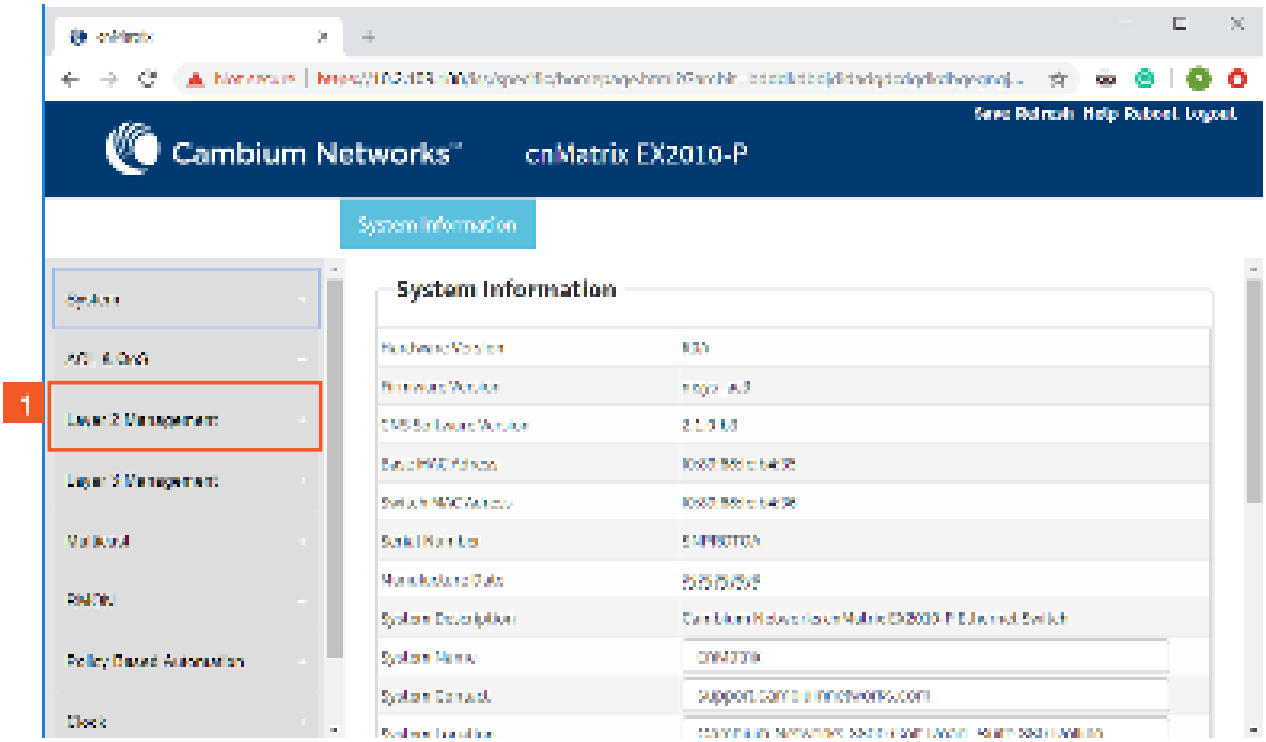
9 Click the **Apply** button.

3.2 Routed Interface

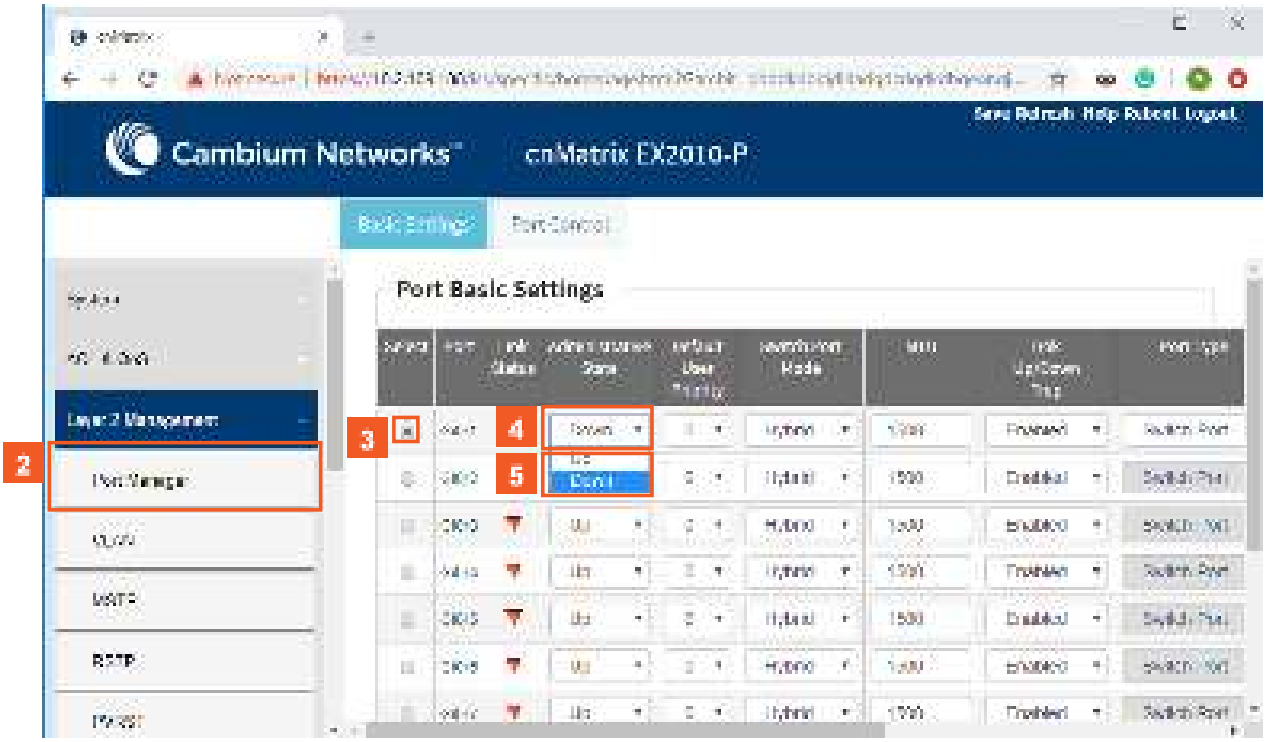
3.2.1 Configuring Routed Interfaces in WEB Interface

Starting with version 2.1, the **Routed Interfaces** feature is available in WEB GUI.

How to Create Routed Ports



1 Click the **Layer 2 Management** tab.

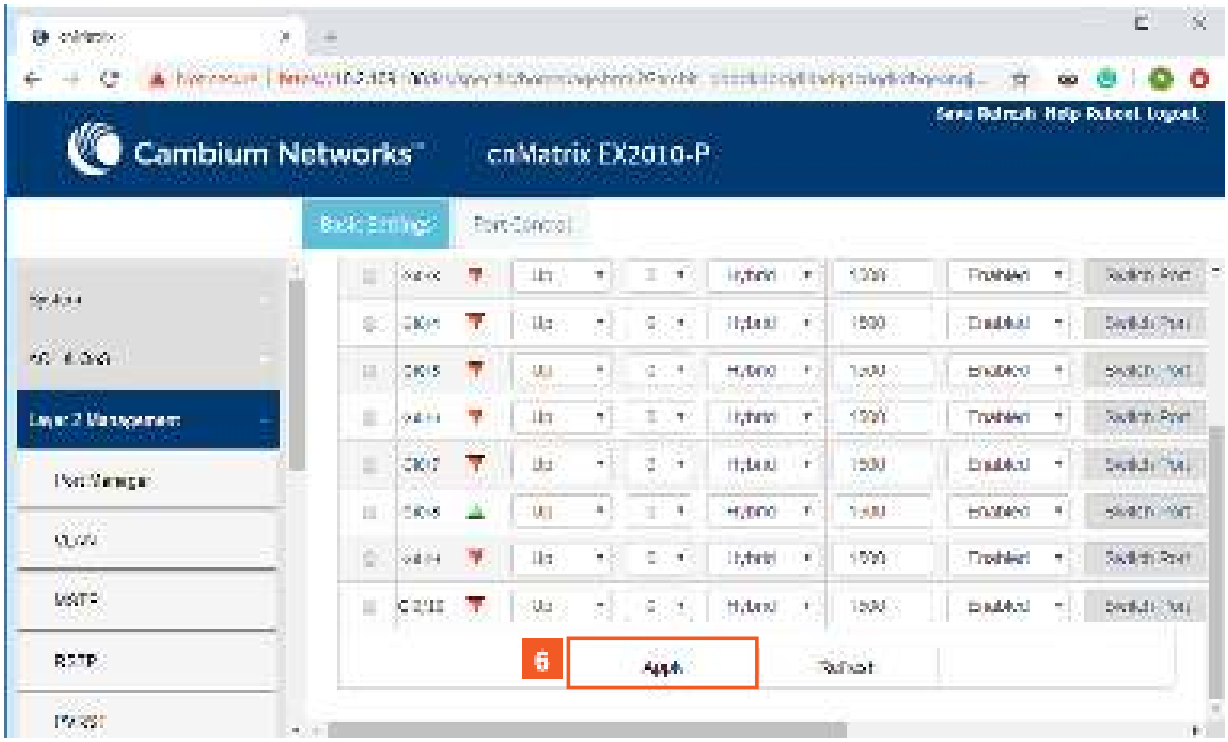


2 Click the **Port Manager** menu item.

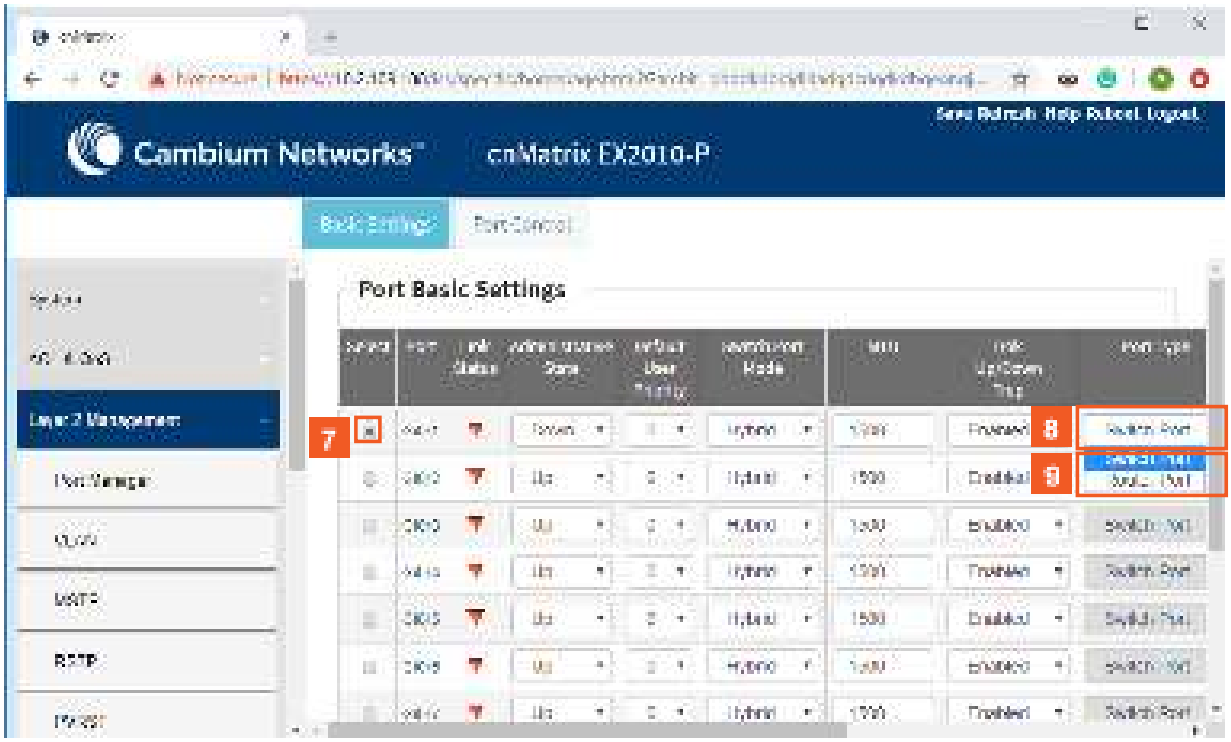
3 Check the radiobutton for a specific interface (line).

4 Click the **Administrative State** drop-down list to select the desired state of the port.

5 Select the **Down** list item to block the port from transmitting/receiving the traffic.



6 Click the **Apply** button.

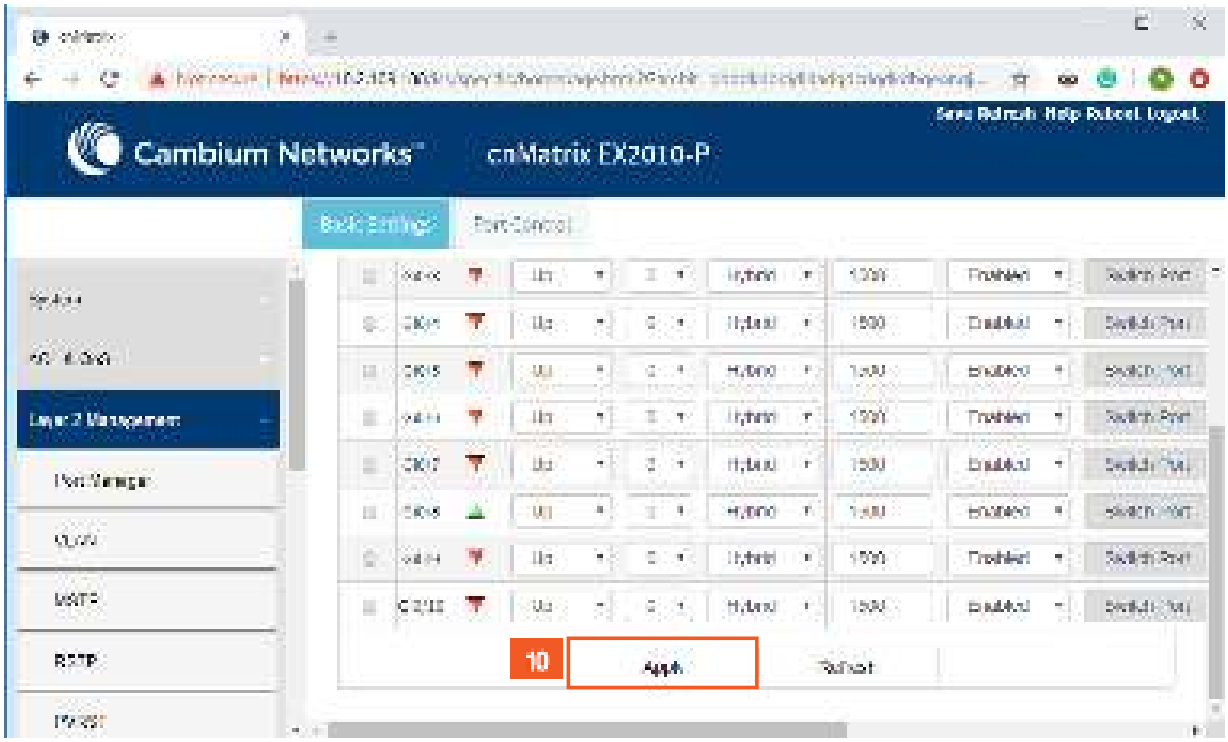


7 Check the radiobutton for the same interface (line)..

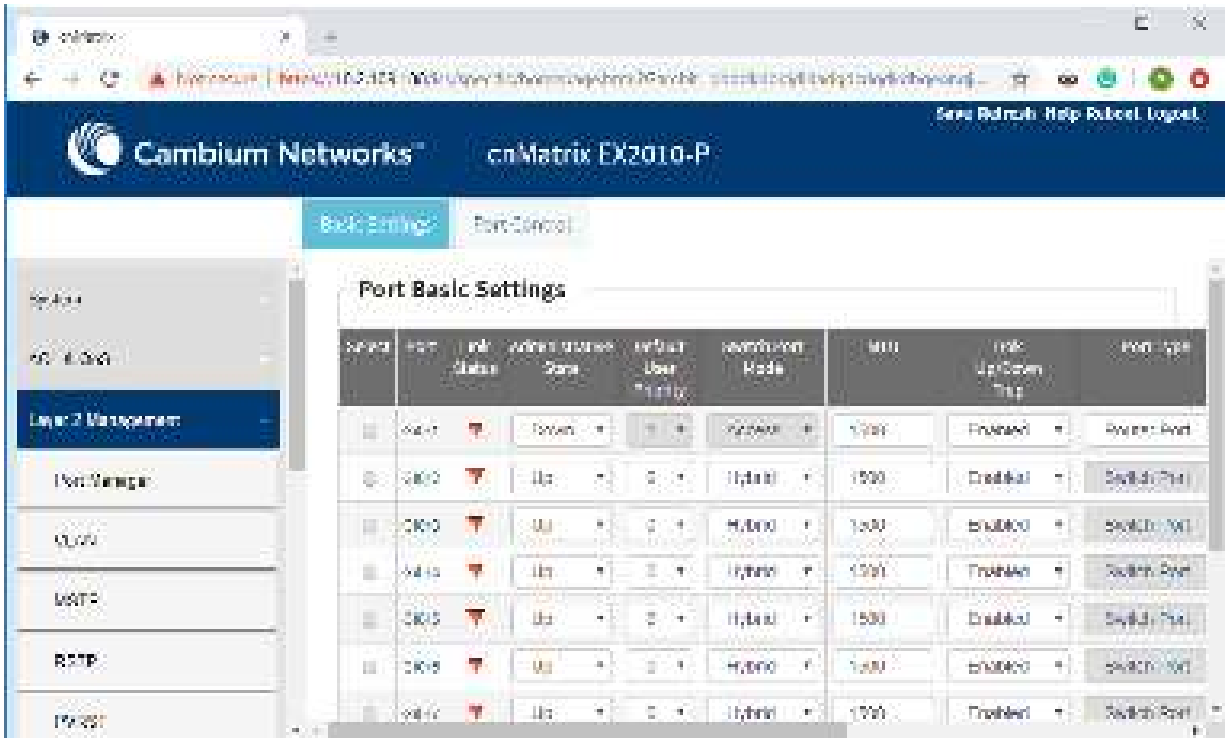
8 Click the **Port Type** drop-down list to select the port type to operate the port as an Layer 2 or Layer 3 port.

9 Select the **Router Port** list item to set the port as an Layer 3 port and to forward traffic based on the IP address.

Note: This field is available only if you previously selected the **Down** option in the **Administrative State** column.



10 Click the **Apply** button.



3.3 IP Routing

3.3.1 Managing IP Routing

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

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

Standards

- RFC791

Scaling Numbers

- A maximum of 64 IPv4 interfaces is supported.

Limitations

- IP routing cannot be disabled on the system.

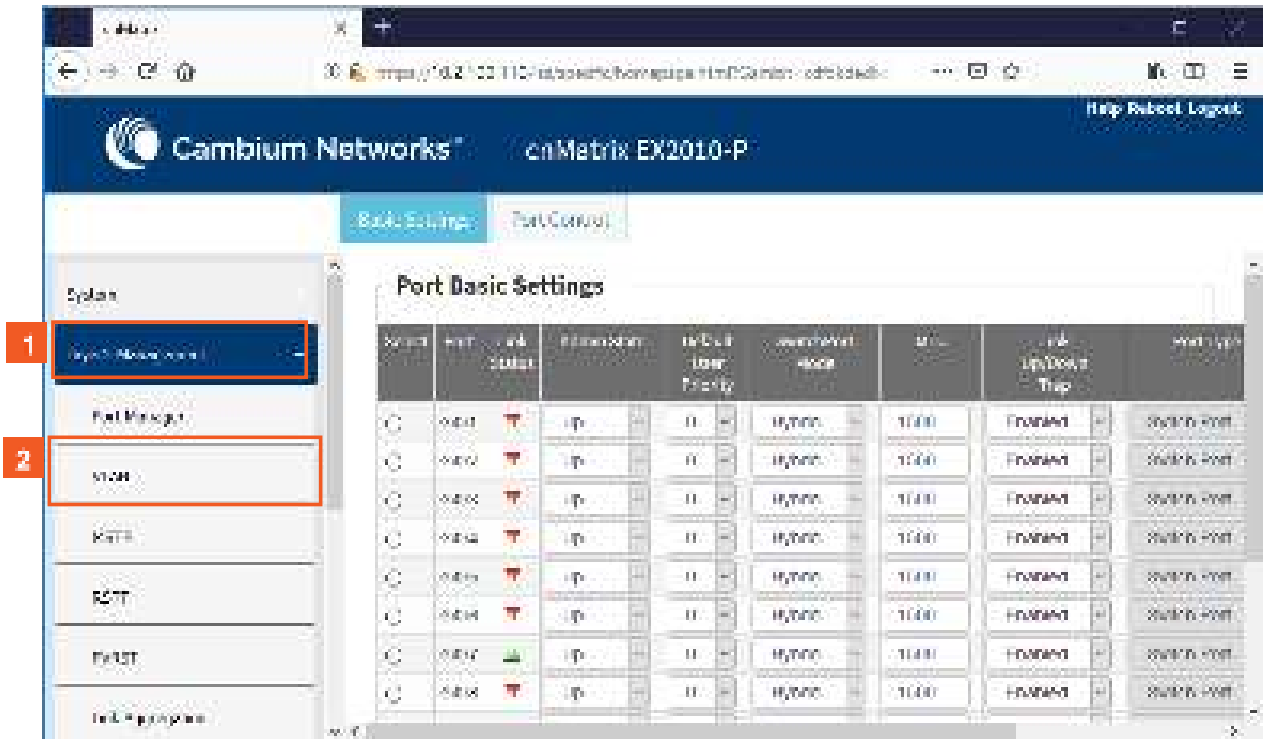
Default Values

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

Prerequisites

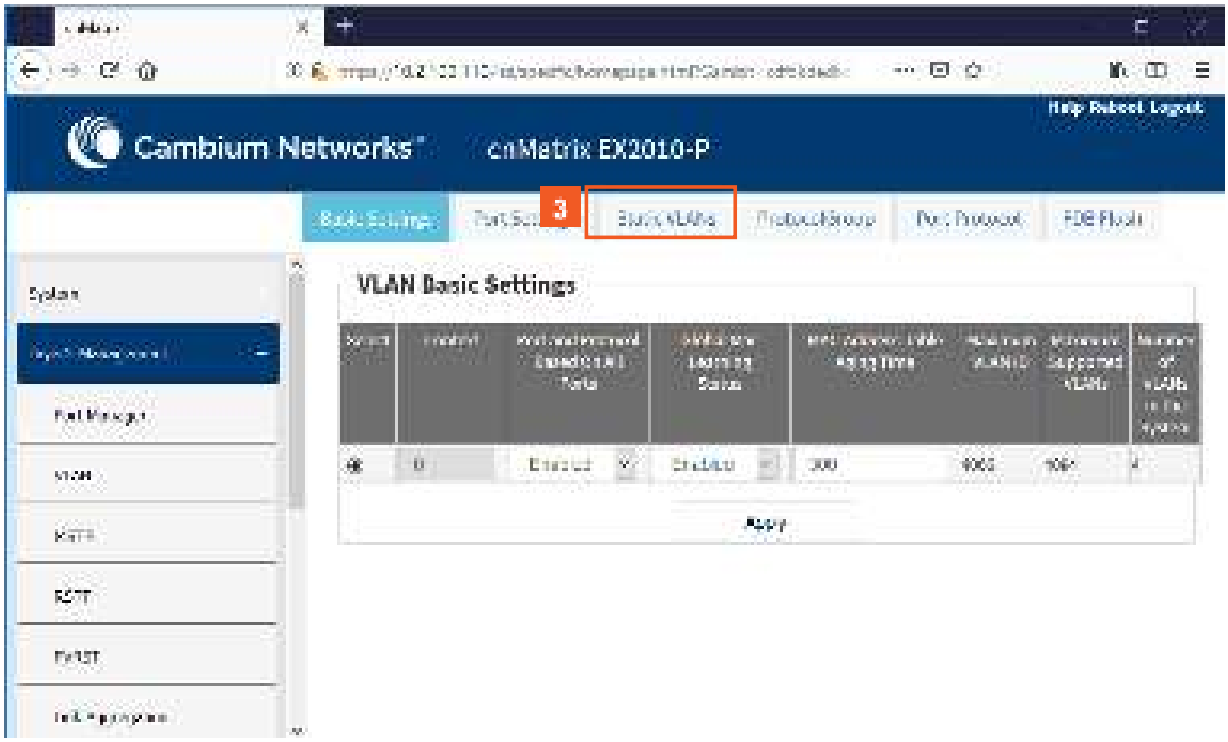
- N/A

3.3.2 How to Enable and Configure IP Routing in WEB Interface

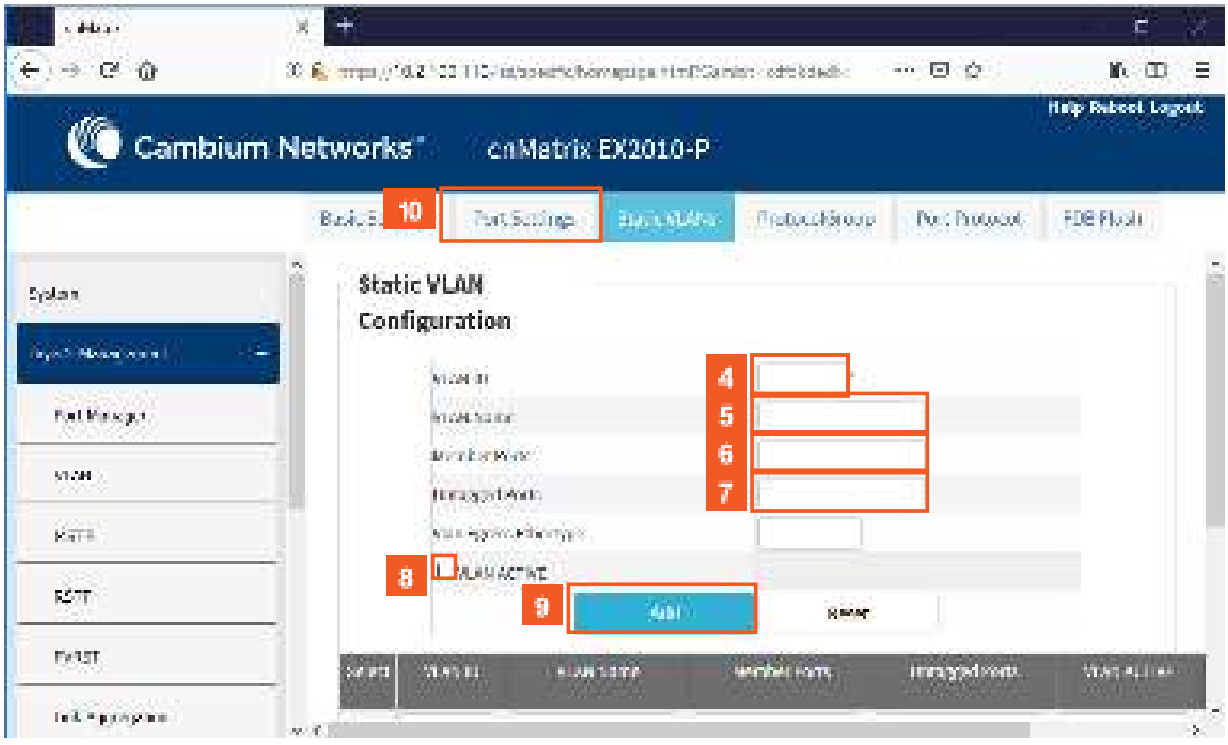


1 Click the **Layer2 Management** tab. The **L2 Features** are displayed.

2 Click the **VLAN** menu item.



3 Click the **Static VLANs** tab. The **Static VLAN Configuration** window is displayed.



4 Type the value **100** in the **VLAN ID** field.

100 = the **VLAN ID** that uniquely identifies a specific VLAN. the maximum value for VLAN ID is: 4066

5 Type the value **vlan100** in the **VLAN Name** field.

vlan100 = an administratively assigned string, used to identify the VLAN.

6 Type the value **Gi0/1-3** in the **Member Ports** field.

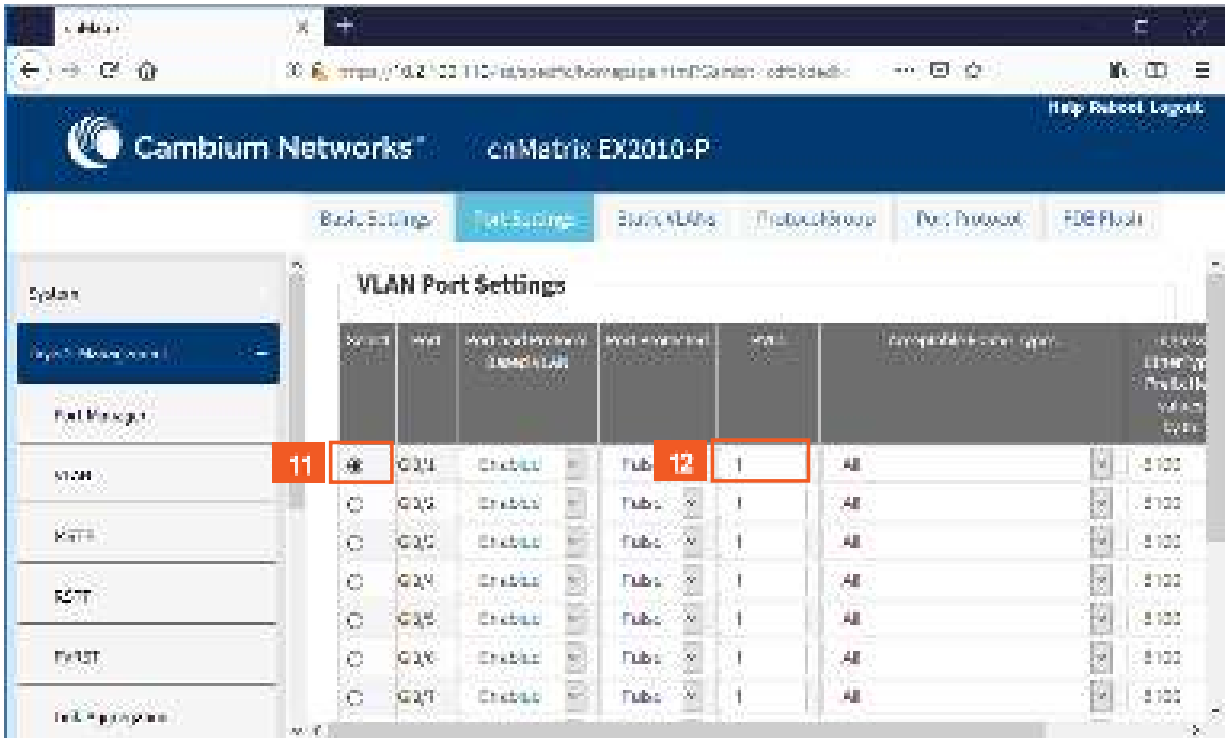
7 Type the value **Gi0/1-3** in the **Untagged Ports** field.

Gi0/1-3 = a port or set of ports, which should transmit egress packets for the VLAN as untagged packets.

8 Click the **VLAN ACTIVE** check box.

9 Click the **Add** button.

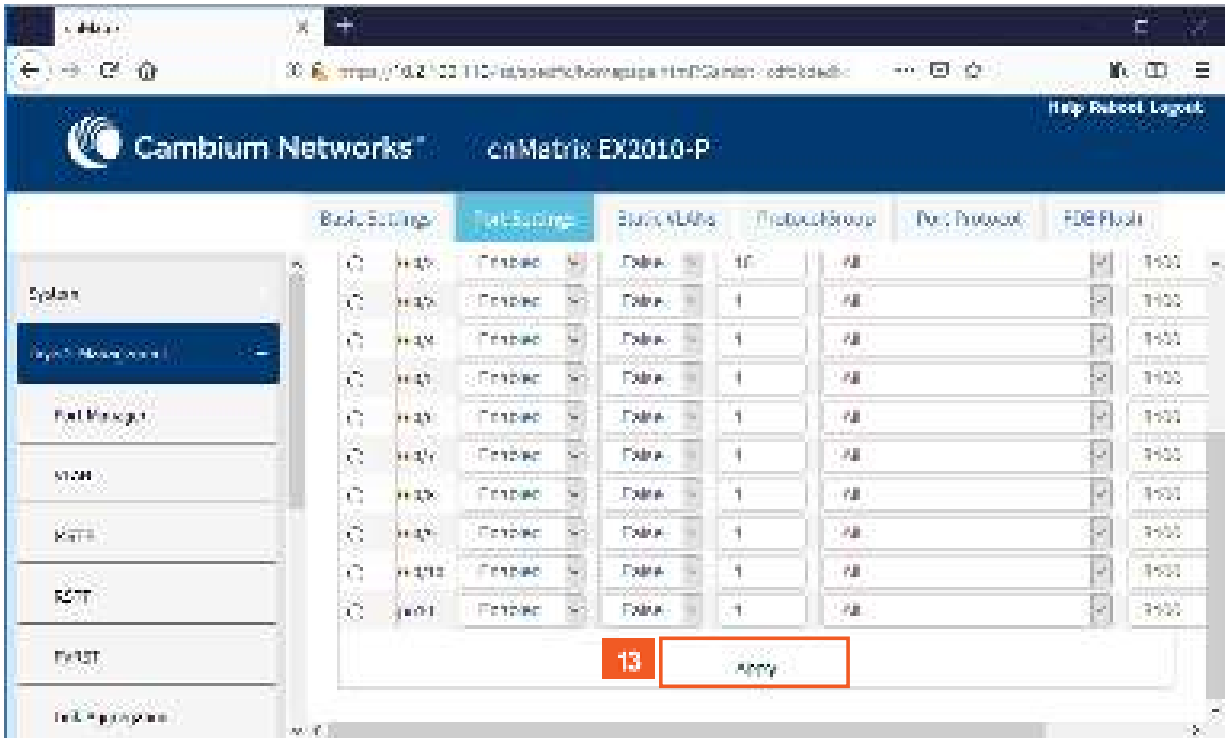
10 Click the **Port Settings** tab. The **VLAN Port Settings** window is displayed.



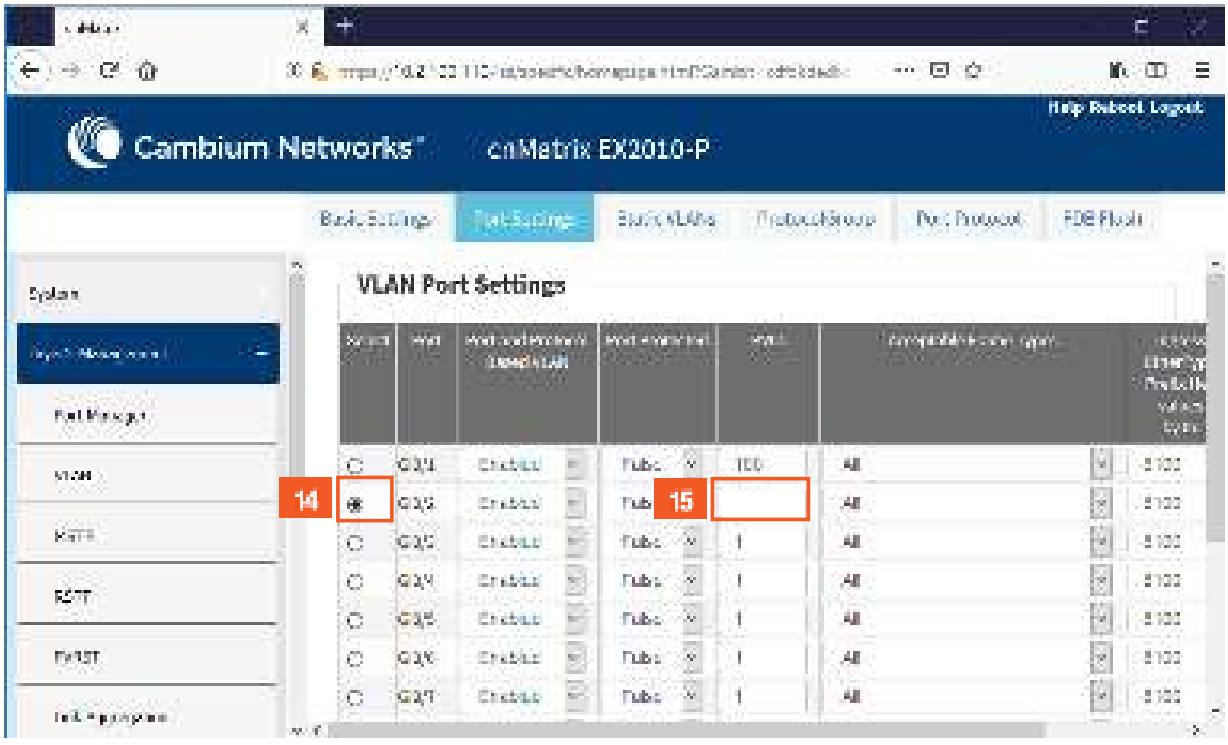
11 Click the **Select** radio button to select the port for which the configuration needs to be done. For example, click the radio button that is on the same line with the **Gi0/1** port.

12 Type the value **100** in the PVID field.

The value **100** represents the VLAN ID assigned to untagged frames or priority-tagged frames received on the port.

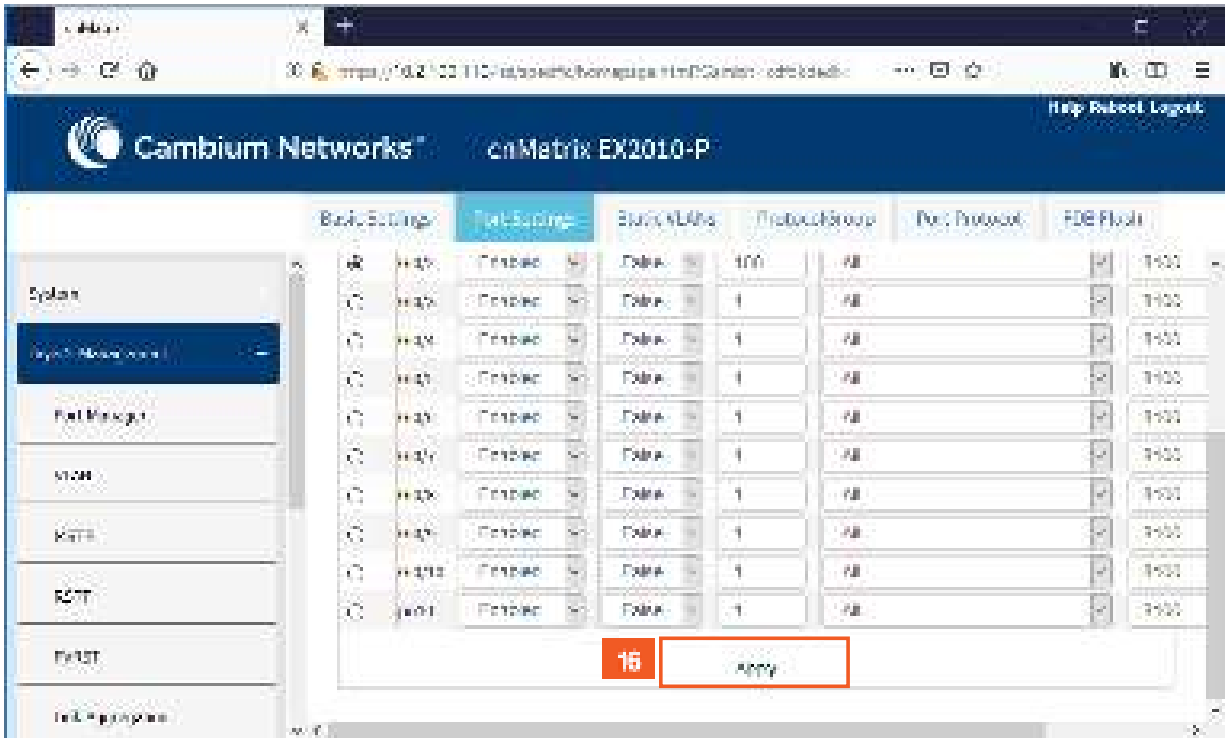


13 Click the **Apply** button.

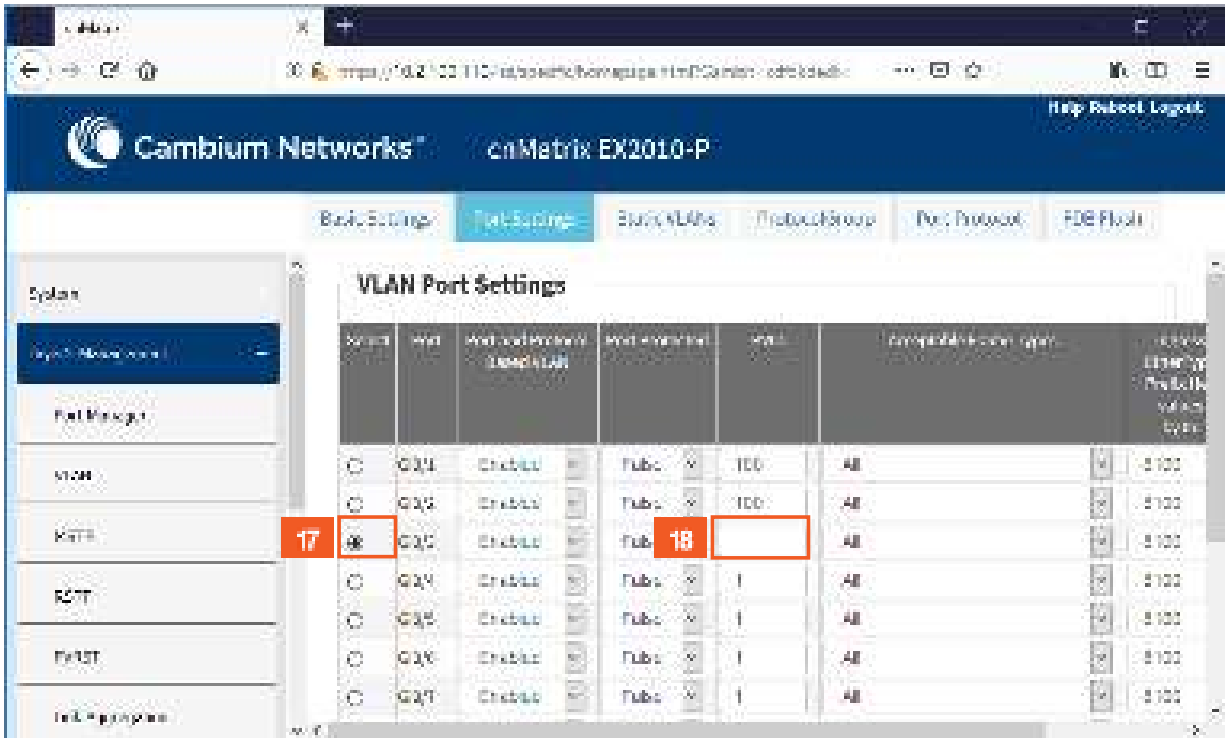


14 To add more ports, click the **Select** radio button to select another port for which the configuration needs to be done. For example, click the **Gi0/2** radio button.

15 Type the value **100** in the PVID field.

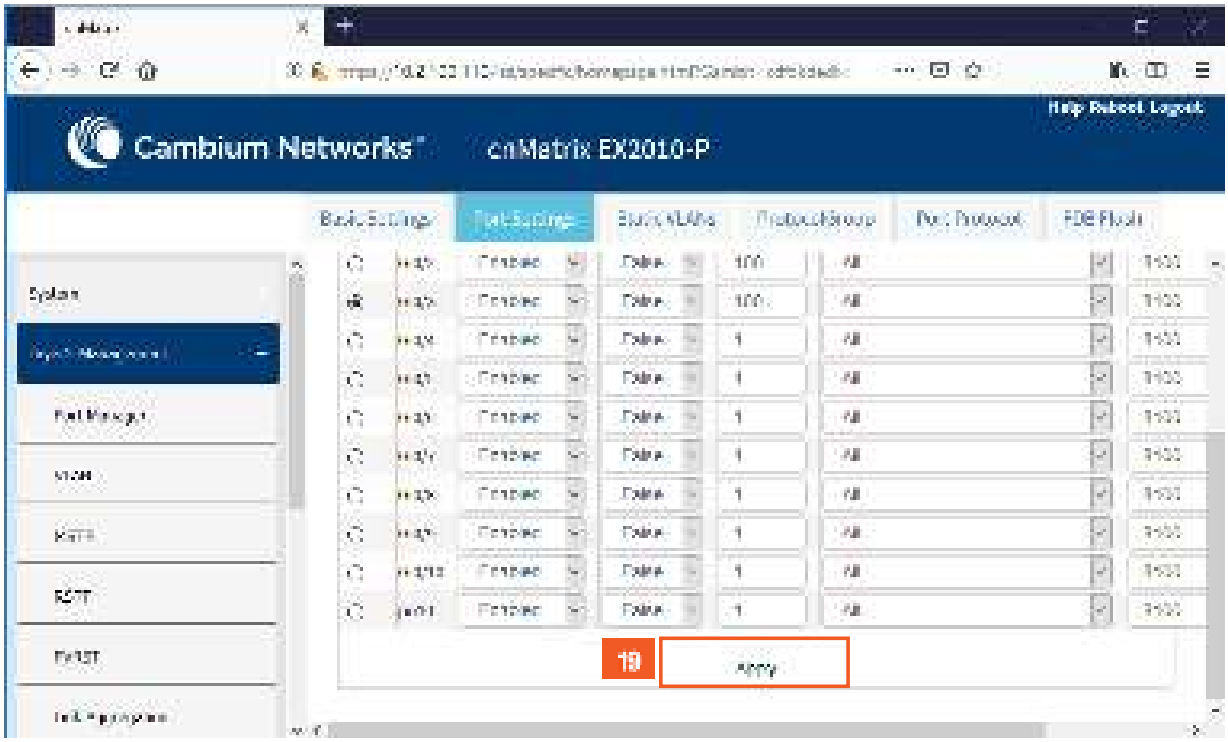


16 Click the **Apply** button.

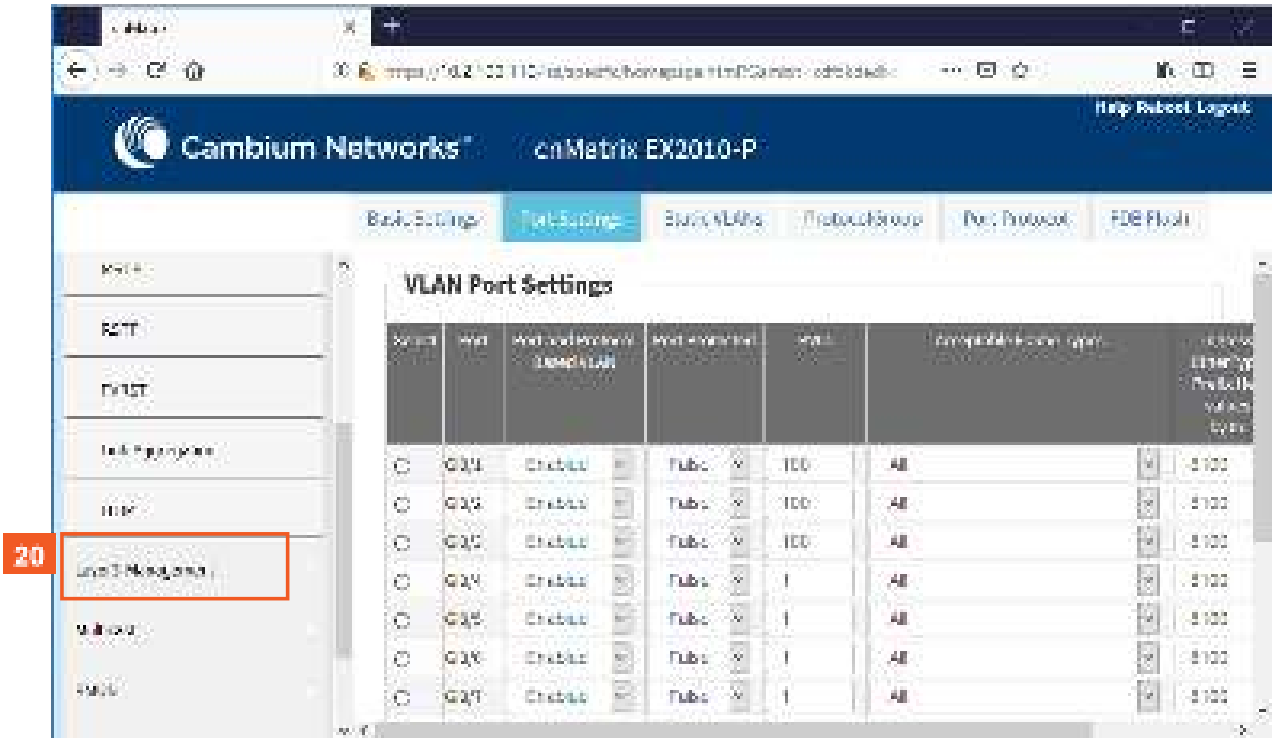


17 In order for you to add more ports, click the **Select** radio button and select the port for which the configuration needs to be done. For example, click the **Gi0/3** radio button.

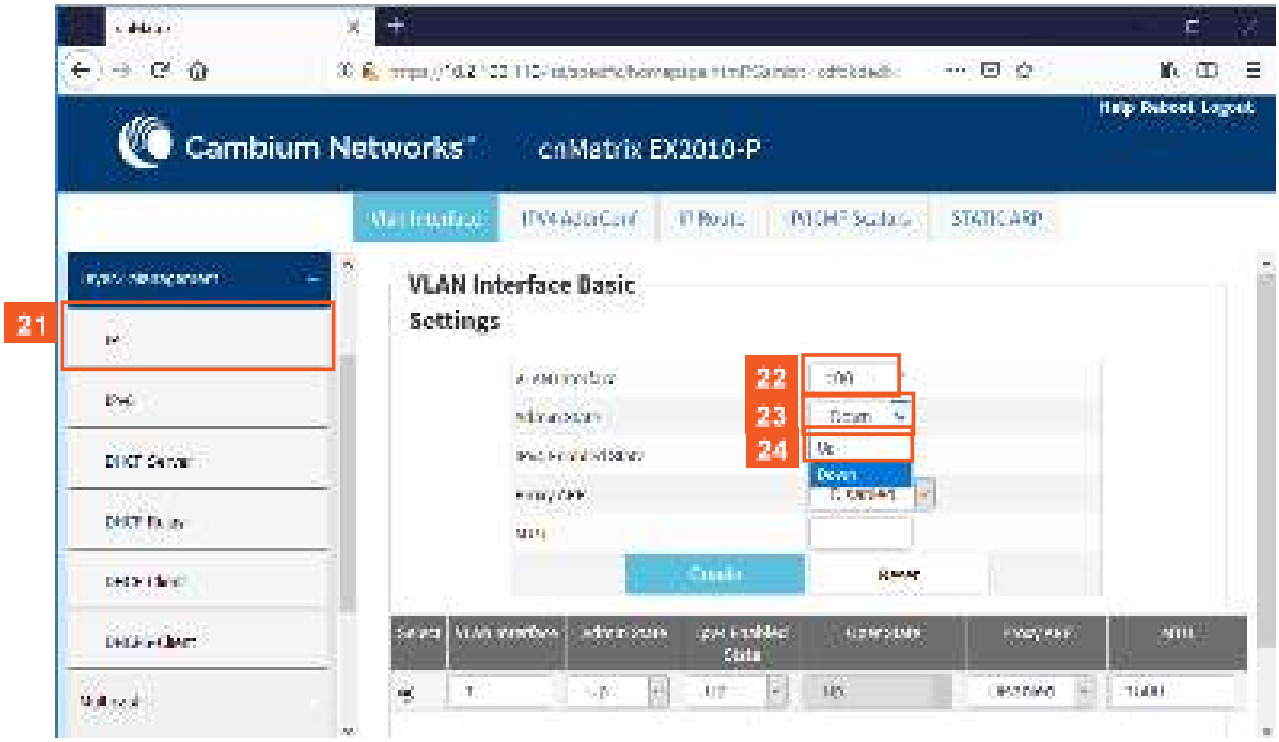
18 Type the value **100** in the **PVID** field.



19 Click the **Apply** button.



20 Click the **Layer3 Management** tab. The **L3 Features** are displayed.



21 Click the **IP** menu item.

22 Type the value **100** in the **VLAN Interface** field.

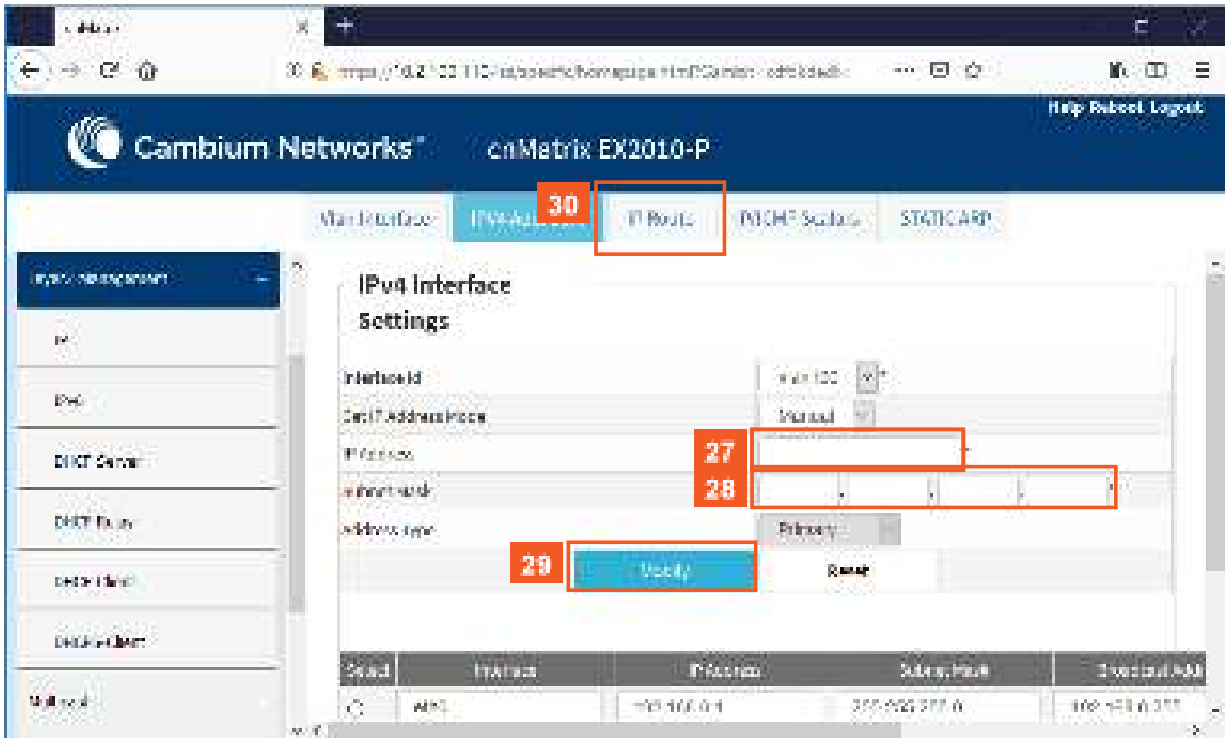
The value **100** represents the VLAN ID for the interface to be created.

23 Click the **Admin State** drop-down list to select the admin status of the VLAN interface..

24 Select the **Up** list item.

25 Click the **Create** button.

26 Click the **IPV4 Address Configuration** tab. The **IPv4 Interface Settings** window is displayed.

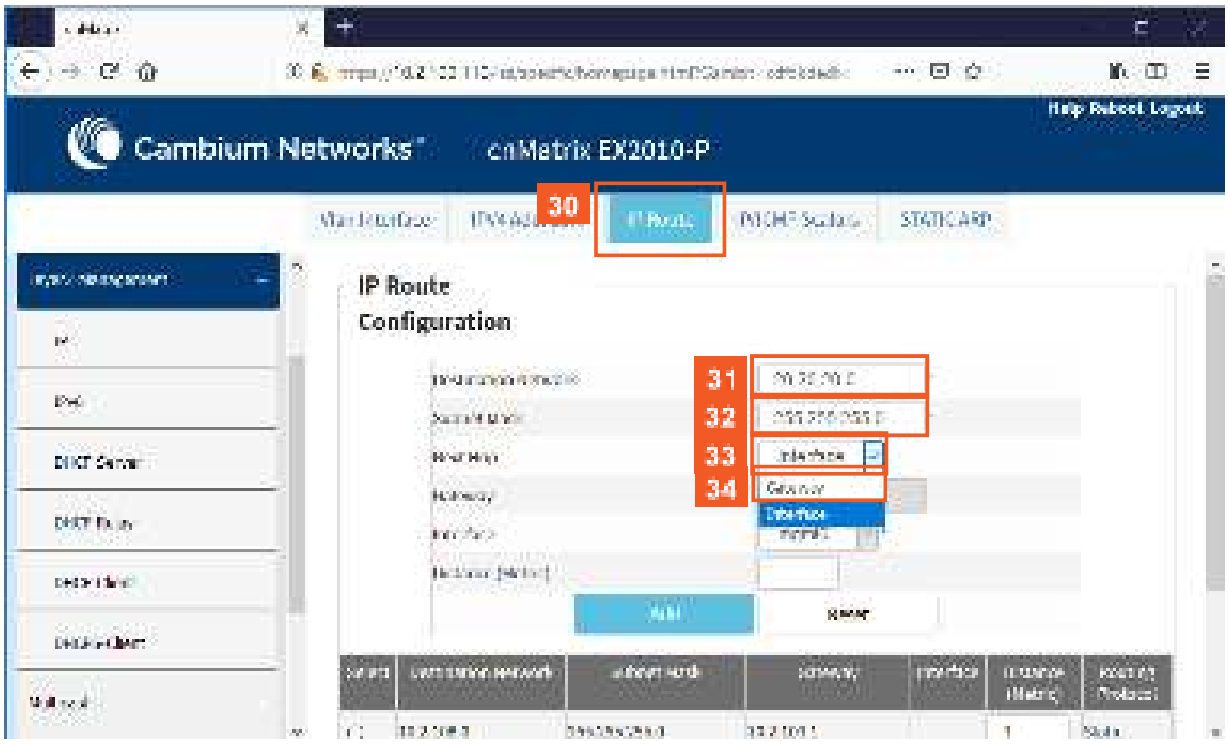


27 Type the value **10.10.10.1** in the **IP Address** field.

28 Type the value **255.255.255.0** in the **Subnet Mask** field.

29 Click the **Modify** button.

30 Click the **IP Route** tab. The **IP Route Configuration** window is displayed.

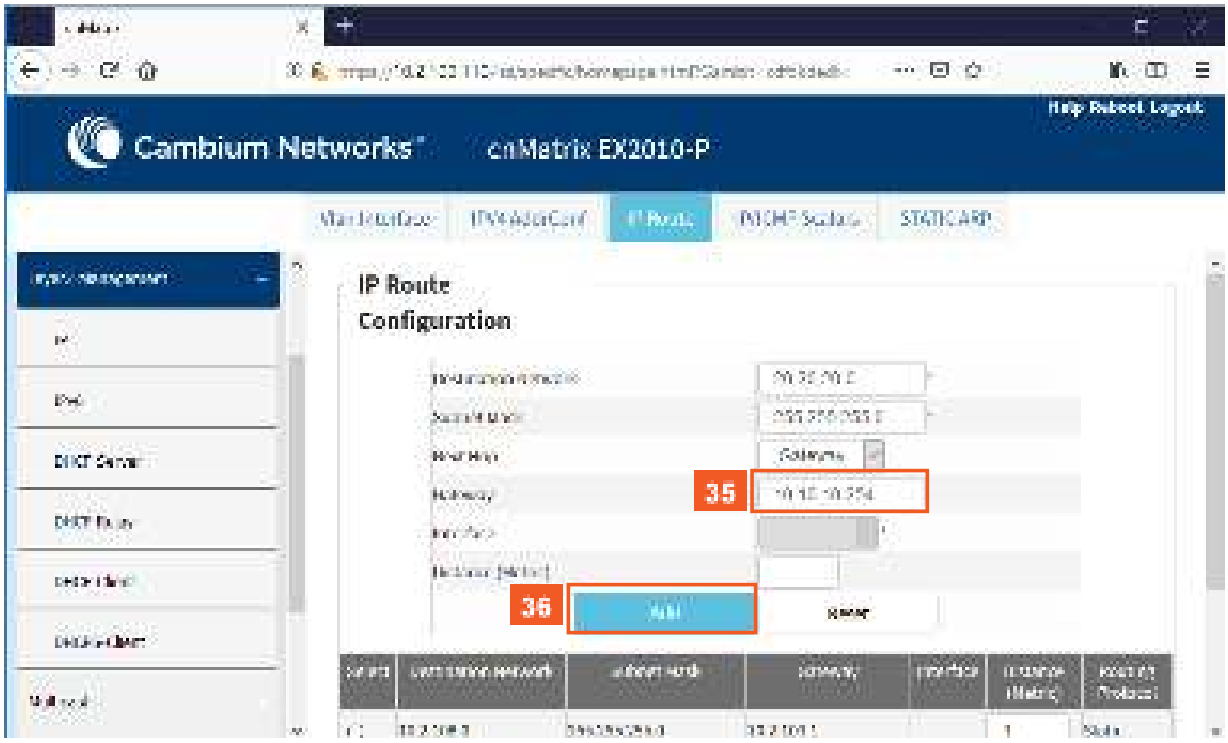


31 Type the value **20.20.20.0** in the **Destination Network** field. (IP address of the route)

32 Type the value **255.255.255.0** in the **Subnet Mask** field. (Subnet mask for the Destination Network address)

33 Click the **Next Hop** drop-down list.

34 Select the **Gateway** list item.



35 Type the value **10.10.10.254** in the **Gateway** field.

The **10.10.10.254** value represents the next hop gateway to reach the destination network.

36 Click the **Add** button.

3.4 OSPF (Starting with version 2.1)

3.4.1 Managing OSPF

3.4.1.1 Feature Overview

Feature Overview

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

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

Standards

- RFC 1583
- RFC 3509
- RFC 2328

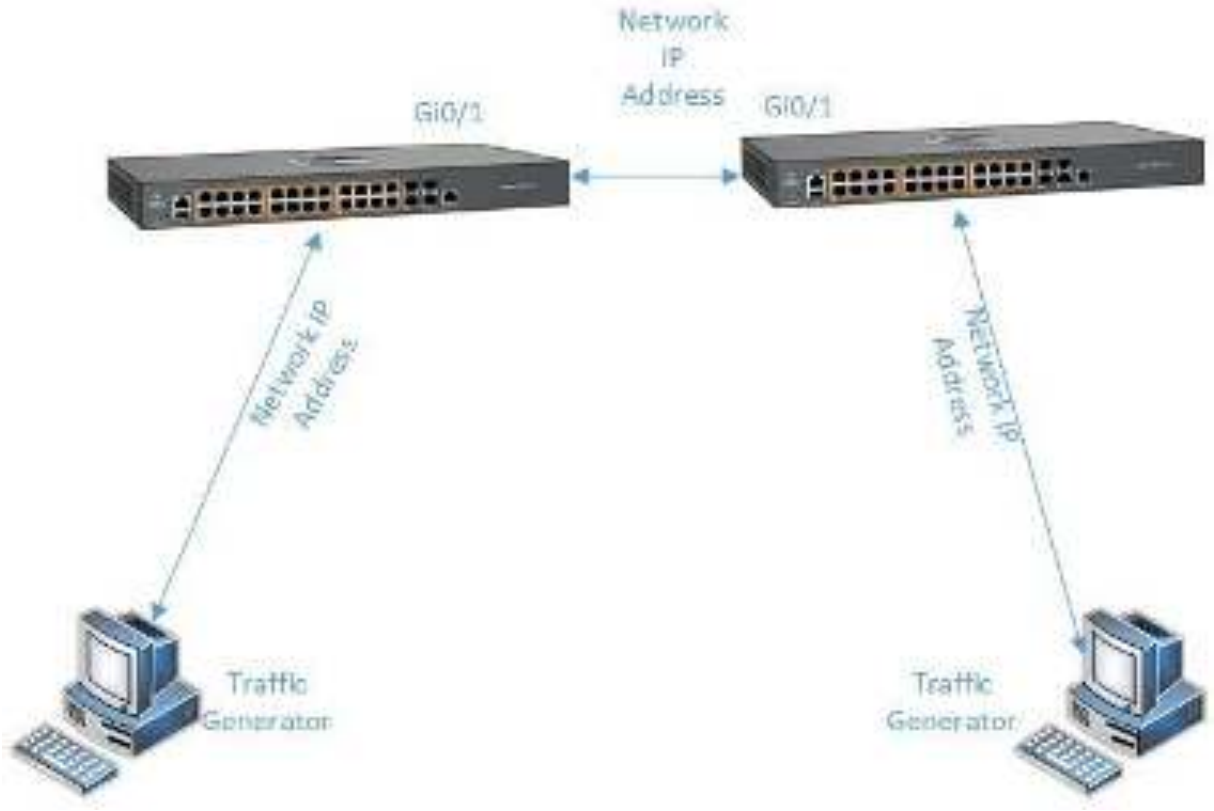
Default Values

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

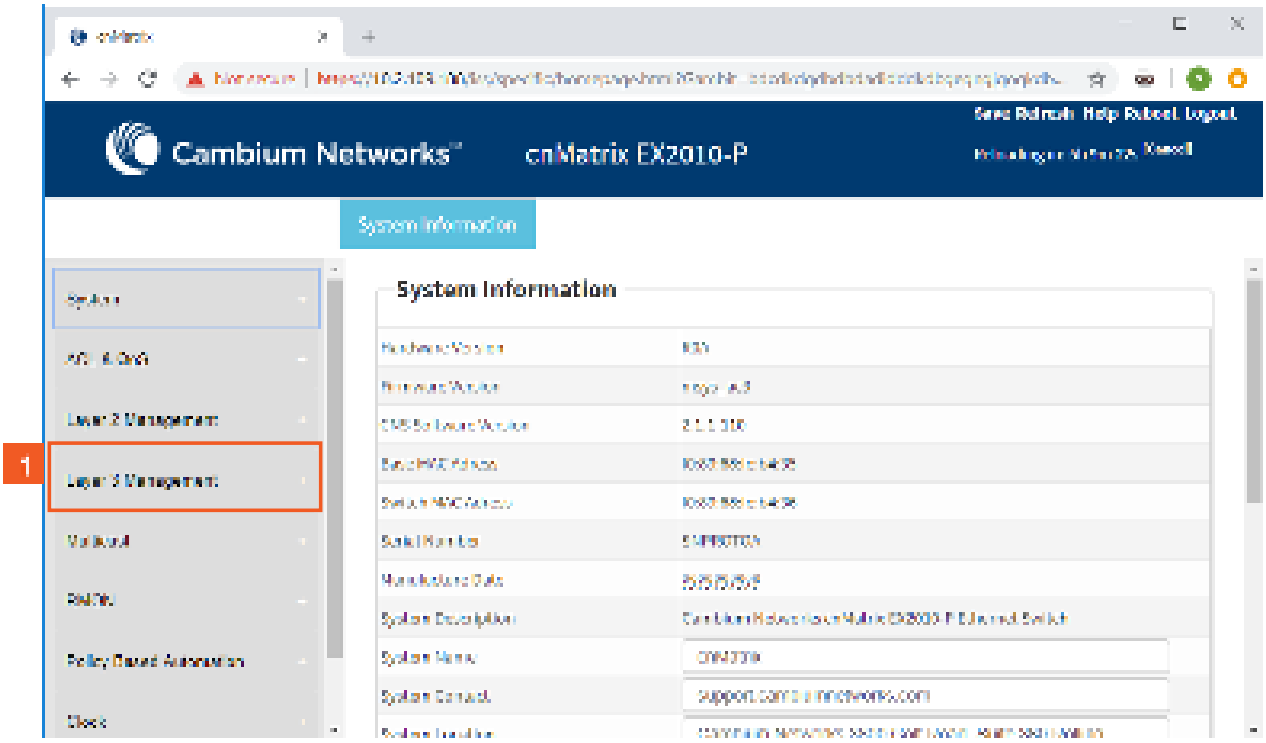
Prerequisites

- N/A

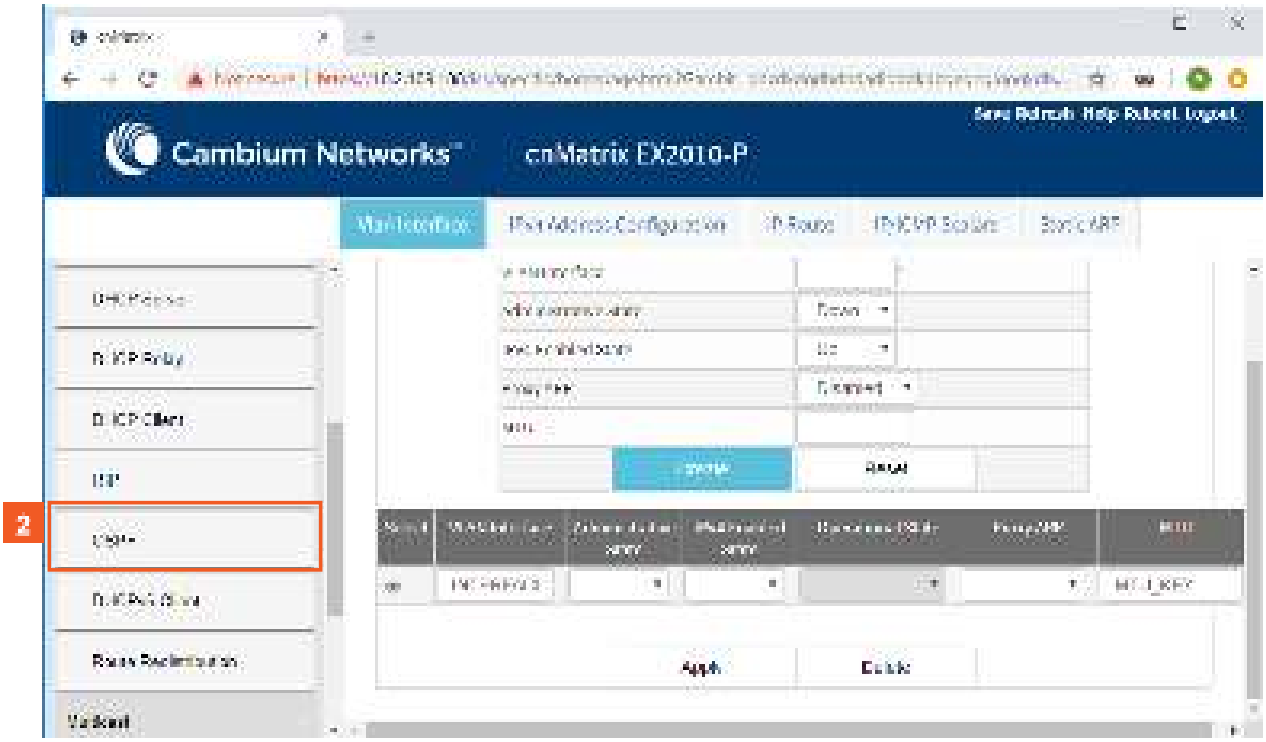
3.4.1.2 Network Diagram



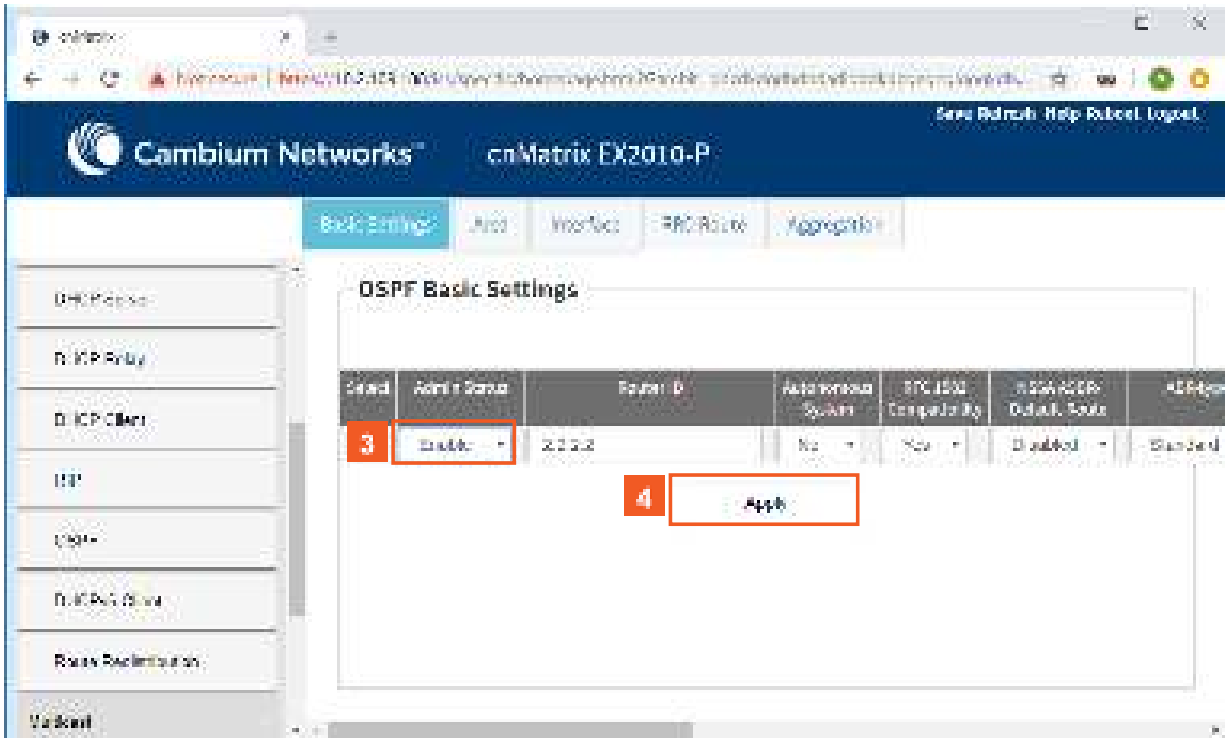
3.4.2 How to Enable OSPF in WEB Interface



1 Click the **Layer 3 Management** tab.



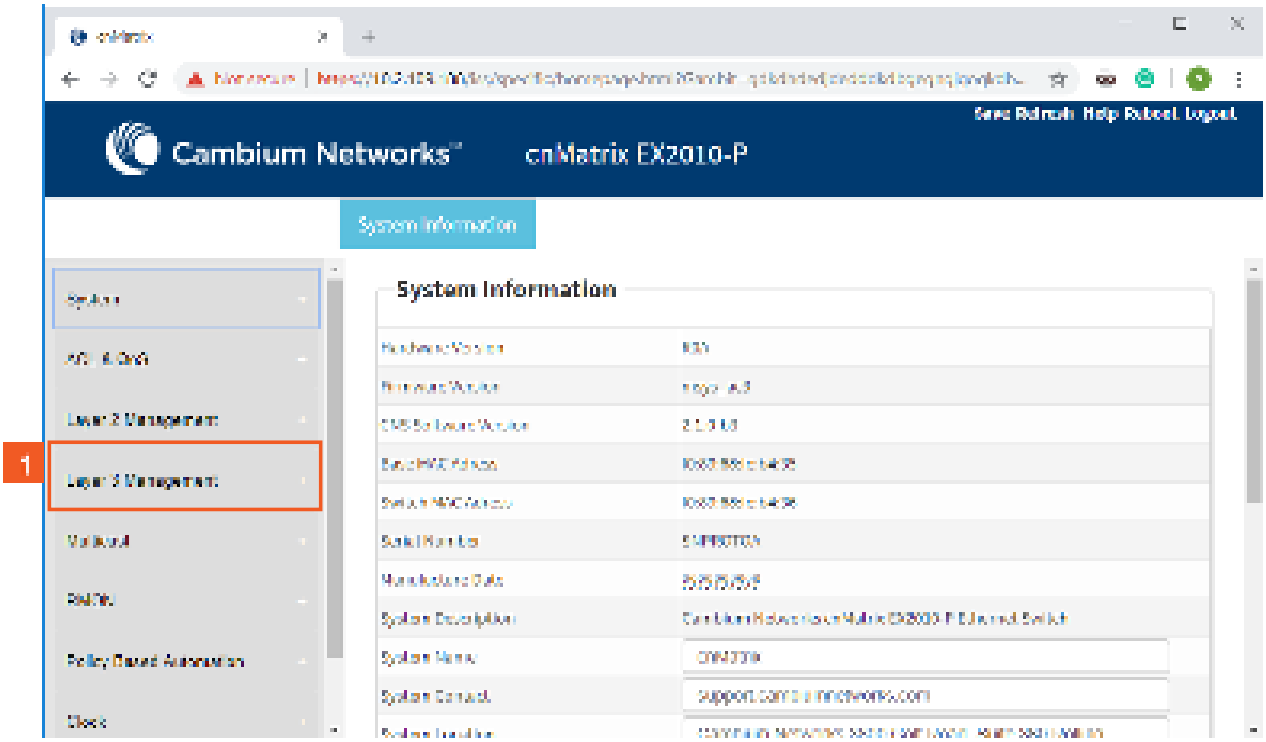
2 Click the **OSPF** menu item.



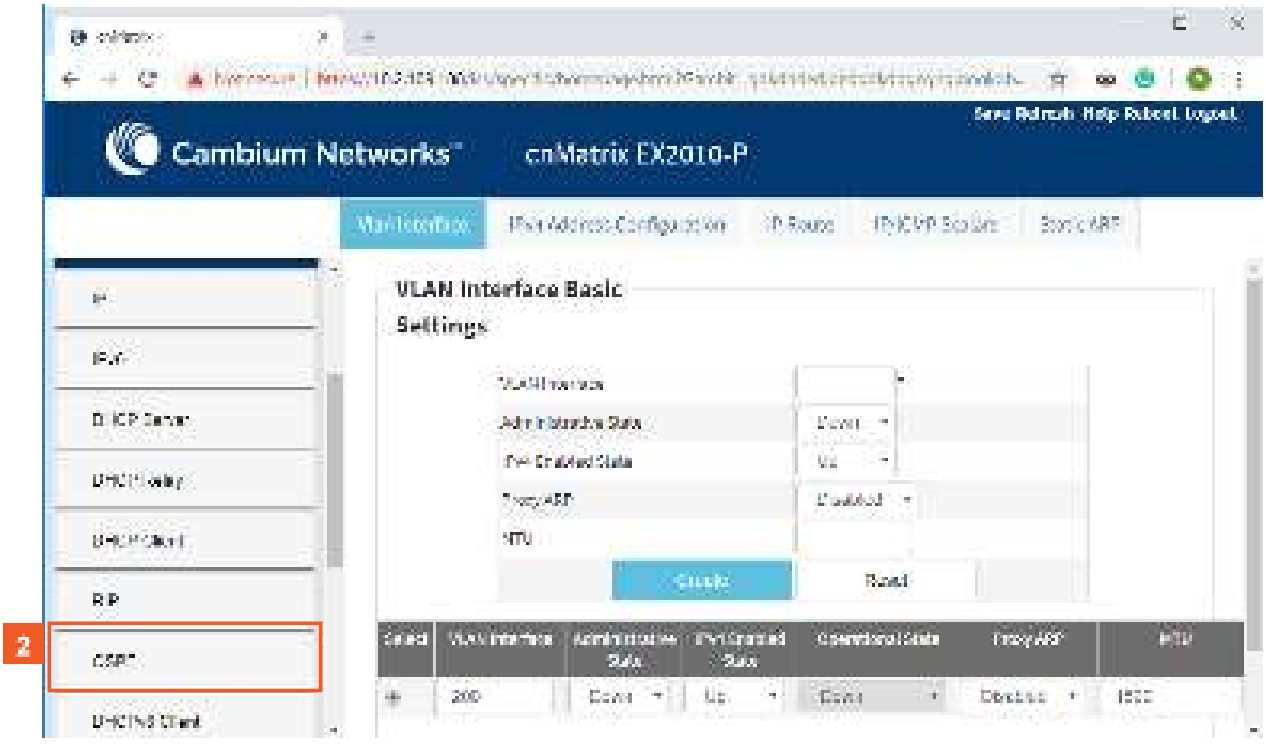
3 Click the **Admin Status** drop-down list to select the administrative status of the OSPF feature for a selected port. Select the **Enable** list item in the **Admin Status** column.

4 Click the **Apply** button.

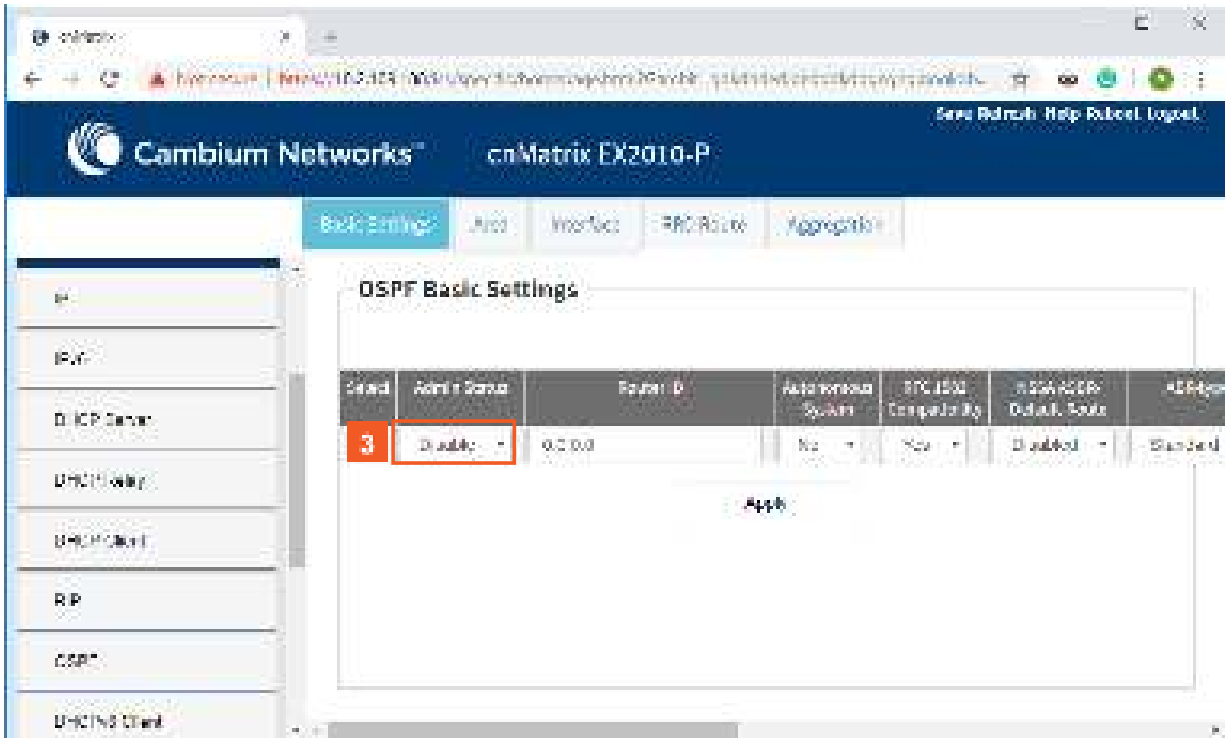
3.4.3 How to Configure OSPF in WEB Interface (example)



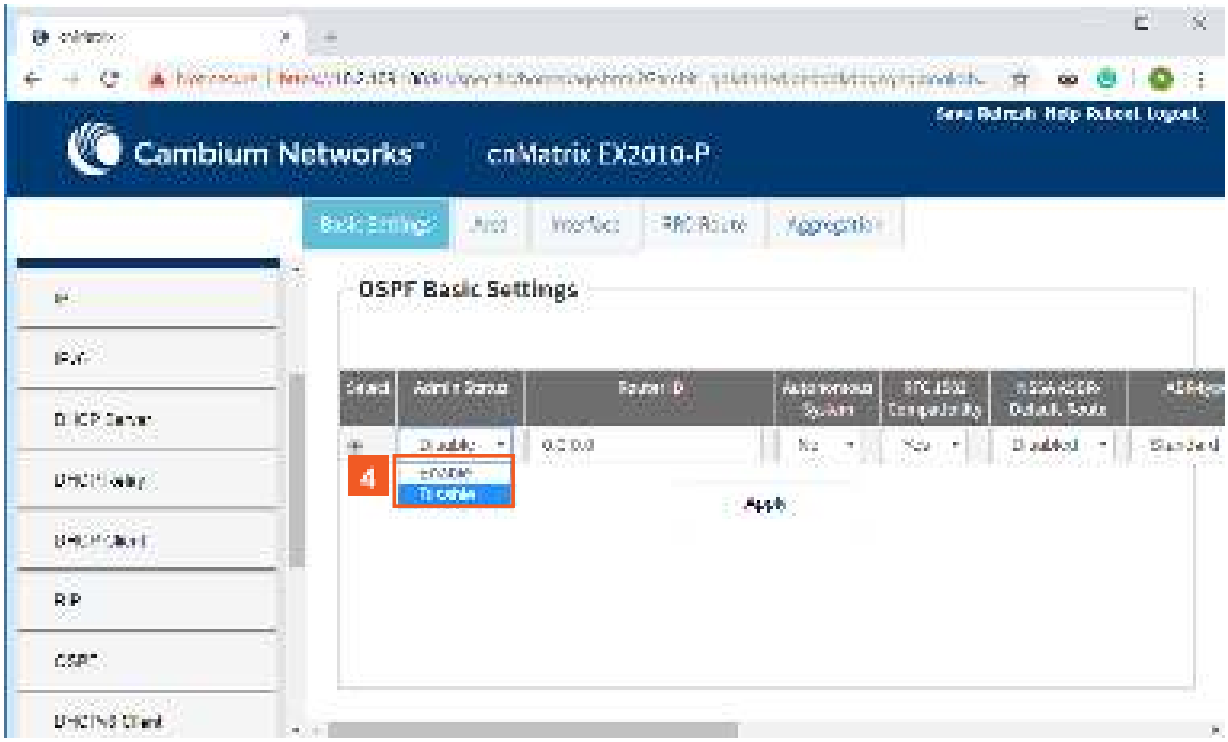
1 Click the **Layer 3 Management** tab. The **Layer 3 Features** are displayed.



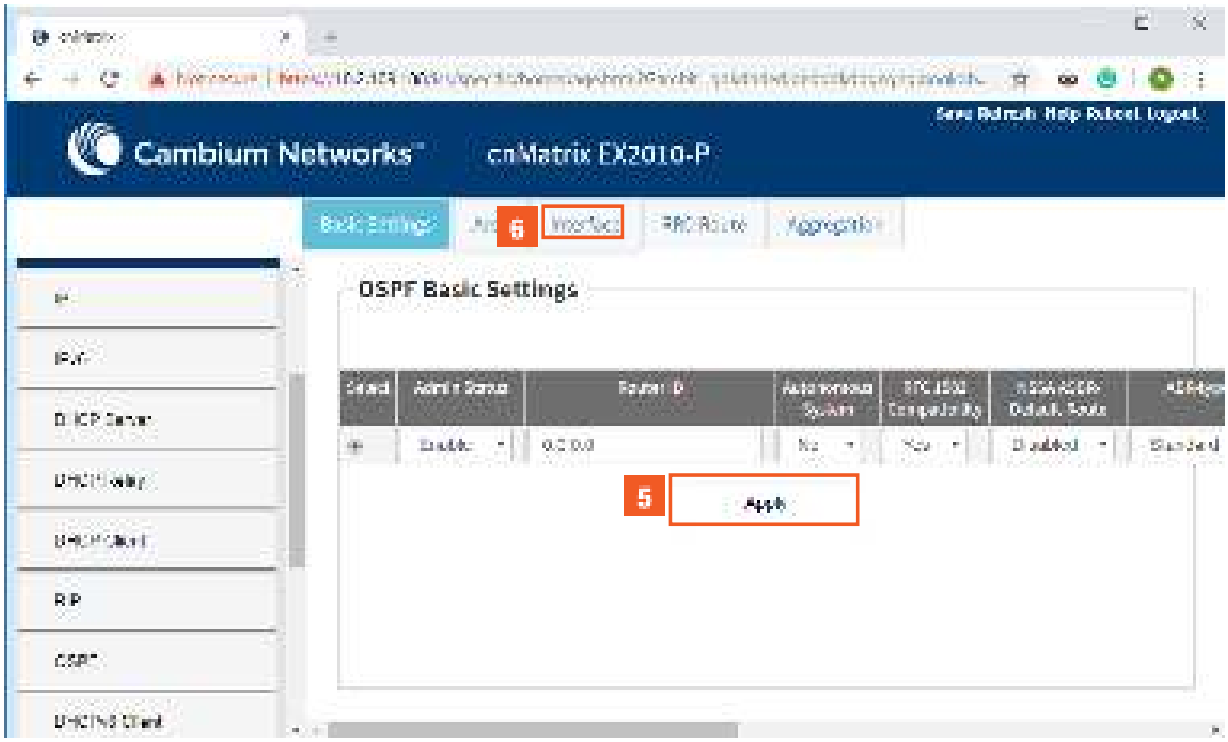
2 Click the **OSPF** menu item.



3 Click the **Admin Status** drop-down list to select the administrative status of the OSPF feature for a selected port.

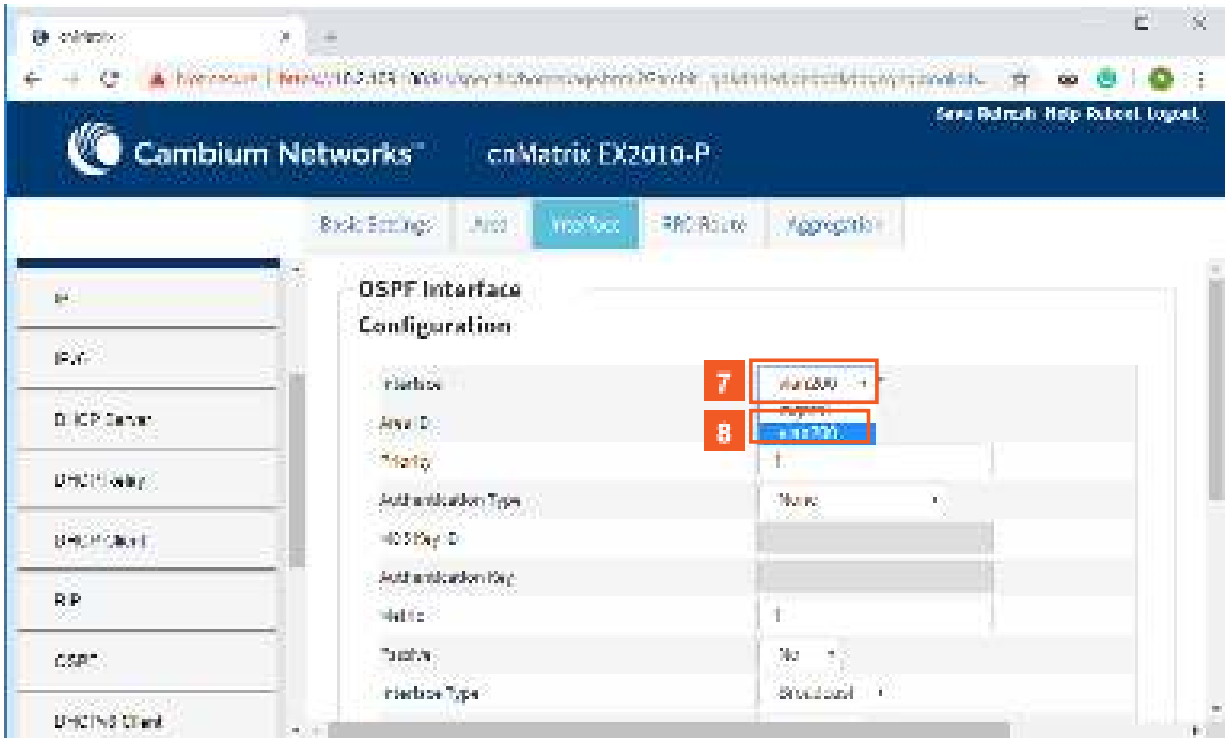


4 Select the **Enable** list item.



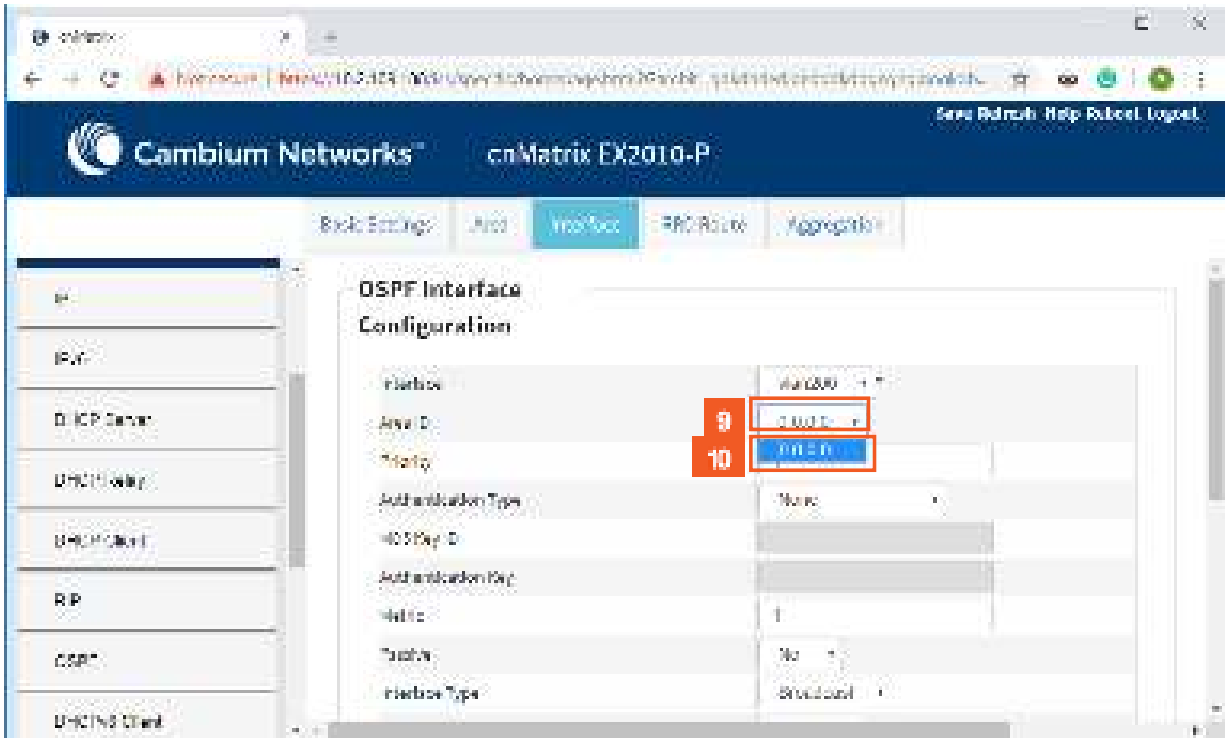
5 Click the **Apply** button.

6 Click the **Interface** tab. The **OSPF Interface Configuration** window is displayed.



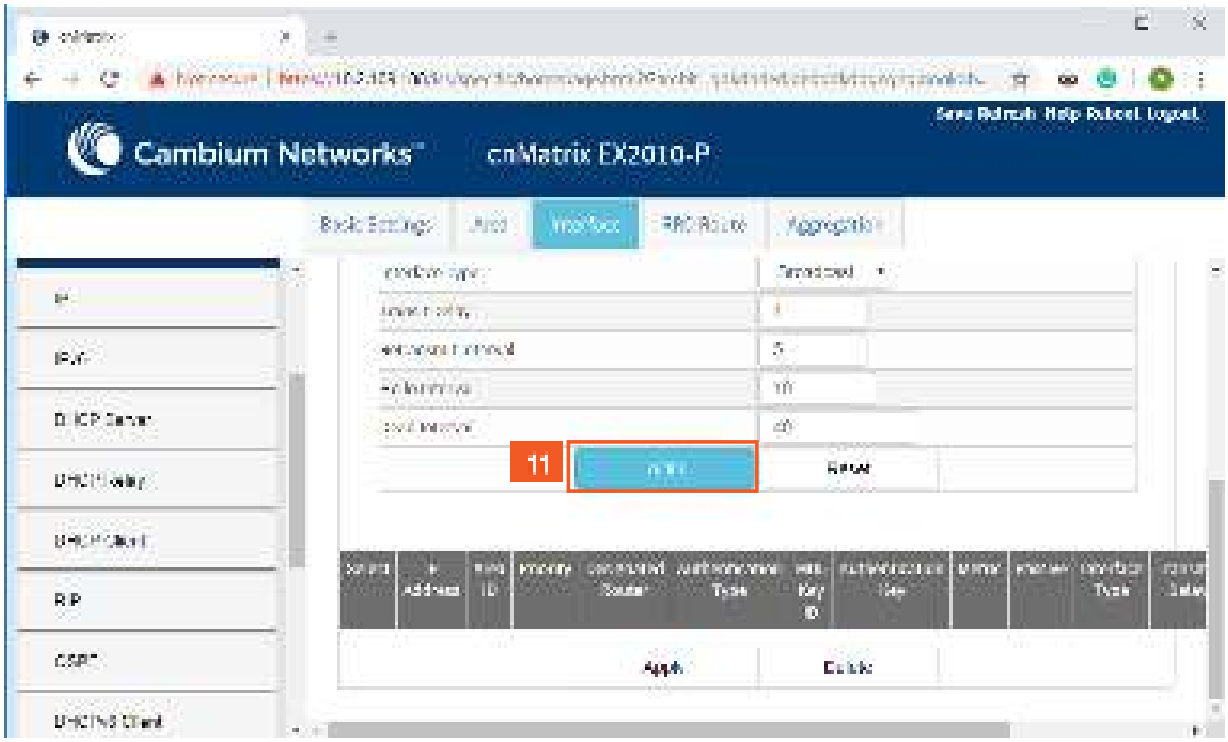
7 Click the **Interface** drop-down list and select a previously configured interface on which you want to enable the OSPF feature.

8 Select the **vlan200** list item.

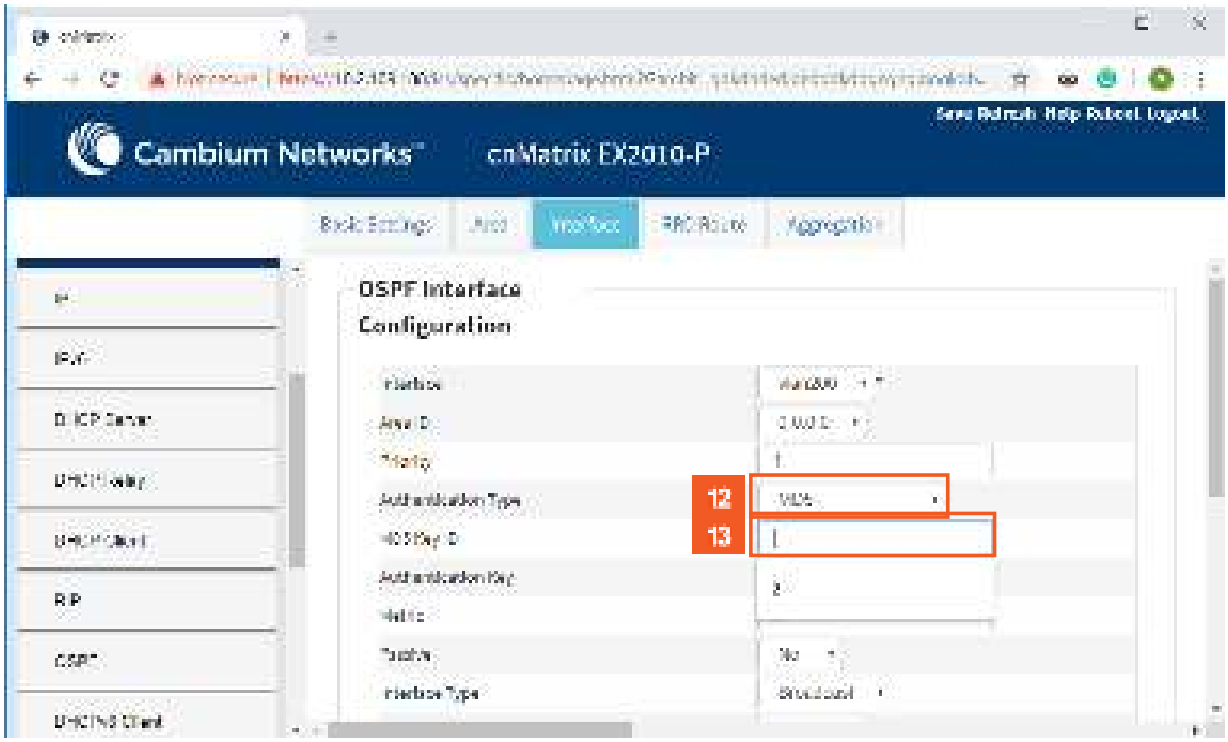


9 Click the **Area ID** drop-down list to select an area ID.

10 Select the **0.0.0.0** list item.



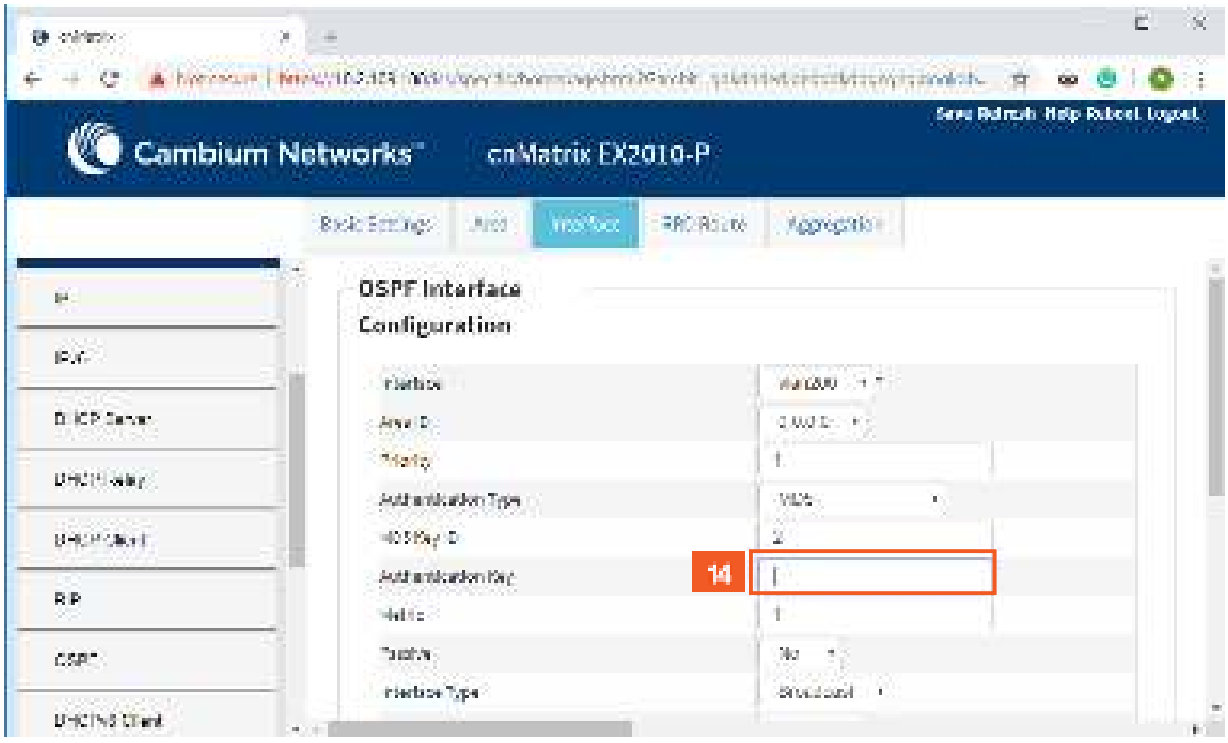
11 Click the **ADD** button.



12 Click the **Authentication Type** drop-down list to select the type of authentication used on the interface. In this example, select the **MD5** list item (not mandatory).

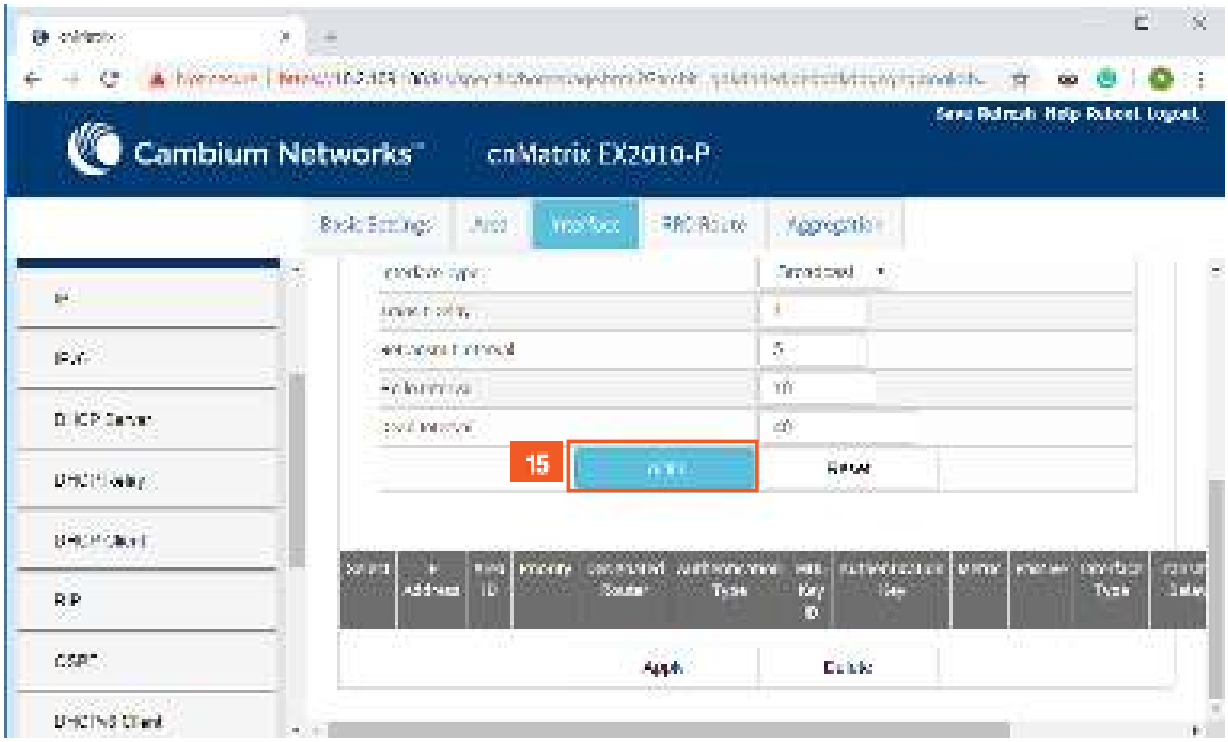
13 Type the value **2** into the **MD5 Key ID** field to specify the secret key ID used to create the message digest appended to the OSPF packet (not mandatory).

.

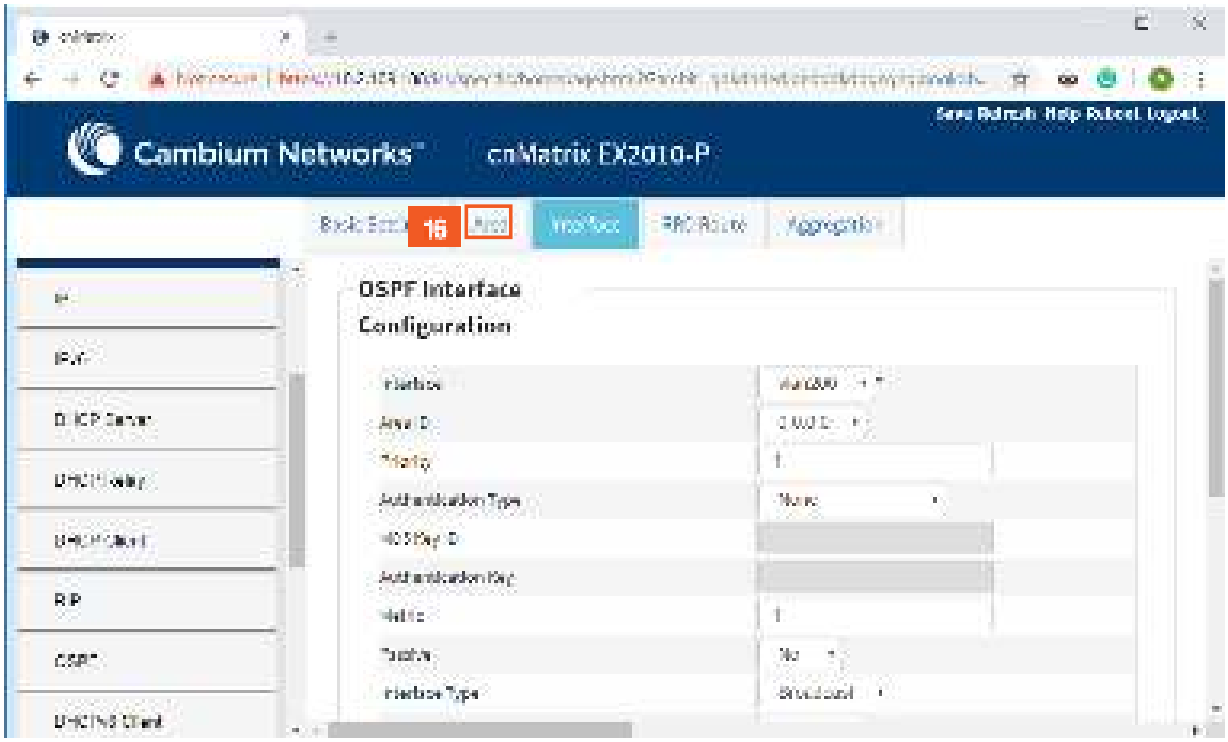


14 Type **cnMatrix2019** into the field, representing the authentication key used on the interface (not mandatory).

.

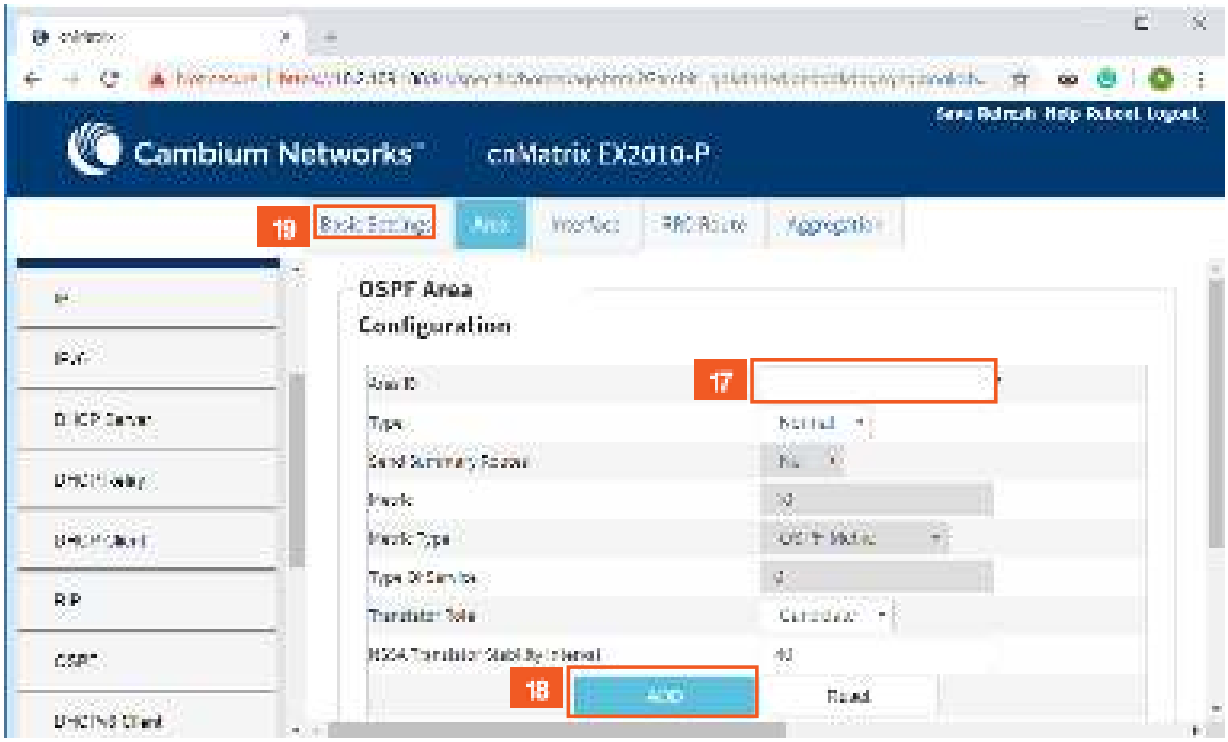


15 Click the **ADD** button.



16 Click the **Area** tab. The **OSPF Area Configuration** window is displayed (not mandatory).

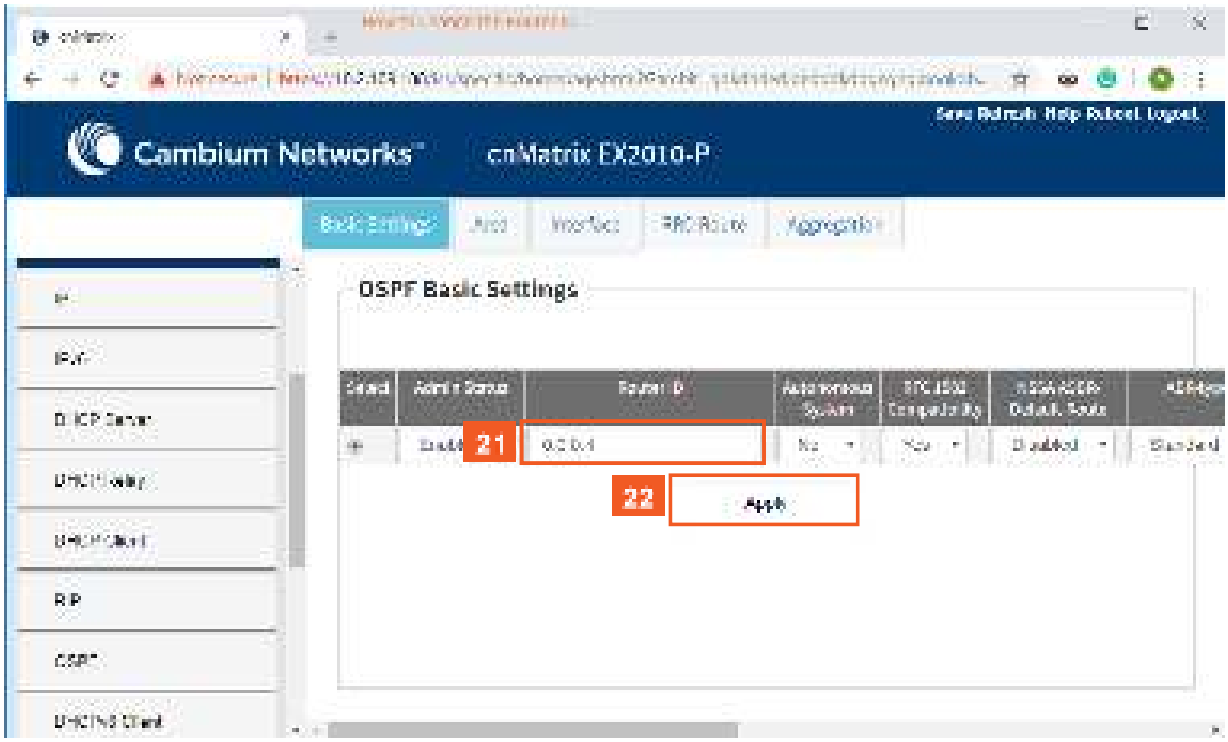
.



17 Type **0.0.0.7** into the **Area ID** field if you want to add another area in the OSPF process (this is not a mandatory step in the OSPF configuration).

18 Click the **ADD** button.

19 Click the **Basic Settings** tab. The **OSPF Basic Settings** window is displayed.



20 **If you want to change the router ID**:

Remove the default value from the **Router ID** field.

21 Type **0.0.0.4** into the **Router ID** field to create a new 32 bit integer that uniquely identifies the originating router in the Autonomous System.

22 Click the **Apply** button.

For more information, see OSPF WEB Fields.

3.5 RIP (Starting with version 2.1)

3.5.1 Managing RIP

3.5.1.1 Feature Overview

Feature Overview

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

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

Note: RIP uses port number 520.

Scaling Numbers

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

Limitations

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

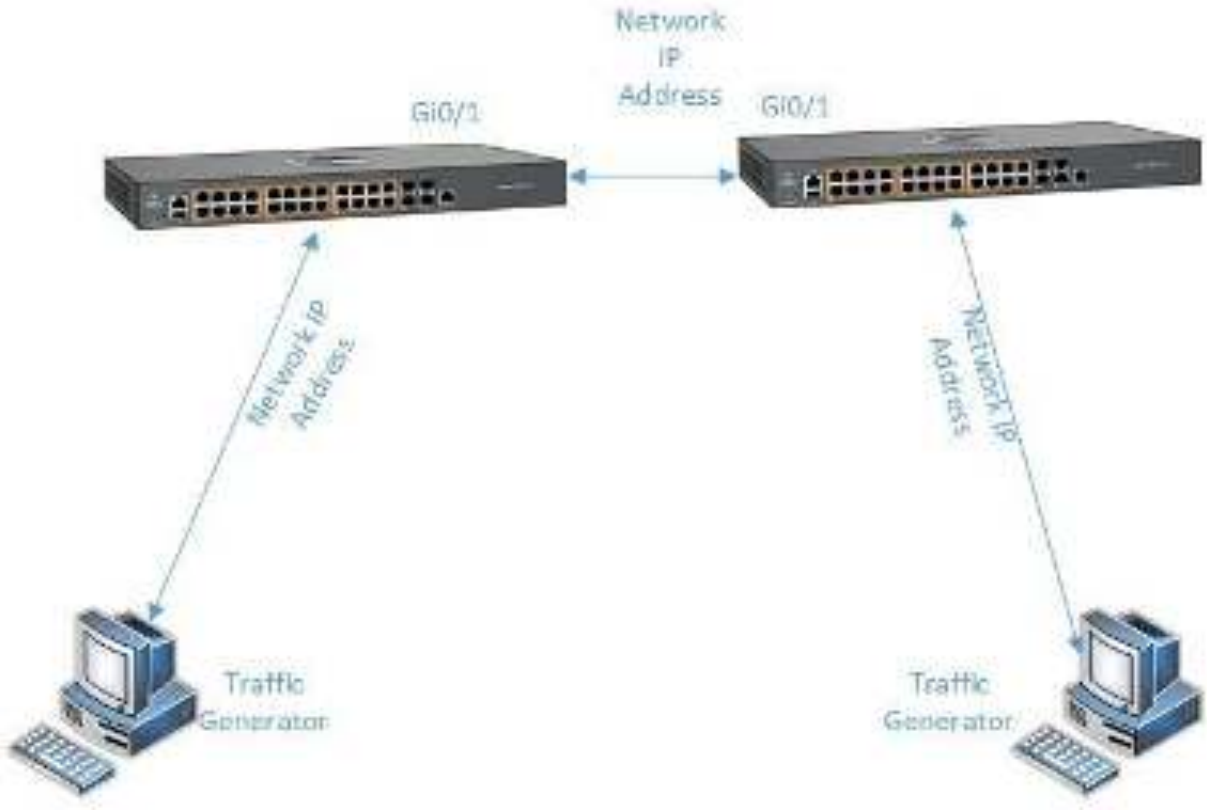
Default Values

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

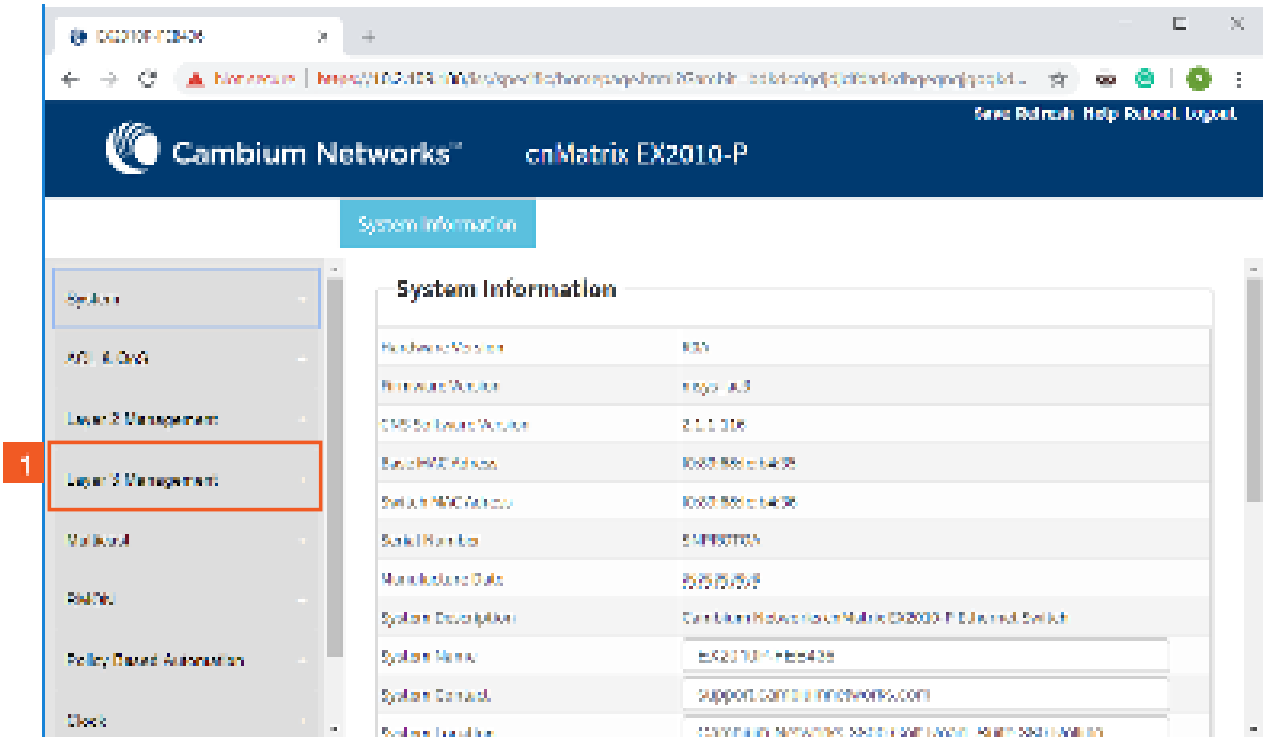
Prerequisites

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

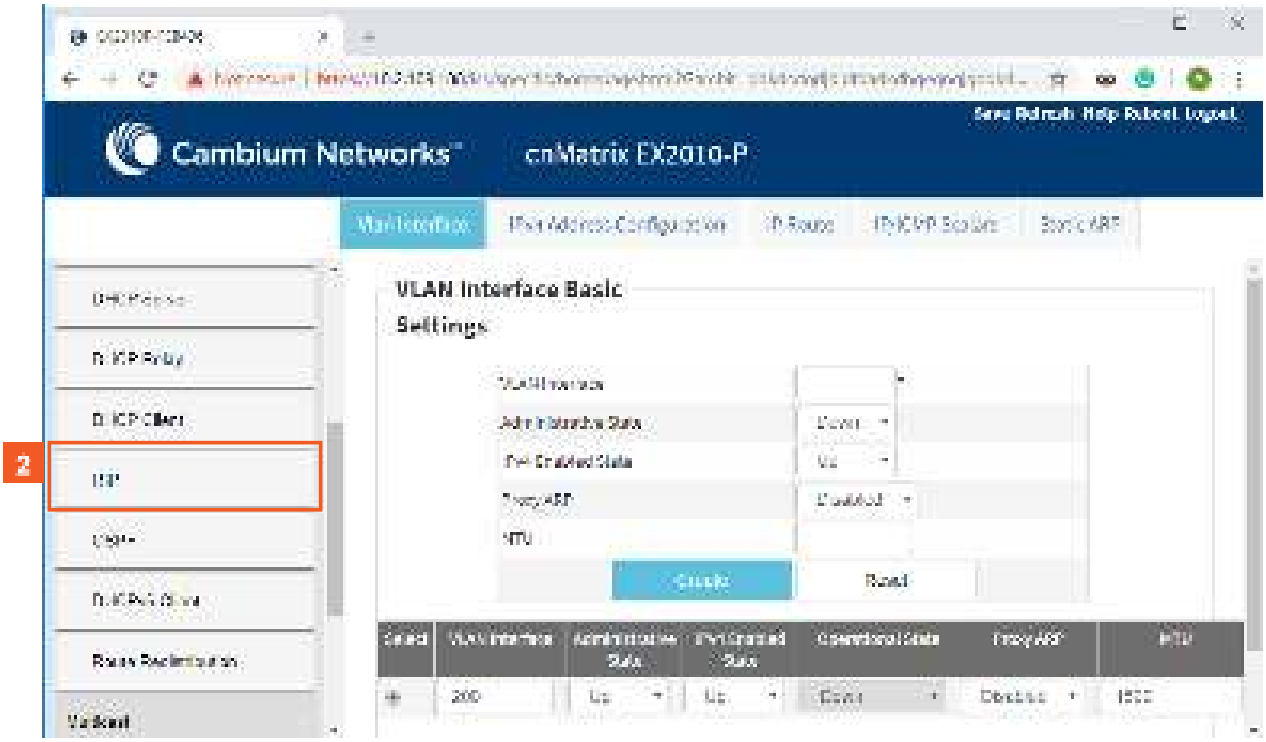
3.5.1.2 Network Diagram



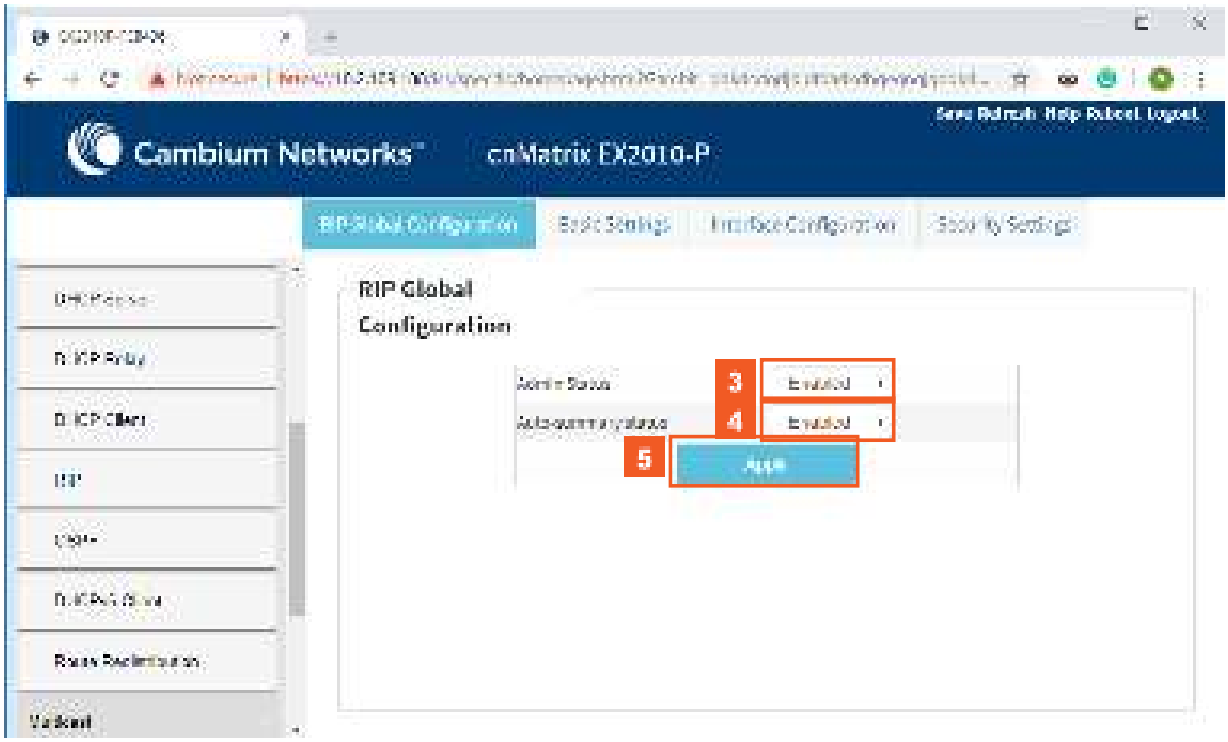
3.5.2 How to Enable RIP in WEB Interface



1 Click the **Layer 3 Management** tab. The **L3 Features** are displayed.



2 Click the **RIP** menu item.

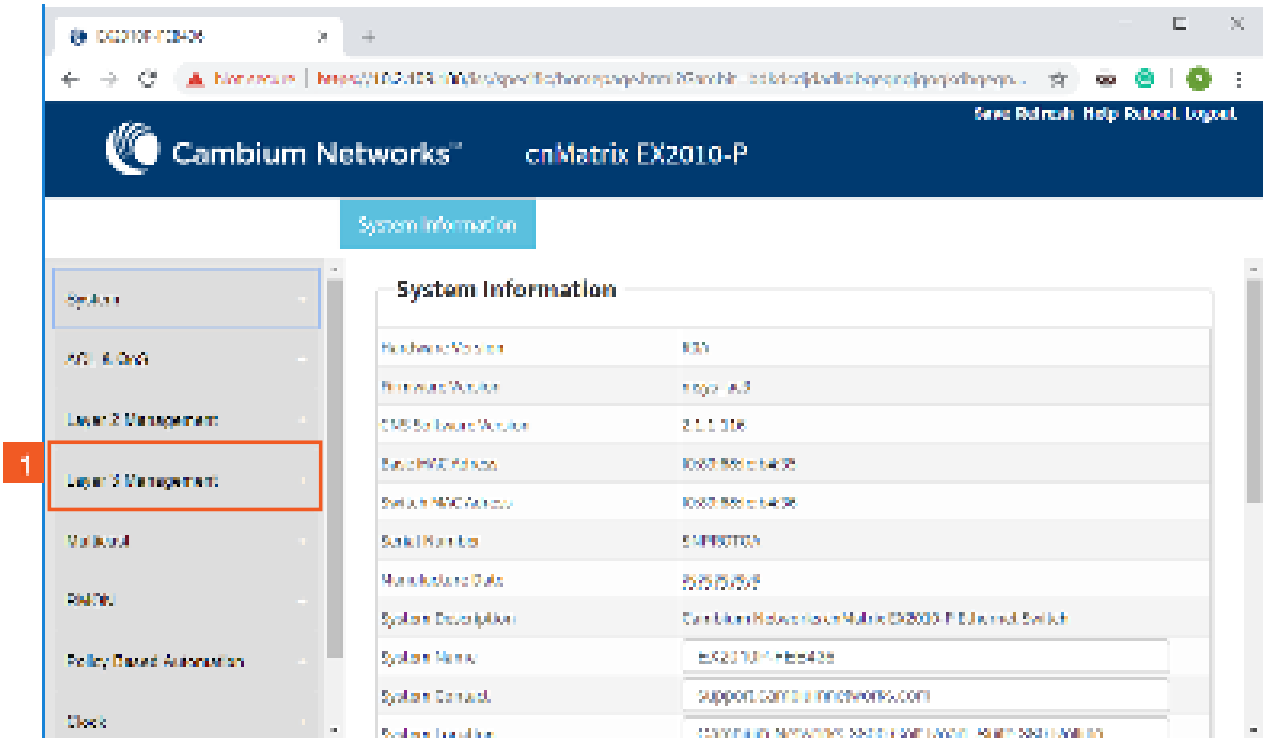


3 Click the **Admin Status** drop-down list to select the administrative module status of the RIP feature.

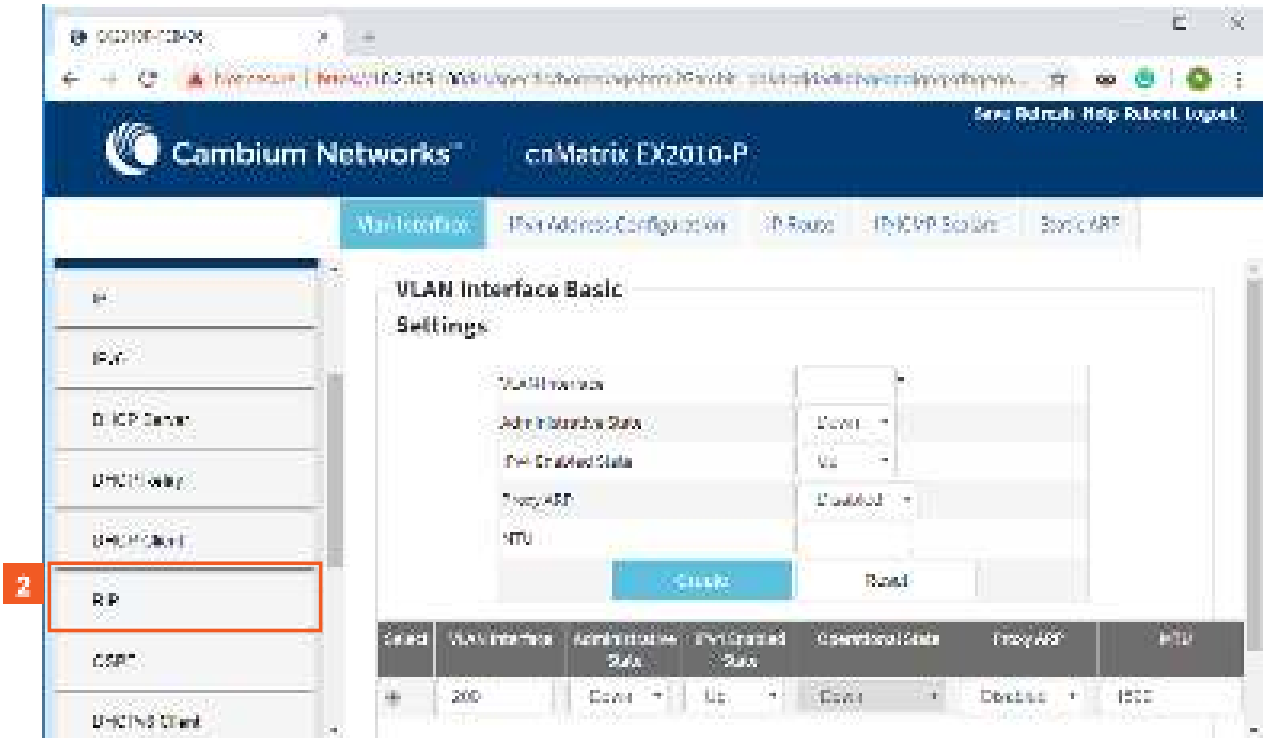
4 Select the **Enabled** list item.

5 Click the **Apply** button.

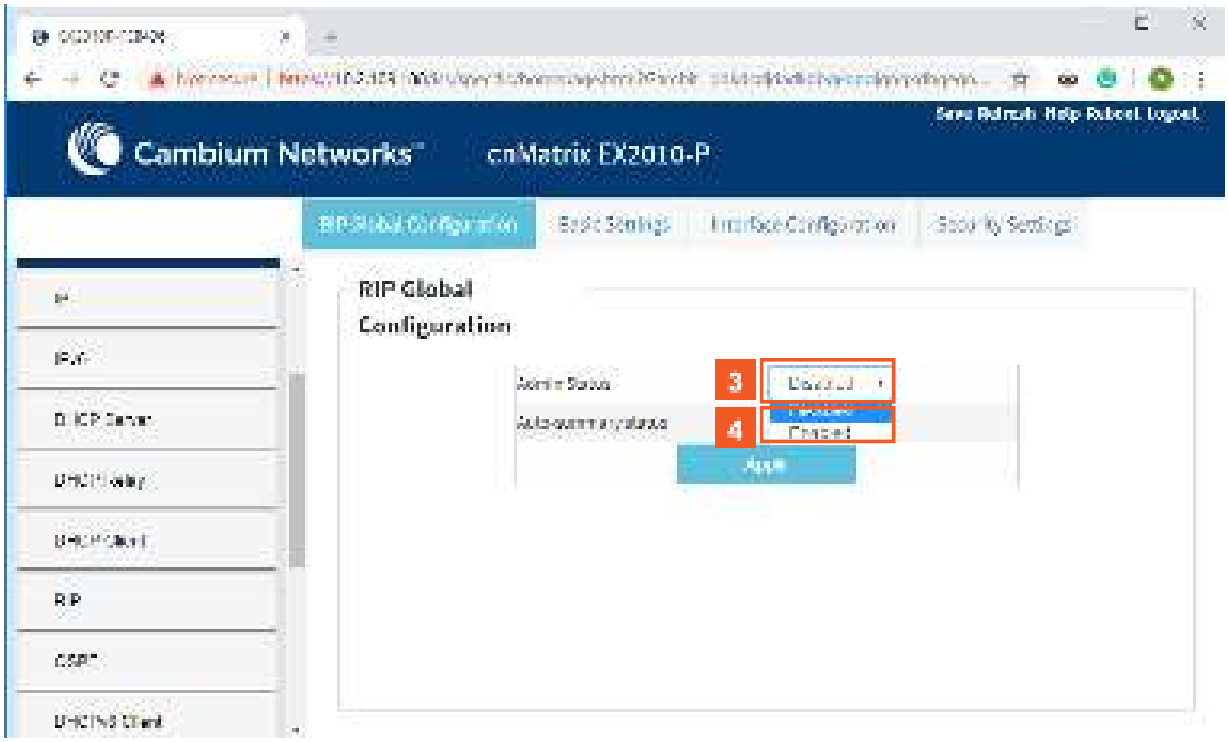
3.5.3 How to Configure RIP in WEB Interface (example)



1 Click the **Layer 3 Management** tab. The **L3 Features** are displayed.

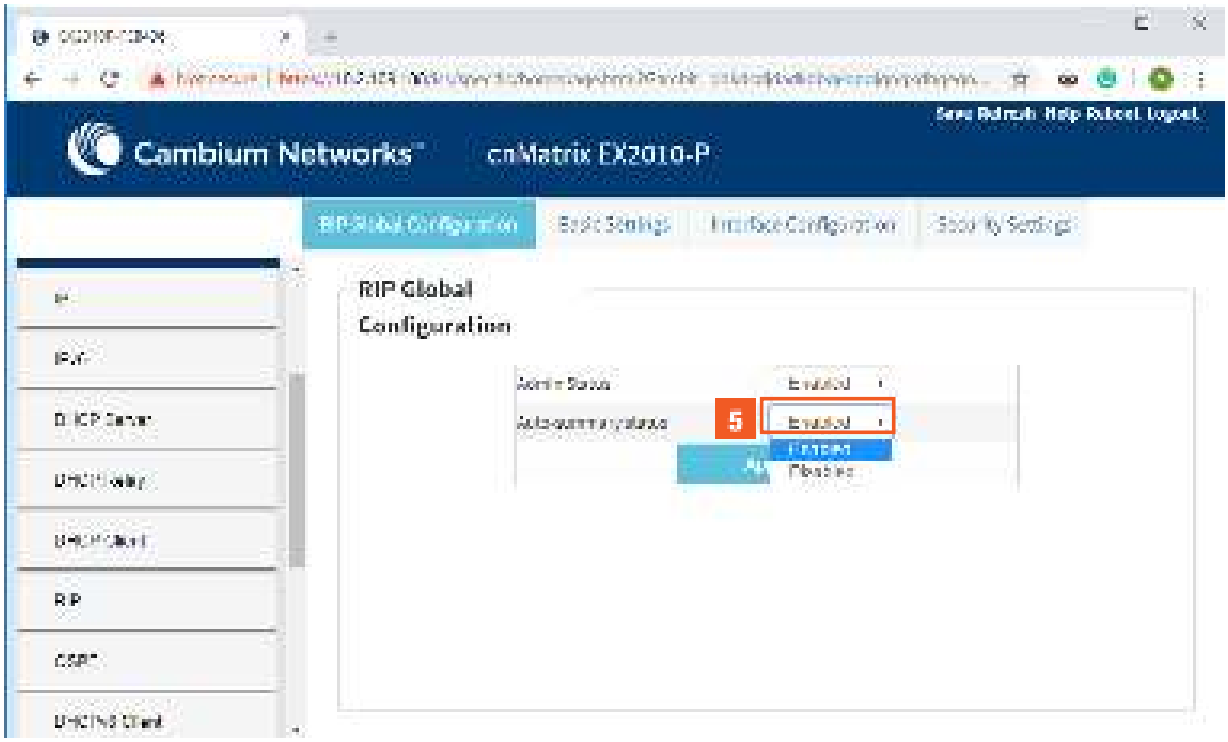


2 Click the **RIP** menu item.

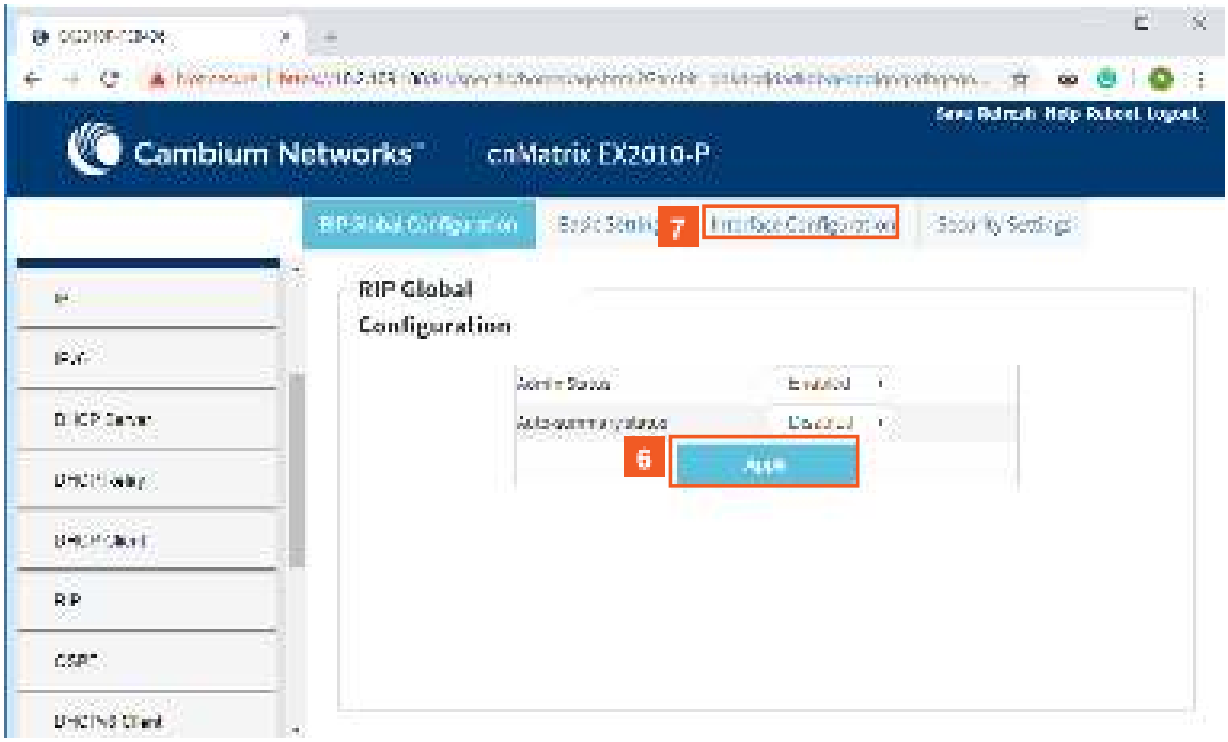


3 Click the **Admin Status** drop-down list to select the administrative module status of the RIP feature.

4 Select the **Enabled** list item.

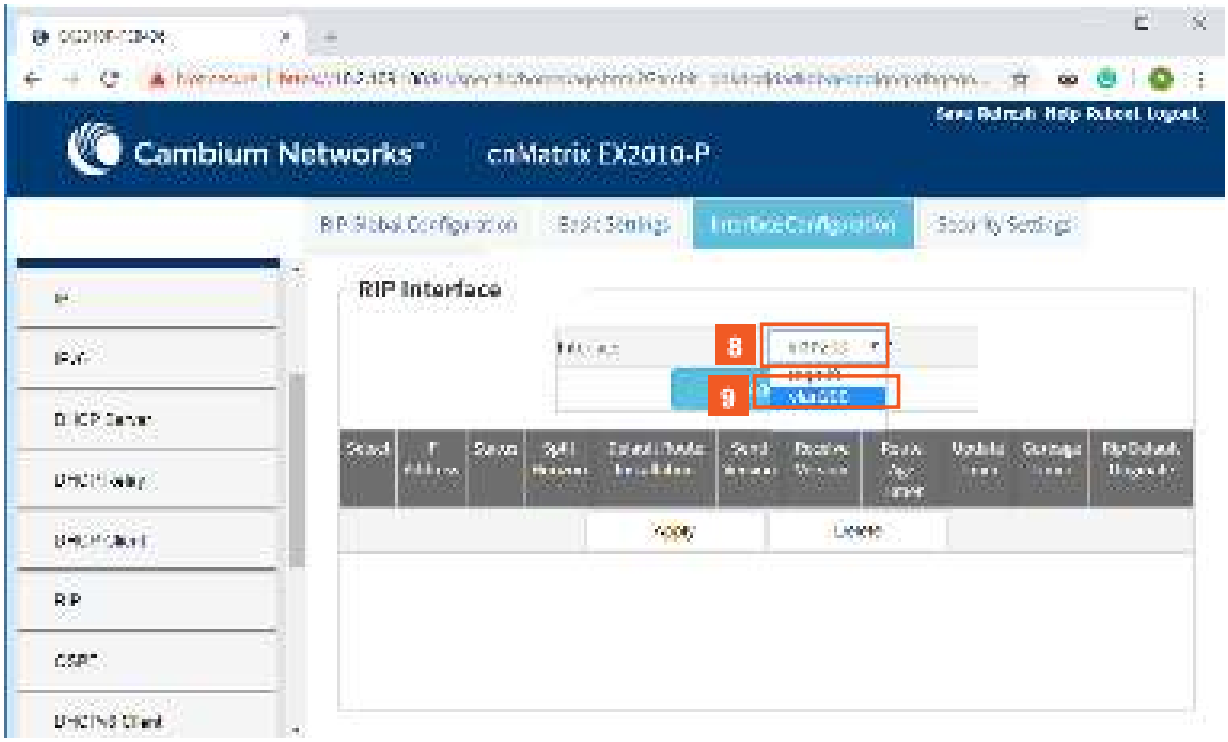


5 Click the **Auto-summary status** drop-down list to select the status of the RIP domain context. Select the **Disabled** list item.



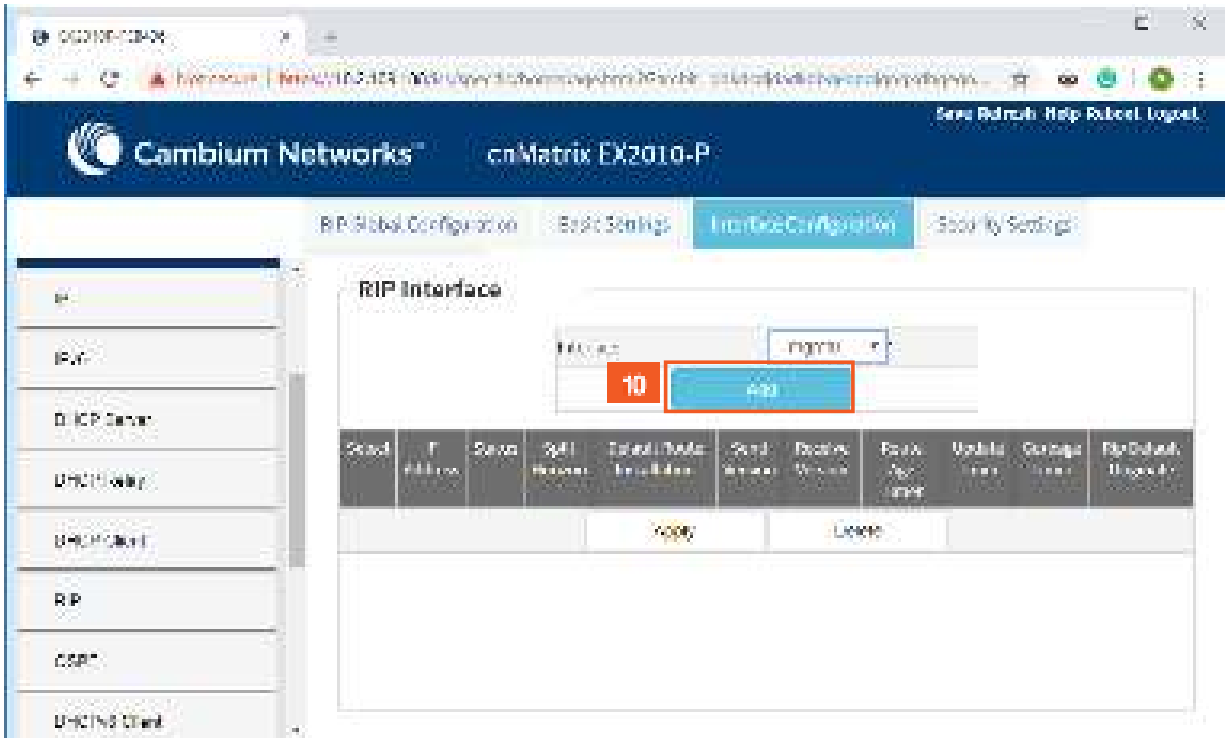
6 Click the **Apply** button.

7 Click the **Interface Configuration** tab. The **RIP Interface** window is displayed.

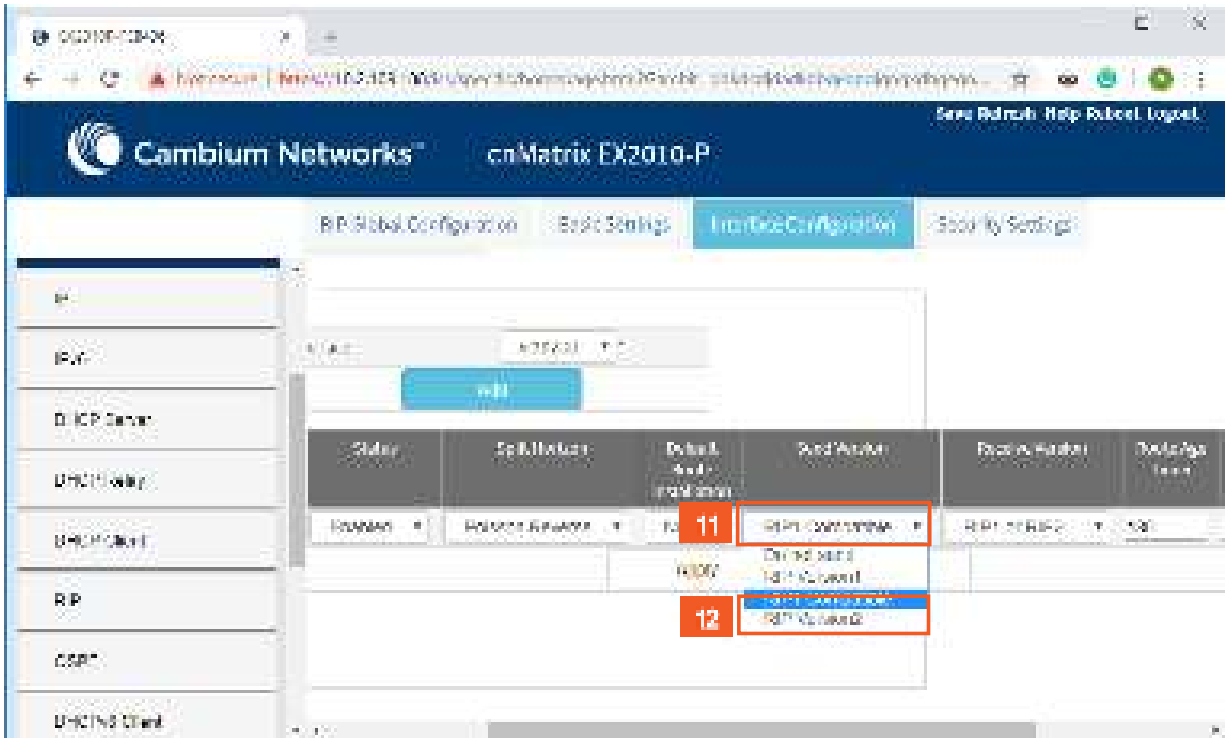


8 Click the **Interface** drop-down list to select a previously configured interface.

9 Select the **vlan 200** list item.

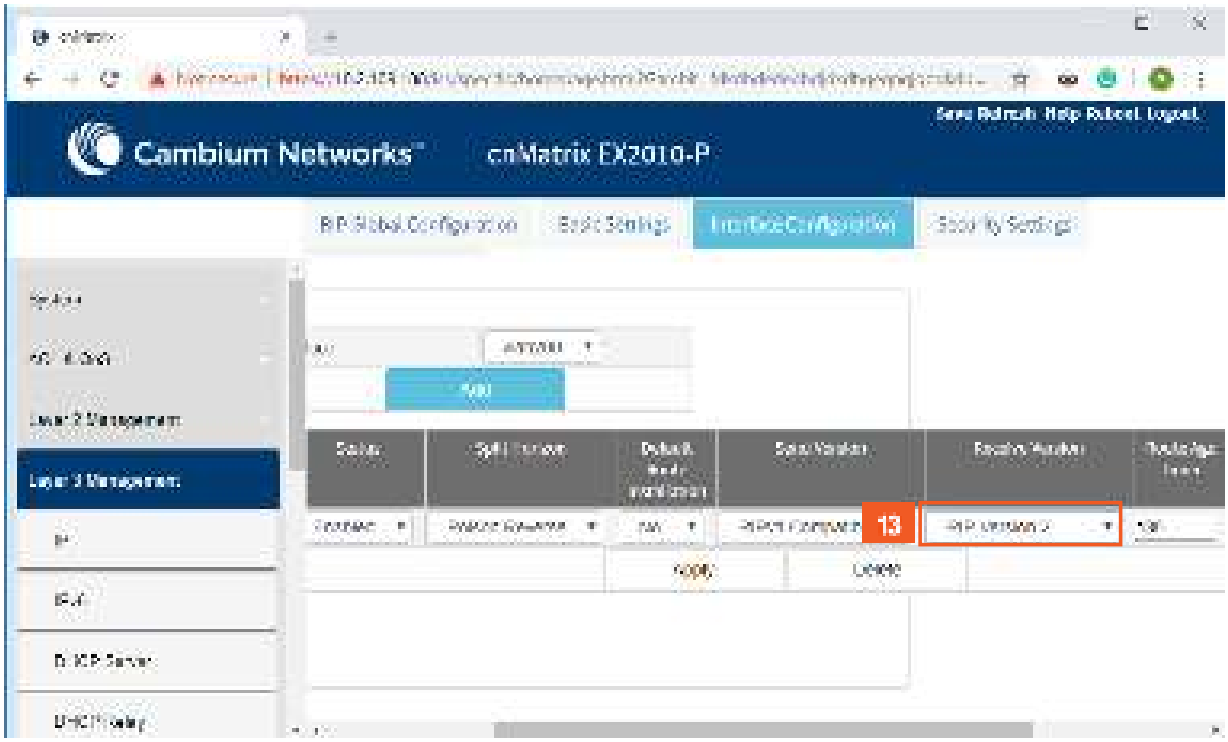


10 Click the **Add** button.

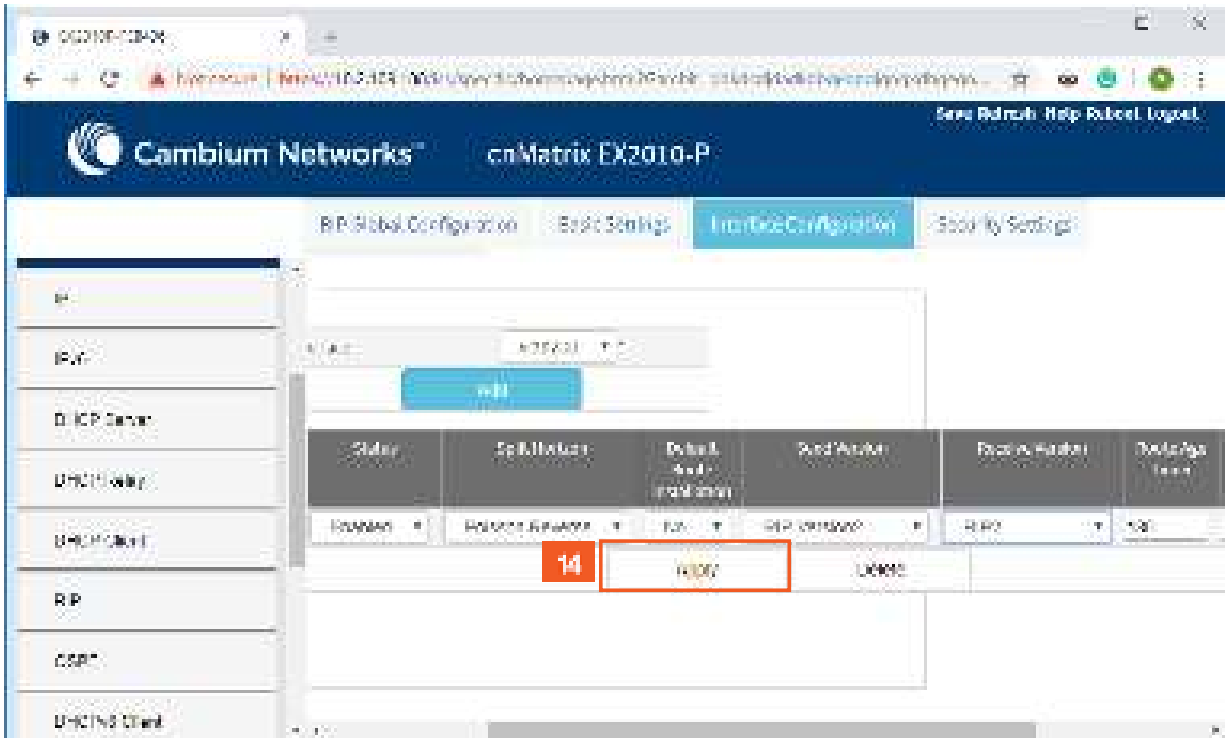


11 Click the **Send Version** drop-down list to select the send version of the RIP feature.

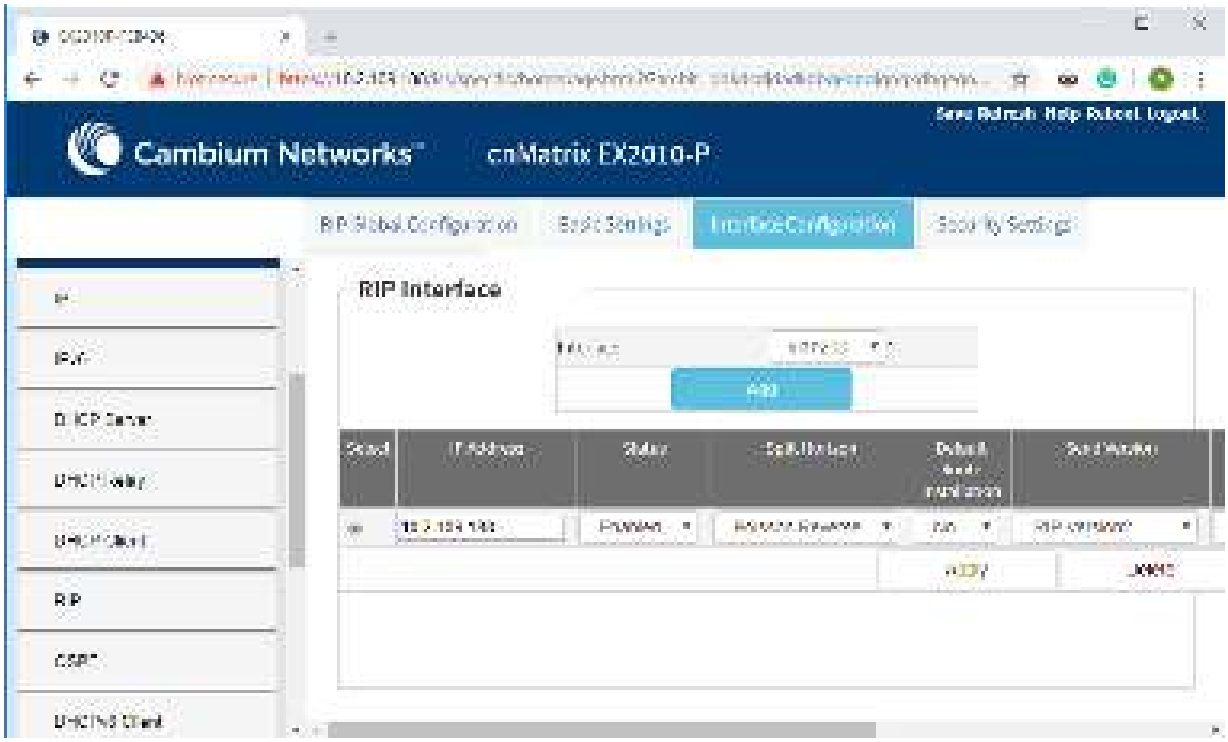
12 Select the **RIP Version 2** list item.



13 Click the **Receive Version** drop-down list and select the **RIP Version 2** list item.



14 Click the **Apply** button.



4 Management Features

4.1 DHCP Client

4.1.1 Managing DHCP Client

Feature Overview

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

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

Standards

- RFC 2131

Scaling Numbers

- DHCP Client can be enabled on 64 IPv4 Interfaces.

Limitations

N/A

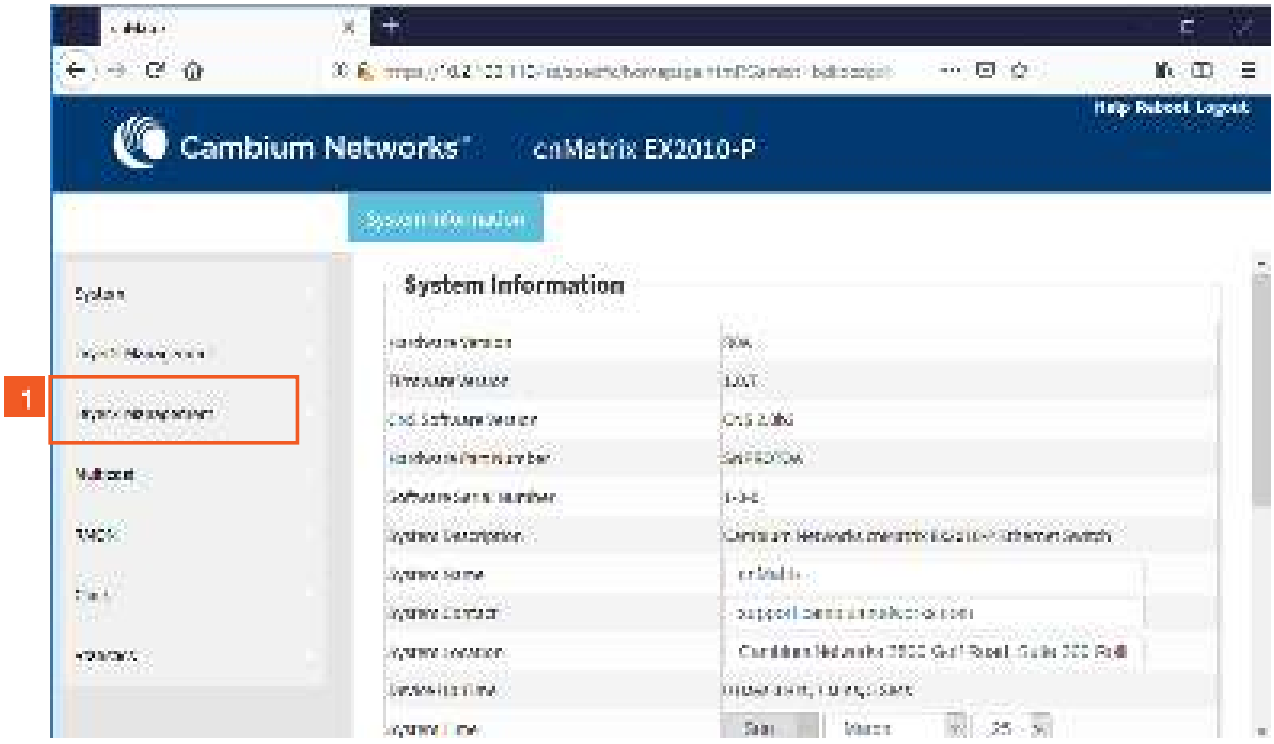
Default Values

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

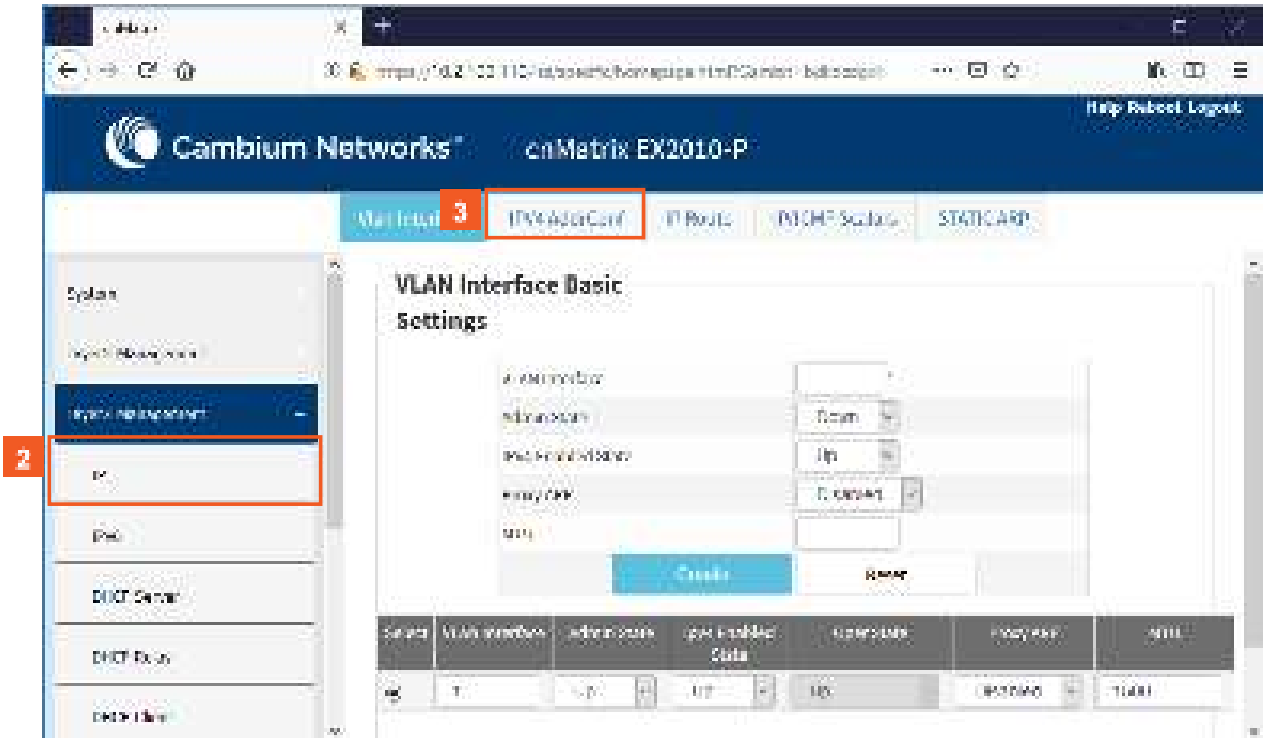
Prerequisites

N/A

4.1.2 How to Enable DHCP Client in WEB Interface

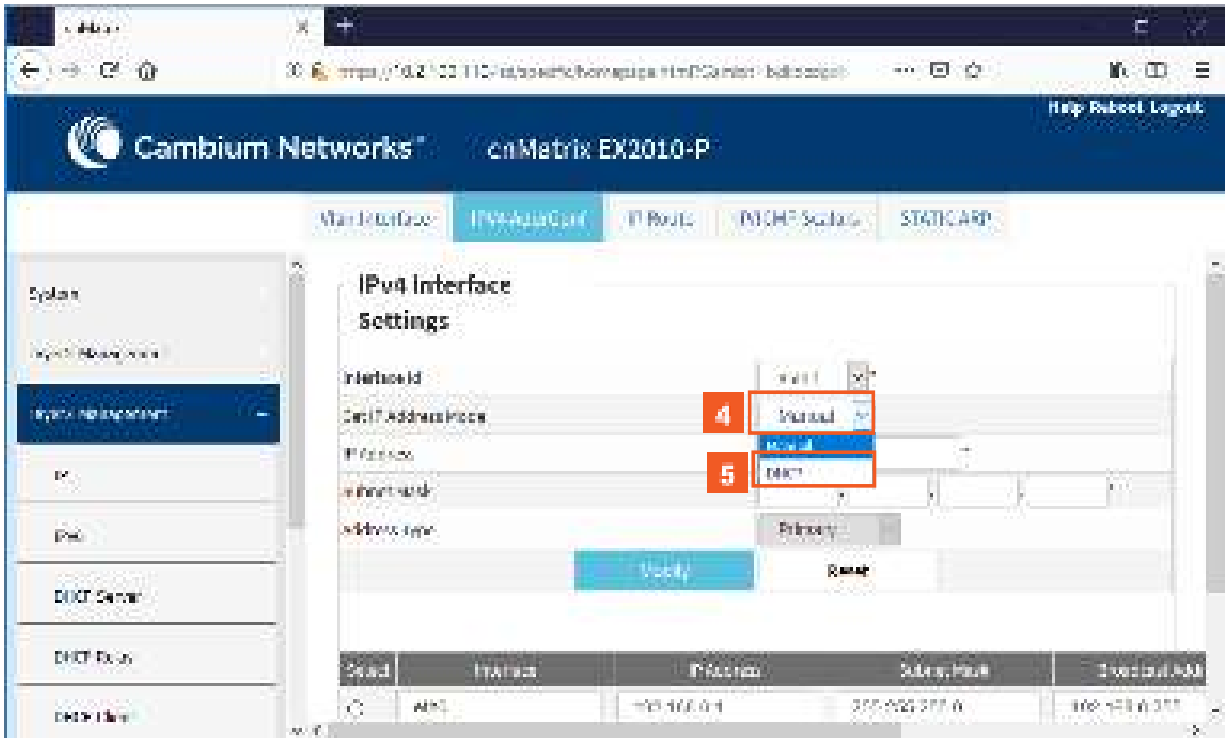


1 Click the **Layer3 Management** tab. The **L3 Features** are displayed.



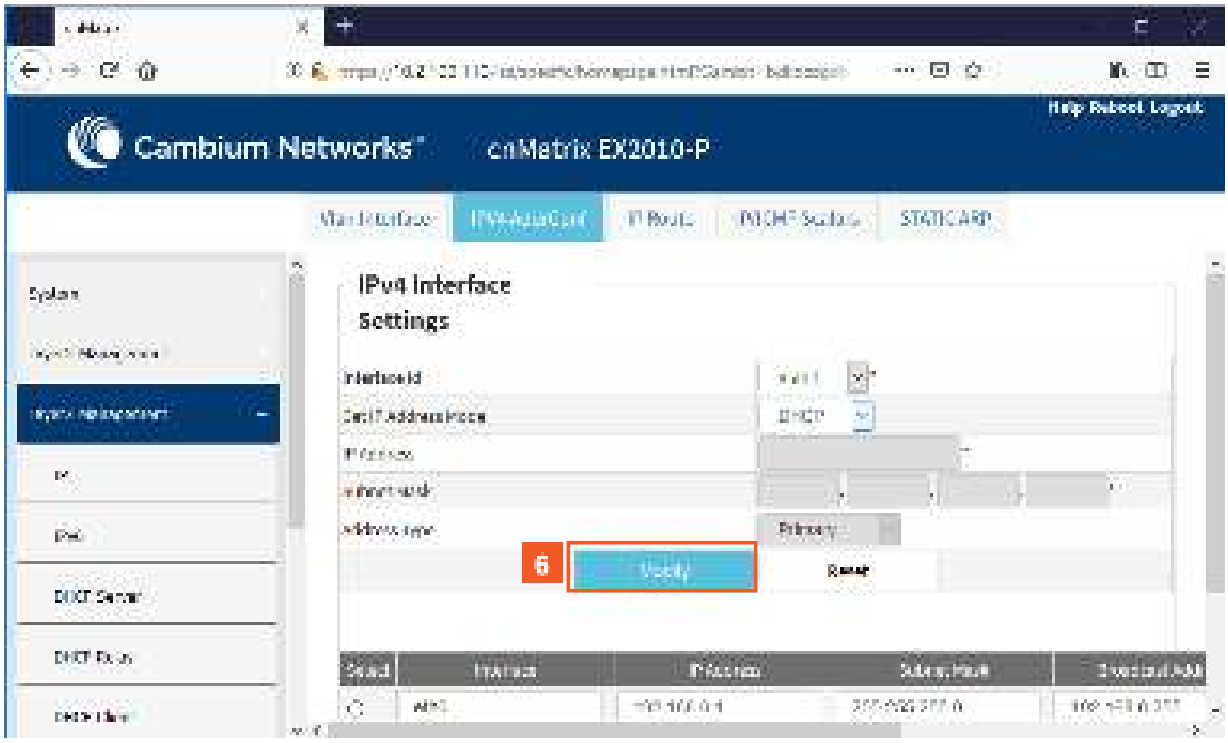
2 Click the **IP** menu item.

3 Click the **IPV4 Address Configuration** tab. The **IPv4 Interface Settings** window is displayed.



4 Click the **Get IP Address Mode** drop-down list and select the protocol to be used to obtain the IP address from the interface.

5 Select the **DHCP** option.



6 Click the **Modify** button.

4.2 DHCP Server

4.2.1 Managing DHCP Server

4.2.1.1 Feature Description

Feature Overview

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

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

Standards

- RFC 2131
- RFC 2132

Scaling Numbers

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

Limitations

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

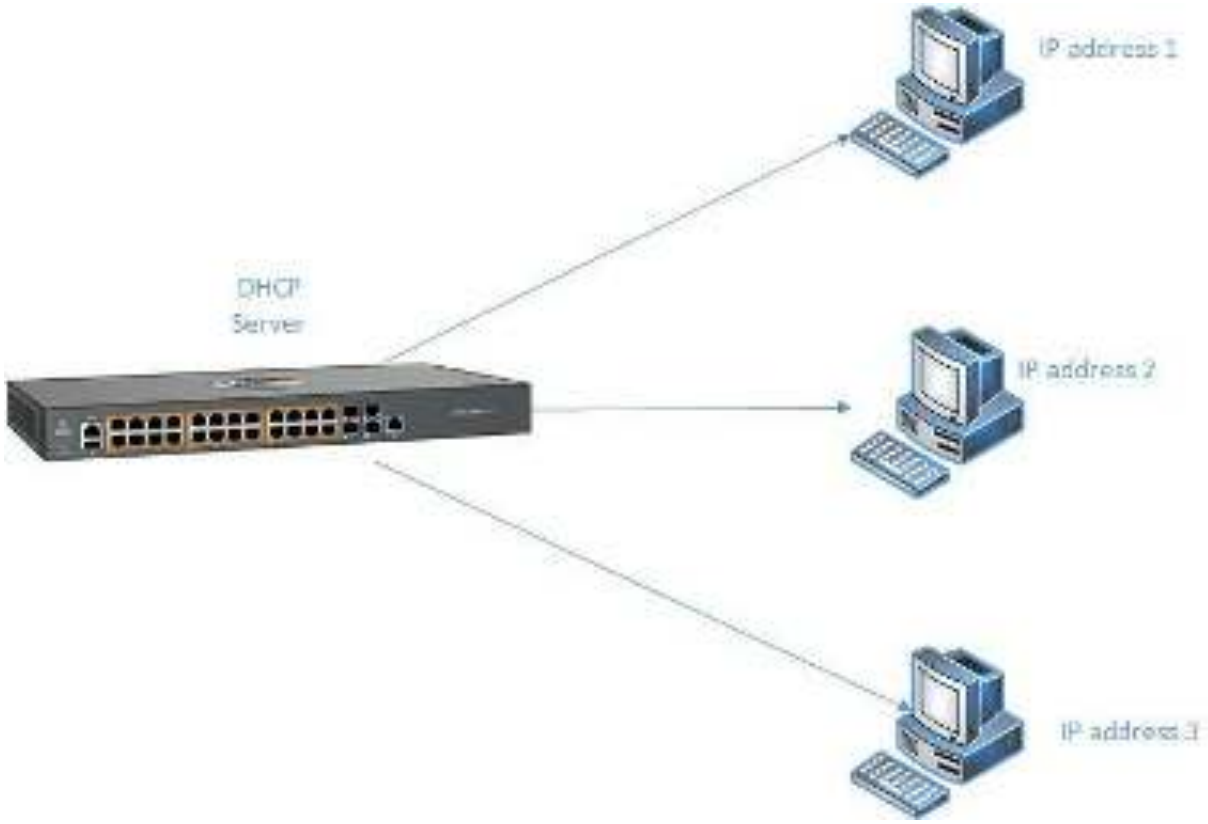
Default Values

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

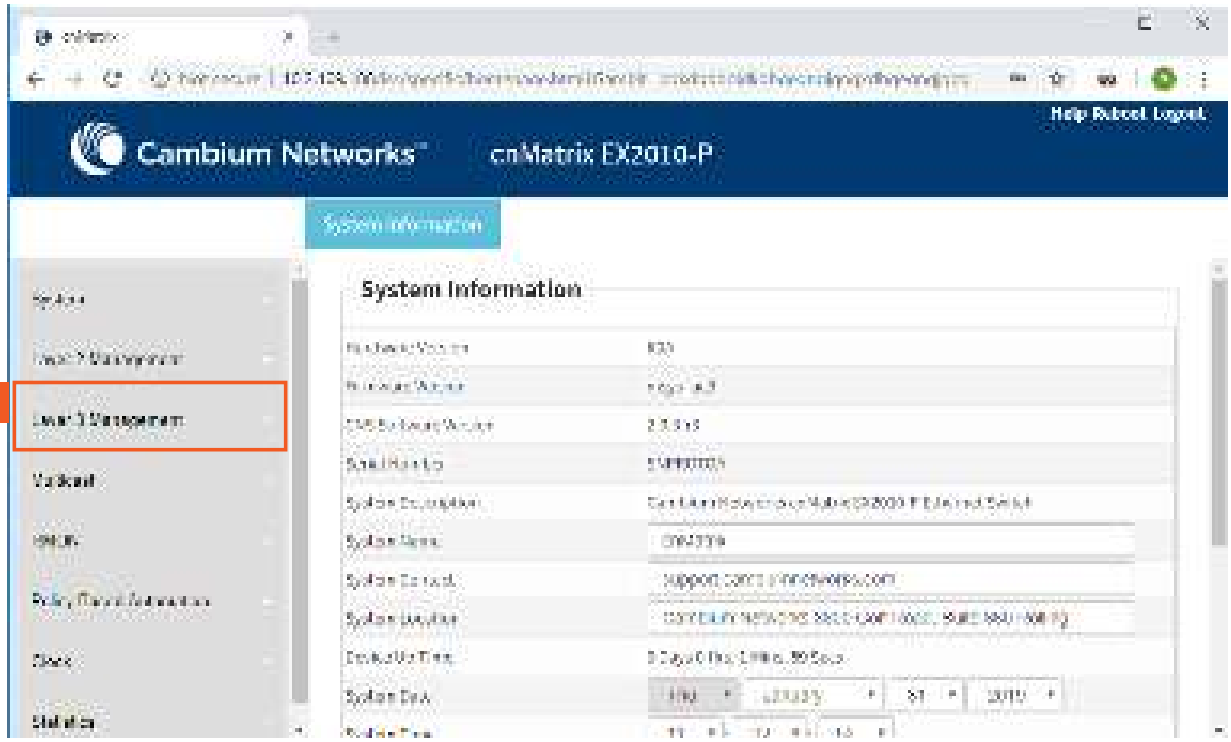
Prerequisites

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

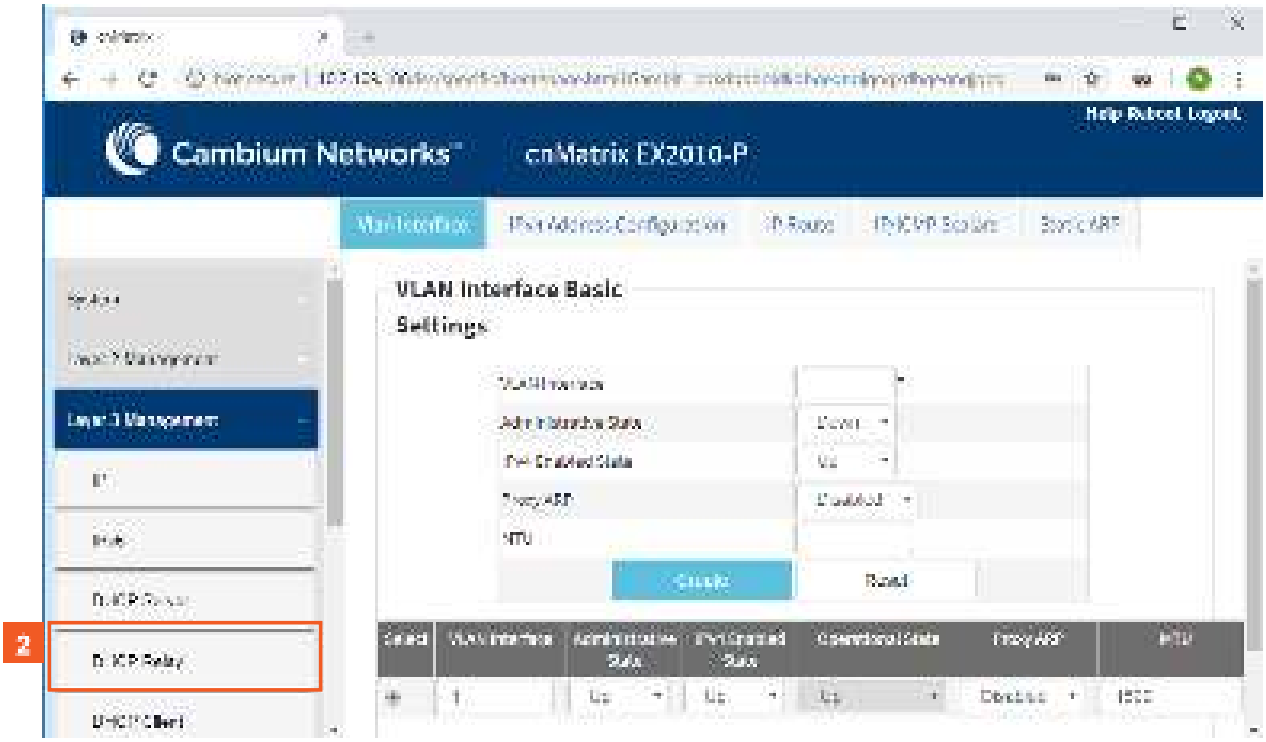
4.2.1.2 Network Diagram



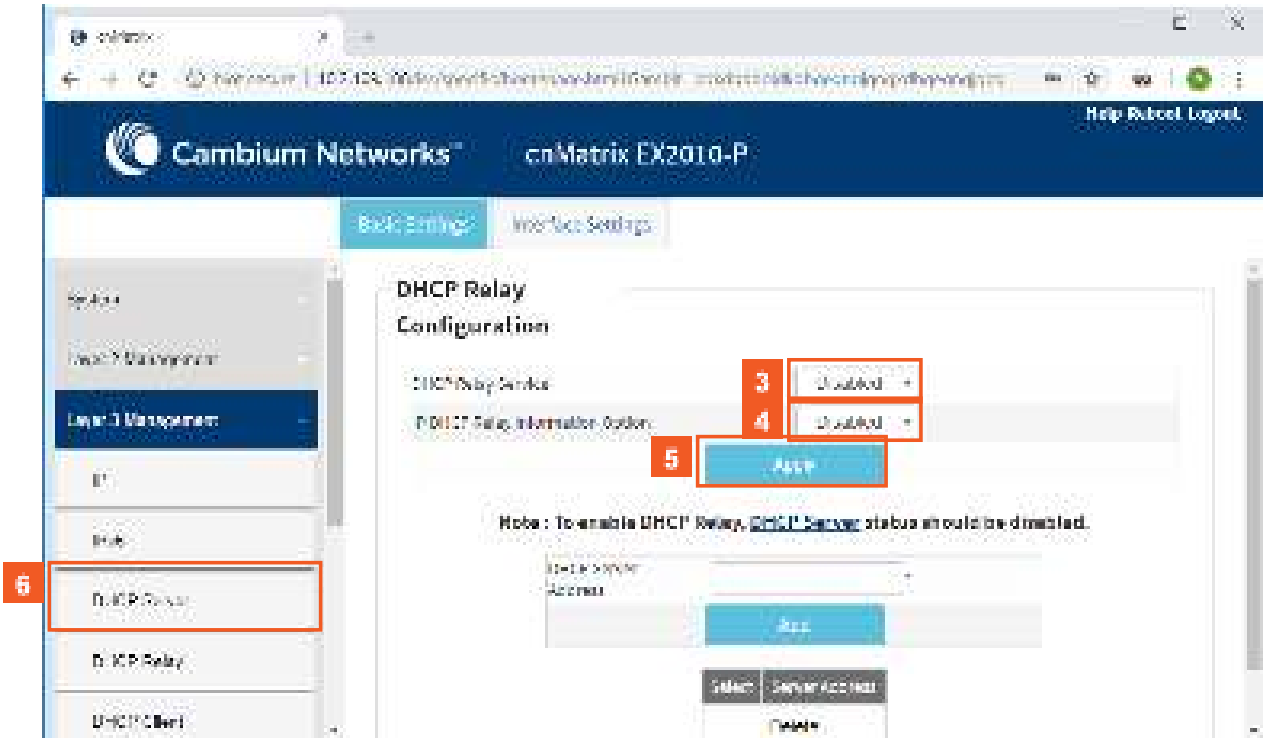
4.2.2 How to Enable DHCP Server in WEB Interface



1 Click the **Layer3 Management** tab. The **L3 Features** are displayed.



2 Click the **DHCP Relay** menu item.

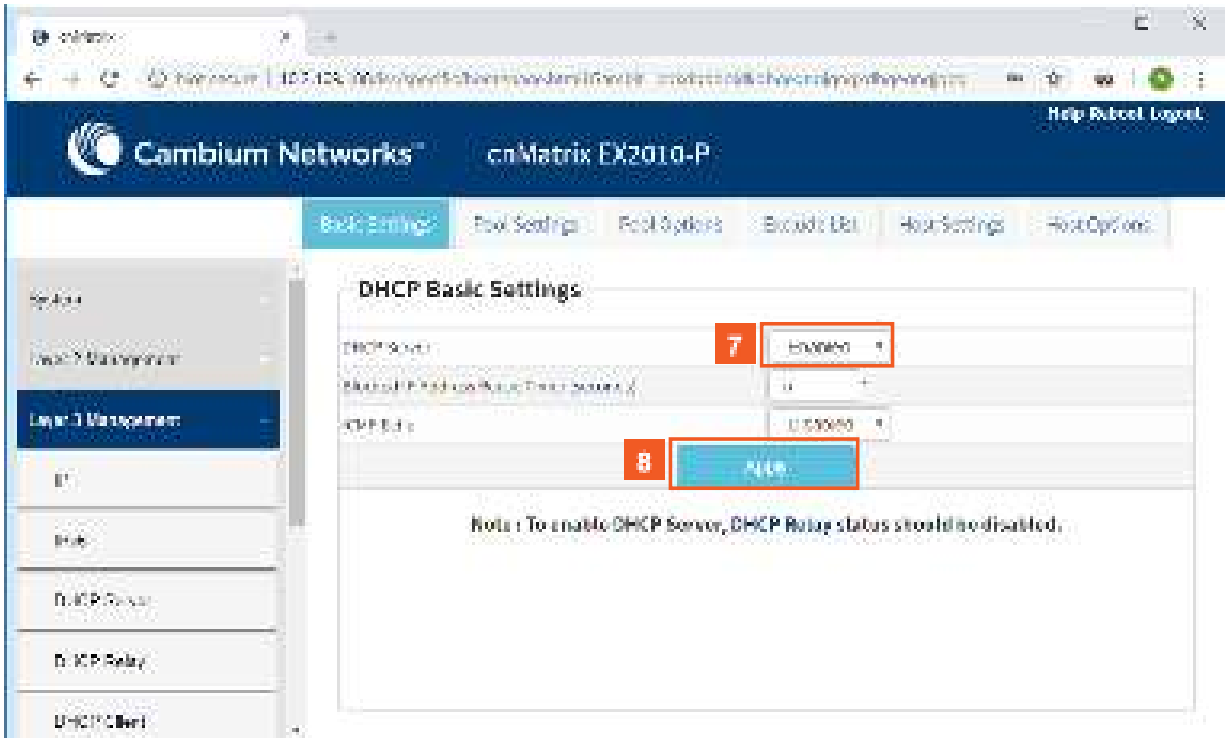


3 Click the **DHCP Relay Service** drop-down list to select the DHCP Relay service status in the switch.

4 Select the **Disabled** list item.

5 Click the **Apply** button.

6 Click the **DHCP Server** menu item. The **DHCP Basic Settings** window is displayed.



7 Click the **DHCP Server** drop-down list and select the **Enabled** option (the new DHCP server status in the router).

8 Click the **Apply** button.

4.3 Out-of-Band Management

4.3.1 Managing Out-of-Band Ethernet Management

4.3.1.1 Feature Description

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

Benefits:

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

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

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

Standards

N/A

Scaling Numbers

N/A

Limitations

- IPv6 not supported on OOB port.

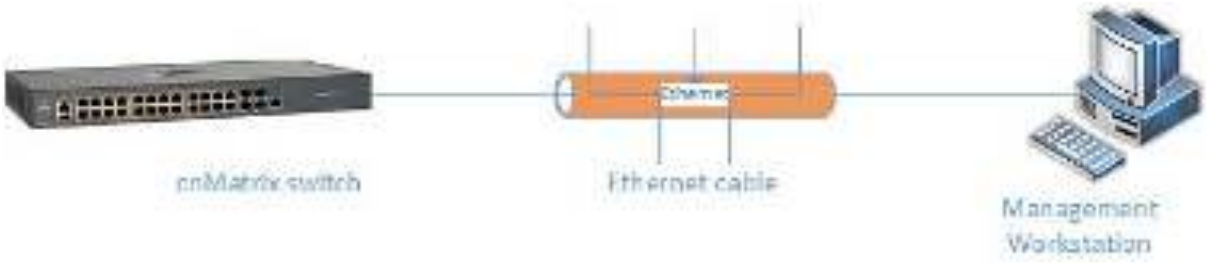
Default Values

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

Prerequisites

N/A

4.3.1.2 Network Diagram



4.3.2 Configuring Out-of-Band Ethernet Management in WEB Interface

The **Out-of-Band Ethernet Management** feature is not available in WEB interface.

4.4 Telnet Client

4.4.1 Managing Telnet Client

Telnet Client is an industry standard tool for remote connectivity using TCP protocol. This tool is used to connect to a remote system and open a CLI or Shell session.

Standards

- RFC 854

Scaling Numbers

- 1 session

Limitations

- It is recommended to open only one Telnet Client session.
- Telnet client doesn't work with IPv6 link local addresses.

Default Values

- The Telnet Client feature is enabled by default.
- Remote TCP port value is 23.

Prerequisites

N/A

4.4.2 Configuring Telnet Client in WEB Interface

The **Telnet Client** feature is not available in WEB interface.

4.5 Telnet Server

4.5.1 Managing Telnet Server

Feature Overview

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

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

Standards

- RFC 854

Scaling Numbers

- 8 sessions are accepted.

Limitations

N/A

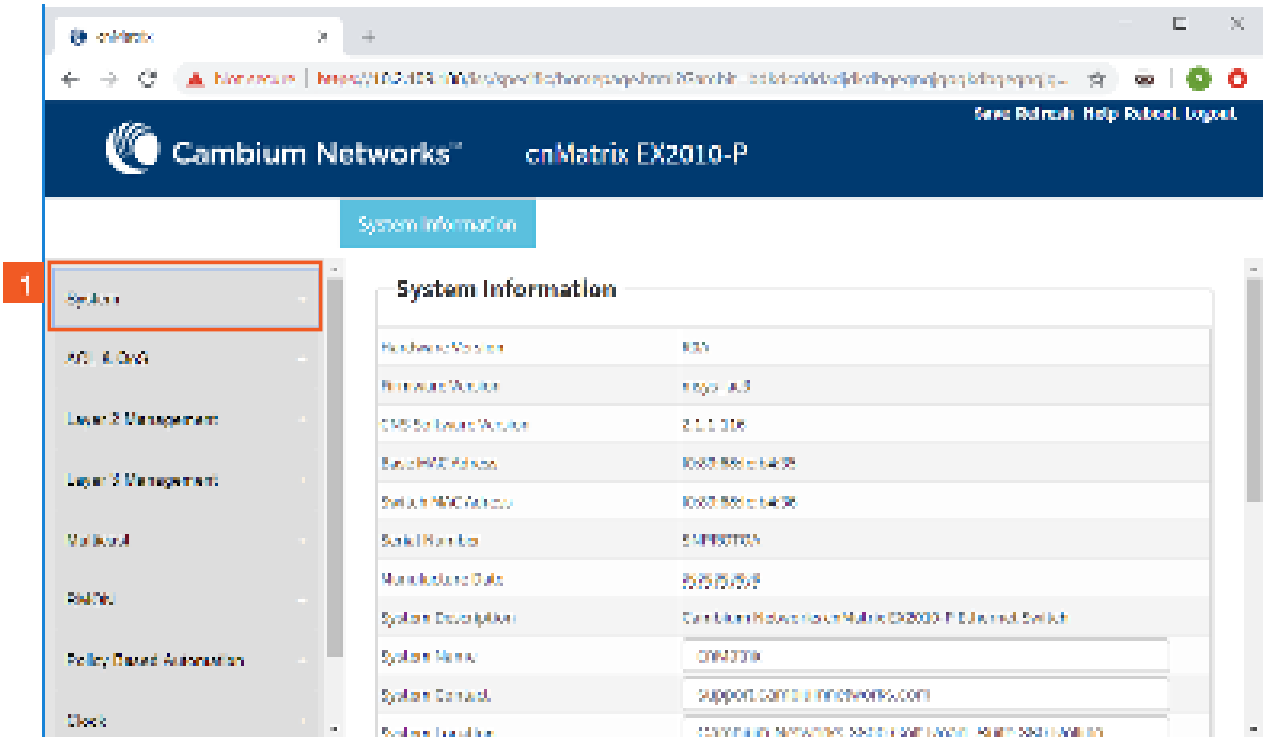
Default Values

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

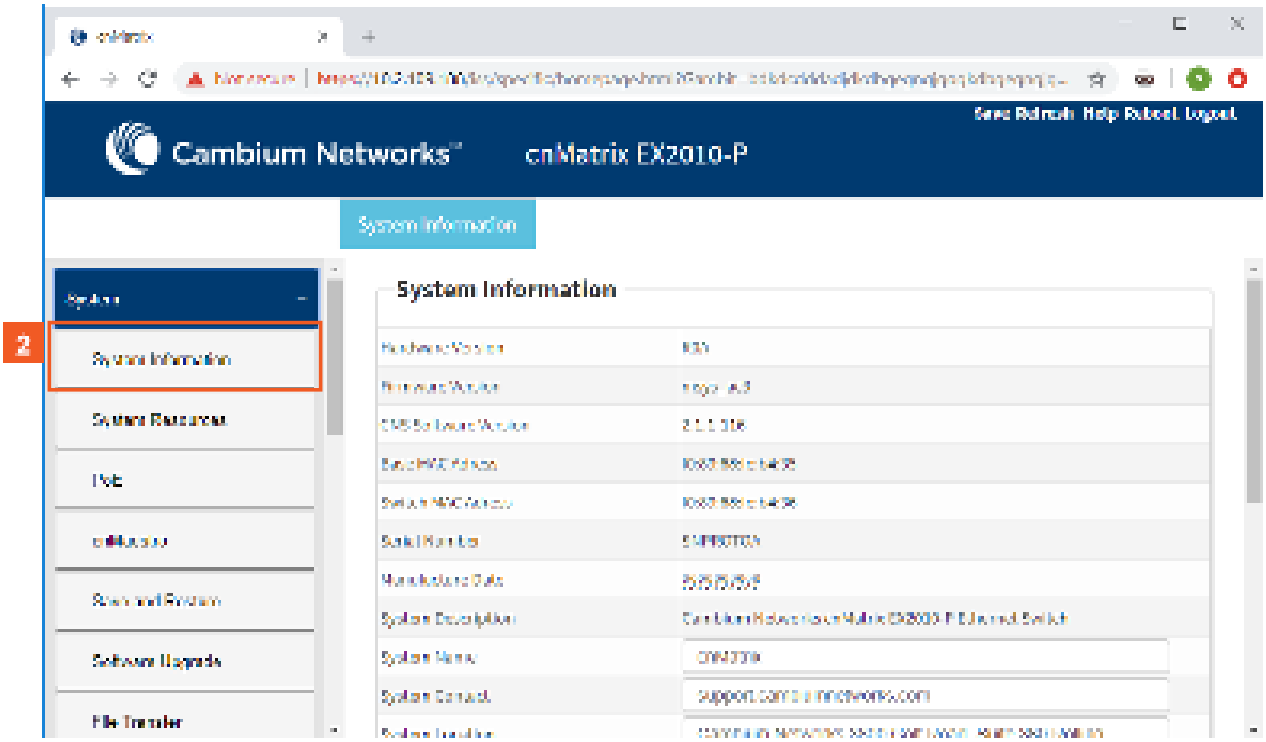
Prerequisites

N/A

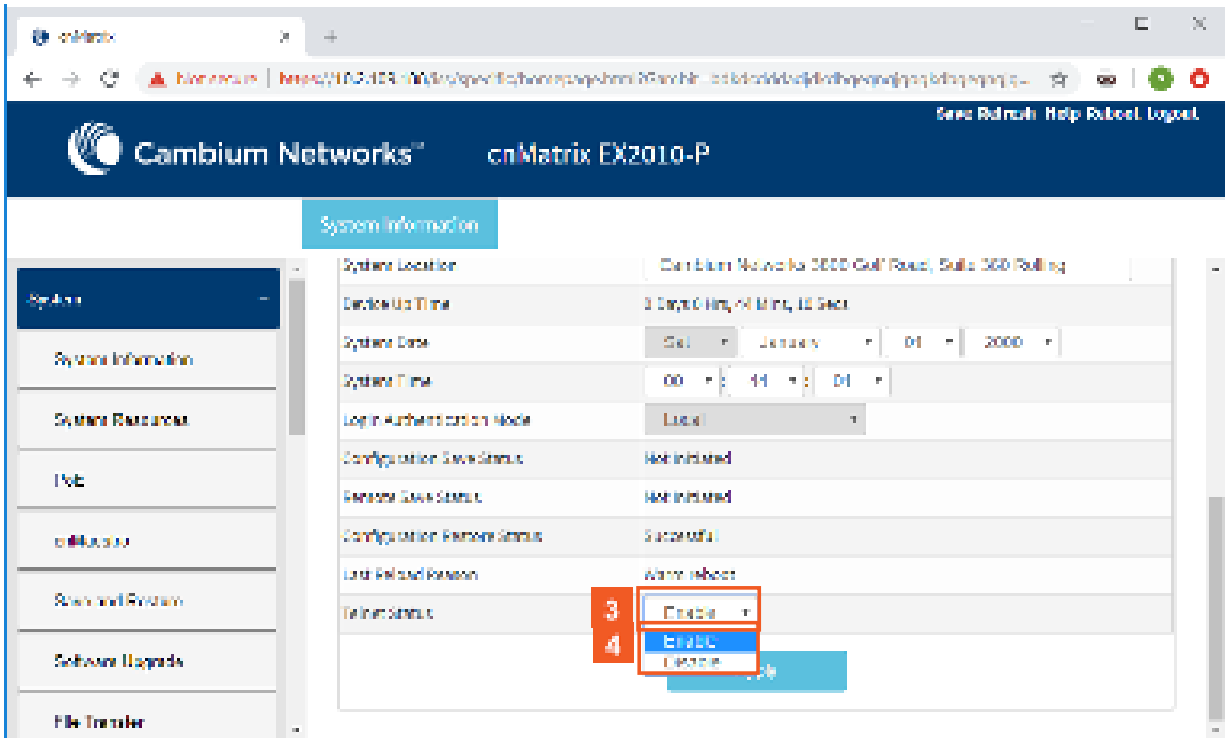
4.5.2 How to Enable/Disable Telnet Server in WEB Interface



1 Click the **System** tab.

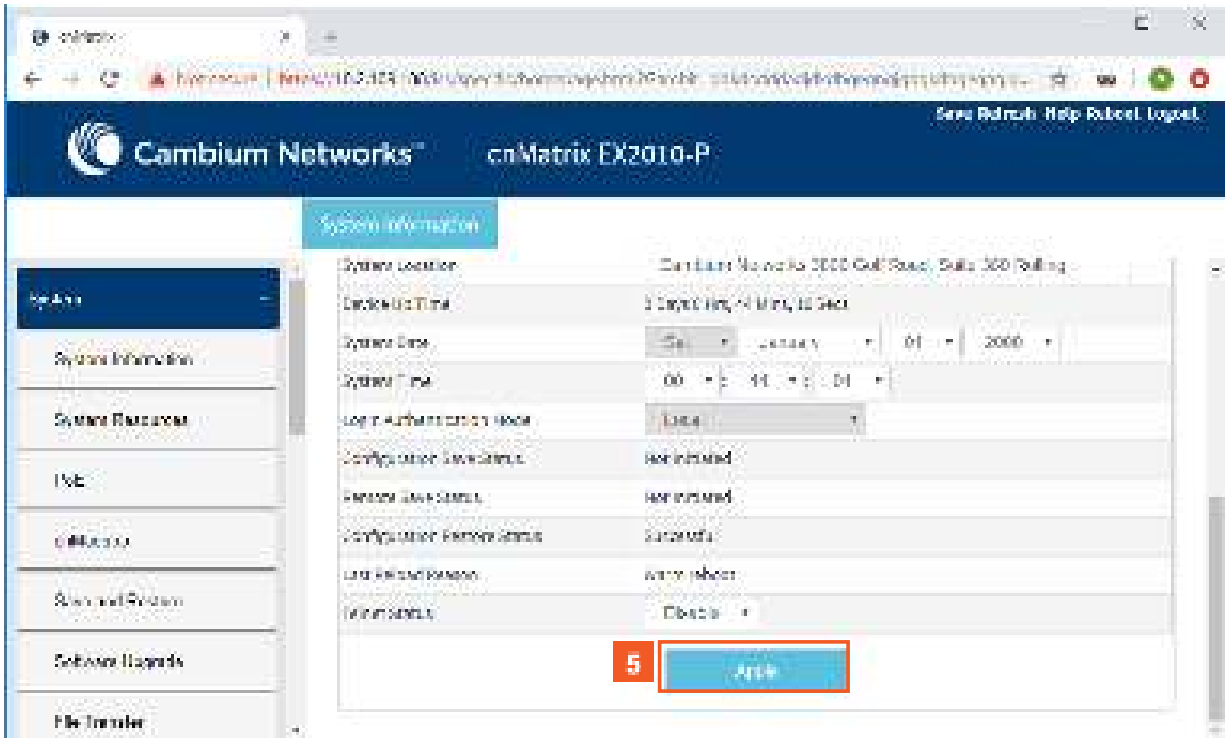


2 Click the **System Information** menu item.



3 Click the **Telnet Status** drop-down list.

4 Select one of the Enable Disable list items (depending if you want to enable or disable the Telnet Server feature).



5 Click the **Apply** button.

4.6 System Resource Monitoring

4.6.1 Managing System Resource Monitoring

Feature Overview

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

Standards

N/A

Scaling Numbers

N/A

Limitations

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

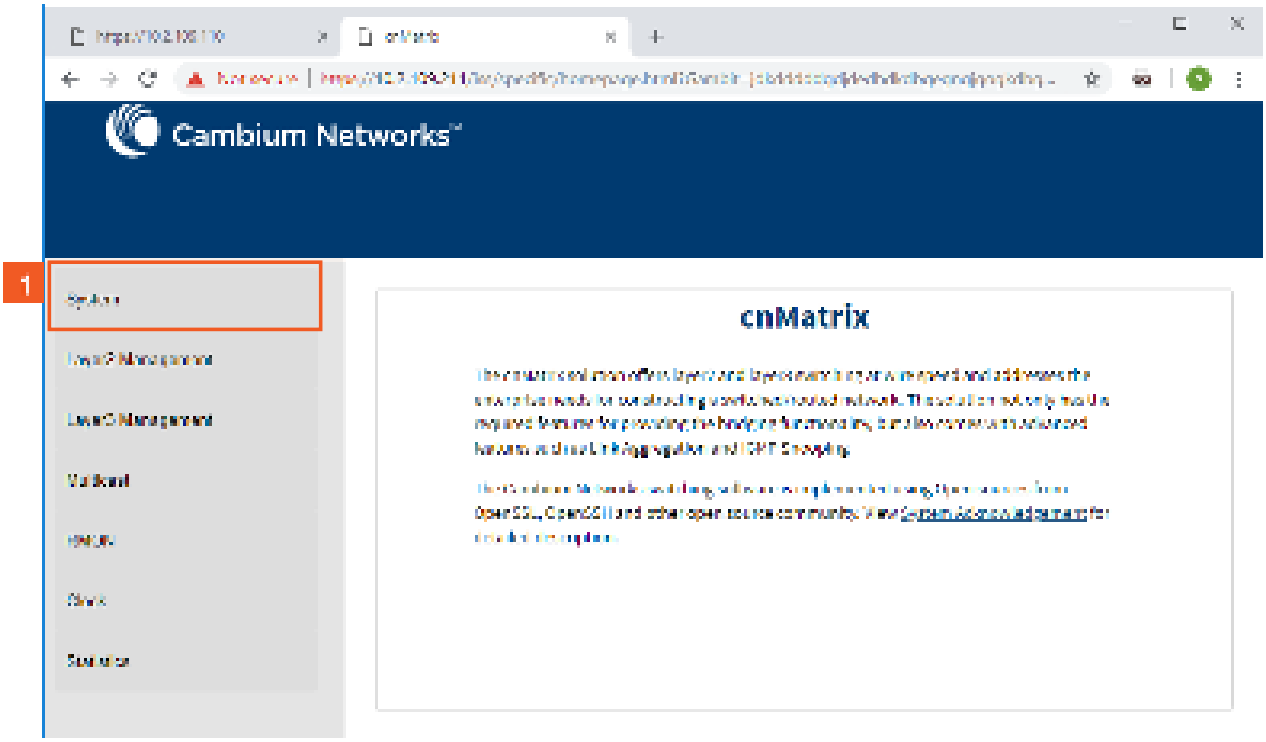
Default Values

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

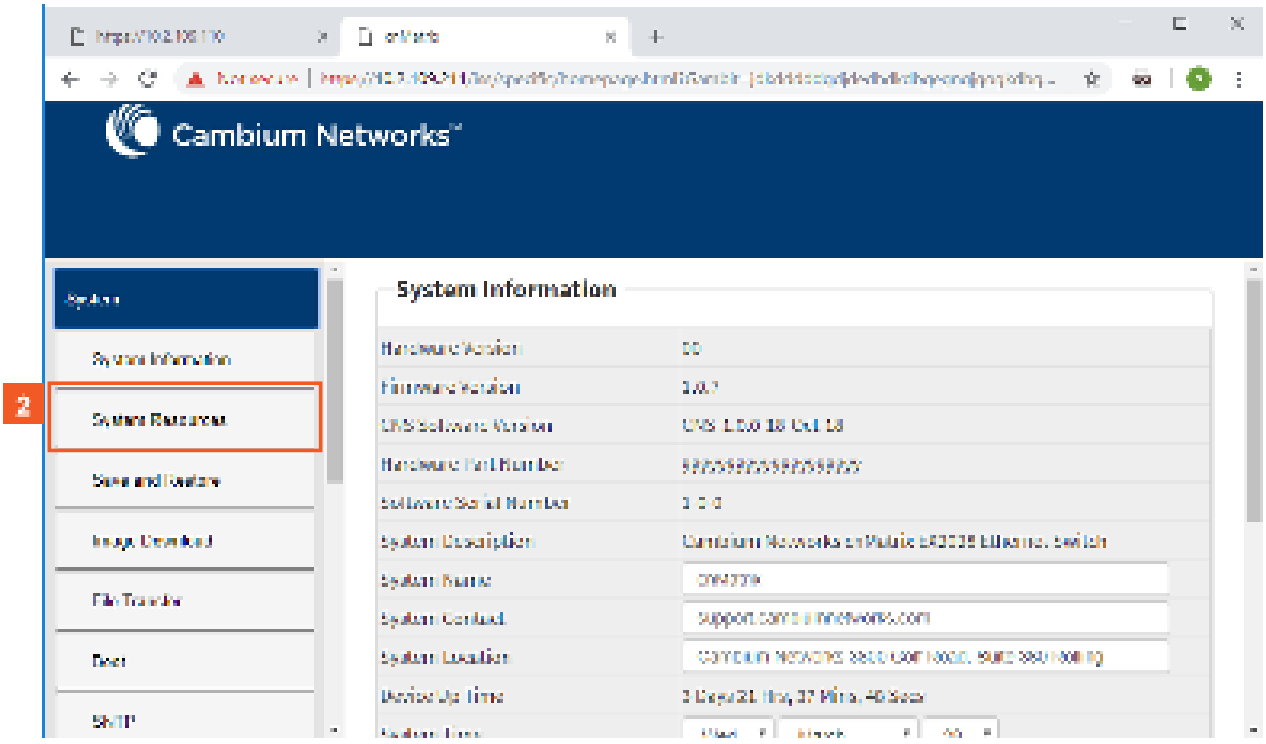
Prerequisites

N/A

4.6.2 How to Enable System Resource Monitoring in WEB Interface



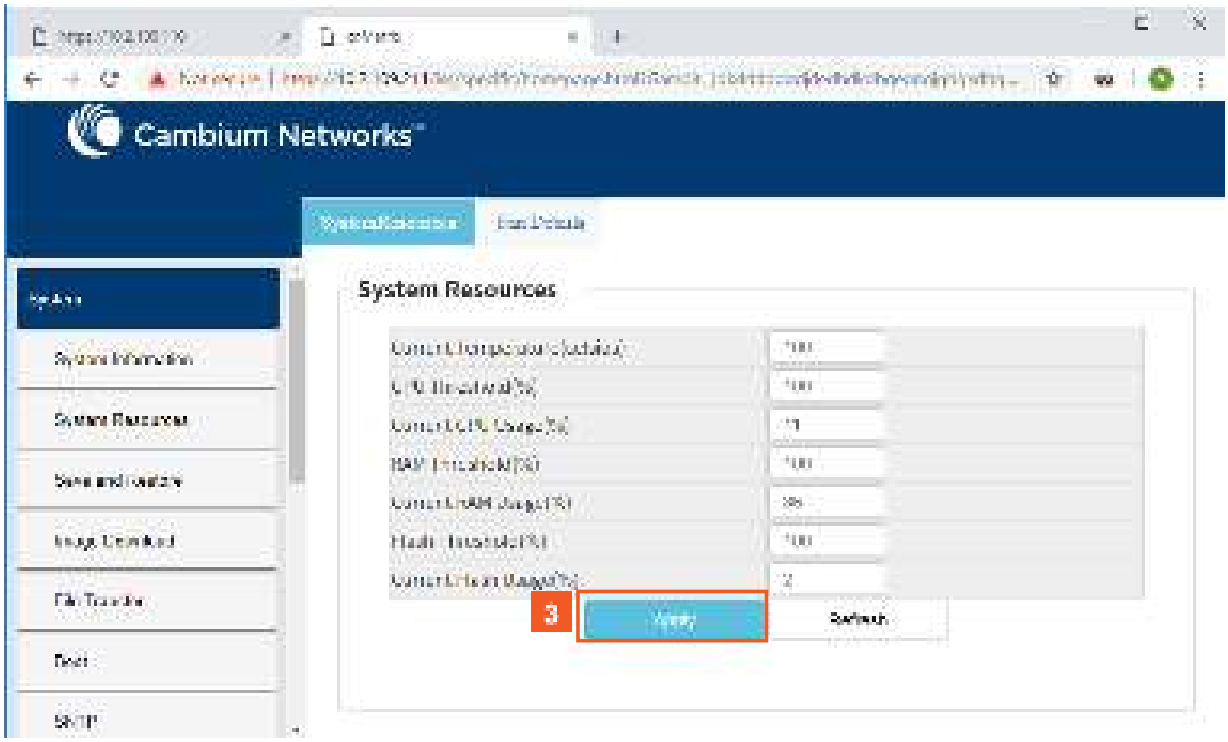
1 Click the **System** tab.



2 Click the **System Resources** menu item.

In the CPU Threshold (%) field, set the desired threshold.

Threshold can be set for CPU, RAM and Flash



3 Click the **Apply** button.

For more information, see System Resources WEB Fields.

4.7 Syslog

4.7.1 Managing Syslog

Feature Overview

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

Standards

- The syslog protocol is described in RFC5424.

Scaling Numbers

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

Limitations

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

Default Values

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

Prerequisites

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

4.7.2 Configuring Syslog in Web Interface

The **Syslog** feature is not available in WEB interface.

4.8 SNMP

4.8.1 Managing SNMP

4.8.1.1 Feature Description

Feature Overview

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

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

Standards

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

Scaling Numbers

- N/A

Limitations

- N/A

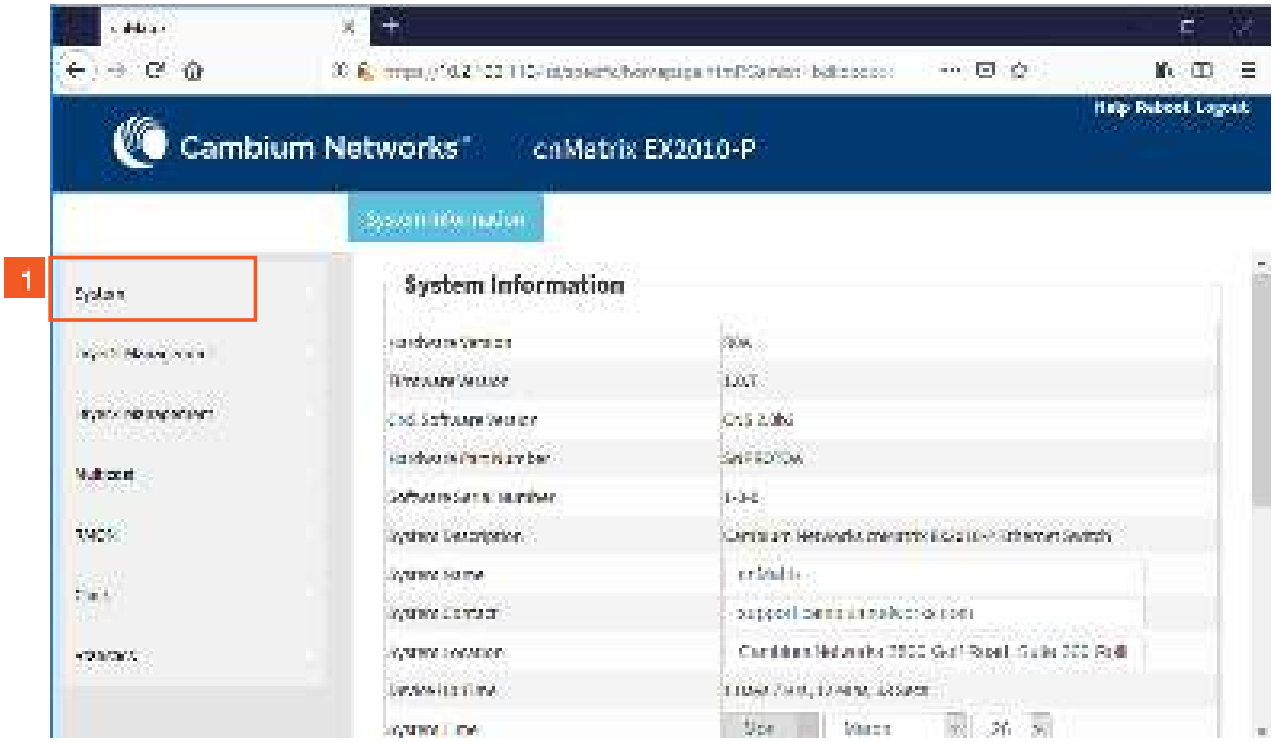
Default Values

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

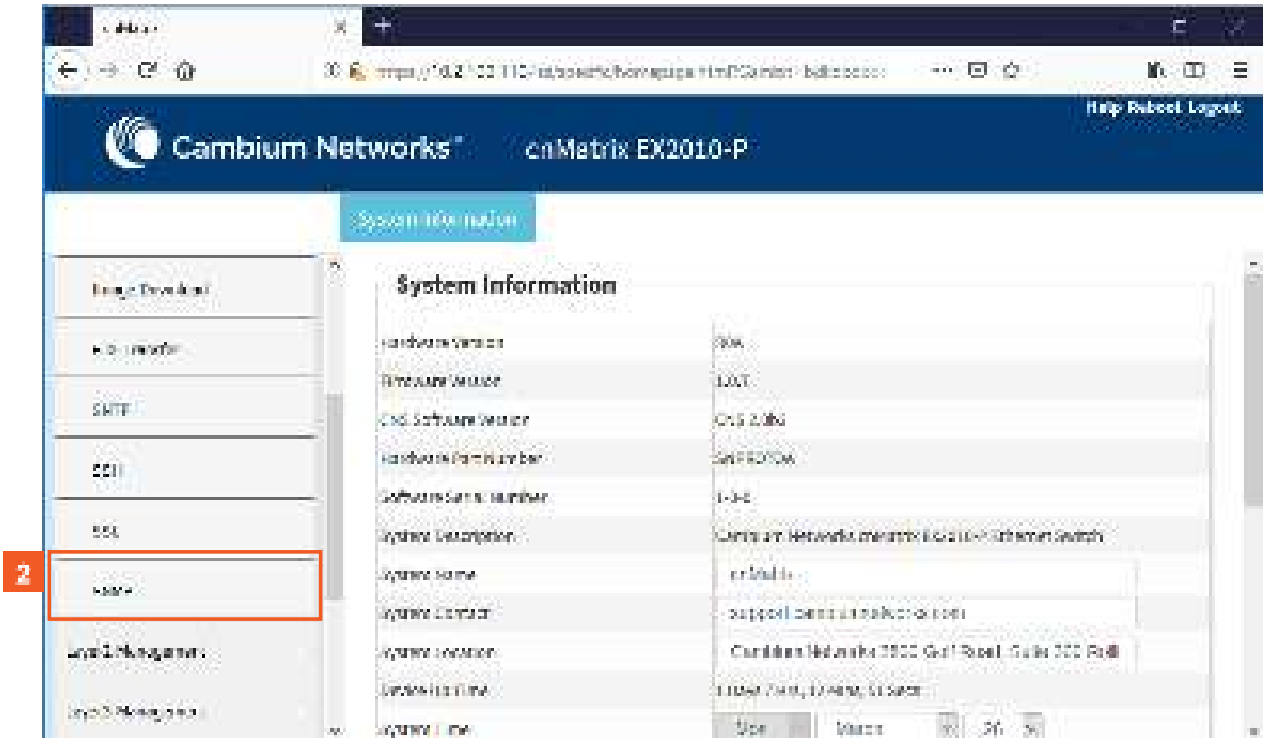
4.8.1.2 Network Diagram

4.8.2 How to Enable and Configure SNMP V2 in WEB Interface

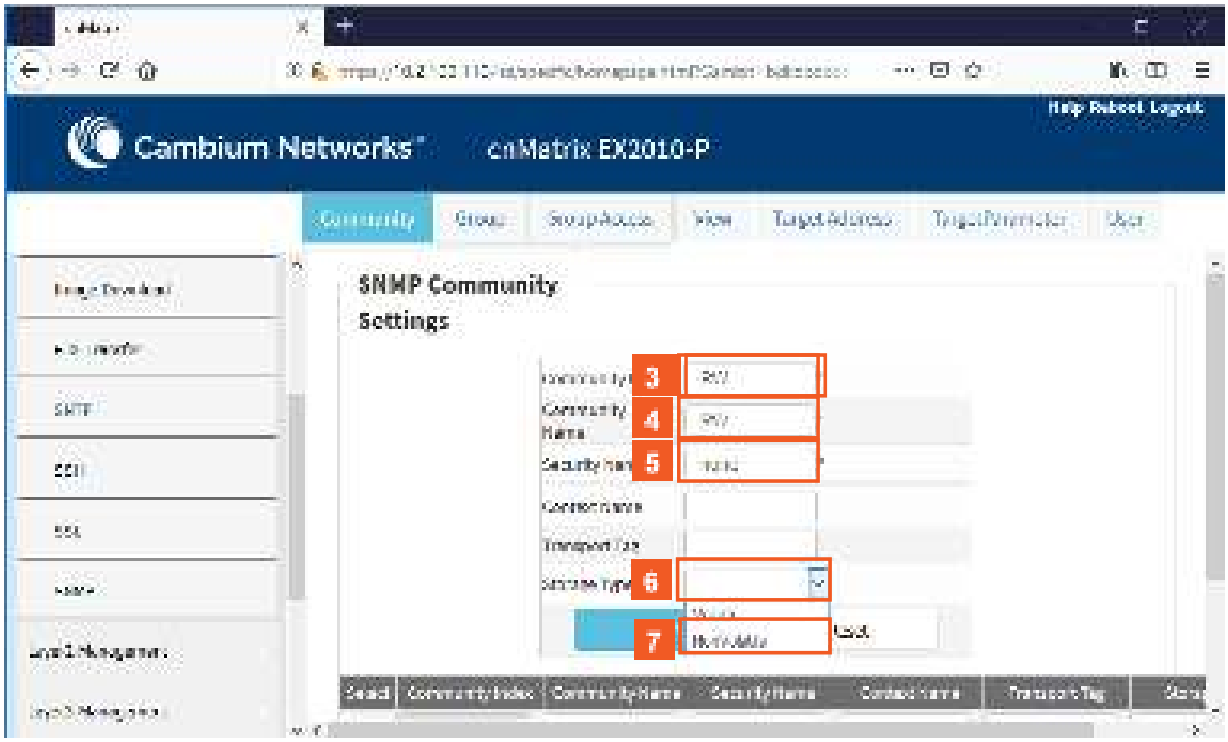
4.8.2.1 Configuring SNMP V2



1 Click the **System** tab.



2 Click the **SNMP** menu item. The **SNMP Community Settings** window is displayed.



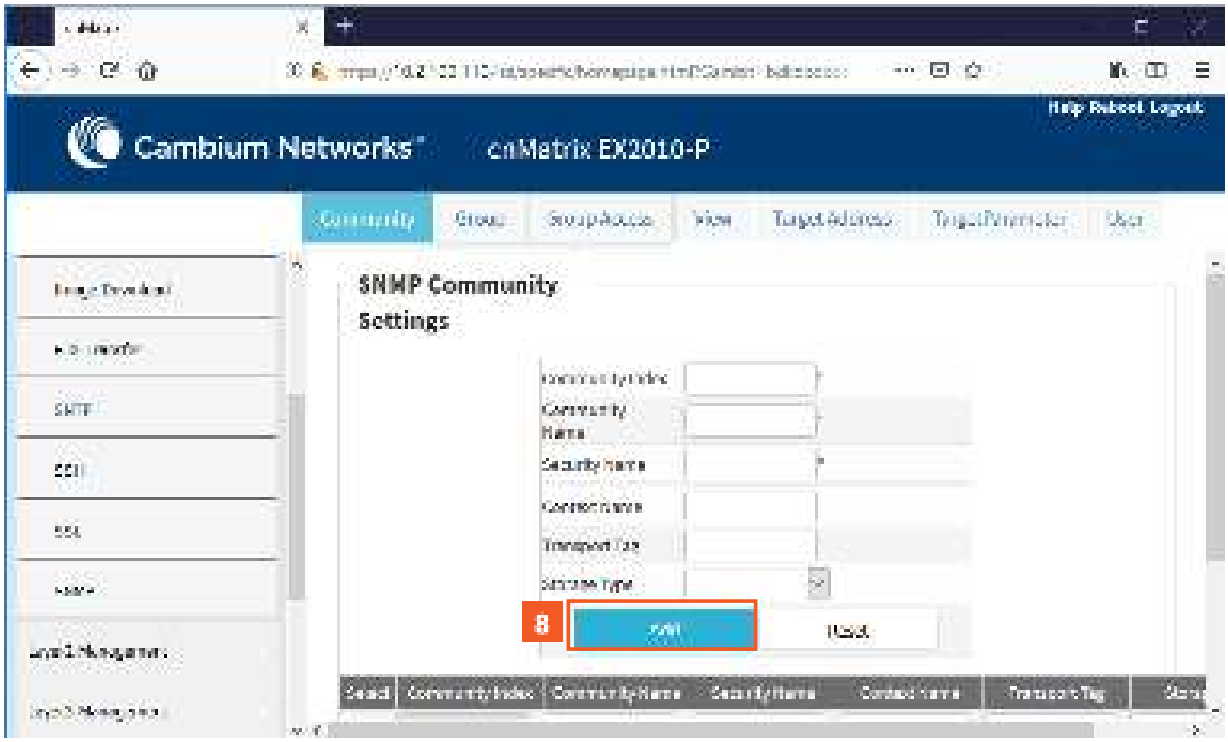
3 Type a community name index. For example, **RW** into the **Community Index** field.

4 Type a community name to reference. For example, **RW** into the **Community Name** field.

5 Type the value **none** into the **Security Name** field.

6 Click the **Storage Type** drop-down list and select the required storage type for the community.

7 Select the **NonVolatile** list item.



8 Click the **Add** button.

Section complete. Click X to close.

4.9 SSH

4.9.1 Managing SSH

4.9.1.1 Feature Description

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

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

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

Standards

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

Scaling Numbers

- The number of simultaneous supported SSH sessions is 8.

Default Values

- The SSH server and SSH client are enabled by default.
- The debugging option is disabled by default.

- The maximum number of bytes allowed in an SSH transport connection is set to 32768 by default.
- The default primary port number: 22.
- The following cipher algorithms are set by default: CHACHA20-POLY1305, 3DES-CBC, AES128-CBC, AES256-CBC, AES128-CTR, AES256-CTR, AES128-GCM, and AES256-GCM
- The default MAC algorithms: HMAC-SHA2-512-ETM, HMAC-SHA2-256-ETM, HMAC-SHA2-512, HMAC-SHA 2-256.

Limitations

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

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

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

The cnMatrix SSH server implementation supports the following:

- Algorithms:
  - Cipher algorithms – CHACHA20-POLY1305, 3DES-CBC, AES128-CBC, AES256-CBC, AES128-CTR, AES256-CTR, AES128-GCM, and AES256-GCM.
  - MAC algorithms - HMAC-SHA2-512-ETM, HMAC-SHA2-256-ETM, HMAC-SHA2-512, HMAC-SHA 2-256.
  - Version compatibility flag (SSH 1.0 support) – a user can use this to change the protocol version support to SSH 1.0 or SSH 2.0.
  - The key exchange algorithms supported are Diffie-hellman-group1sha1 and Diffie-hellman-group14-sha1. The SSH server uses the key generated during the key exchange for data encryption and providing data integrity.

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

- Authentication using username and password.

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

The SSH server implementation does not support the following:

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

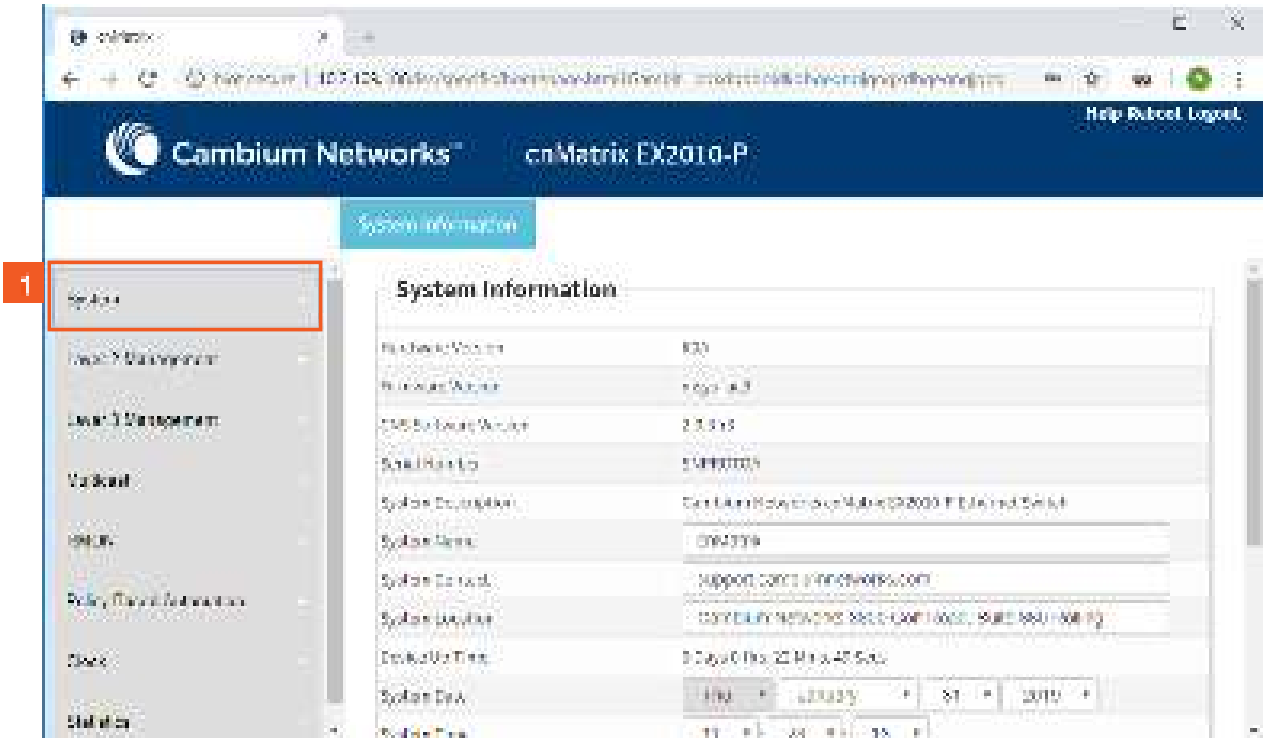
The SSH Client functionality is implemented in cnMatrix by integrating PuTTY (version 0.60) open source code. The SSH client session to any reachable host can be established from cnMatrix through CLI. SSH client feature can be enabled or disabled through SNMP and CLI. SSH client supports both Ipv4 and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

Options supported in SSH client :

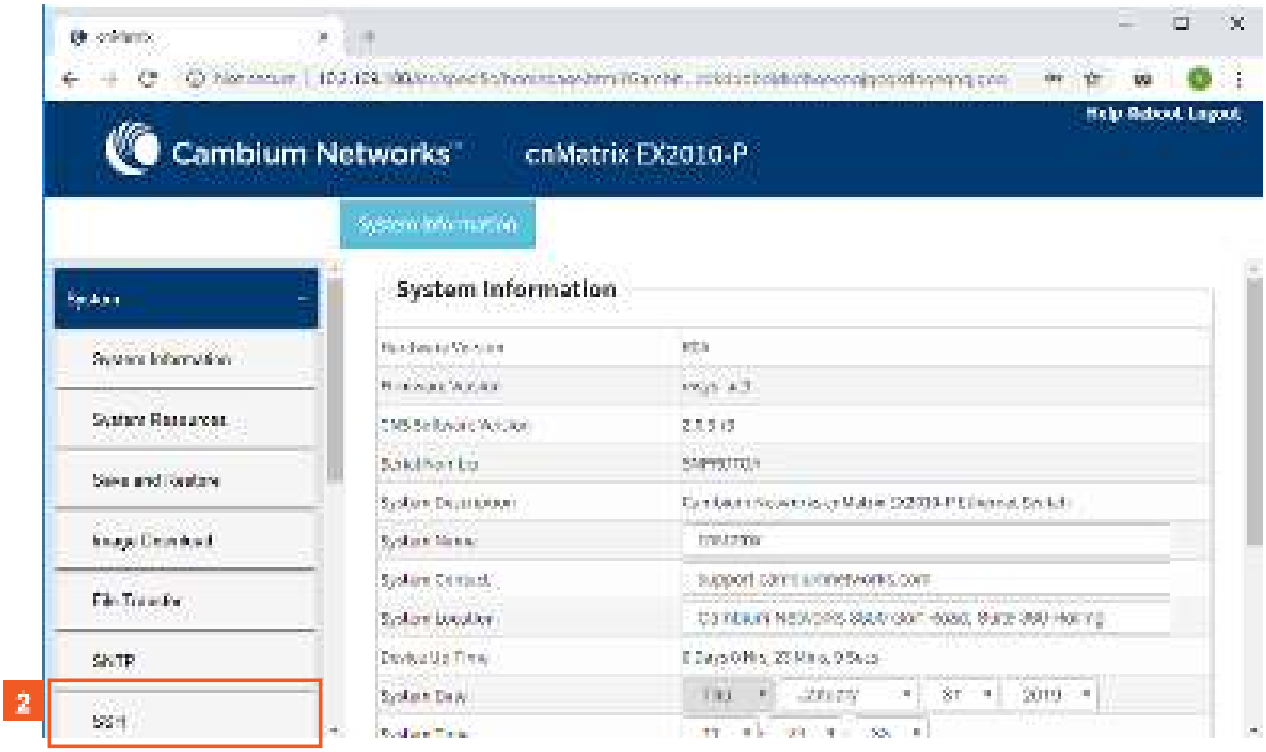
- - 1 - Forces SSH to try protocol version 1 only.
- - 2 - Forces SSH to try protocol version 2 only.
- - 4 - Forces SSH to use Ipv4 addresses only.
- - 6 - Forces SSH to use Ipv6 addresses only.
- - A - Enables forwarding of the authentication agent connection.
- - a - Disables forwarding of the authentication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

4.9.1.2 Network Diagram

4.9.2 How to Enable SSH in WEB Interface

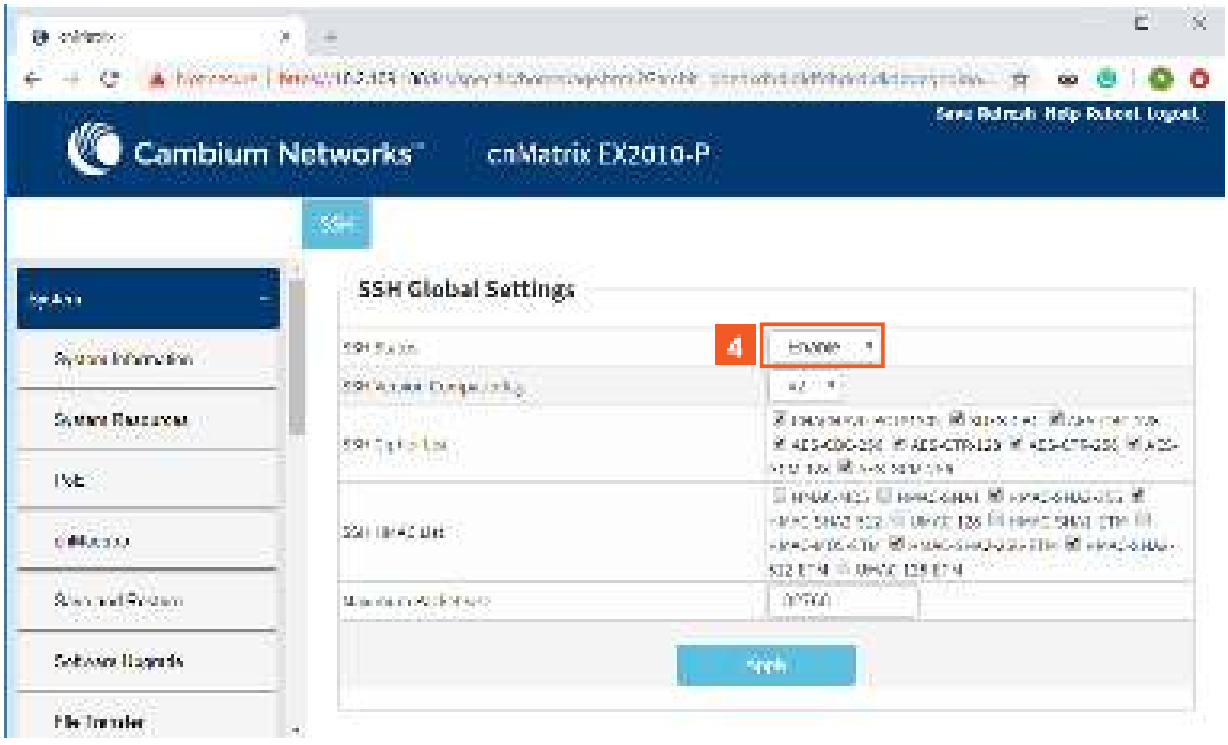


1 Click the **System** tab.



2 Click the **SSH** menu item.

3 Click the **SSH Status** drop-down list to select the status of the SSH module.



4 Select the **Enable** list item.

5 Click the **Apply** button.

4.10IPv6 Management

4.10.1Managing IPv6 Management

Feature Overview

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

Standards

- RFC2460

Scaling Numbers

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

Limitations

- IPv6 is not supported on routed interfaces.

Default Values

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

Prerequisites

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

```
no ipv6 unicast-routing
```

The IPv6 addresses are not case-sensitive.

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

4.10.2Configuring IPv6 Management in WEB Interface

The **IPv6 Management** feature is not available in WEB Interface.

4.11Reload (Starting with version 2.1)

4.11.1Managing Reload

Feature Overview

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

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

There are two ways of scheduling a reload system:

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

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

Limitations

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

Default Values

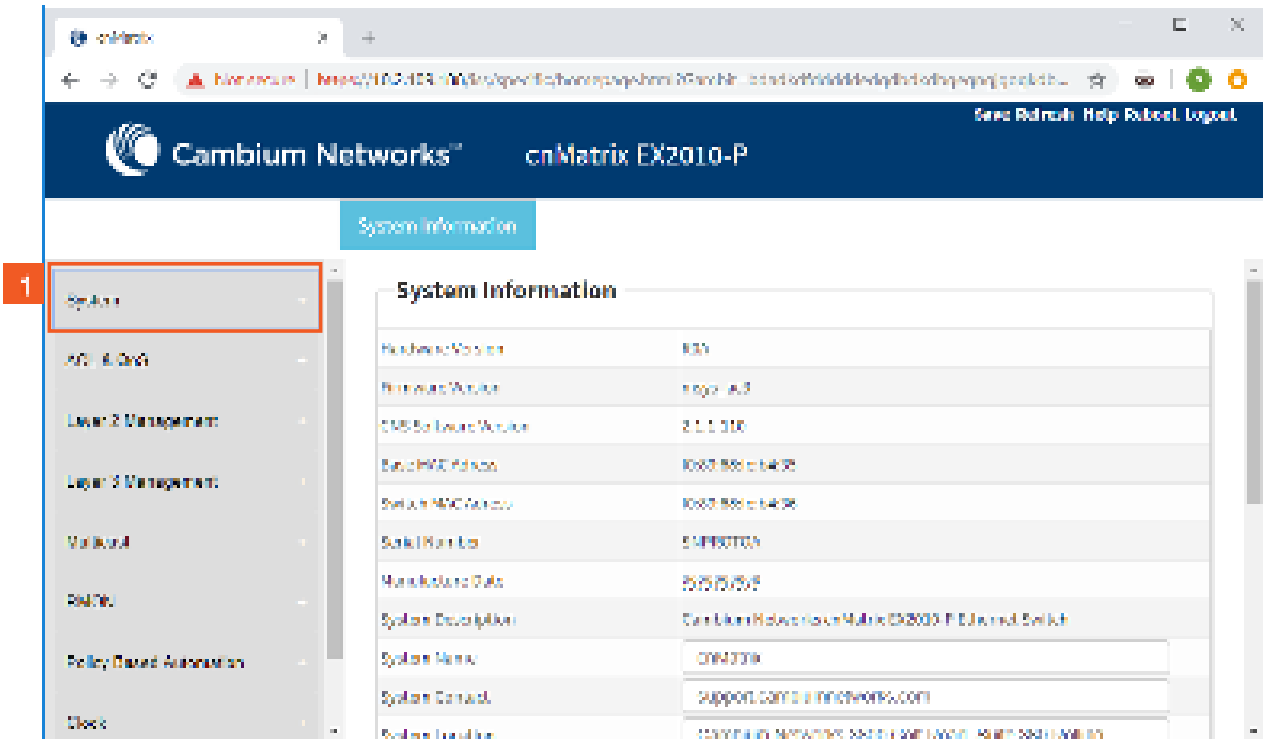
- No reload is scheduled by default.

Prerequisites

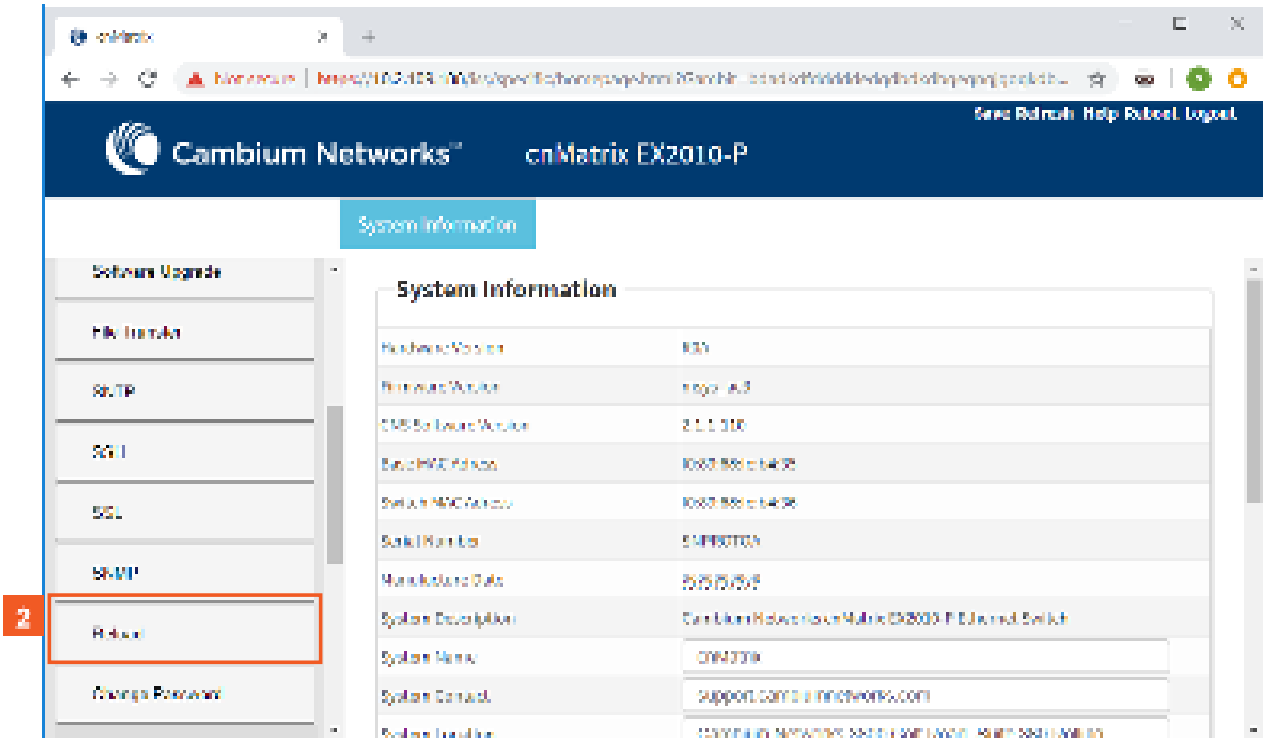
- N/A

4.11.2 How to Schedule Reload on your cnMatrix Switch in WEB Interface

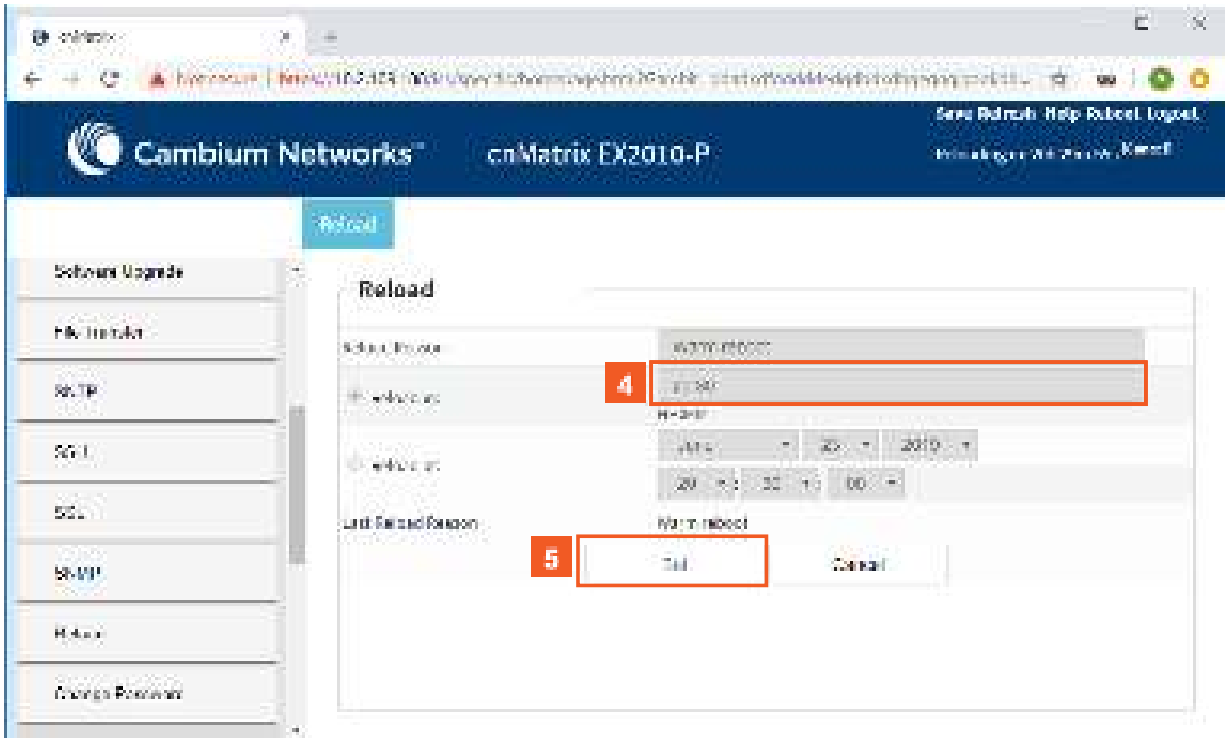
4.11.2.1 Schedule Reload in a Specific Amount of Time



1 Click the **System** tab.



2 Click the **Reload** menu item. The **Reload** window is displayed.

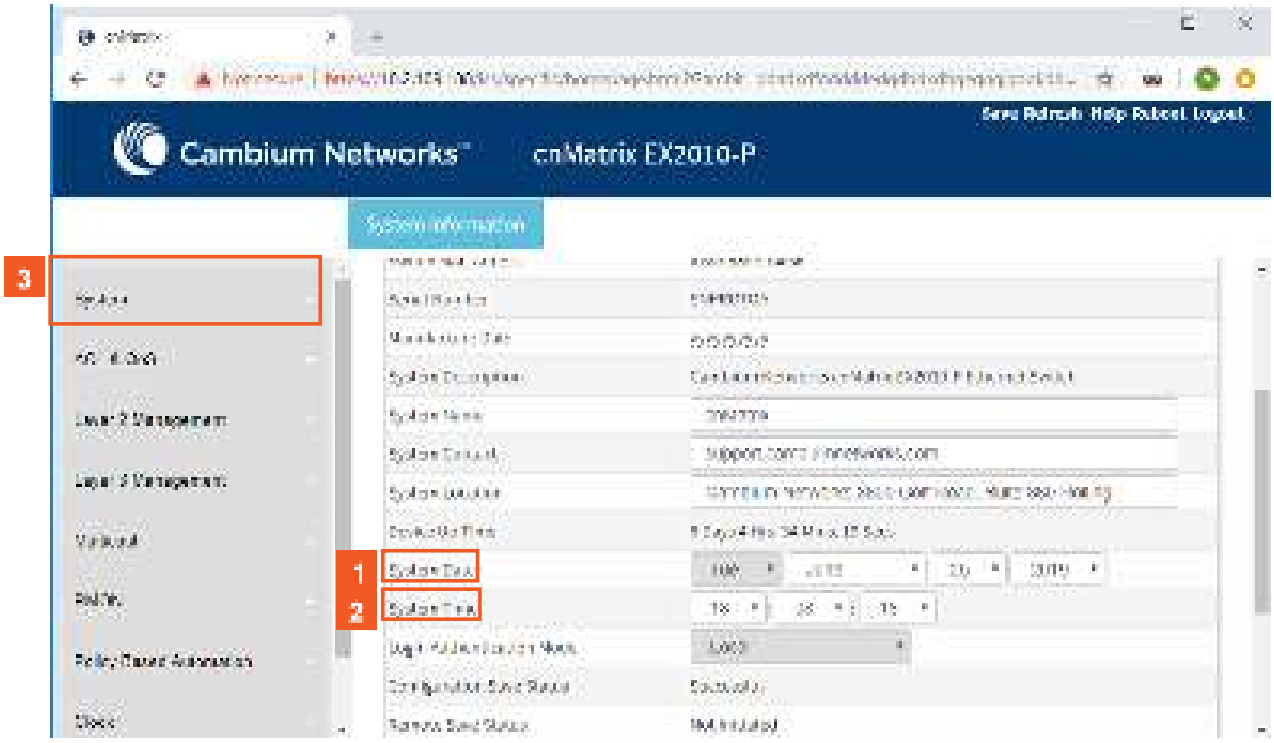


3 Delete the default value of the **Reload in** field and enter the specific amount of time when you want your cnMatrix switch to reboot itself.

4 Type the value **20:30** into the **Reload in** field.

5 Click the **Set** button to schedule reload in 20 hours and 30 minutes.

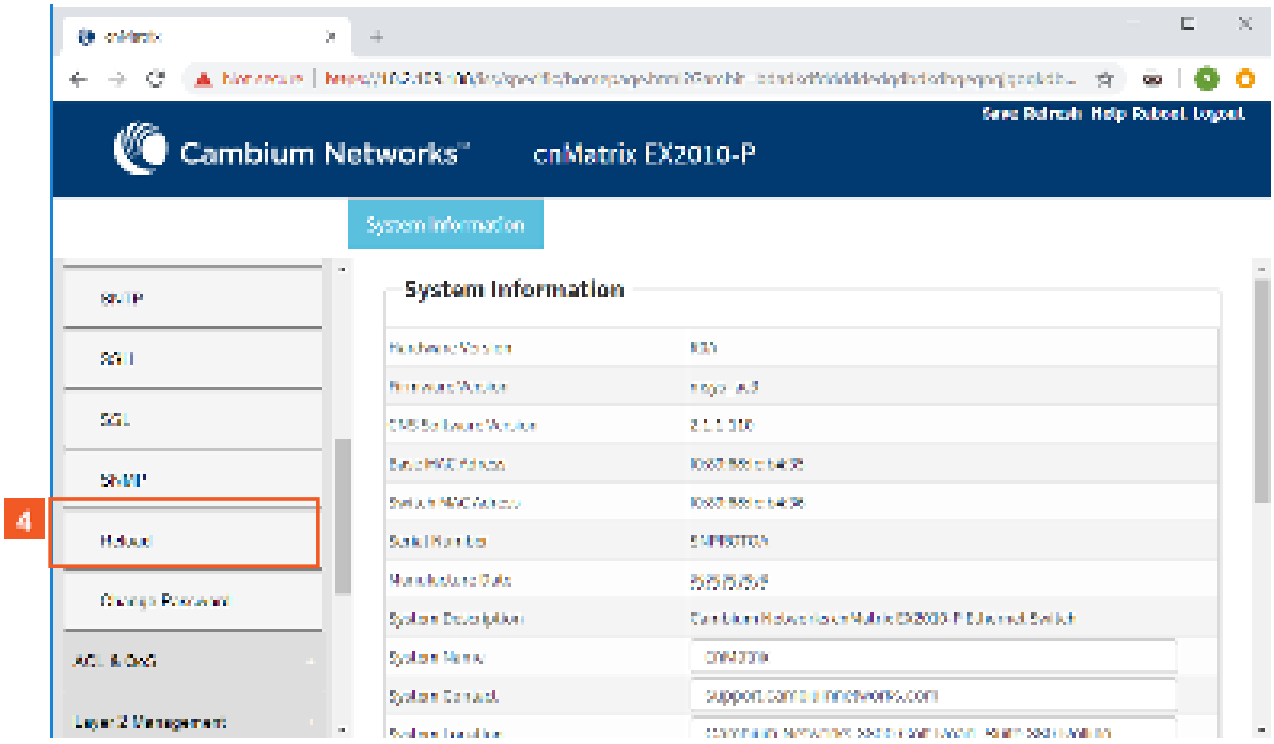
4.11.2.2 Schedule Reload at a Specific Time and Date in the Future



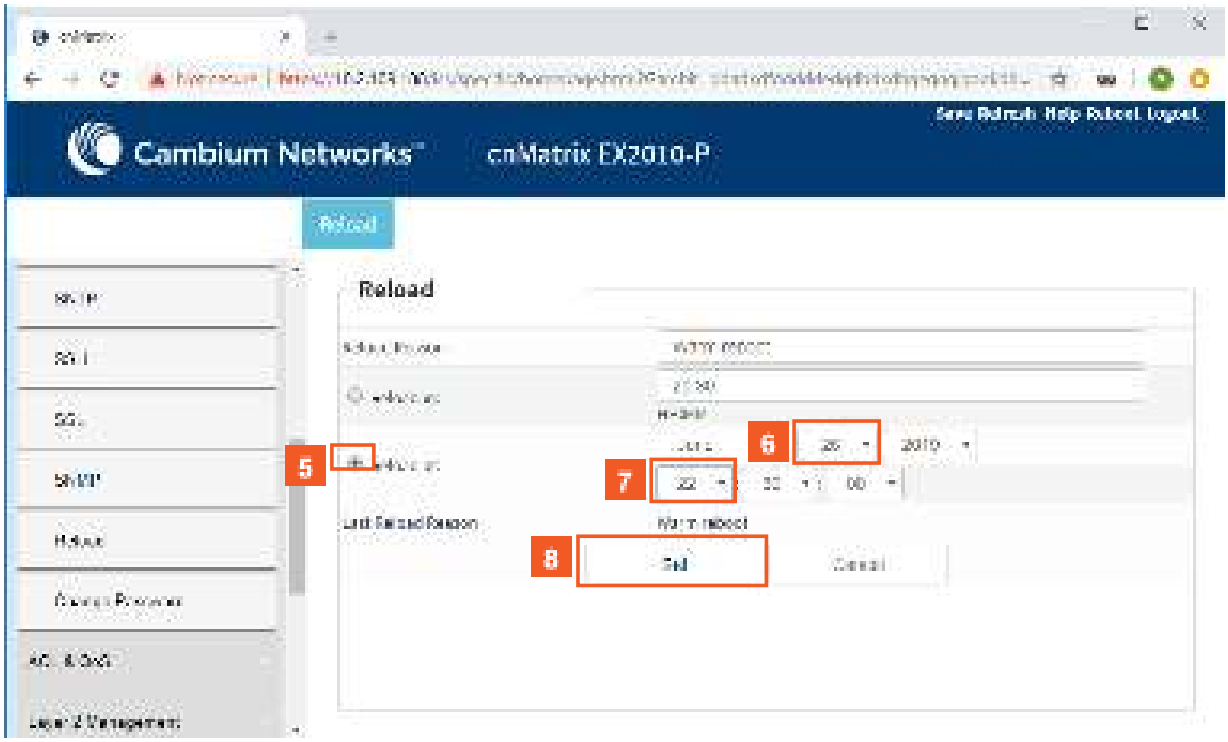
1 Verify if the **System Date** field displays the current day.

2 Verify if the **System Time** field displays the current time.

3 Click the **System** menu item.



4 Click the **Reload** menu item. The **Reload** window is displayed.



5 Check the **Reload at** radio button.

6 Select a date (present or in the future).

7 Select a specific time, to schedule a reload at a certain time in the future.

8 Click the **Set** button to schedule the reload.

4.12 USB (Starting with version 2.1)

4.12.1 Managing USB

Feature Overview

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

The USB has the following capabilities:

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

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

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

Manually mounting the device is not mandatory.

Limitations

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

Default Values

- No USB device is present by default.

5 Security Features

5.1 RADIUS

5.1.1 Managing RADIUS

5.1.1.1 Feature Description

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

The **cnMatrix Radius (IPv4/IPv6) client** is a security feature that offers the ability for cnMatrix to communicate with a Radius central server with the purpose of **authenticating** users and **authorizing** their access to the system or a specific service. cnMatrix Radius (IPv4/IPv6) client is used with the login and PNAC features.

Standards

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

Scaling Numbers

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

Limitations

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

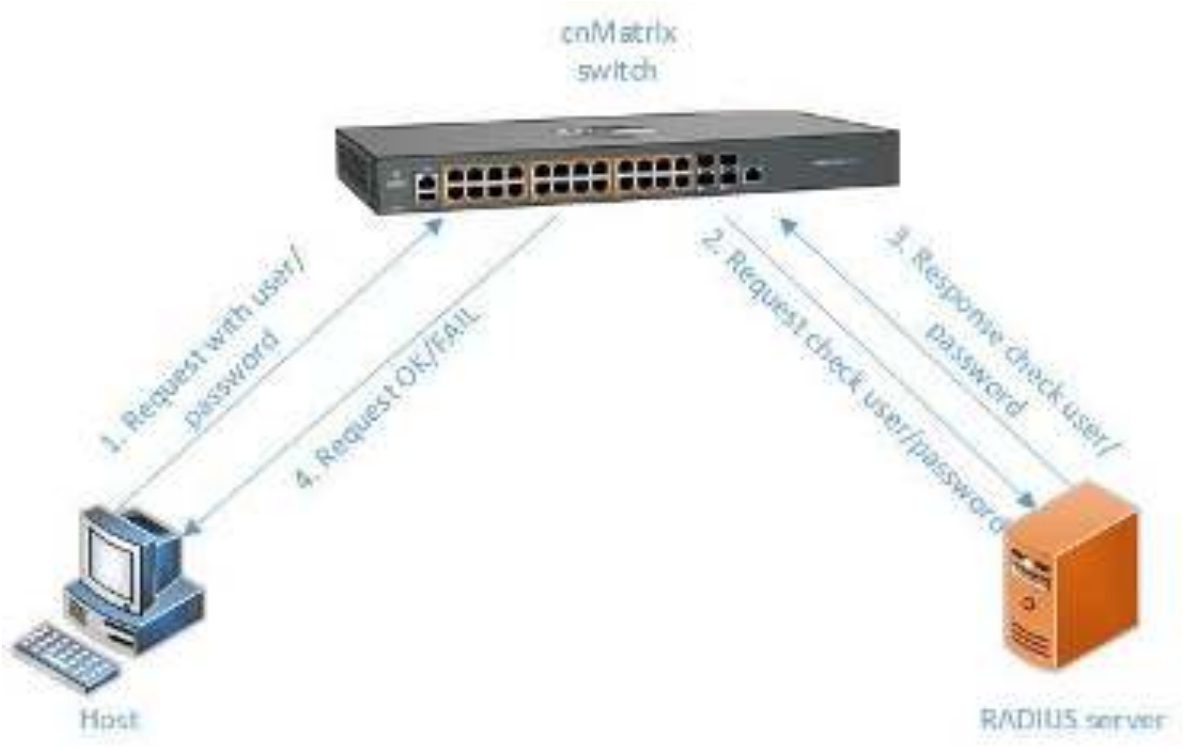
Default Values

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

Prerequisites

N/A

5.1.1.2 Network Diagram



5.1.2 Configuring RADIUS in WEB Interface

The **RADIUS** feature is not available in WEB interface.

5.2 TACACS

5.2.1 Managing TACACS

5.2.1.1 Feature Description

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

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

Standards

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

Scaling Numbers

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

Limitations

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

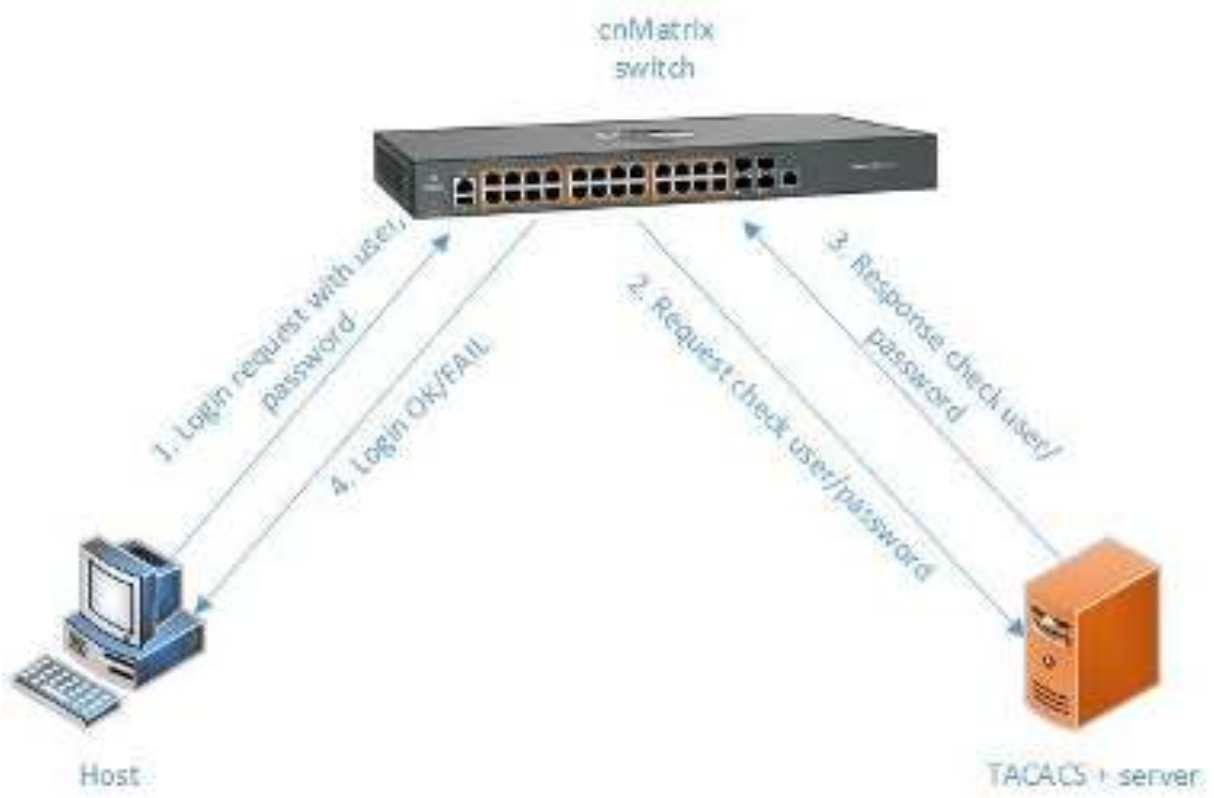
Default Values

- 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

5.2.1.2 Network Diagram



5.2.2 Configuring TACACS in WEB Interface

The **TACACS** feature is not available in WEB interface.

5.3 IGMP Snooping

5.3.1 Managing IGMP Snooping

5.3.1.1 Feature Description

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

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

Standards

- N/A

Scaling Numbers

- N/A

Limitations

- A maximum of 256 IGMP groups are supported.

Default Values

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

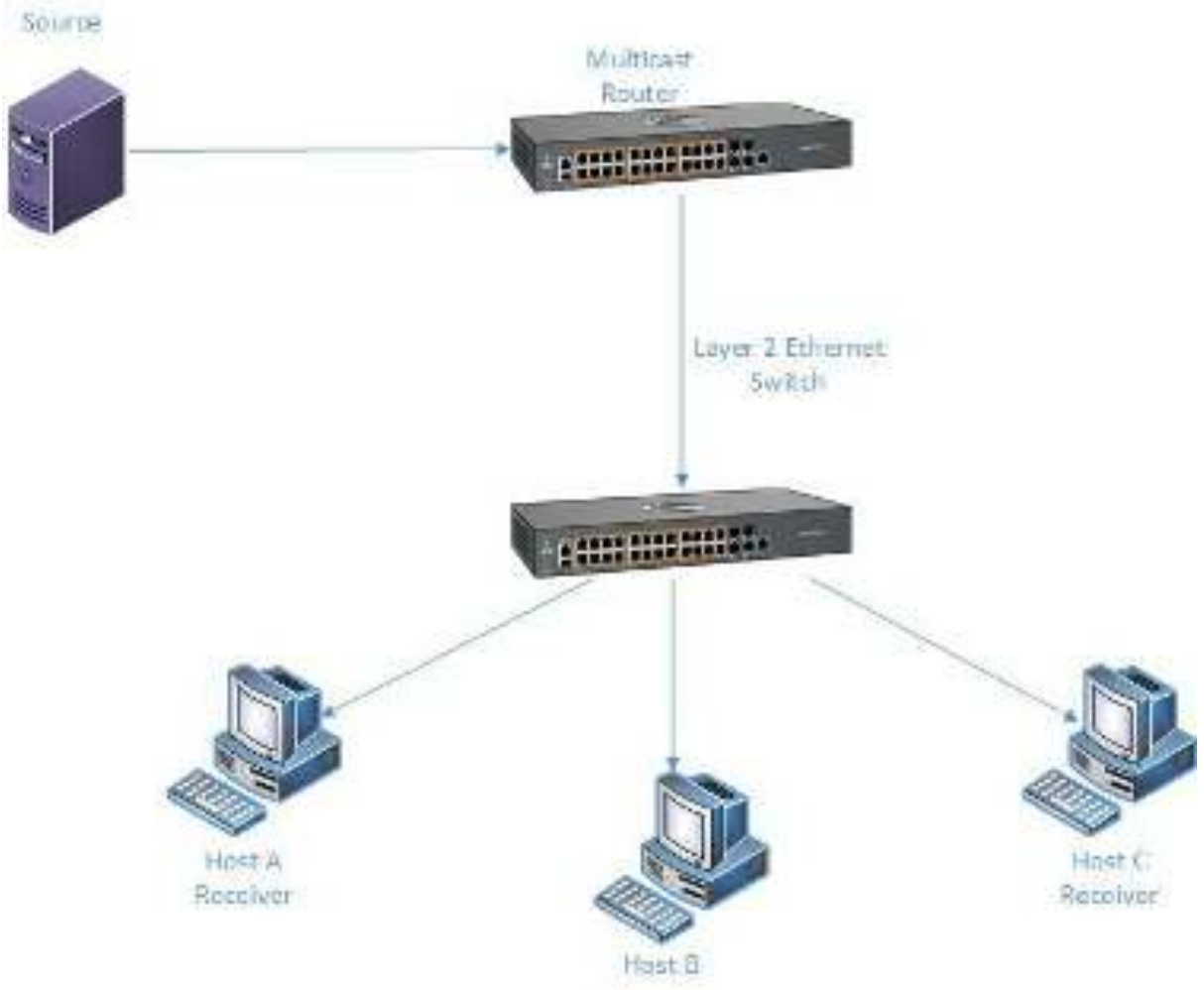
Prerequisites

- N/A

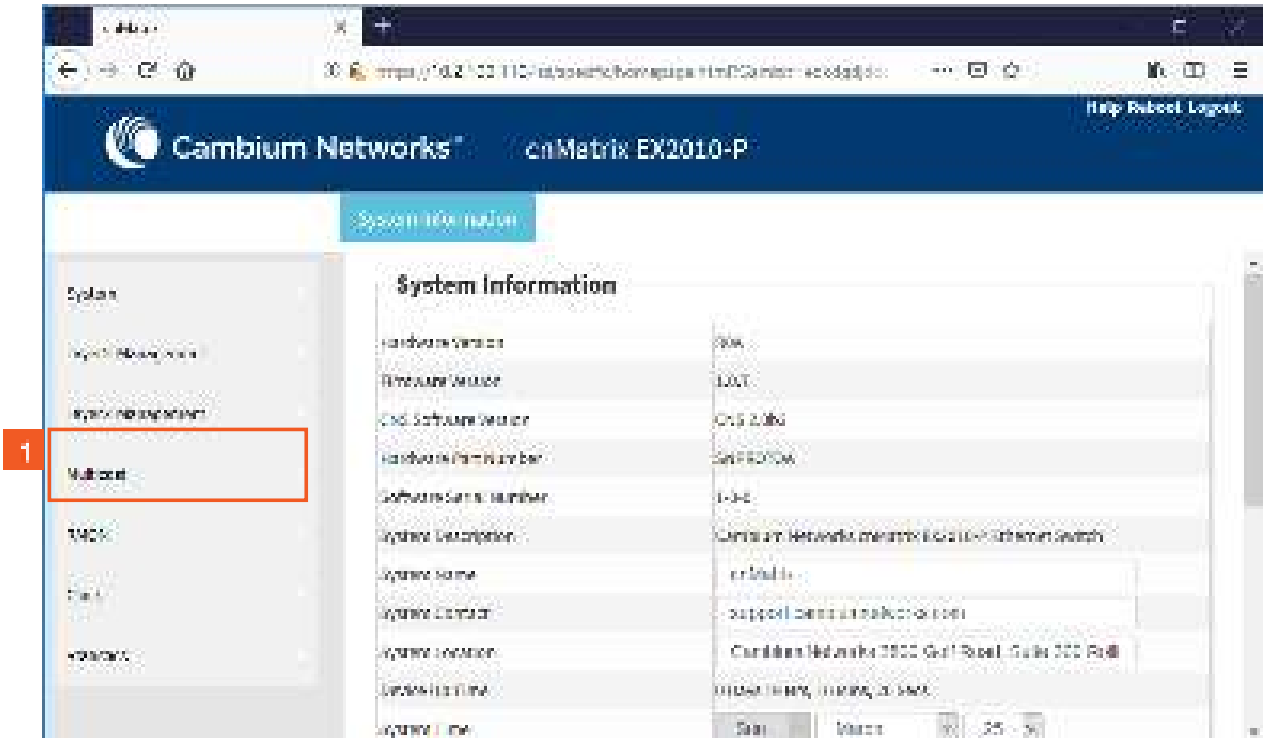
SNMP

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

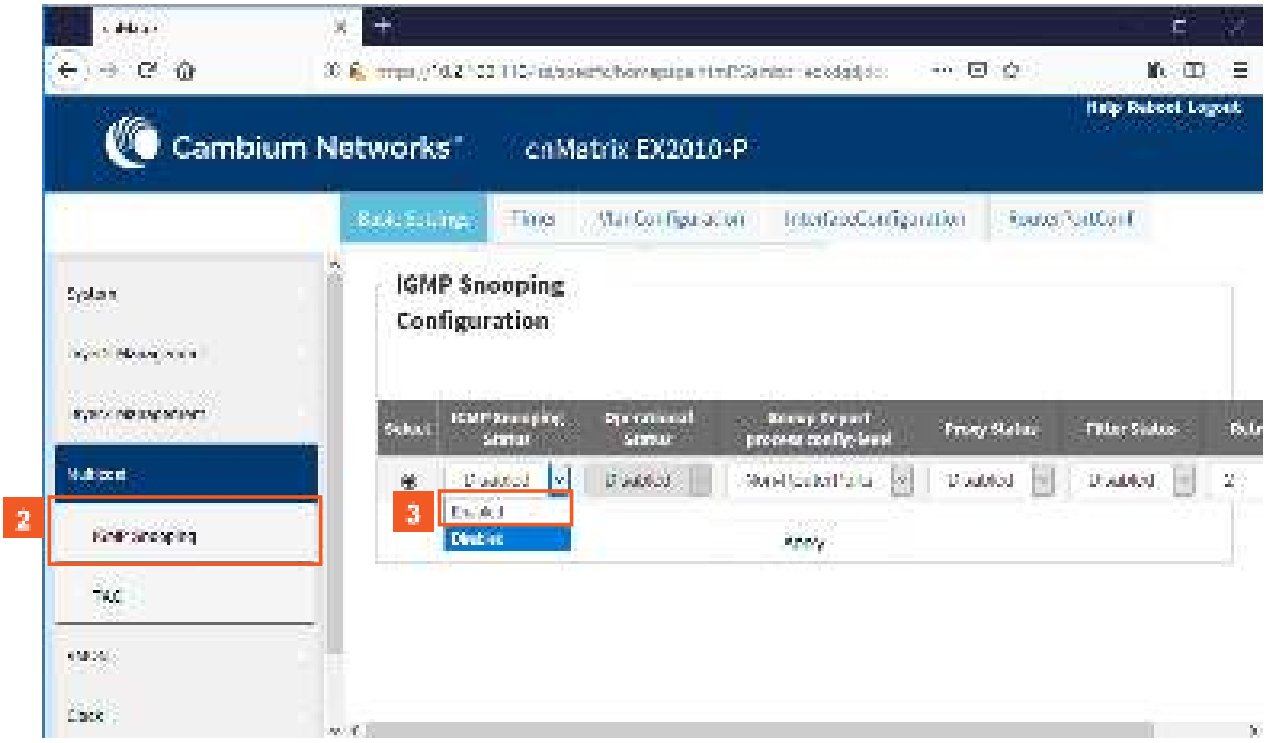
5.3.1.2 Network Diagram



5.3.2 How to Enable IGMP Snooping in WEB Interface

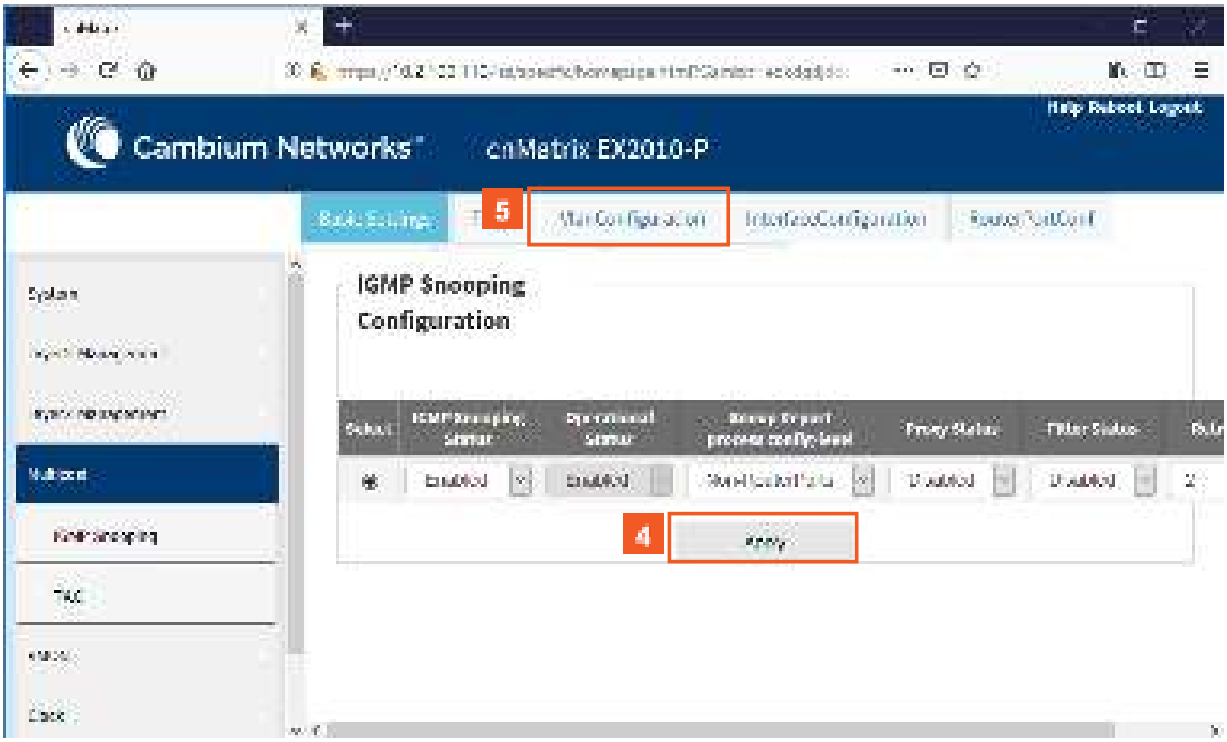


1 Click the **Multicast** tab.



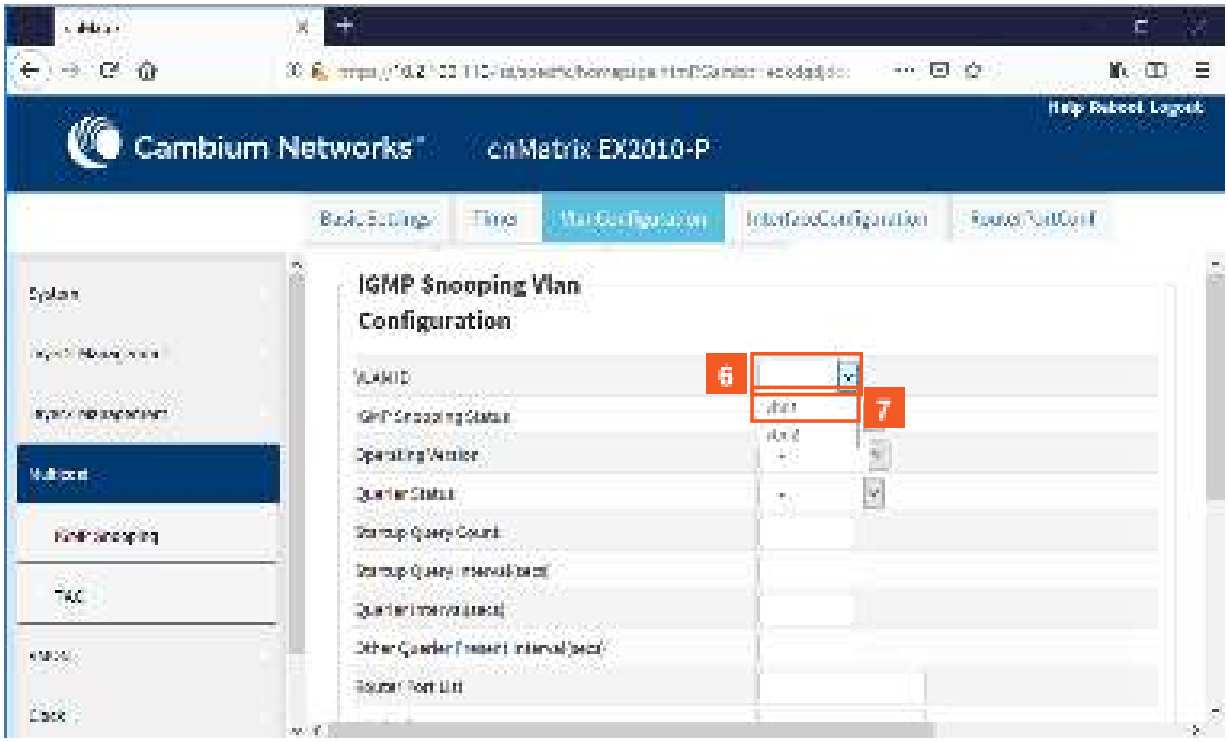
2 Click the **IGMP Snooping** menu item.

3 Click the **IGMP Snooping Status** drop-down list to select the global status of the IGMP Snooping feature in the switch. Select the **Enabled** list item to enable the IGMP SNooping feature.



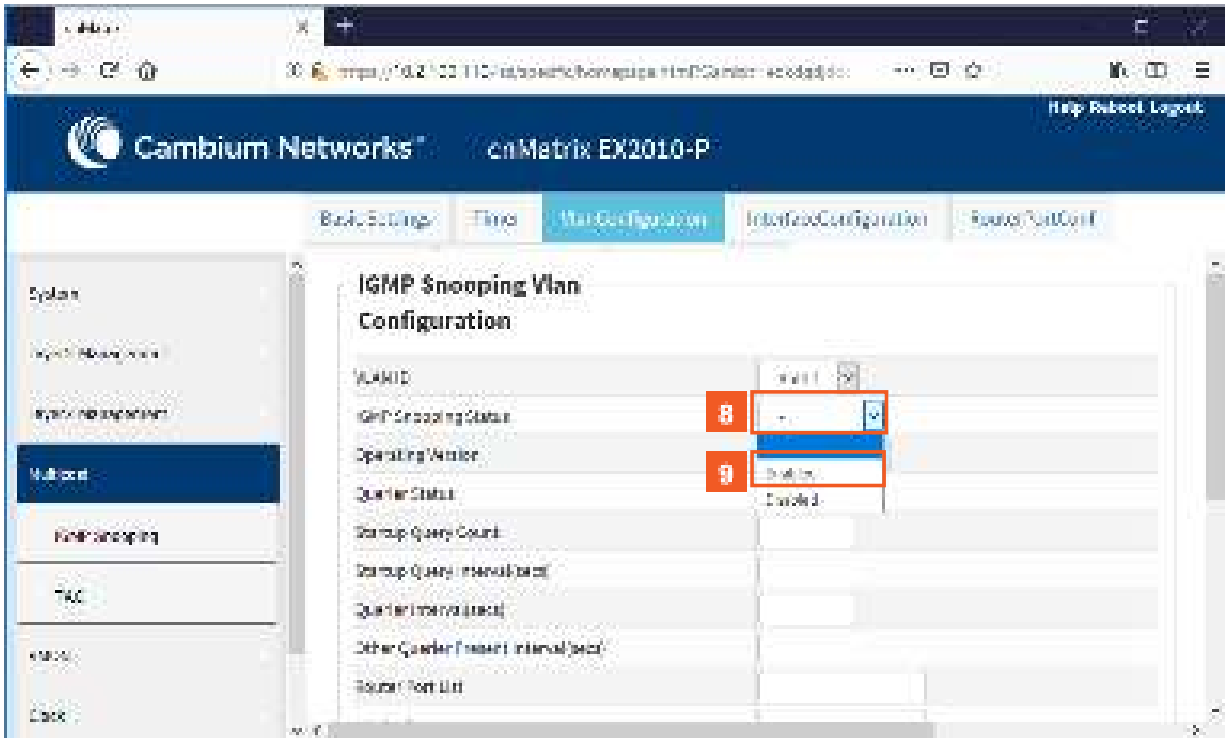
4 Click the **Apply** button.

5 Click the **VlanConfiguration** tab. The **IGMP Snooping VLAN Configuration** window is displayed.



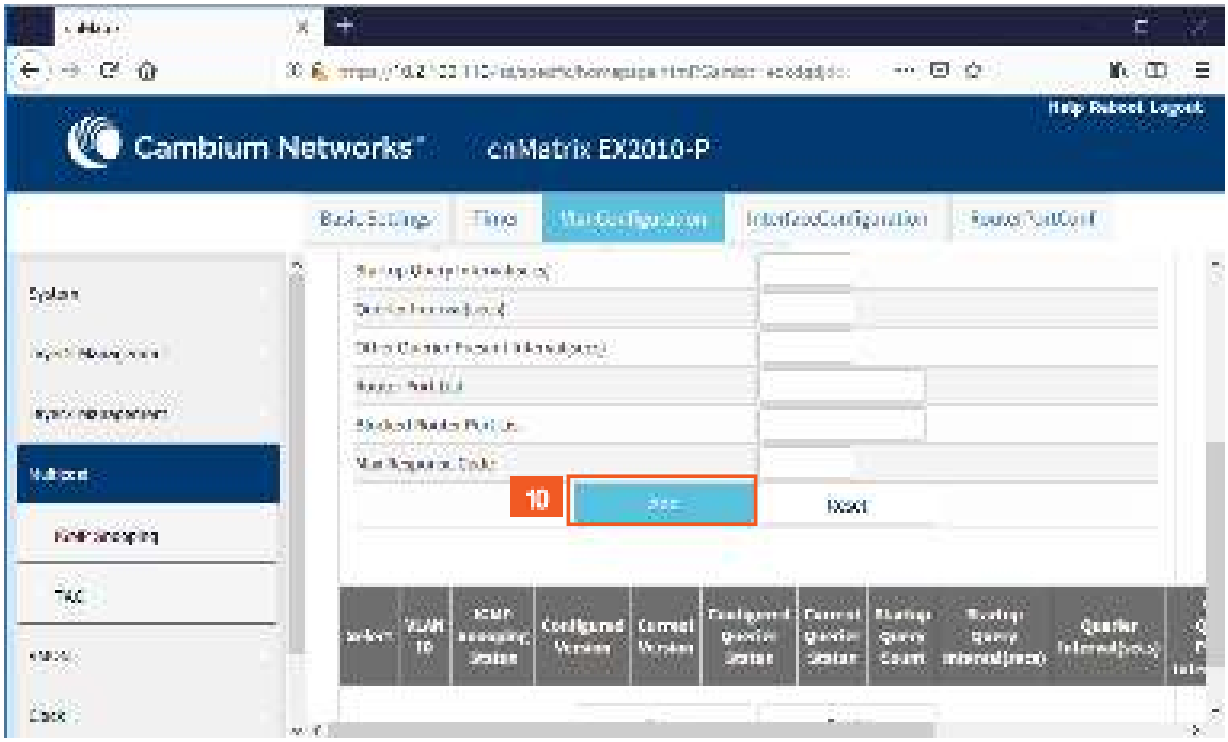
6 Click the **VLAN ID** drop-down list and select the VLAN identifier that uniquely identifies a specific VLAN from the available list.

7 For example, select the **vlan1** list item.

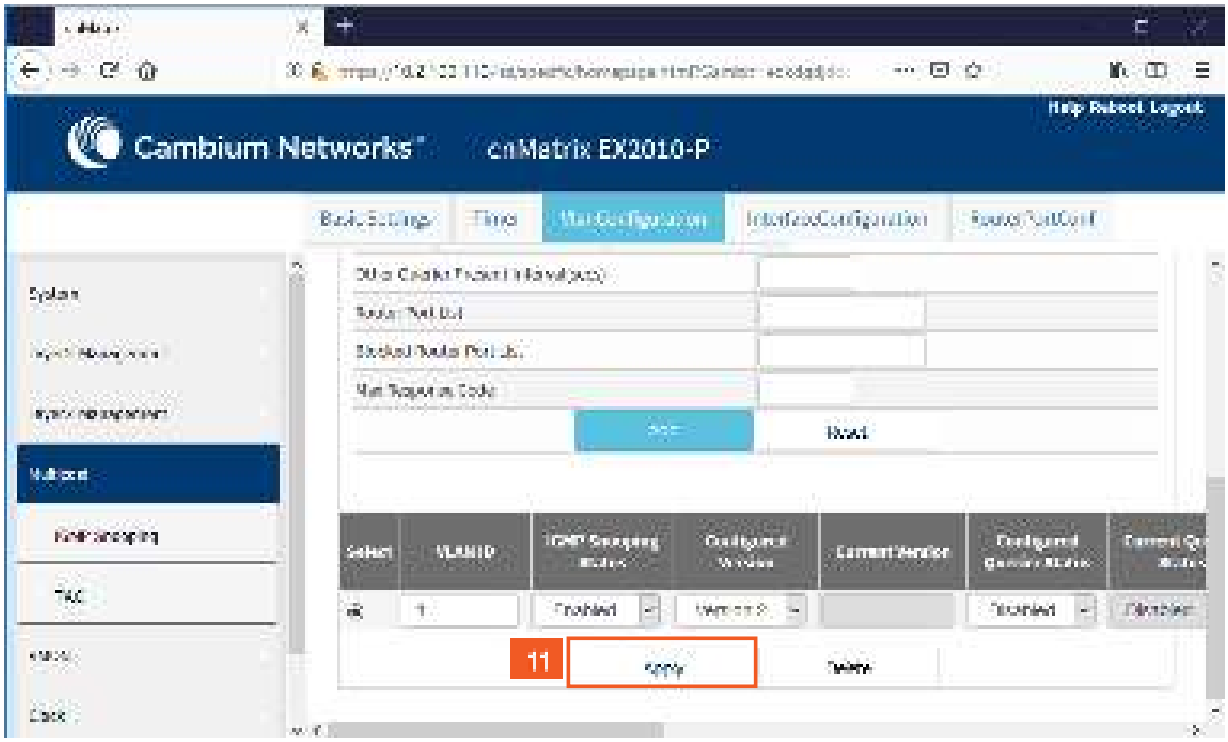


8 Click the **IGMP Snooping Status** drop-down list and select the status of the IGMP Snooping feature on the selected VLAN.

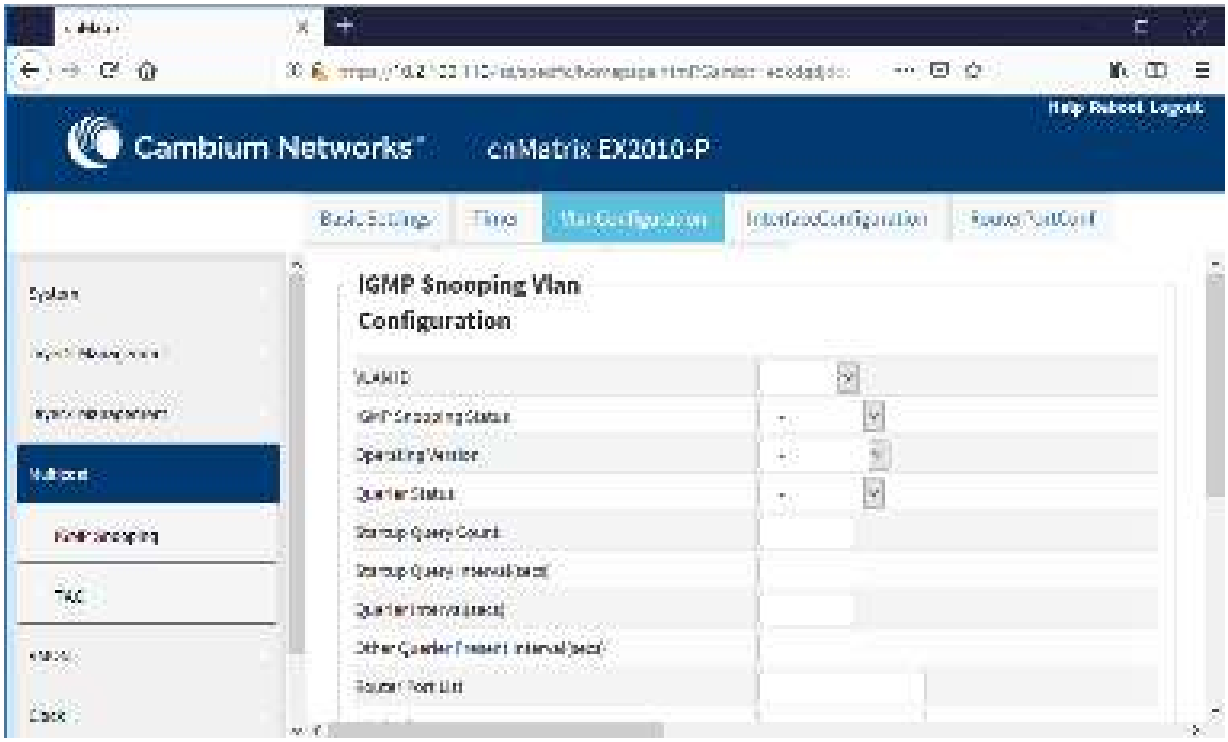
9 Select the **Enabled** list item.



10 Click the **Add** button.

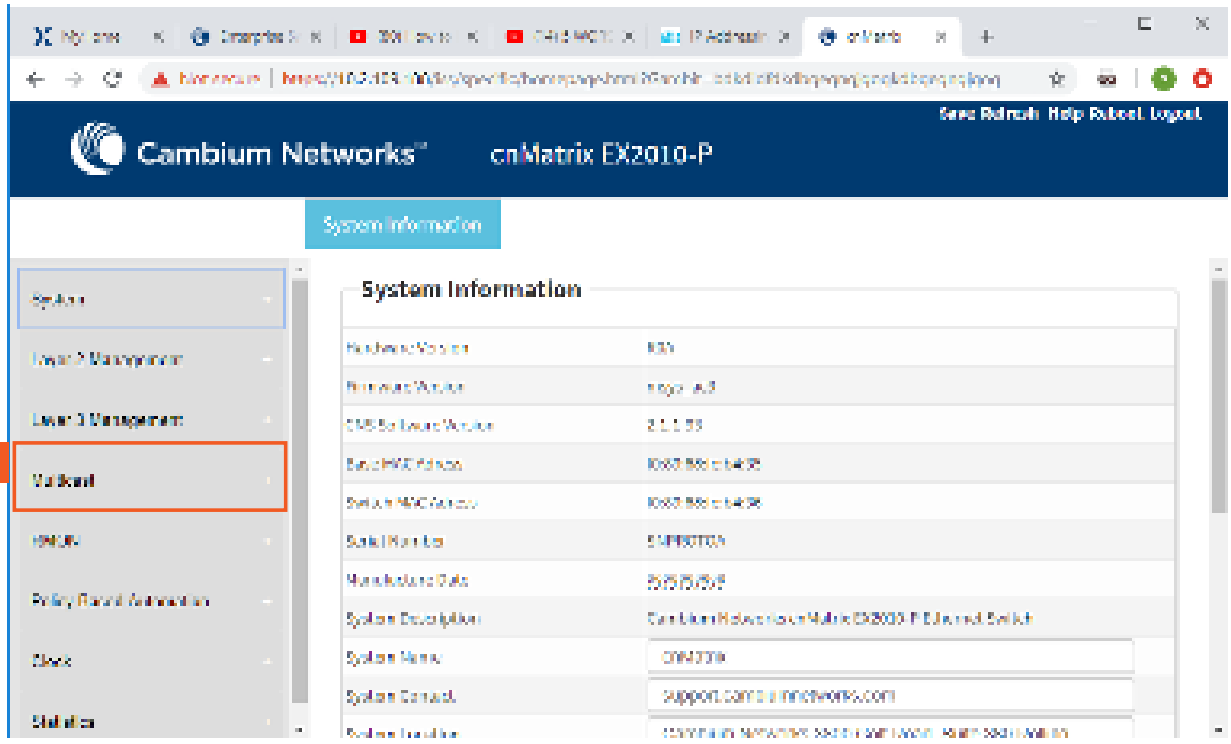


11 Click the **Apply** button.

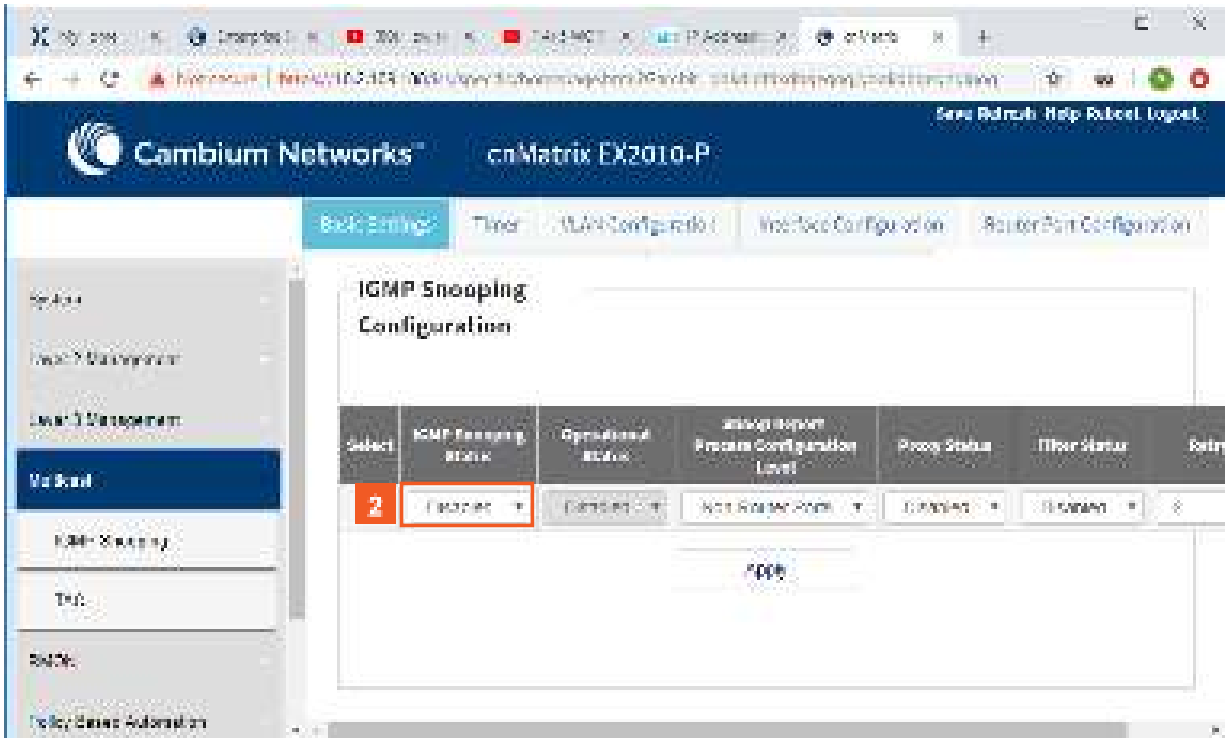


5.4 IGMP Snooping Filtering

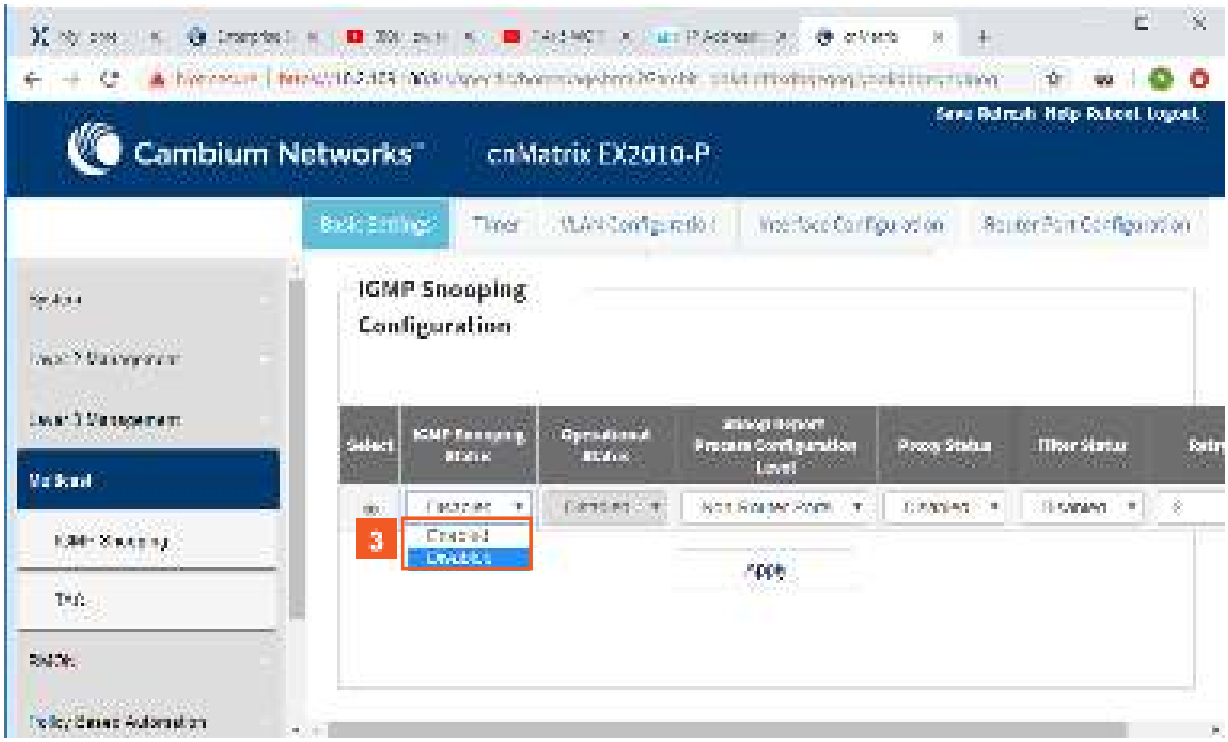
5.4.1 How to Enable, Configure and Apply IGMP Profiles in WEB Interface



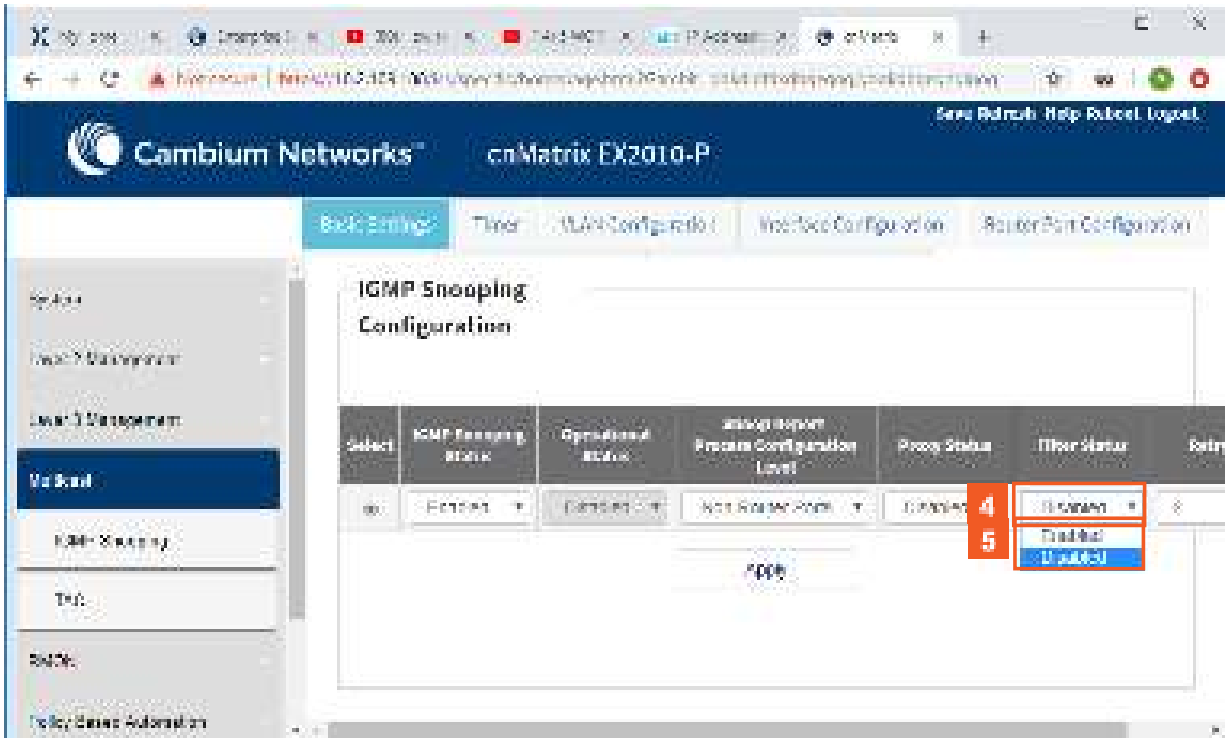
1 Click the **Multicast** tab. The **IGMP Snooping Configuration** window is displayed.



2 Click the **IGMP Snooping Status** drop-down list to select the global status of the IGMP Snooping feature in the switch. .

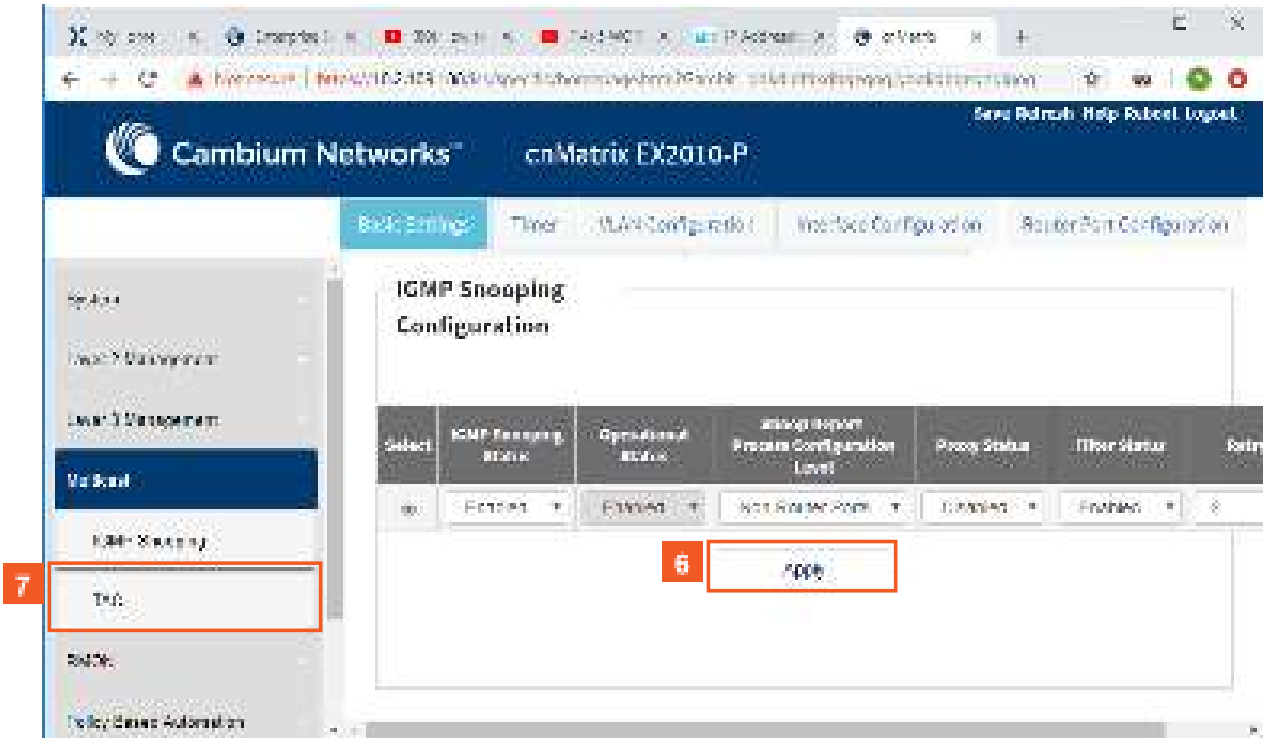


3 Select the **Enabled** list item to enable the global status of the IGMP Snooping feature.



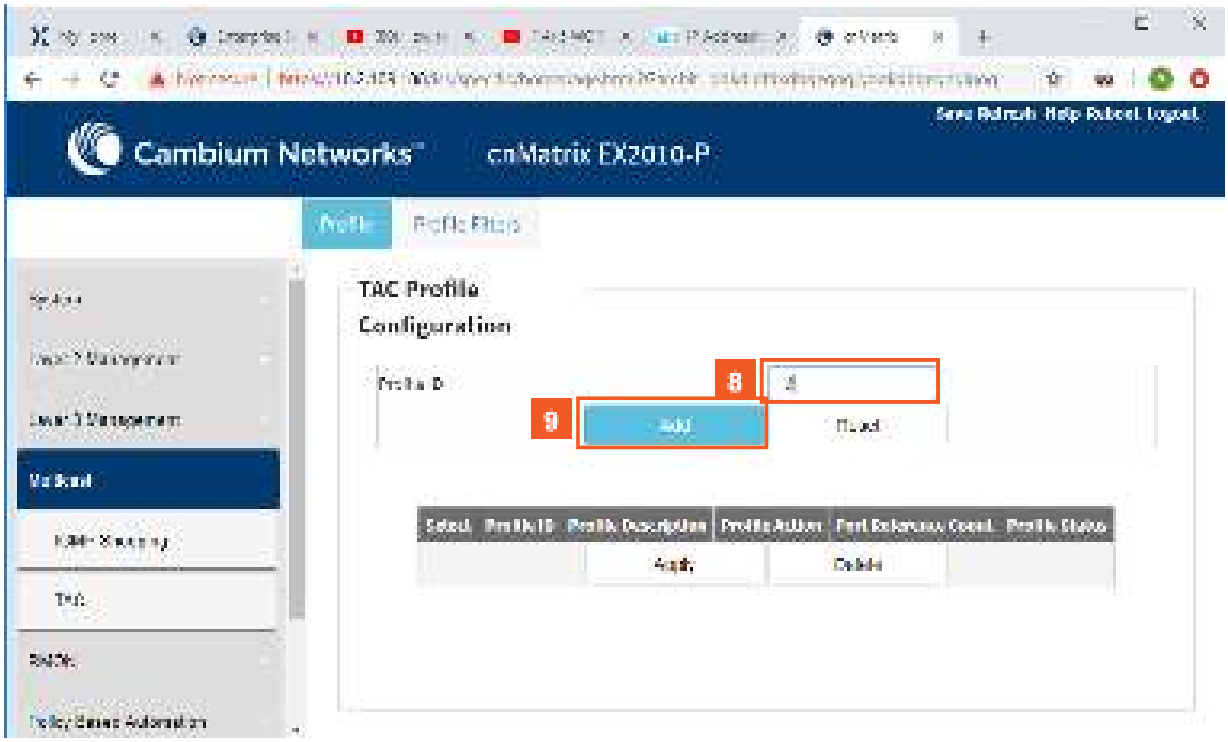
4 Click the **Filter Status** drop-down list to select the filter status.

5 Select the **Enabled** list item to enable the filter status.



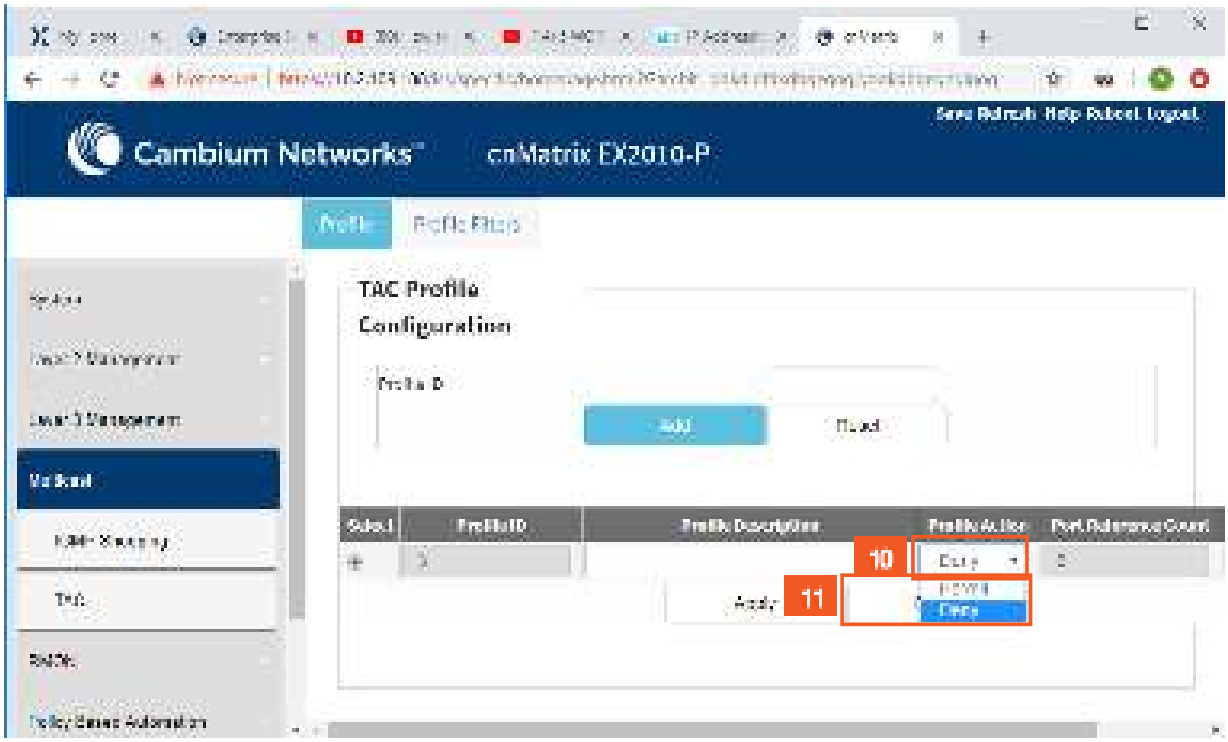
6 Click the **Apply** button.

7 Click the **TAC** menu item. The **TAC Profile Configuration** window is displayed.



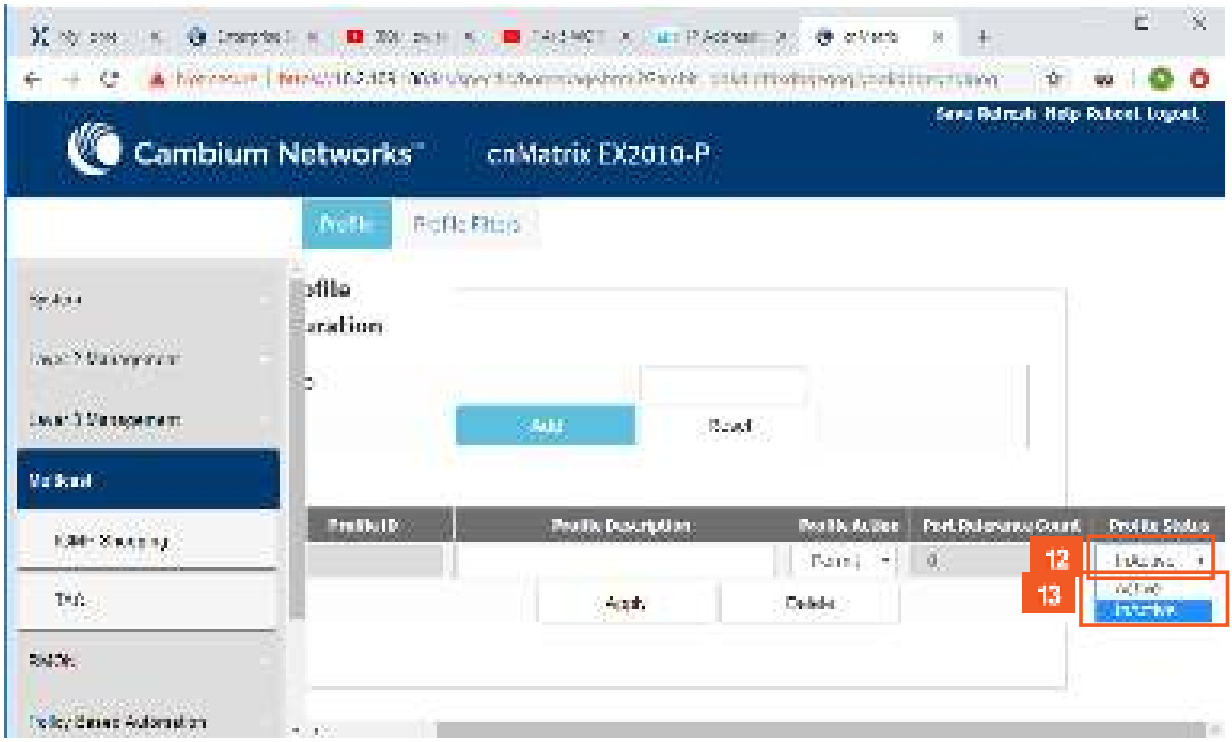
8 Type the value **3** into the **Profile ID** field to set a unique identifier for a multicast profile.

9 Click the **Add** button.



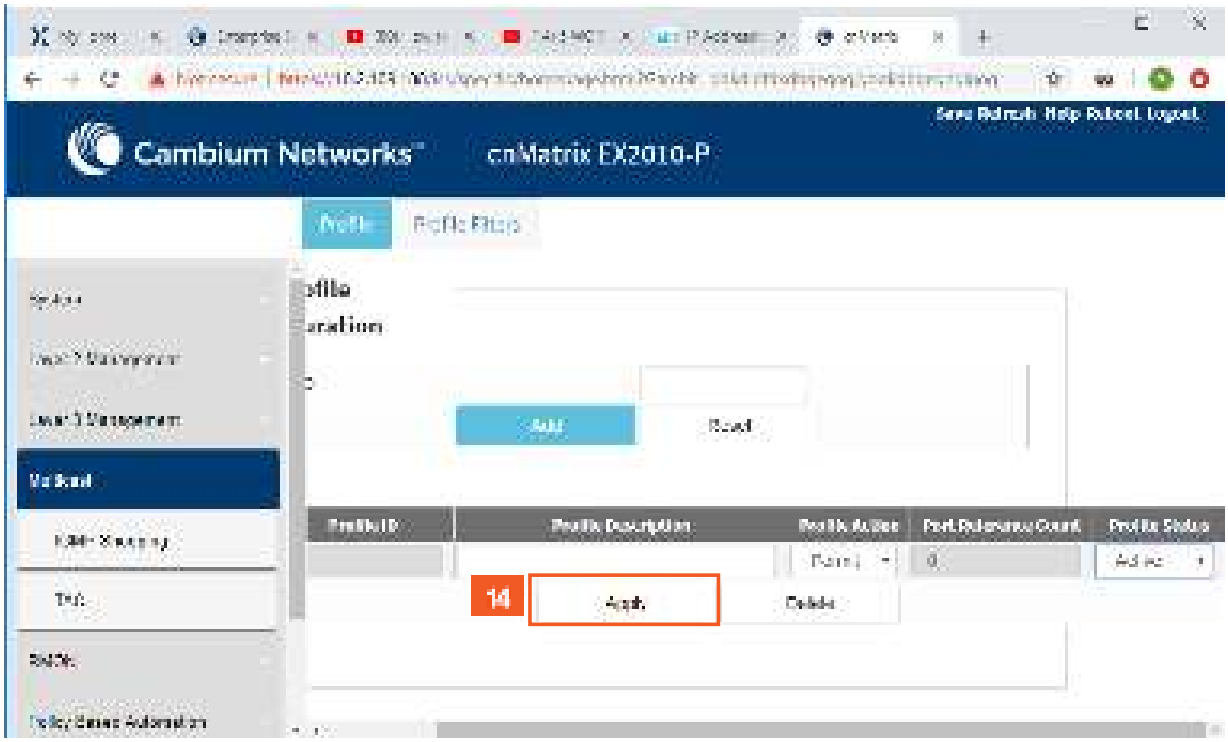
10 Click the **Profile Action** drop-down list.

11 Select the **Permit** list item.

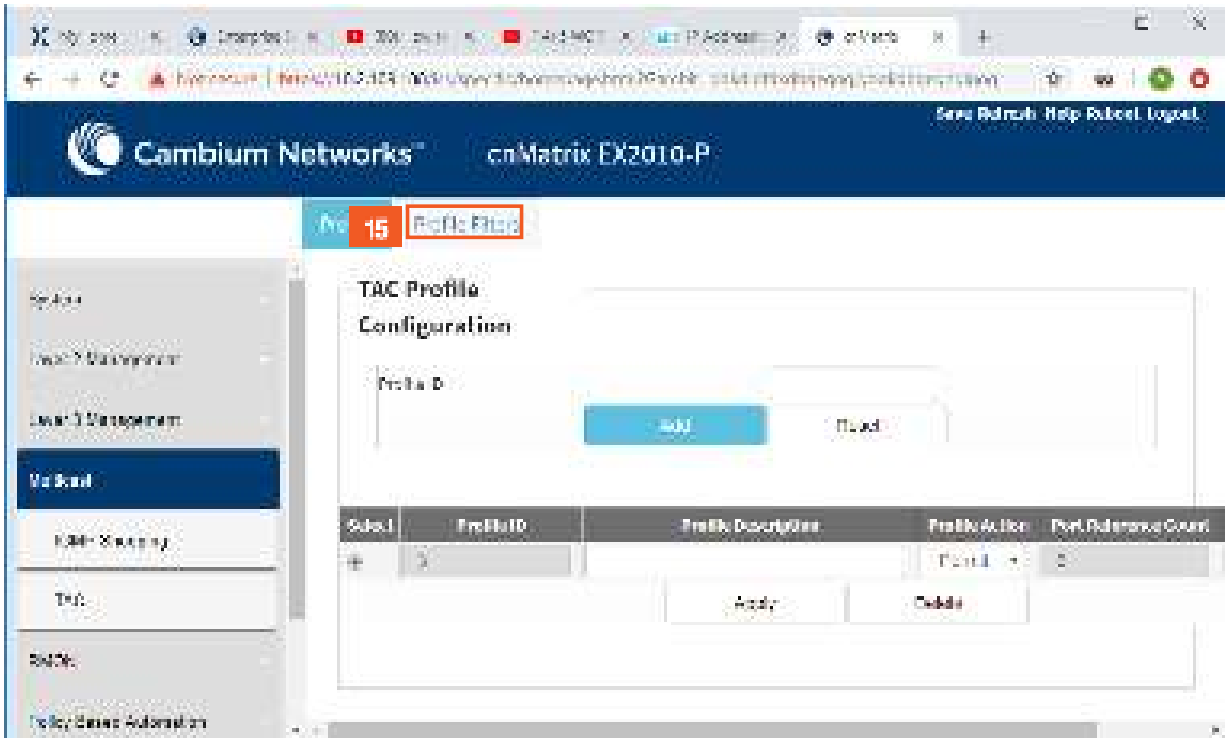


12 Click the **Profile Status** drop-down list.

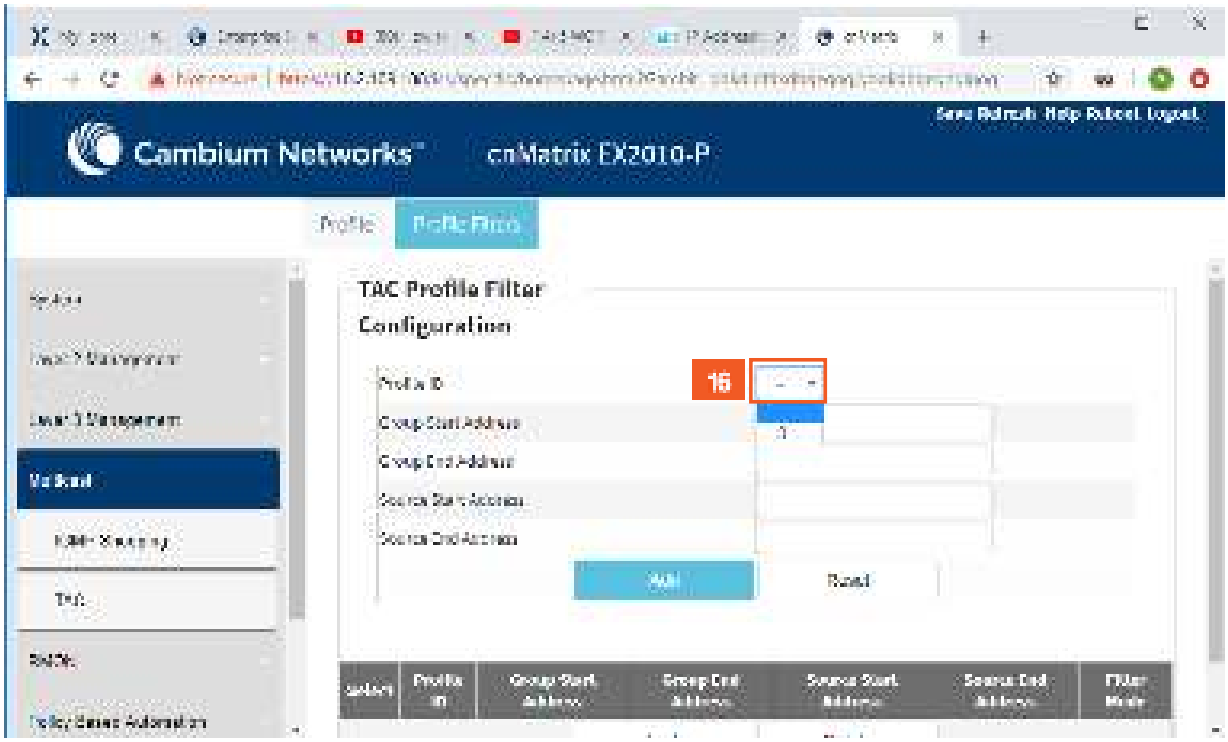
13 Select the **Active** list item.



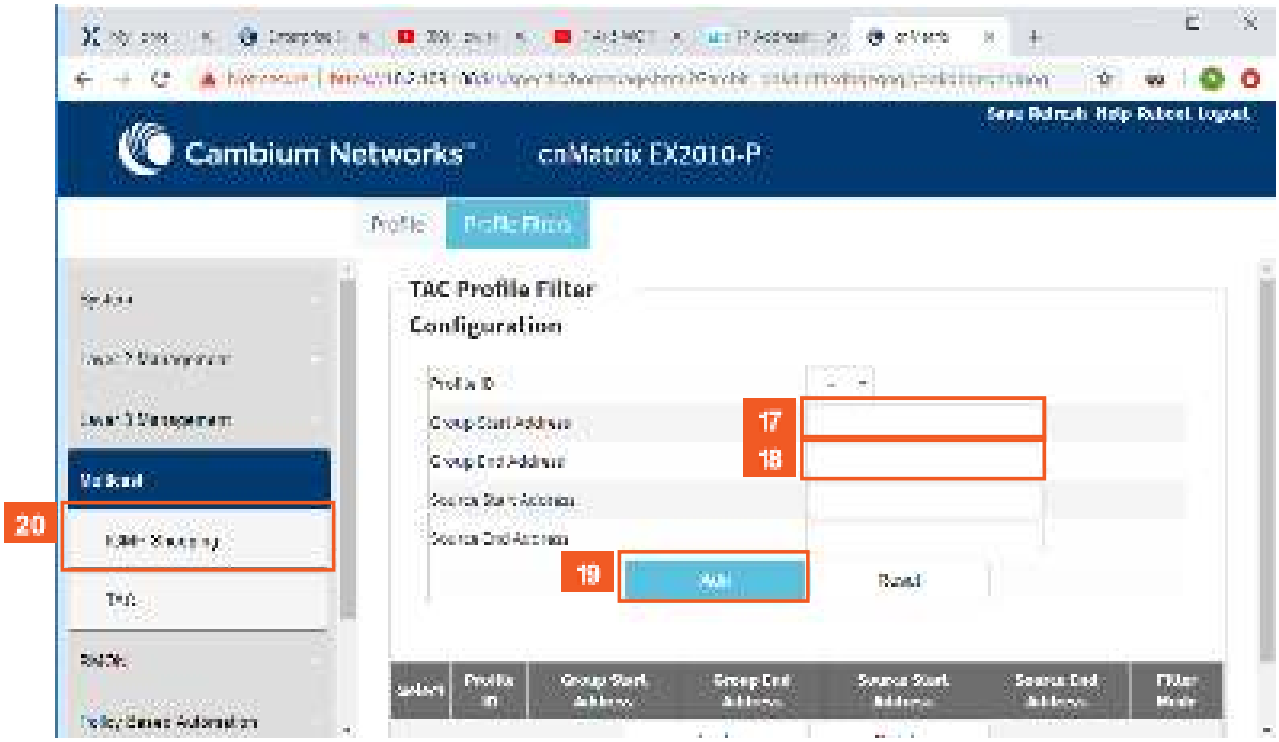
14 Click the **Apply** button.



15 Click the **Profile Filters** tab. The **TAC Profile Configuration** window is displayed.



16 Select from the **Profile ID** drop-down list the profile ID that was previously created in the **TAC Profile Configuration** window.

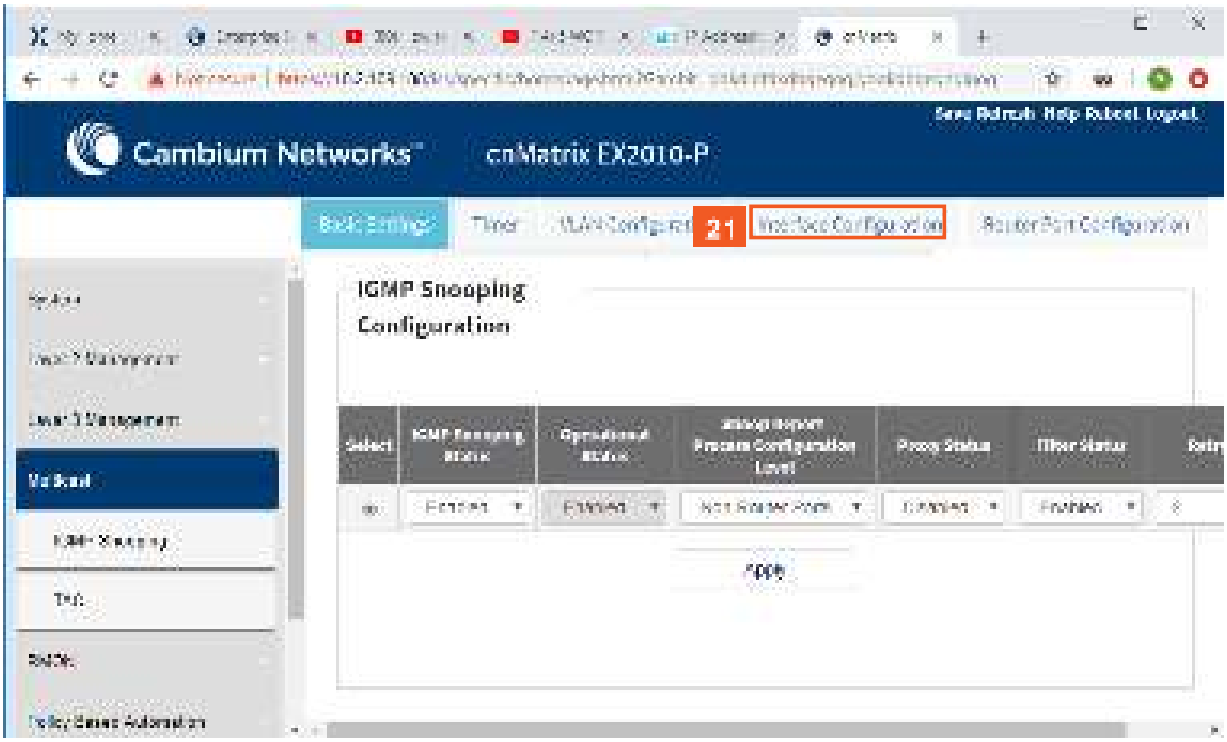


17 Enter the **227.0.0.10** multicast address into the **Group Start Address** field (start of multicast group address range).

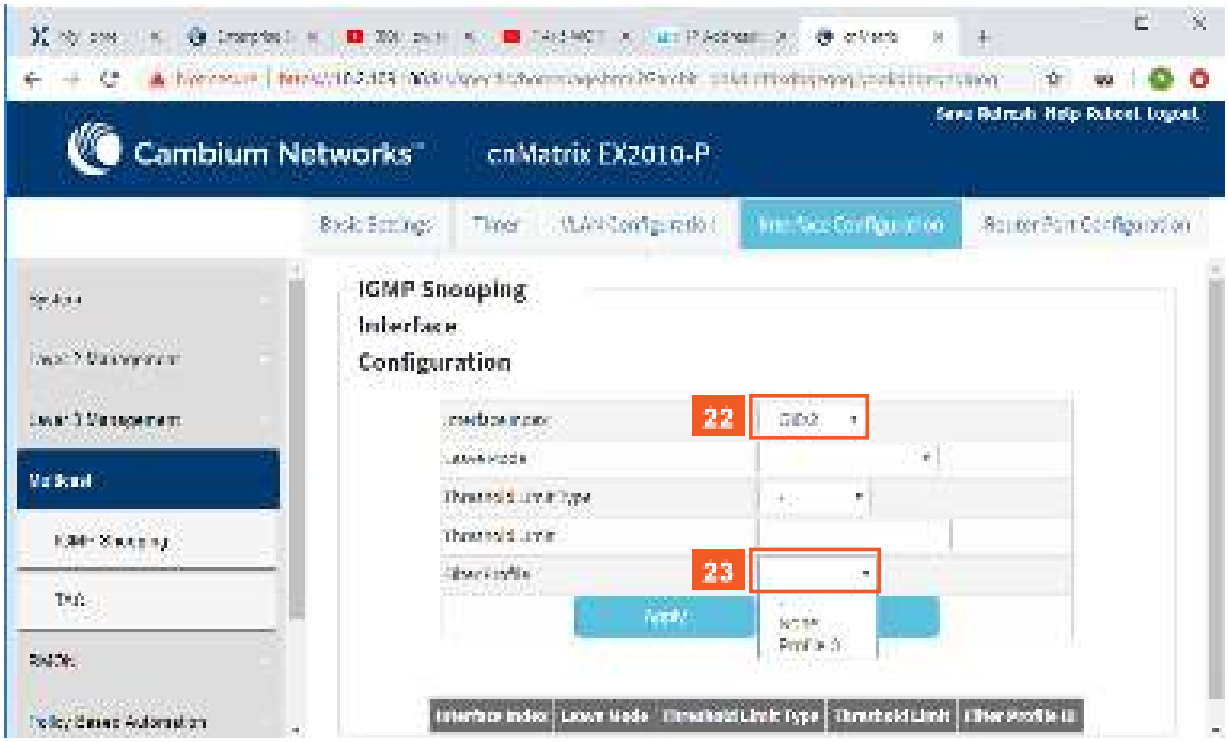
18 Enter the **227.0.0.50** multicast address into the **Group End Address** field (end of multicast group address range) .

19 Click the **Add** button.

20 Click the **IGMP Snooping** menu item. The **IGMP Snooping Configuration** window.

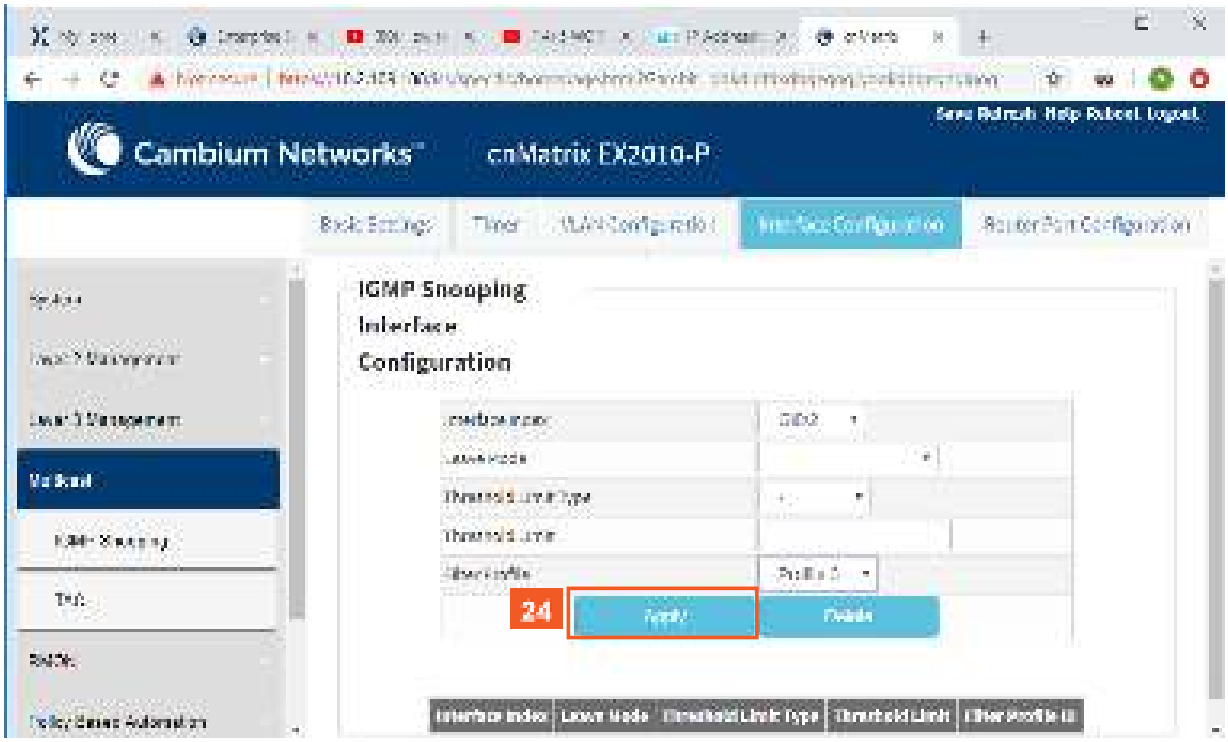


21 Click the **Interface Configuration** tab.

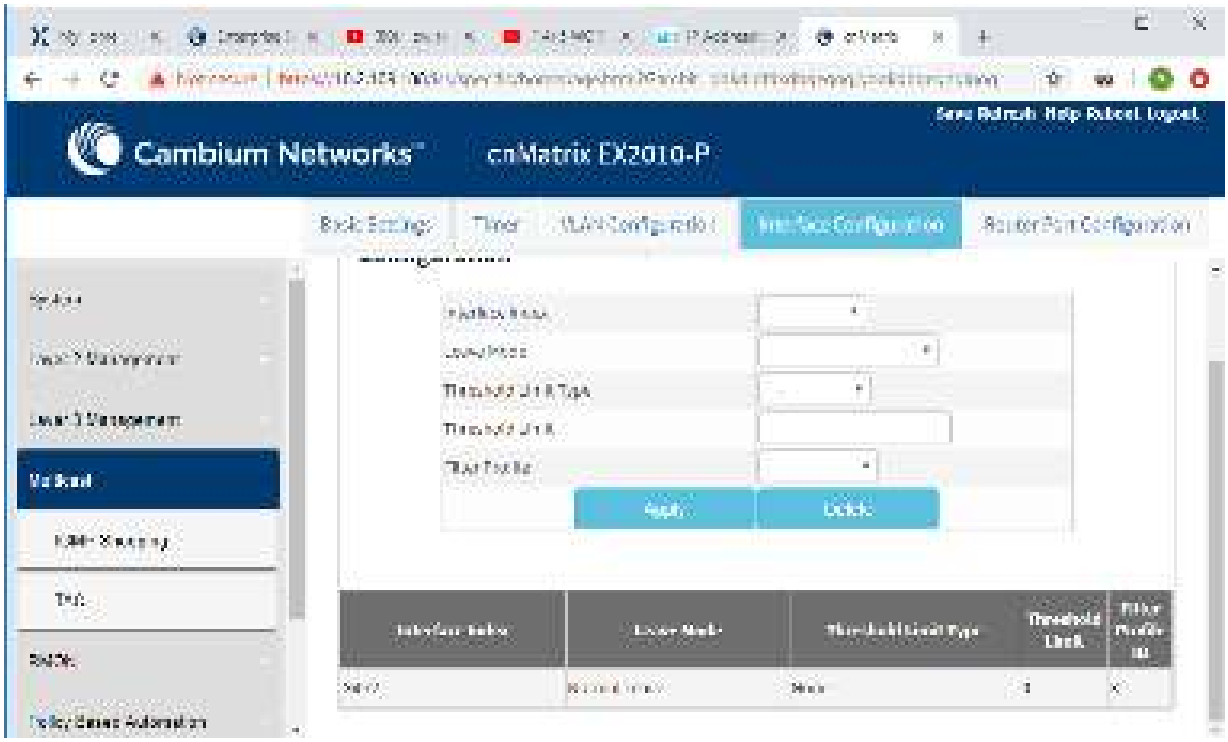


22 Click the **Interface index** drop-down list and select the **Gi0/10** list item.

23 Click the **Interface index** drop-down list and select the **Profile 3** list item.



24 Click the **Apply** button.



For more information, see IGMP Snooping WEB fields and TAC WEB fields.

5.5 DHCP Snooping

5.5.1 Managing DHCP Snooping

5.5.1.1 Feature Description

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

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

Standards

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

Scaling Numbers

- N/A

Limitations

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

Default Values

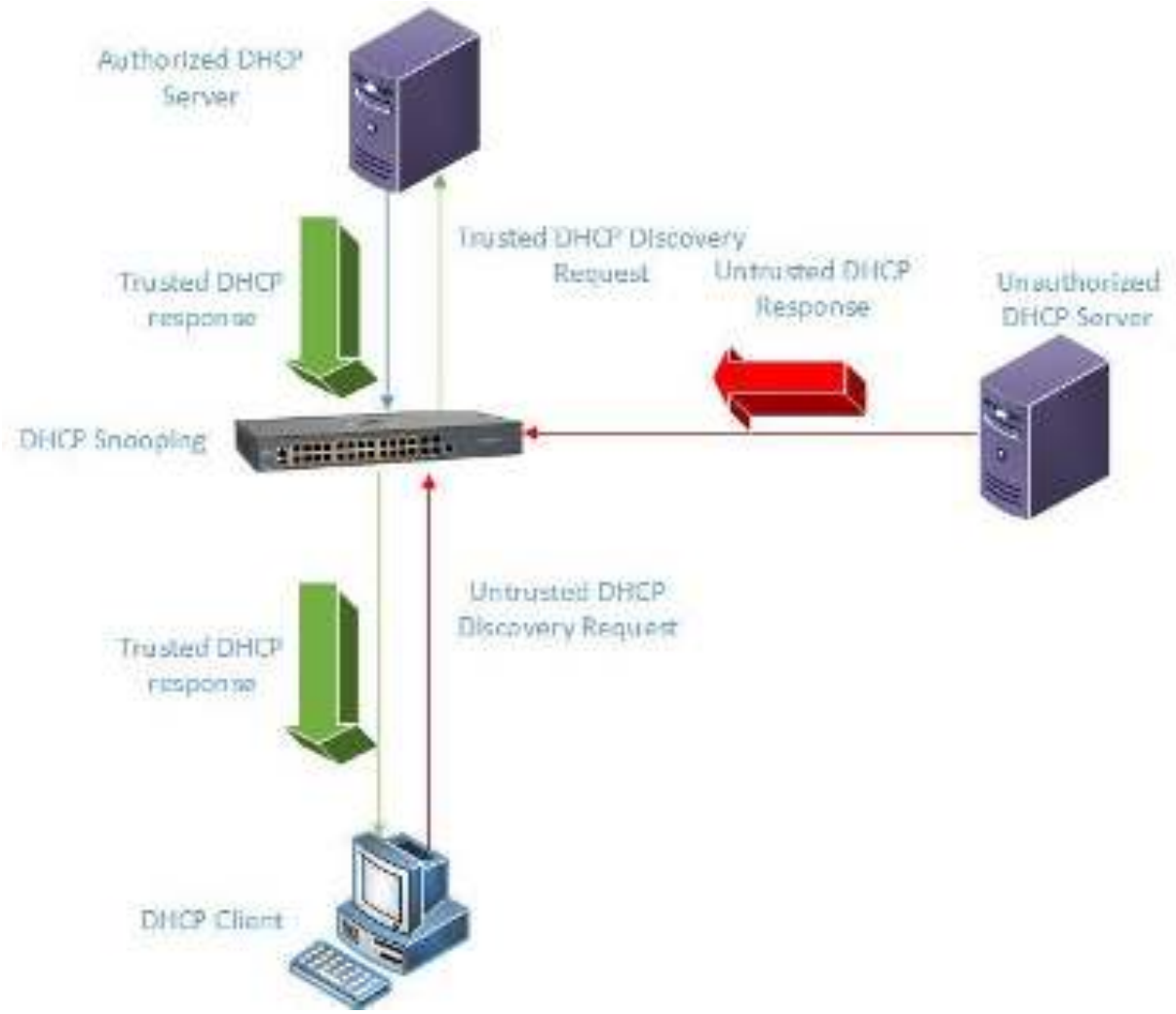
- The DHCP Snooping feature is inactive by default on all VLANs.
- The DHCP MAC address verification is inactive by default.
- All ports are considered as untrusted by default.

Prerequisites

- N/A

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

5.5.1.2 Network Diagram



5.5.2 Configuring DHCP Snooping in Web Interface

The **DHCP Snooping** feature is not available in WEB interface.

5.6 ACL

5.6.1 Managing ACL

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

An ACL consists of three parts:

- **Rule** – a set of fields from the packet, and a set of values that the selected fields have to match.

- **Action** – what to do with the packets that match the rule (permit, deny, redirect).
- **Interface** - where the rule is applied (on ingress or egress direction).

There are three types of ACLs:

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

There are two modes of configuring the ACL feature:

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

Standards

N/A

Scaling Numbers

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

Limitations

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

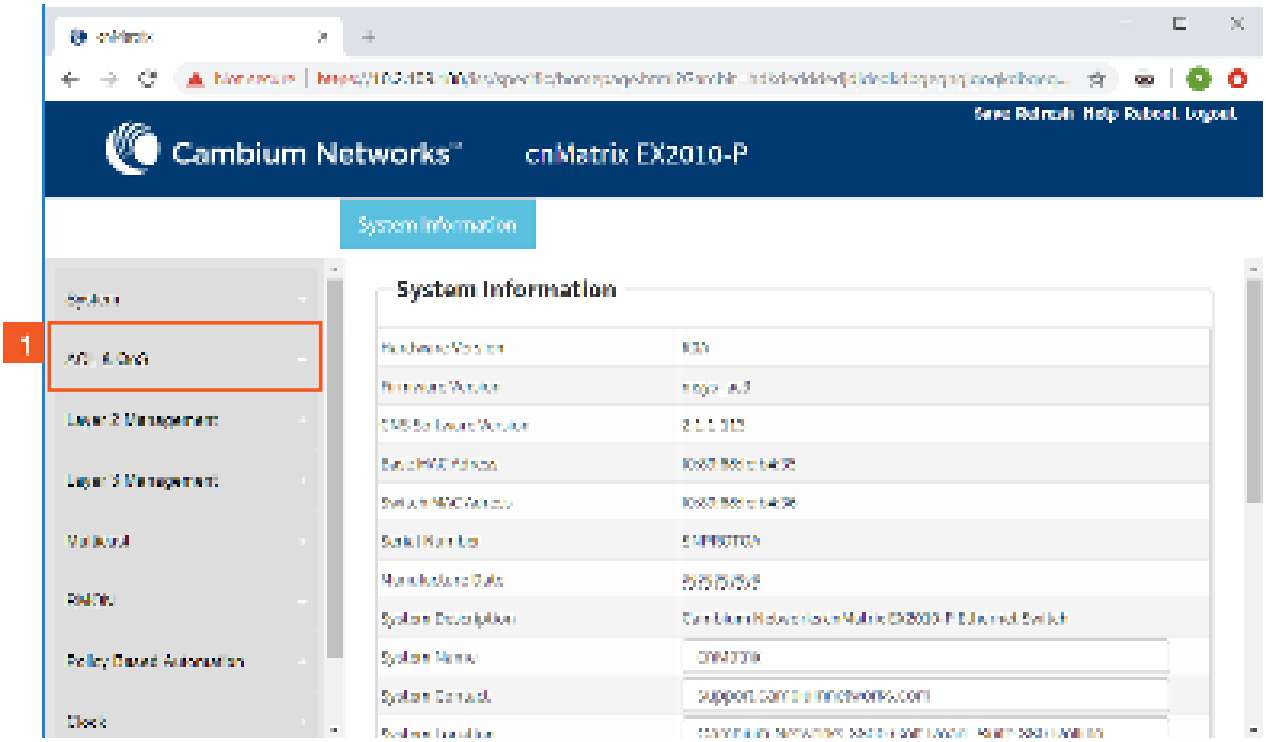
Default Values

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

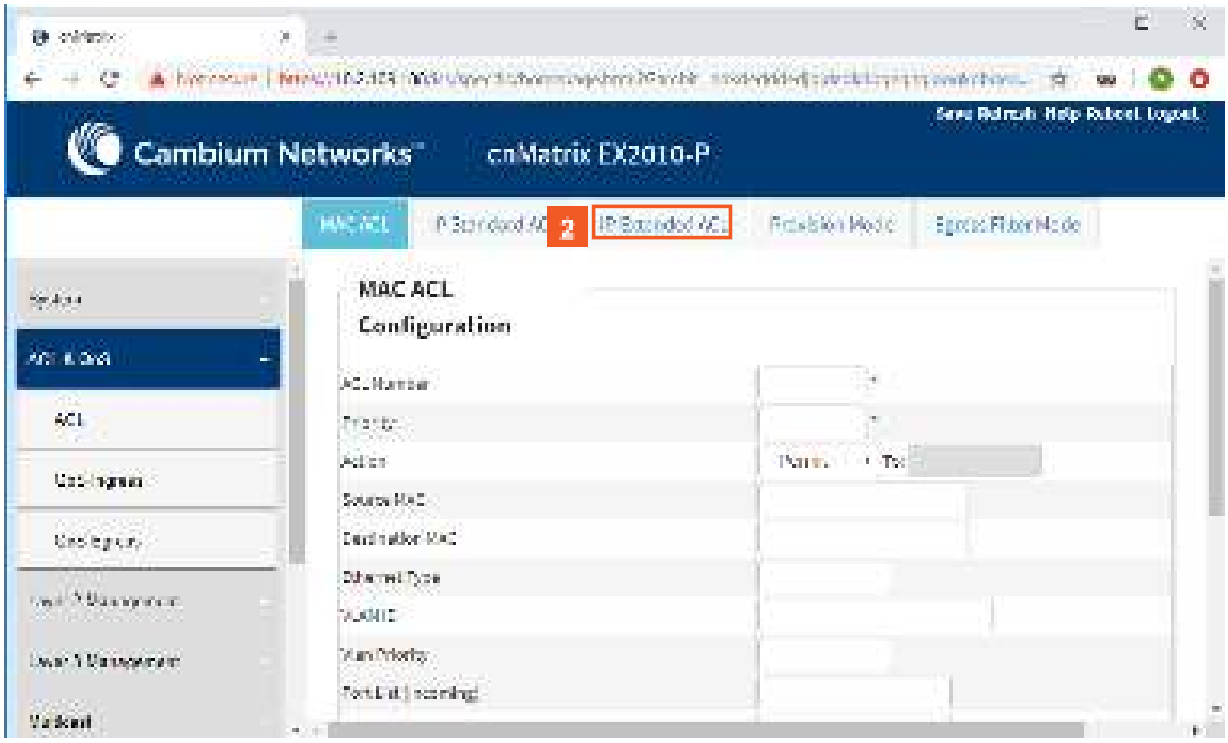
5.6.2 Configuring ACL in WEB Interface

The **ACL (Access Control Lists)** feature is not available in WEB interface. **Starting with version 2.1**, the **ACL (Access Control Lists)** feature is available in WEB interface.

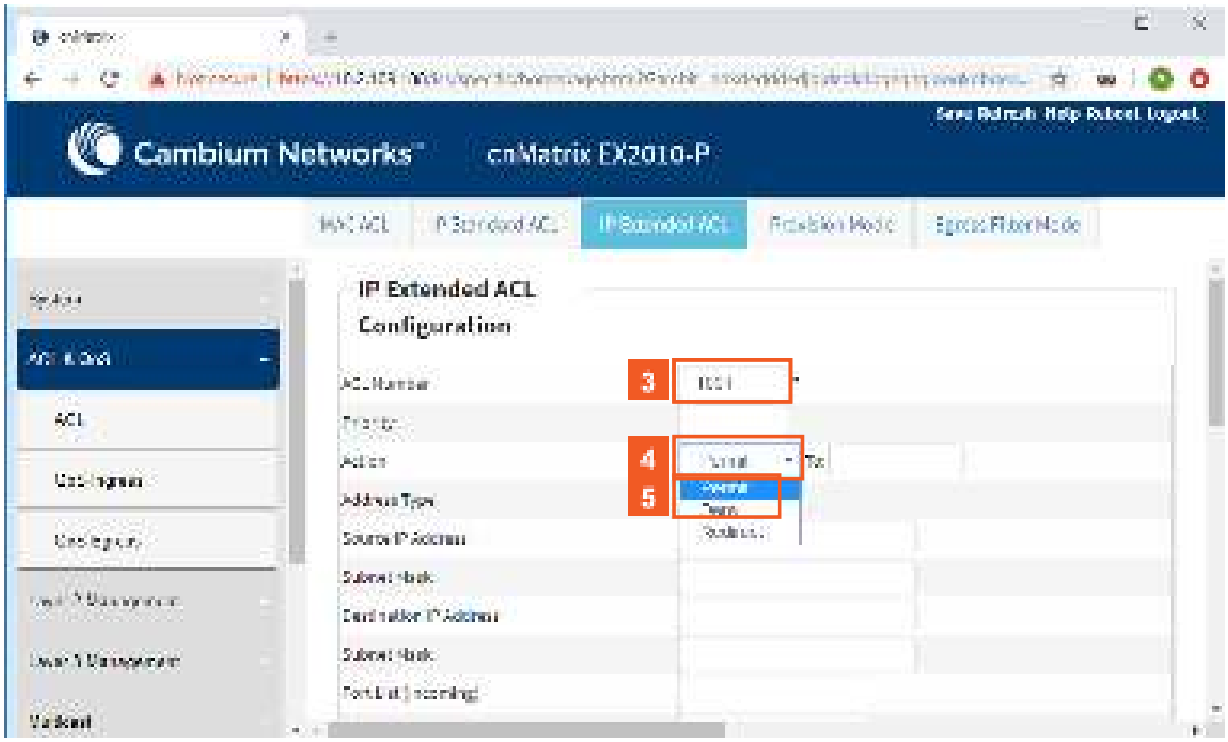
5.6.3 Configuring ACL in WEB Interface - Immediate mode (Starting with version 2.1)



1 Click the **ACL & QoS** tab.



2 Click the **IP Extended ACL** tab.

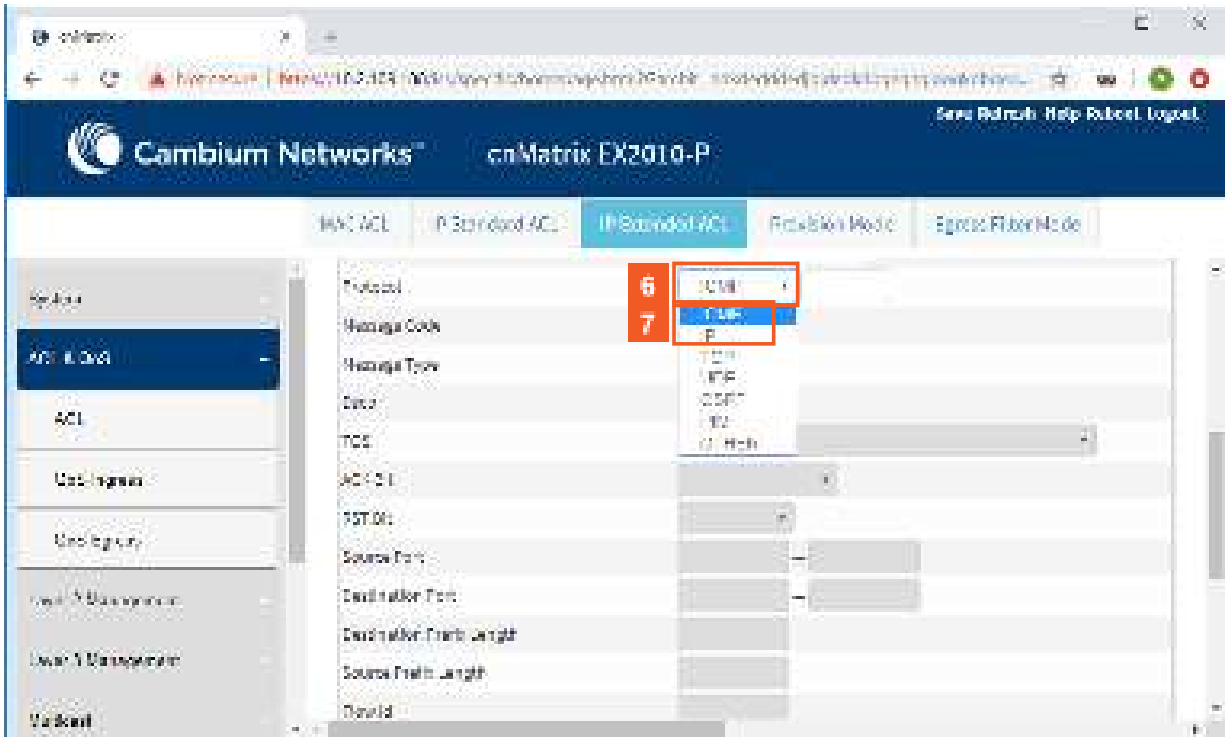


3 Type the value **1001** into the **IP Extended ACL Configuration** field.

1001 - represents an extended MAC access list number.

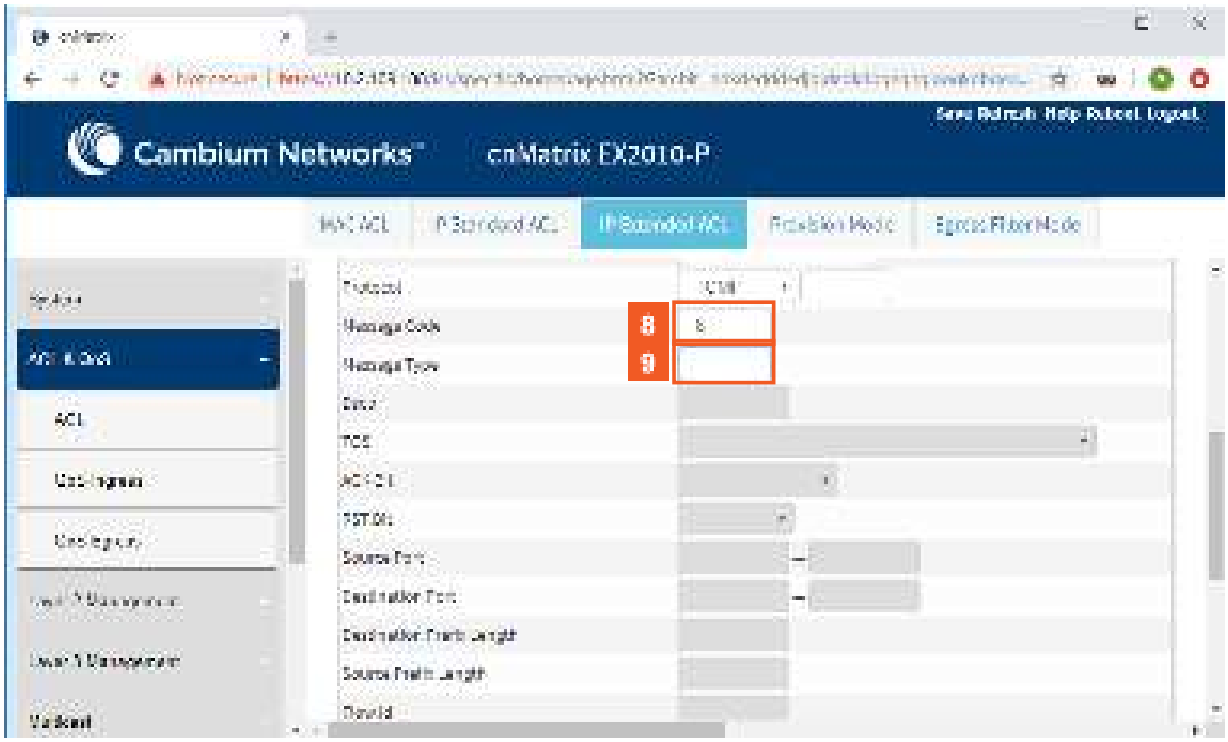
4 Click the **Action** drop-down list to set the action for the incoming packets of the specified access list.

5 Select the **Deny** list item.



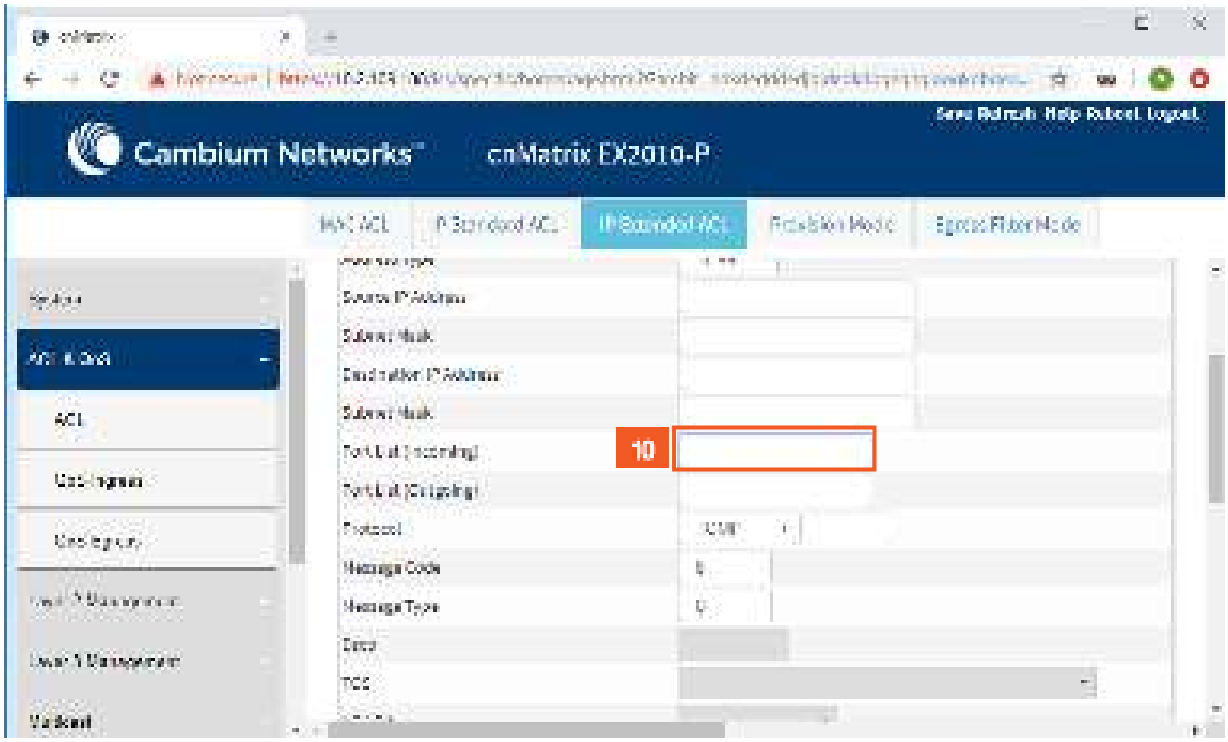
6 Click the **Protocol** drop-down list.

7 Select the **ICMP** list item to specify that the filter will be applied for ICMP packets.

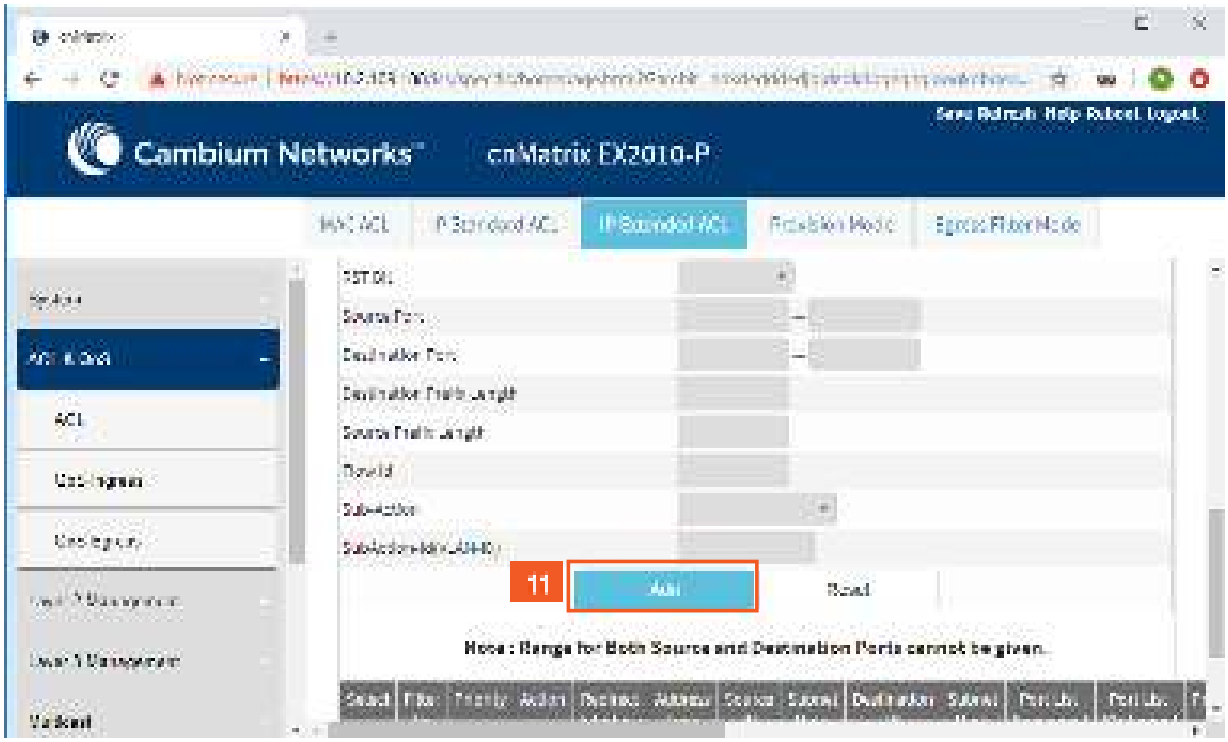


8 Type a value in the **Message Code** field (for example 8) to set a message code to be checked for ICMP packets.

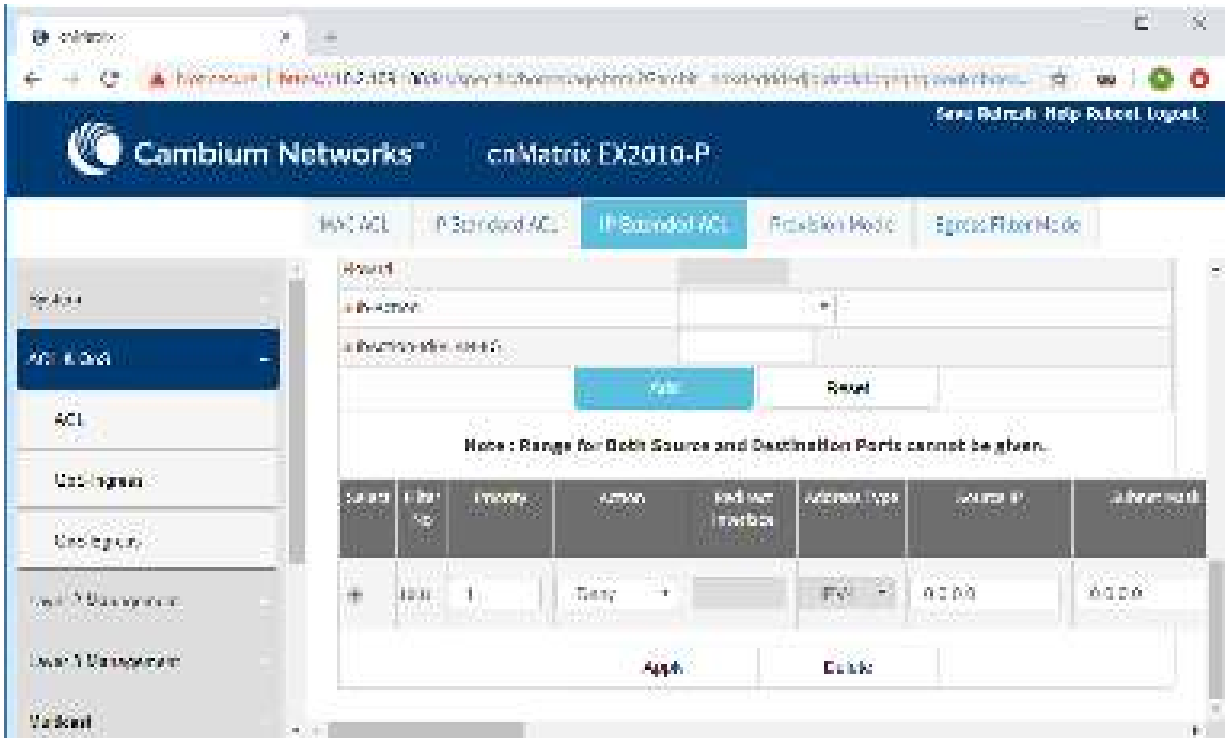
9 Type a value in the **Message Type** field (for example 0) to set a message type to be checked for ICMP packets.



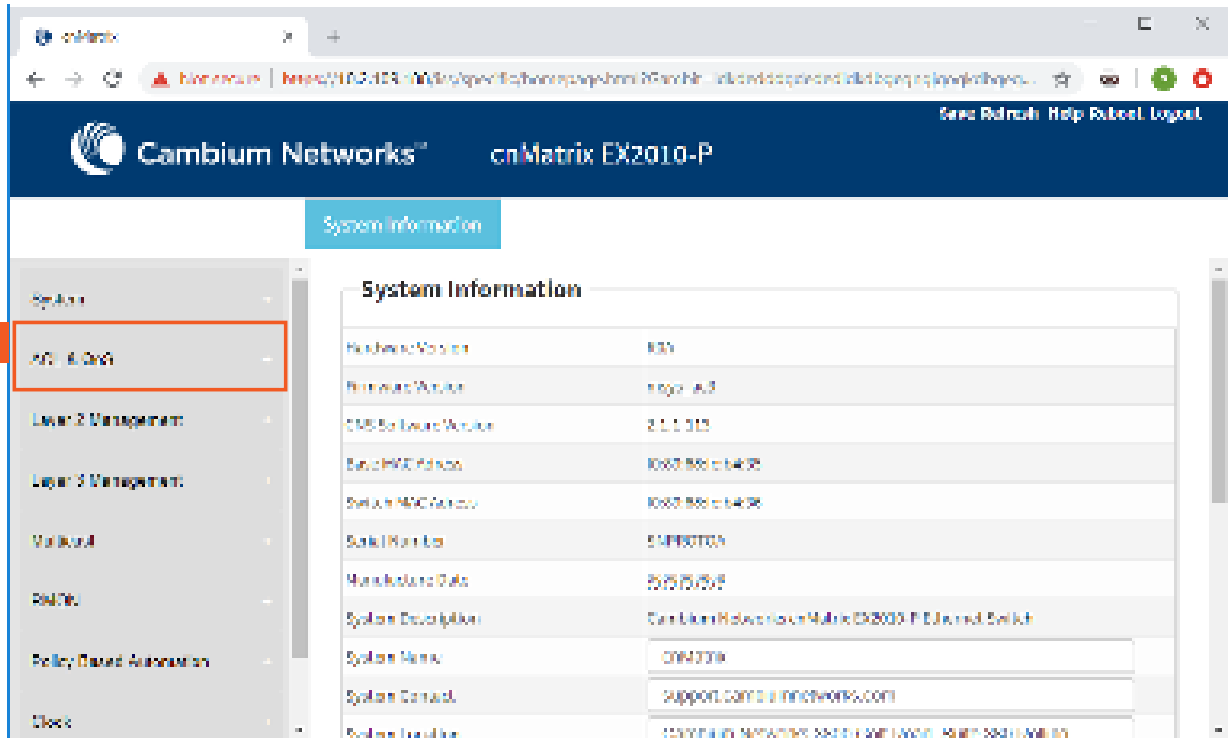
10 Type an interface name in the **Port List(Incoming)** field (for example gi0/5) to specify the incoming port range.



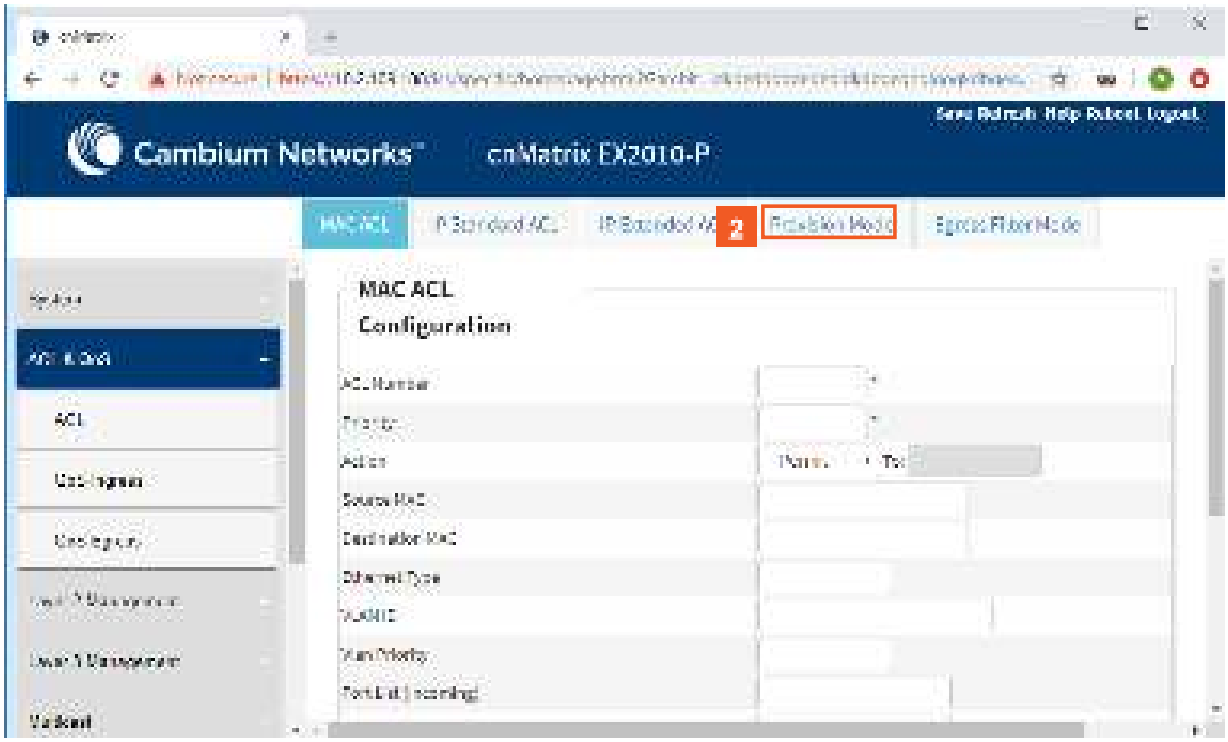
11 Click the **Add** button.



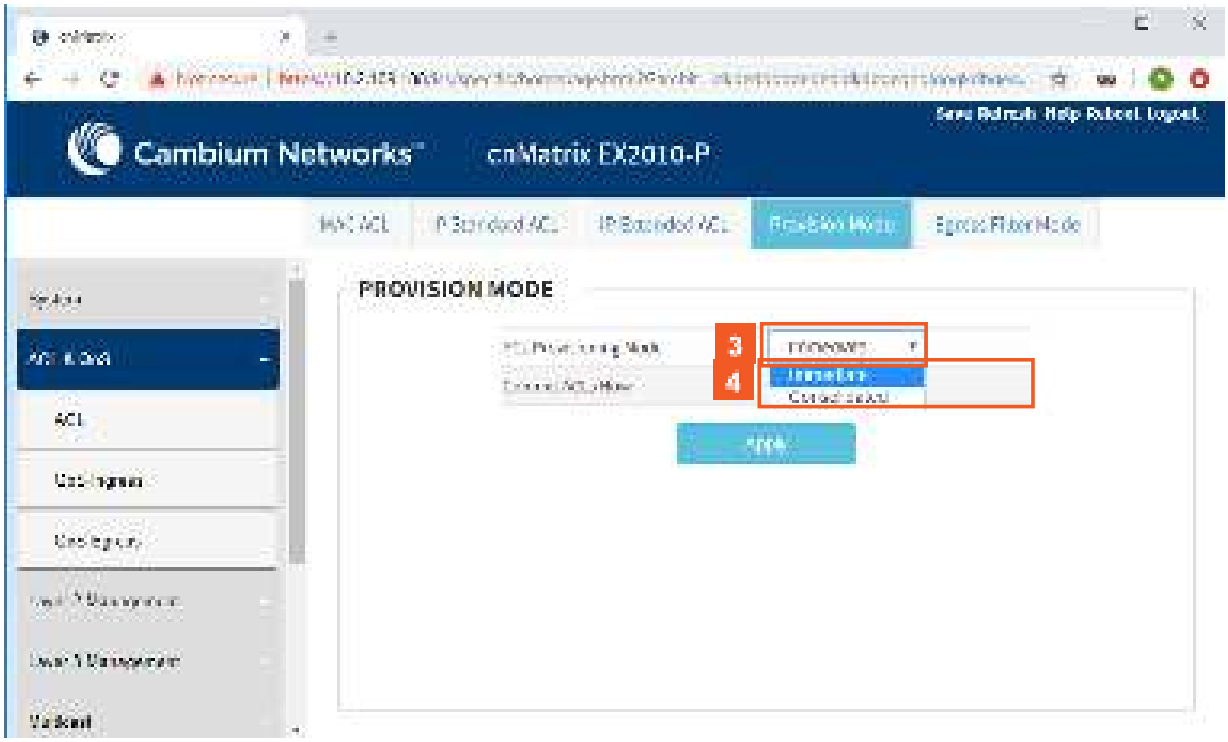
5.6.4 Configuring ACL in WEB Interface- Consolidated mode (Starting with version 2.1)



1 Click the **ACL & QoS** tab.

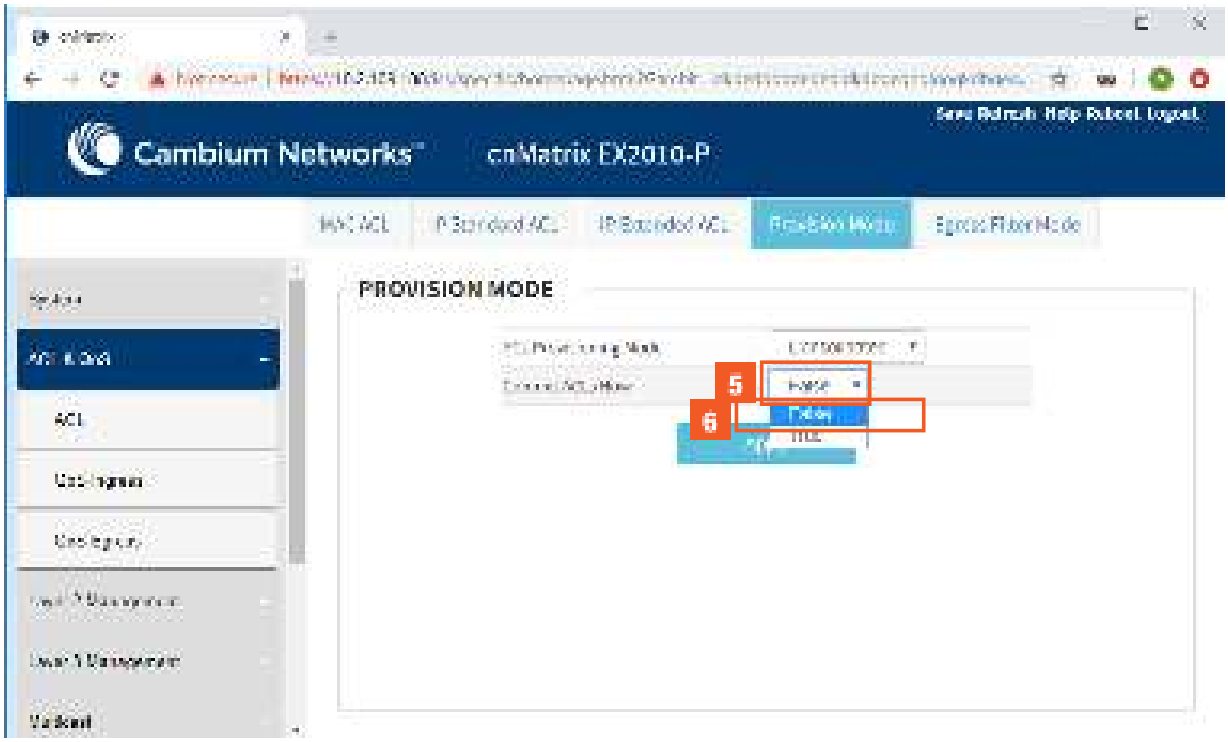


2 Click the **Provision Mode** tab.



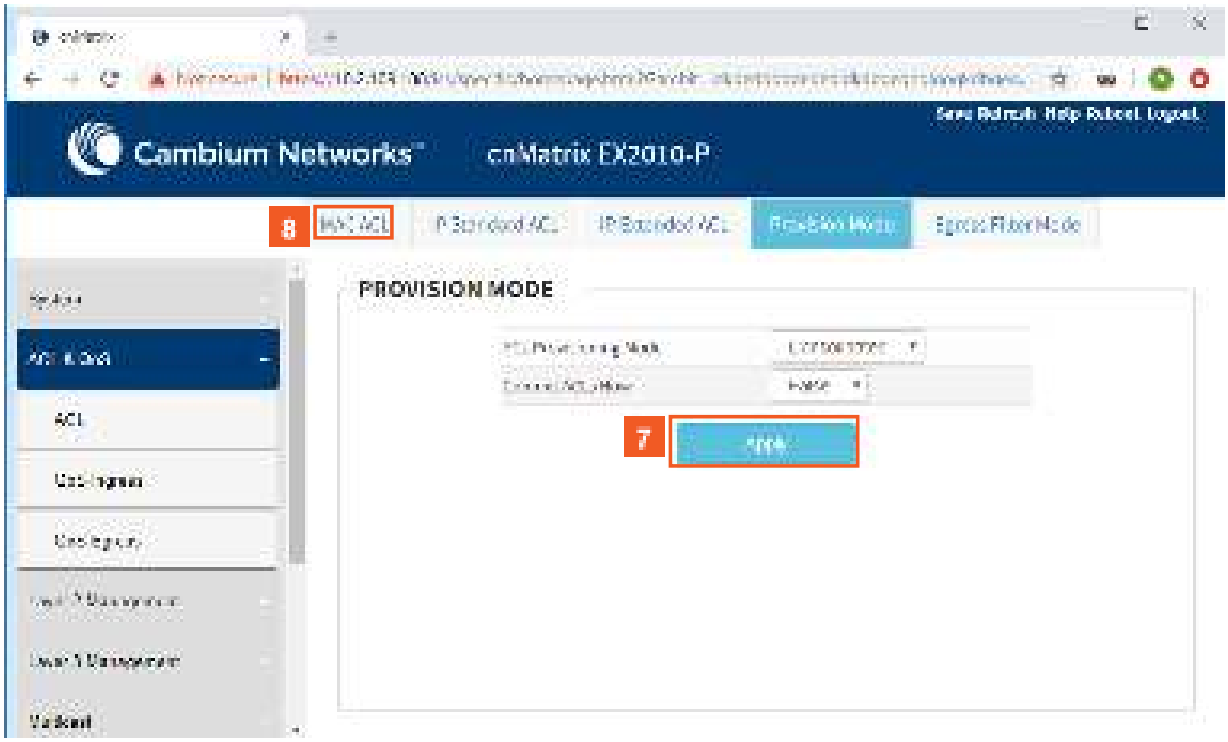
3 Click the **ACL Provisioning Mode** drop-down list to select the commit support for which the access control rule needs to be applied.

4 Select the **Consolidated** list item to apply the rules after the commit is issued.



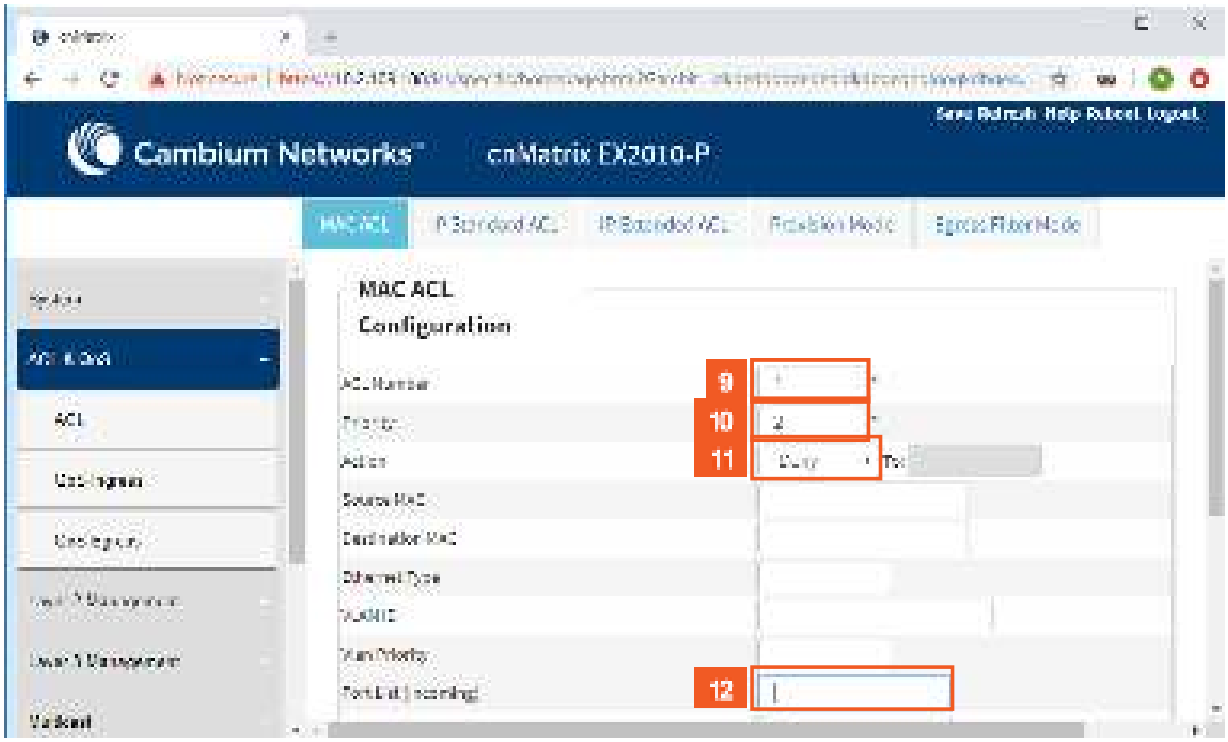
5 Click the **Commit ACLs Now** drop-down list to select the commit action to be taken for the access list.

6 Select the **False** list item (no commit action is set).



7 Click the **Apply** button.

8 Click the **MAC ACL** tab.

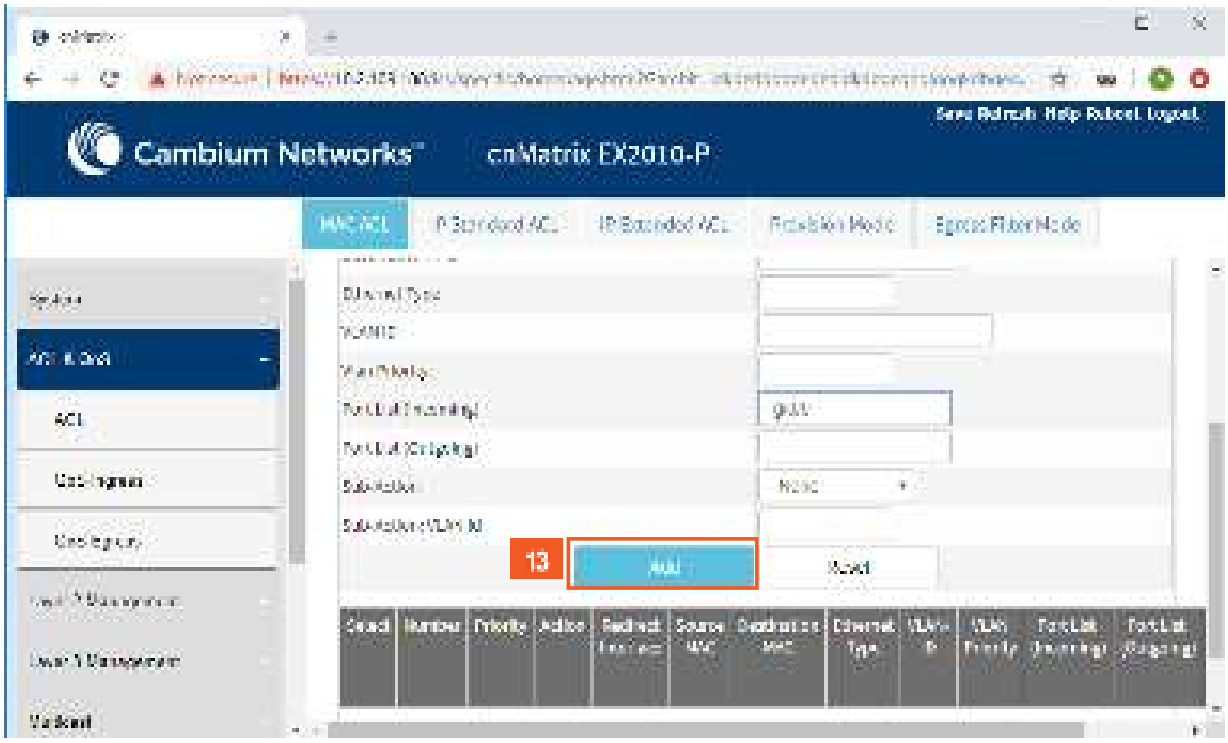


9 Enter **1** into the **ACL Number** field to specify an extended MAC access list number.

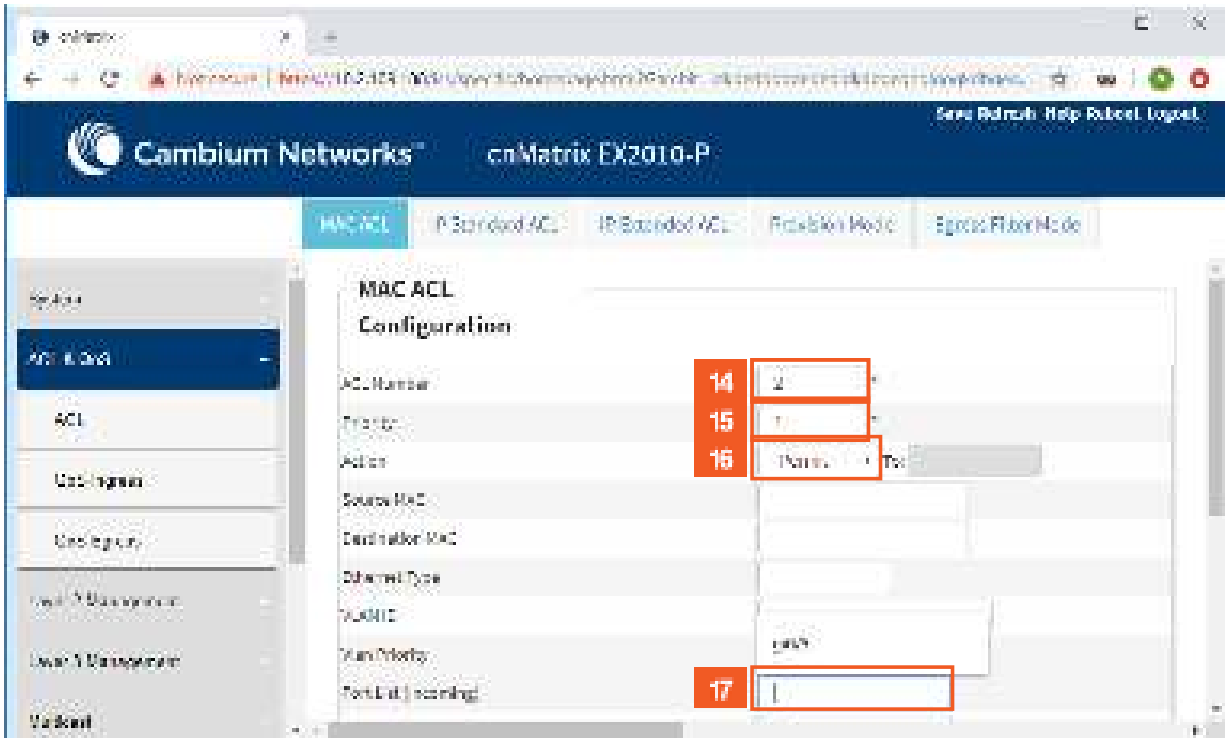
10 Enter **2** into the **Priority** field to set the priority of the L3 filter to decide which filter rule is applicable when the packet matches with more than one filter rule.

11 Click the **Action** drop-down list to select the action for the incoming packets of the specified access list (in this example select the **Deny** list item).

12 Enter **gi0/5** into the **Port List (Incoming)** field to set the port list for the incoming ports for which the access list has to be applied.



13 Click the **Add** button.

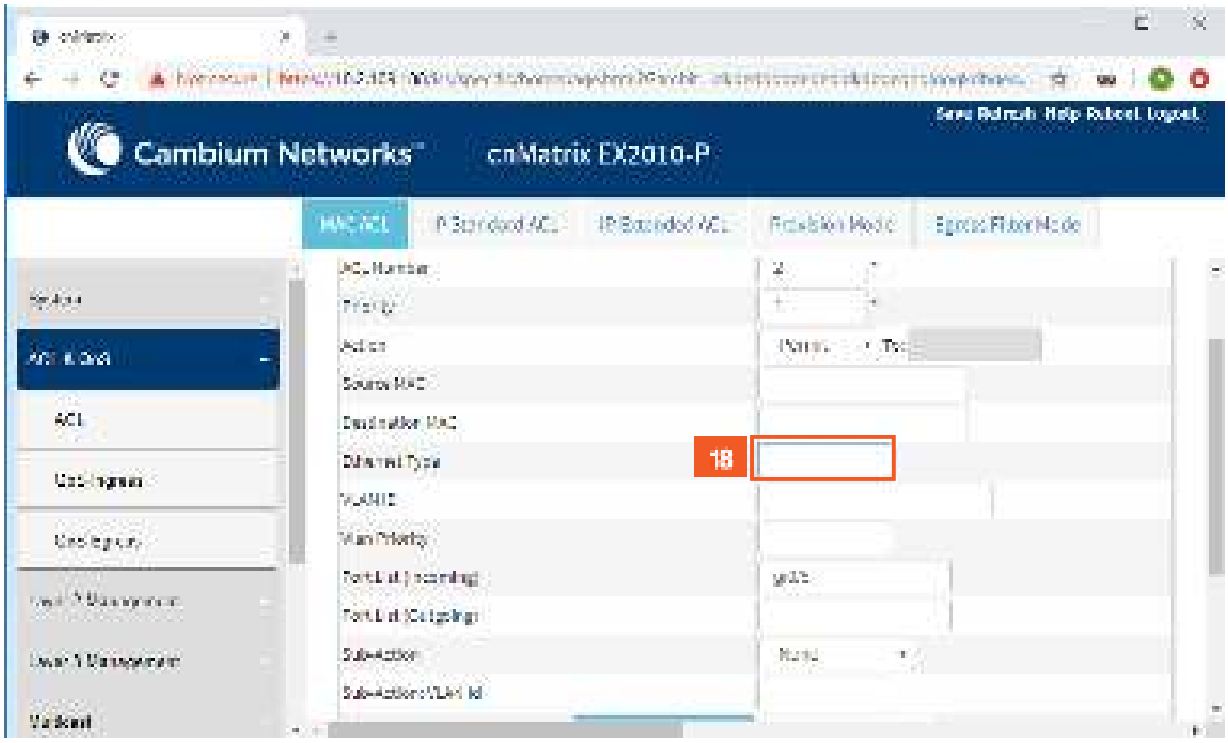


14 Enter 2 into the ACL Number field to specify an extended MAC access list number.

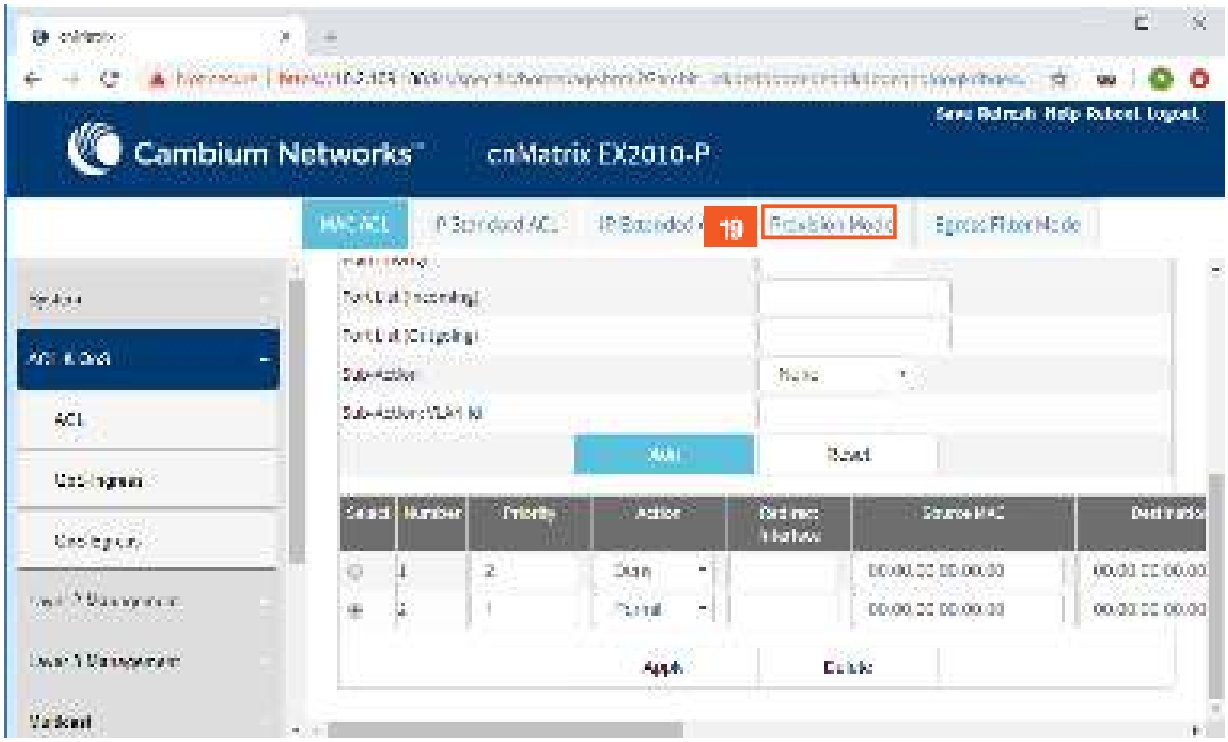
15 Enter **2** into the **Priority** field to set the priority of the L3 filter (which filter rule is applicable when the packet matches with more than one filter rule.

16 Click the **Action** drop-down button and select the action for the incoming packets of the specified access list (in this example select the **Permit** list item).

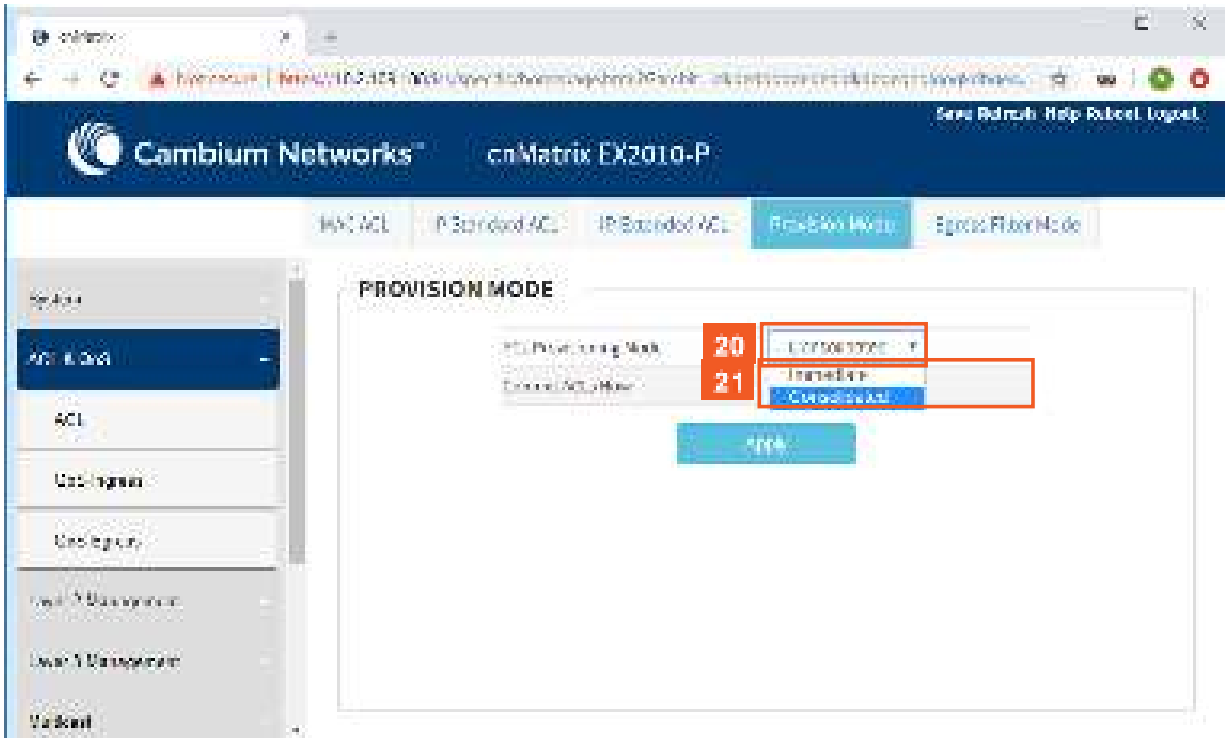
17 Enter **gi0/5** into the **Port List (Incoming)** field to set the port list for the incoming ports for which the access list has to be applied.



18 Enter **2048** into the **Ethernet Type** field.

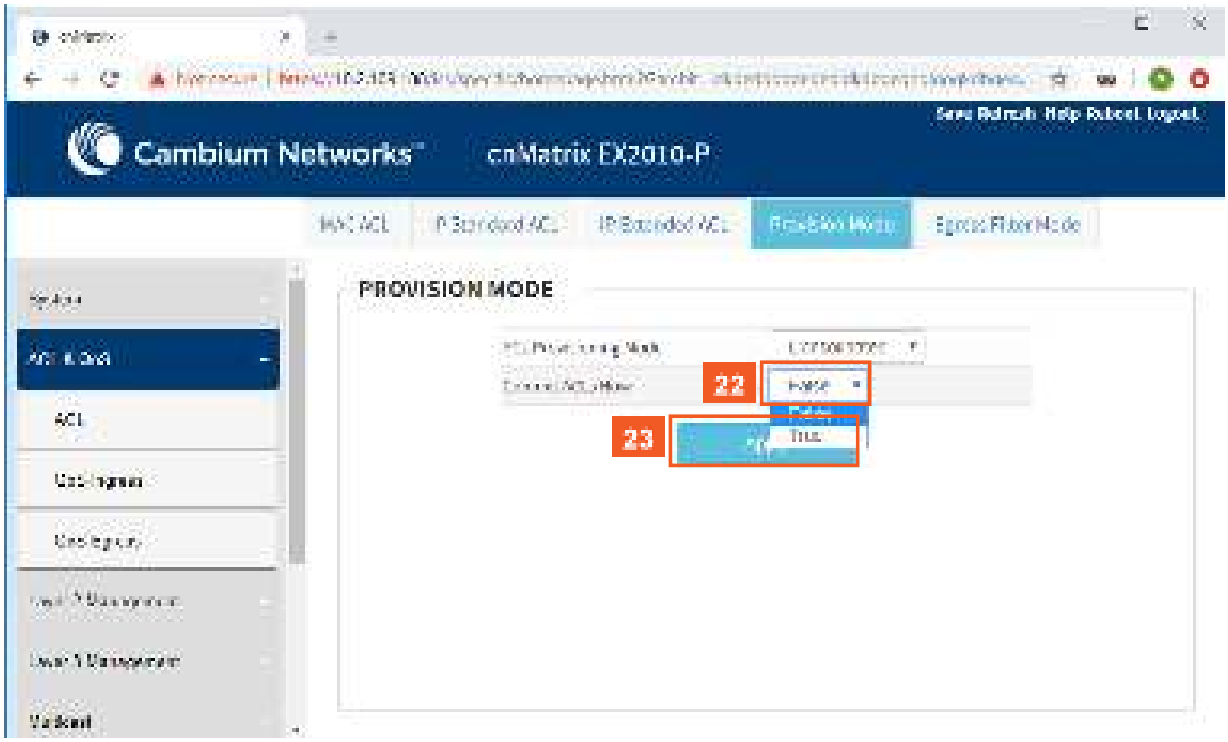


19 Click the **Provision Mode** tab.



20 Click the **ACL Provisioning Mode** drop-down list to select the commit support for which the access control rule needs to be applied. Select the **Consolidated** list item.

21 Click the **Commit ACLs Now** drop-down list to select the commit action to be taken for the access list.



22 Select the **True** list item to set the commit action.

23 Click the **Apply** button.

5.7 Static MAC

5.7.1 Managing Static MAC

The switch allows the user to configure a **static MAC** address and assign it to a specific VLAN ID and to a specific port. The MAC addresses configured in this manner are immune to automatic MAC address aging and migration.

Normally, with a dynamically learned MAC address, traffic that enters the switch through a different port than the one currently present in the mac-address-table will be forwarded, and the entry's port will be migrated to the new value.

Traffic that enters the switch through a port and has a source MAC address that is statically configured to a different port will be dropped, and its source address will not be migrated.

Standards

- IEEE 802.1q.

Scaling Numbers

- 256 static MAC addresses can be configured on the switch.

Limitations

- Only unicastMAC addresses can be configured using this switch.
- A valid entry in the mac-address-table is a MAC/VLAN id pair, and assigning the same pair to more than one port will cause the switch to retain only the value configured last.

Default Values

- The status of the static unicast entry is set to permanent by default.

Prerequisites

- The VLAN to which the MAC address is assigned must be already created at the time the static MAC is configured, or an error message will be displayed.

SNMP

- SNMP support is available via dot1qStaticUnicastEntry in Q-BRIDGE-MIB.

5.7.2 Configuring Static MAC in WEB Interface

The Static MAC feature is not available in WEB interface.

5.8 Local Management User Name and Password

5.8.1 Managing Locally Managed Username and Password

The CLI or Web interfaces can be accessed using locally configured user/password pair. By default, the switch has two users created with read-only and read-write rights.

Password complexity can be configured by setting the minimum number of lowercase, uppercase, numeric and symbols which are accepted.

Standards

- N/A

Scaling Numbers

- A maximum of 15 users are supported.

Limitations

- Only the **admin** user can create new users using this command.
- The **admin** user cannot be deleted.

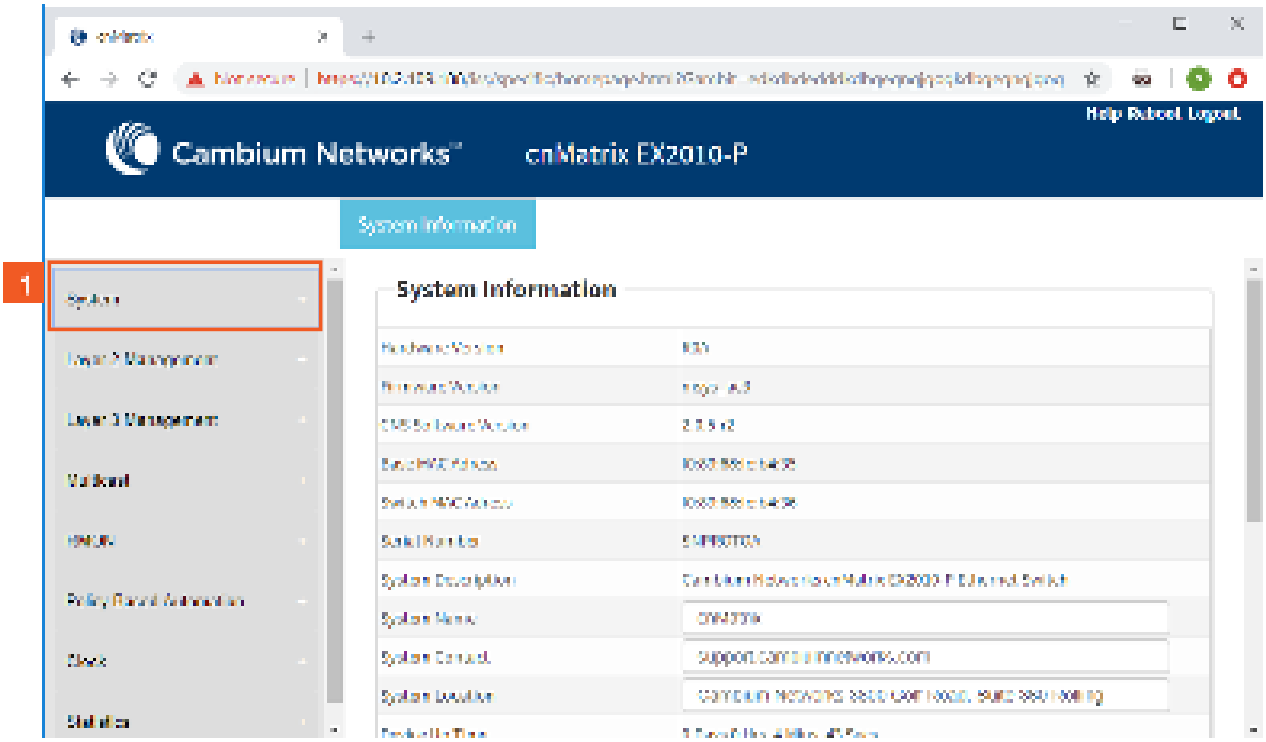
Default Values

- Two users are active by default: **admin** and **guest.**
- **admin** has root privileges (15) and can access configuration commands.
- **guest** user has lower privileges (1), which grant access only to **'clear', 'debug', 'ping'** and **'show'** commands.
- Password expiration: by default the max-life-time value is set to 0, which indicates that the password will not expire.

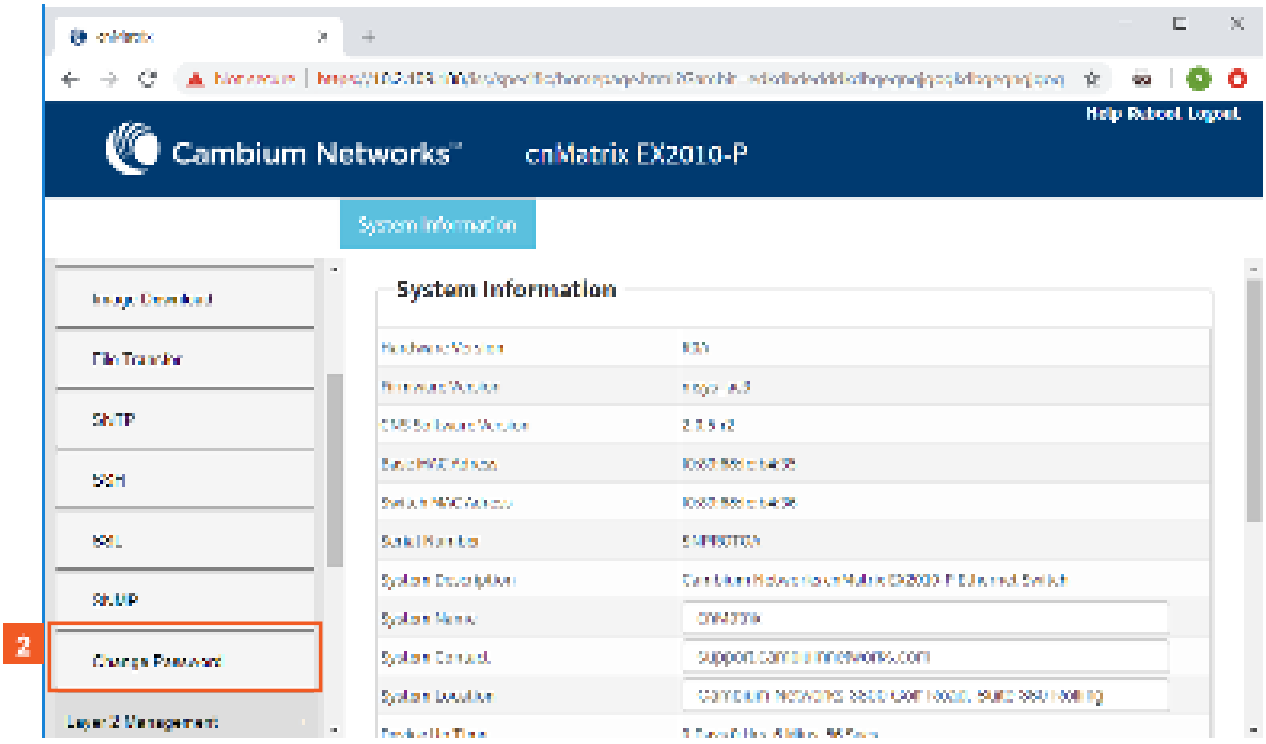
Prerequisites

- N/A

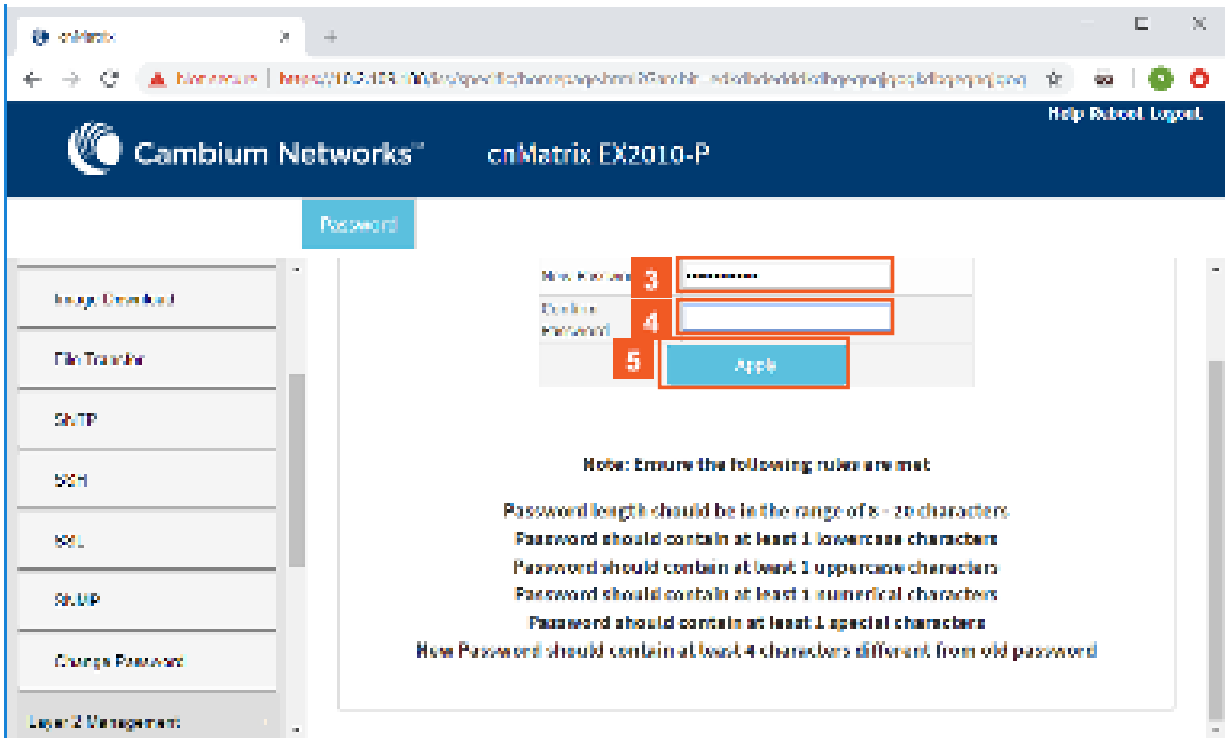
5.8.2 How to Change the Password in WEB Interface



1 Click the **System** tab.



2 Click the **Change Password** menu item.



3 Type **cnMatrix2019*** into the **New Password** field.

After your password is successfully changed, you will use the same password for WEB and CLI interfaces.

The password is case sensitive.

4 Type **cnMatrix2019*** into the **Confirm Password** field to confirm your new password.

5 Click the **Apply** button.

5.9 HTTPS

5.9.1 Managing HTTPS

5.9.1.1 Feature Description

The **cnMatrix HTTP** server works in such a way that it can be reached securely using TLS, or normally using the standard transport layer. A configuration option specifies whether HTTP or HTTPS is active.

SSL (Secure Sockets Layer), is a protocol developed for transmitting private information through an Internet connection. It works by using a public-private key mechanism to encrypt/decrypt data that is transferred over the SSL connection.

HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP for secure communication over an encrypted SSL/TLS connection.

Standards

- The cnMatrix SSL/TLS(IPv4/IPv6) feature is RFC 2246 compliant.

Scaling Numbers

- The maximum number of simultaneous HTTPS WebUI sessions is 4.
- The maximum number of HTTPS sessions supported is 10.

Limitations

- The SSL/TLS server is not compatible with Microsoft Edge and IE 10 browsers.
  - **Starting with version 2.1**, the SSL server is compatible with IE 11 and with Microsoft Edge version 41.16299.1004.0 on Windows 10.
- The crypto key pair that can be generated is either of 512 or of 1024 bits.
  - **Starting with version 2.1**, the default crypto pair that can be generated is of 2048 bits.

Default Values

- The SSL feature is enabled by default and uses a self-signed certificate.
- The default cipherssuite are: rsa-des-sha:rsa-3des-sha:rsa-exp1024-des-sha.
  - **Starting with version 2.1**, the default chipersuites are: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256**.**

Prerequisites

N/A

The cnMatrix SSL/TLS(IPv4/IPv6) feature provides Transport Layer Security as specified in RFC 2246 and is based on the SSL protocol specification supporting SSL 3.1, TLS v1.0 and starting with version 2.1, TLSv1.0, TLSv1.1 and TLSv1.2.

The TLS protocol is composed of two layers: a TLS Record Protocol and a TLS Handshake protocol The SSL server and the SSL client authenticate each other and negotiate encryption algorithm and cryptographic keys before the application transmits or receives data.

cnMatrix offers the capability of using a cnMatrix self-signed certificate or an external certificate given by the user. The external certificate has to be obtained from a certificate request generated on the cnMatrix switch.

The SSL/TLS server interoperates with SSL clients found in the following HTTP browsers:

- IE5 on Win98 and Win2000.
- IE6 on WinXP.
- Netscape7.0 on Win98.
- Netscape6.0 on RedHat-Linux 7.1.
- Google chrome version 70 on Win10.
- Mozilla Firefox version 52.7.2 on CentOS Linux release 7.4.

The TLS server supports the following:

- Algorithms :
  - Encryption Algorithms DES/3DES
  - Hash MD5/SHA
  - Key Negotiation can be done using RSA or Diffie-Hellman.
- Cipher suites:
  - TLS_RSA_WITH_NULL_MD5
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

    - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Port – the standard port used is 443.
- Fragmentation of information blocks into records carrying data in chunks of 2^14 or less.

The TLS server implementation does not support the following configuration:

- The optional compression capability of TLS Record Protocol is not supported due to the fact that the primary application of TLS for cnMatrix is for securing web based configuration in which the data transferred is relatively less.

Starting with version 2.1, the TLS server supports the following:

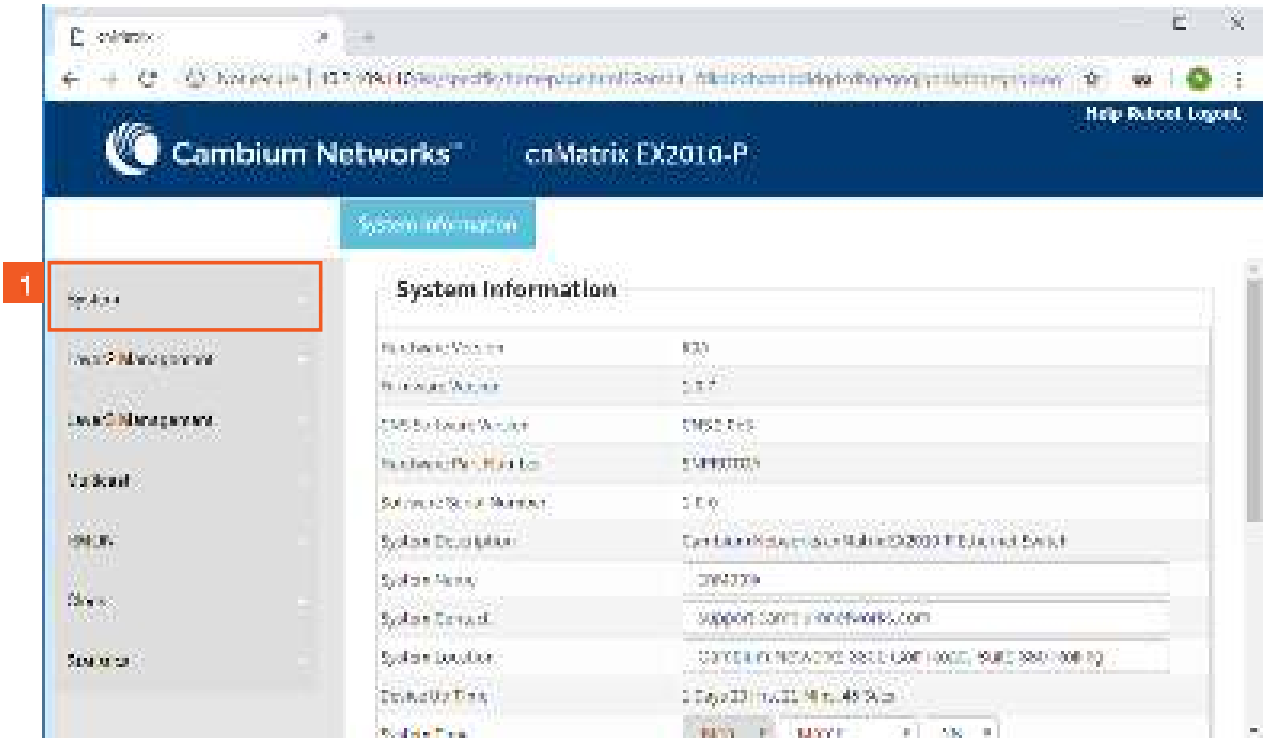
- Algorithms :
    - The key encryption algorithm : ECDHE.
    - The authentication algorithm: RSA.
    - The bulk encryption algorithms :AES128/256 either with or without the GCM mode, and CHACHA20 partnered with poly1350 mac algorithm.
    - The MAC algorithms: SHA256/384 or POLY1350 partnered with chacha20 encryption.
- Cipher suites:
    - TLS1_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS1_ECDHE_RSA_WITH_AES_128_SHA256
    - TLS1_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS1_ECDHE_RSA_WITH_AES_256_SHA384
    - TLS1_ECDHE_RSA_WITH_CHACHA20_POLY1305

The SSL functionality in cnMatrix is implemented using the open source software from http://www.openssl.org, which include software written by Eric A. Young and Tim J. Hudson. All copyrights listed at http://www.openssl.org/ apply. With respect to licensing terms, the same 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.

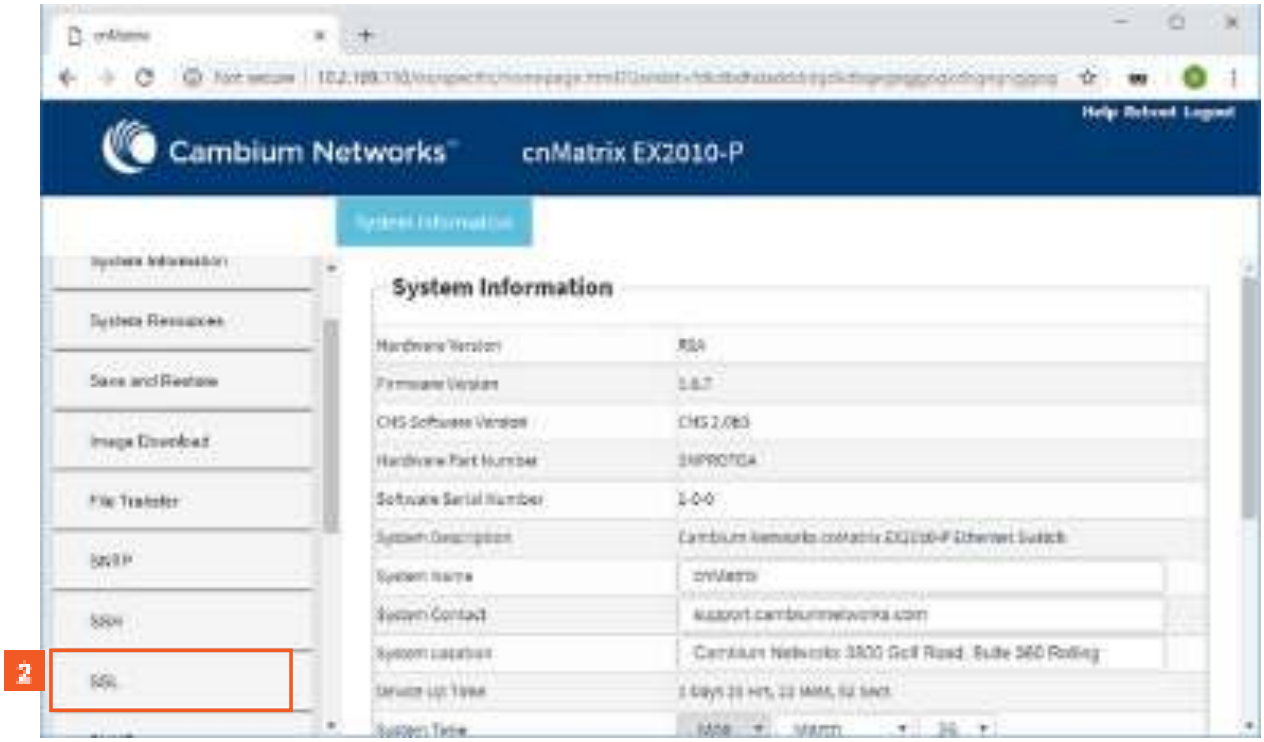
Starting with version 2.1:

5.9.1.2 Network Diagram

5.9.2 How to Enable HTTPS in WEB Interface

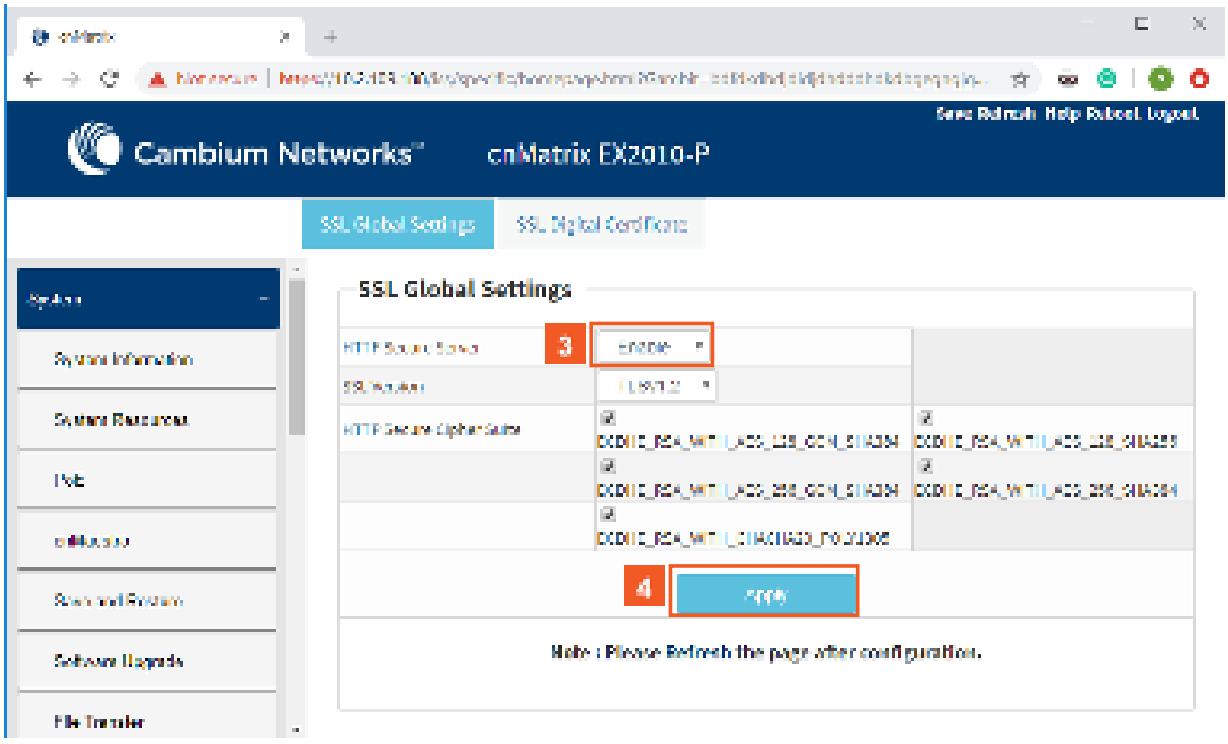


1 Click the **System** tab.



2 Click the **SSL** menu item.

3 Click the **HTTP Secure Server** drop-down list to select the status of the HTTP secure server. Select the **Enable** list item to enable the HTTP secure server



4 Click the **Apply** button.

5.10HTTP

5.10.1Managing HTTP

5.10.1.1 FeatureDescription

The **Hypertext Transfer Protocol** (HTTP) is an application protocol used in the implementation of the cnMatrix WEB user interface.

The cnMatrix switch includes an implementation of the HTTP server that implements the HTTP protocol version 1.1. This implementation is a subset of the HTTP 1.1 specification optimized for embedded systems, and is not a complete implementation of the full HTTP 1.1 specification.

The HTTP server in the software maintains persistent connections with clients over both Ipv4 and Ipv6 addresses, over TCP and over SSL. After the server processes a request from the client, the server immediately closes the socket connection unless the client had sent a KEEP_ALIVE header or indicated the content-type as MULTIPART in its request, if the version of the client is less than 1.1. If the version of the client is 1.1 or greater the server does not close the socket connection immediately. This allows the same socket connection to be reused for serving all the requests from the client. Thus, resulting in better WebUI management performance. The connection is closed if the server receives a close connection token in the request, or if there is no activity on the connection for more than 5 minutes, or if any network or client failure is suspected. In the last case, the server also sends a message with the connection header containing a close connection token.

The HTTP server allows further requests to come from the same client, while processing one request from the client.

The server buffers the requests and dispatches the requests to other internal managed modules in the same order in which the requests arrived.

The server collects the status of the requests and sends responses to the client in the same order in which the requests arrived.

A browser that supports pipelining can take advantage of this capability to reduce the latency associated with multiple requests. The server implements the expiration model and the validation model to allow clients to cache web pages.

All the WebUI management pages implemented for managing features in the cnMatrix, are statically compiled into the cnMatrix image. This allows the client to specify an absolute URL (for example, GET http://www.host.com/path.file.html). The server accepts this and looks for such a file on the file system in the switch. If present, the file is then returned.

The server parses the requests from the clients to find out the character set used in the requests. If the server does not support the requested character set, the server returns an error message to the client. The server also parses the Transfer Encoding header field in the requests from the clients. If the Transfer Encoding is chunked, the server extracts data from the request message depending upon the size of the chunk. A 501 (Unimplemented) error code is returned and the connection is closed, if it receives an entity body with the Transfer Encoding that it does not understand. The response headers are composed of the following:

- HTTP version – 1.1;
- Date header including current time in the form of Greenwich Mean Time;
- Delta seconds (the number of seconds elapsed after receiving the request message from the client);
- Character sets supported – Accept-charset:iso-8859-1;
- Content coding – Used to support compression.
- Connection field – Indicates whether a connection is persistent or will be closed.
- Content length
- Entity tag – Provided for all separate entities send in the response messages.
- Internet Media Types in the Content-Type and Accept header fields.
- Language tags

- Access Authentication field
- Authorization field

The server provides the following response codes:100 (Continue); 200 (OK) ; 202(Accepted);304(Not Modified) ;405(Method Not Allowed); 406(Not Acceptable); 414 (Request-URI Too Long);413(Request Entity Too Large) ;411 (Length Required); 415(Unsupported Media Type; 505(HTTP Version Not Supported).

The HTTP server implementation supports an Authentication Framework that provides three authentication mechanisms:

- DEFAULT - This is a Form-Based proprietary authentication scheme used by the software to authenticate the HTTP clients. In it the client trying to access the Web UI will be presented a Login Page where the user has to enter the Credentials and Submit. The user is allowed access to the Web UI upon successful authentication of the credentials. This is the default authentication scheme used by the software.
- BASIC - This is an HTTP Authentication scheme where the client must authenticate itself with a user-ID and a password for a realm. The HTTP server provides a single protection space called the cnMatrix protection space and a single realm namely “cnMatrix” which corresponds to the software’s protection space. The protection space contains all the web pages of the cnMatrix server. The HTTP server will service the request only if it can validate the user-ID and password for the cnMatrix protection space.
- DIGESTS - This is an HTTP Authentication scheme where the HTTP server challenges the HTTP client using a WWWAuthenticate header containing a nonce value. A valid Authorization request from the client contains a checksum (the MD5 checksum) of the username, the password, the given nonce value, the HTTP method and the requested URI. In response to the Authorization request, the server sends an Authentication-Info header to communicate the status of the authentication attempt. The Authentication framework of the software provides two parameters:
  - Operational Authentication Scheme - governs the scheme to be used to authenticate all the HTTP sessions. This is a READ-ONLY parameter which is initialized at software startup time.
  - Configurable Authentication scheme contains the scheme which can be modified at 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

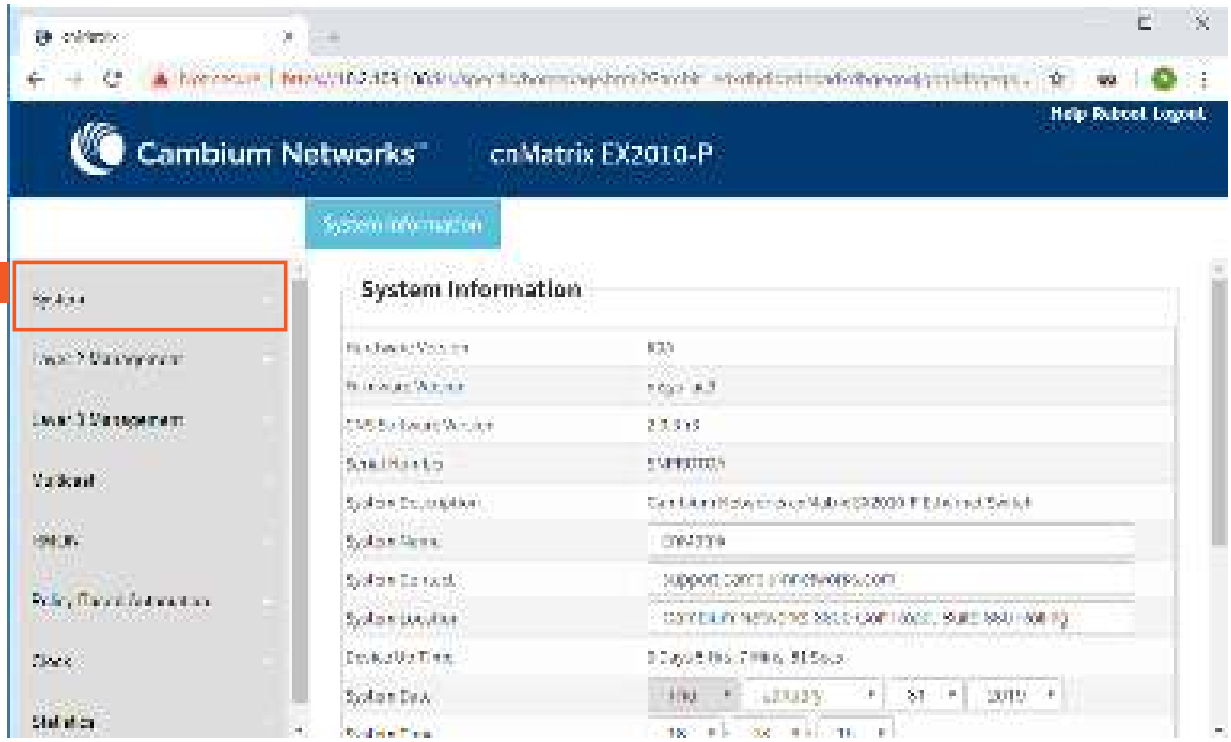
- The HTTP server supports maximum 4 HTTP WEB UI sessions opened simultaneously.

Default Values

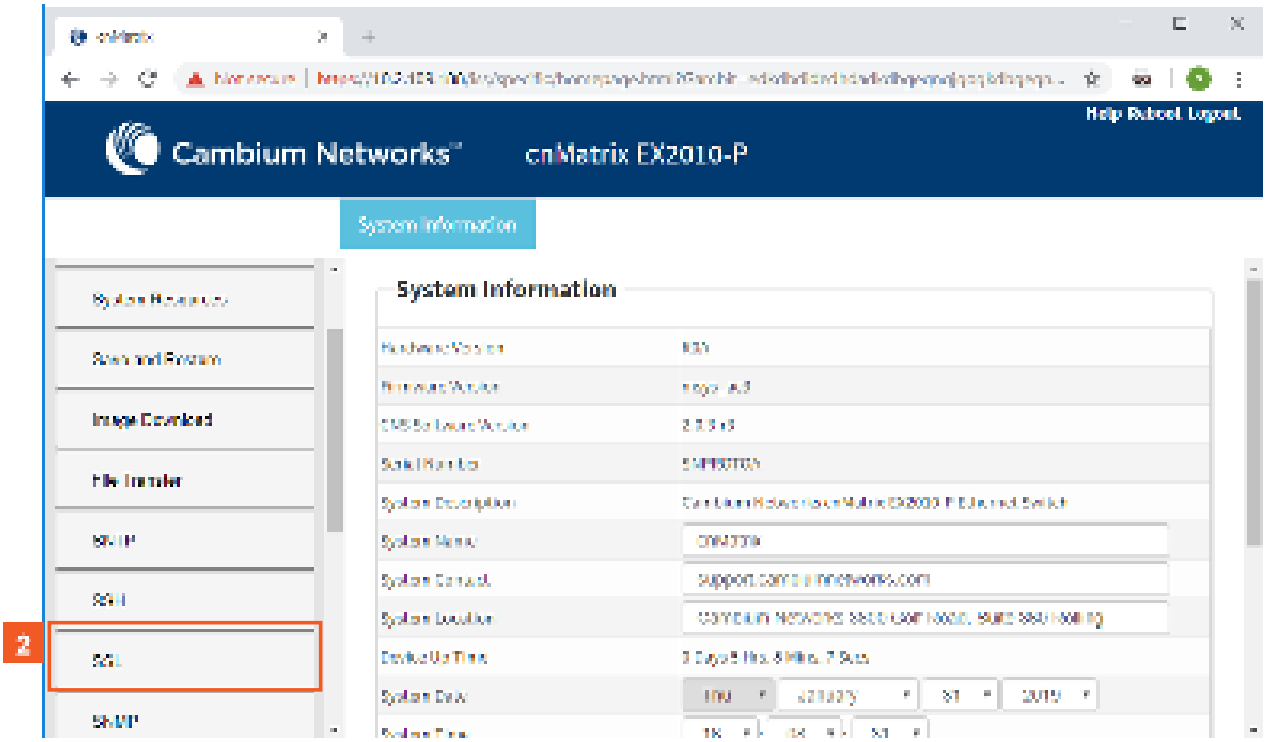
- The default authentication scheme: default.
- The HTTP redirection option is disabled by default.
- The default HTTP port: 80.
- HTTP is disabled by default in the switch.

5.10.1.2 Network Diagram

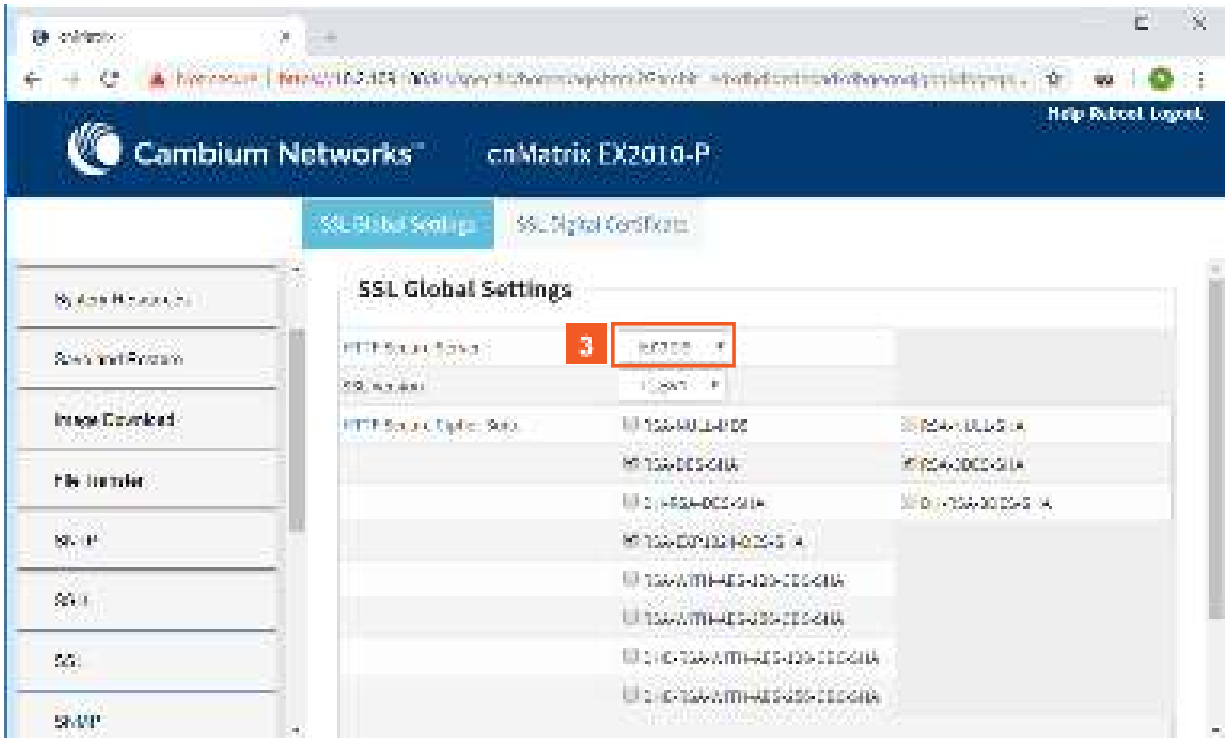
5.10.2 How to Enable HTTP in WEB Interface



1 Click the **System** tab.

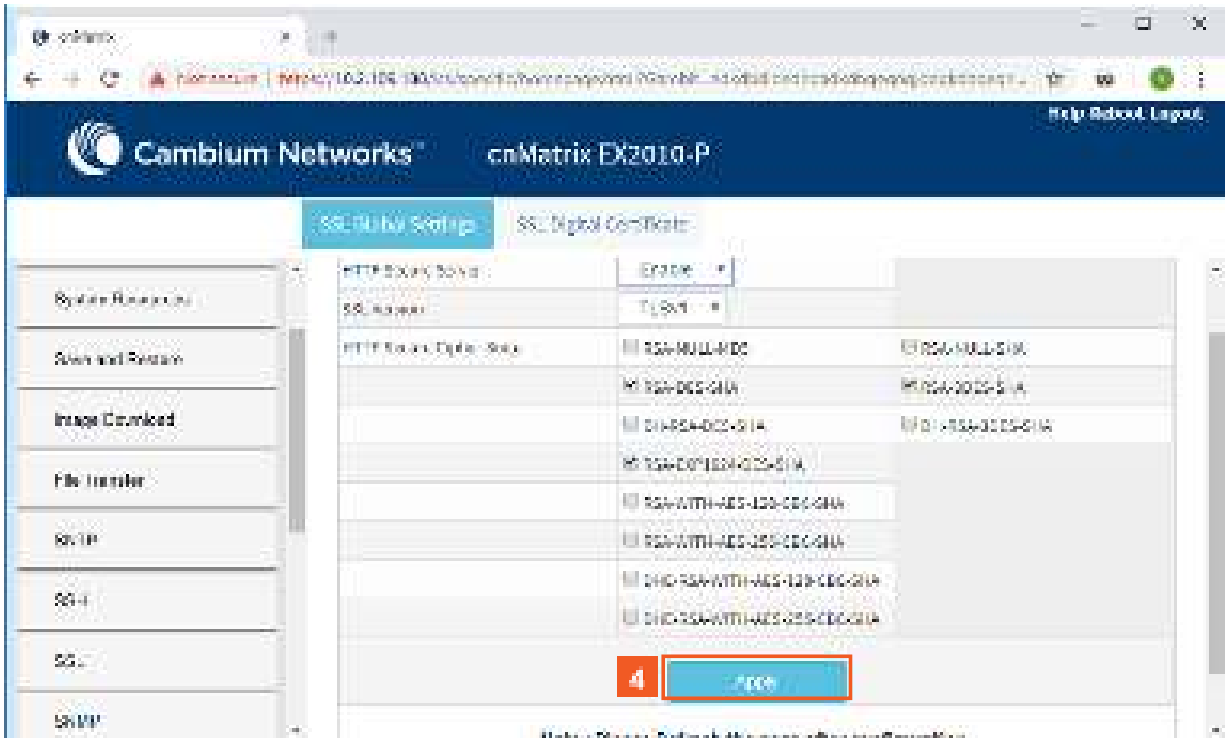


2 Click the **SSL** menu item. The **SSL Global Settings** window is displayed.

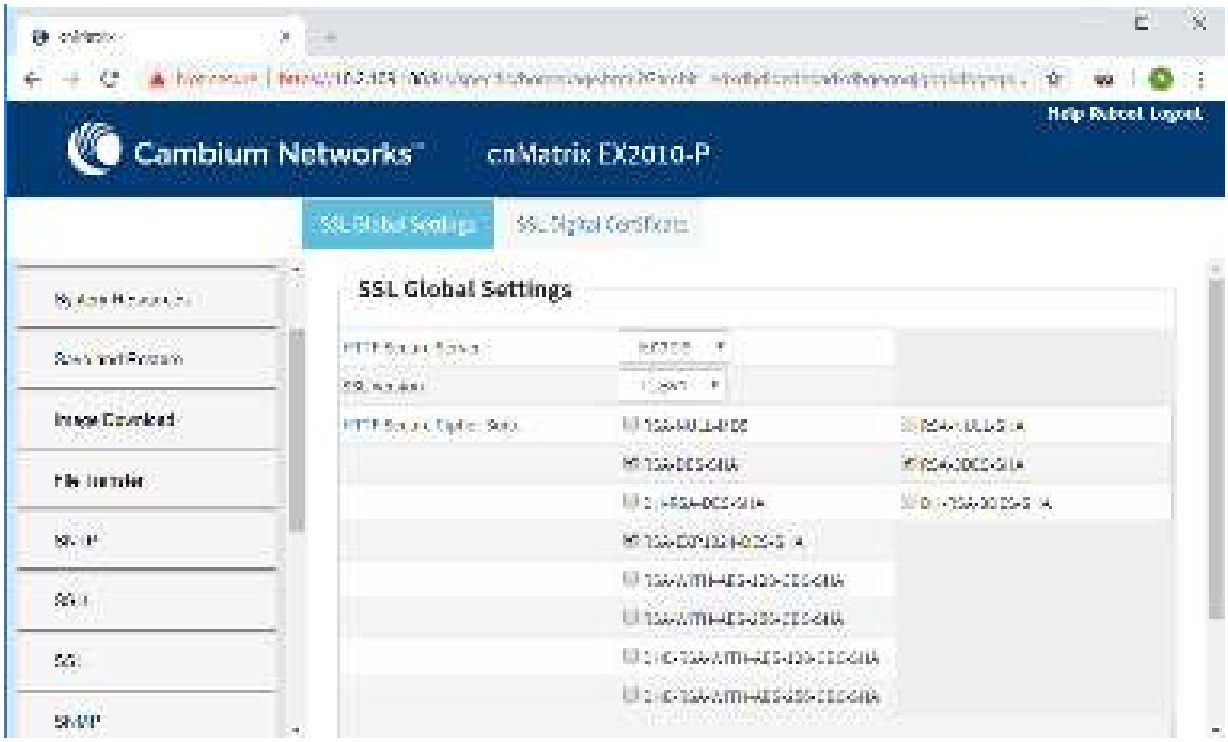


3 Click the **HTTP Secure Server** drop-down list and select the **Disabled** option.

The **Disabled** option represents the status of the HTTP secure server.



4 Click the **Apply** button.



5.11802.1x Authentication

5.11.1Managing 802.1x Authentication

The **802.1X** feature enables network devices authentication on the switch and prevents unauthorized devices from accessing the services provided by the Switch and LAN.

The cnMatrix switch controls physical access to the network based on the authorization status of Client devices. It requests the credentials (Identity and Password) of the Client and submits it to the Authentication Server (RADIUS). In addition, the

cnMatrix switch acts as a RADIUS client and is responsible for encapsulating and decapsulating the EAP frames to interact with the RADIUS server.

The following host modes are available:

- single-host
- multi-host

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

Standards

- IEEE 802.1X
- RFC 2865

Scaling Numbers

- N/A

Limitations

- N/A

Default Values

- 802.1X is disabled by default.
- 802.1X per port Authentication Mode is set to Multi-Host by default.

Prerequisites

- N/A

5.11.2 Configuring 802.1x Authentication in WEB Interface

The 802.1x Authentication feature is not available in WEB Interface.

6 Regulatory and Compliance

6.1 Legal and Regulatory Information

6.1.1 Legal and Reference Information

6.1.1.1 Introduction

This chapter provides legal notices including software license agreements.

Attention

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

The following topics are described in this chapter:

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

6.1.2 Cambium Networks End User License Agreement

6.1.2.1 Introduction

ACCEPTANCE OF THIS AGREEMENT

In connection with Cambium Networks' delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium Networks is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement ("Agreement"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT ORINSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCTTO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUTNOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

DEFINITIONS

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Cambium Networks' fixed wireless broadband devices for which the Software and Documentation is licensed for use.

GRANT OF LICENSE

Cambium Networks Limited ("Cambium") grants you ("Licensee" or "you") a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in "Conditions of use" and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

CONDITIONS OF USE

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.
2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.
3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.
4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for backup purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium Networks copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.
5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

TITLE AND RESTRICTIONS

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium Networks and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this

Agreement will result in automatic termination of this license.

CONFIDENTIALITY

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will

result in irreparable harm to Cambium Networks for which monetary damages would be inadequate and for which Cambium Networks will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the

confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care. You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium Networks prior to such disclosure and provide Cambium Networks with a reasonable opportunity to respond.

RIGHT TO USE CAMBIUM'S NAME

Except as required in "Conditions of use", you will not, during the term of this Agreement or thereafter, use any trademark of Cambium Networks, or any word or symbol likely to be confused with any Cambium Networks trademark, either alone or in any combination with another word or words.

TRANSFER

The Software and Documentation may not be transferred to another party without the express written consent of Cambium Networks, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

UPDATES

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An "Update" means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium Networks makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

MAINTENANCE

Except as provided above, Cambium Networks is not responsible for maintenance or field service

of the Software under this Agreement.

DISCLAIMER

CAMBIUM NETWORKS DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM NETWORKS SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS." CAMBIUM NETWORKS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM NETWORKS MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

LIMITATION OF LIABILITY

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING,

WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of

incidental or consequential damages, so the above exclusion or limitation may not apply to you.)

IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

U.S. GOVERNMENT

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or

disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

TERM OF LICENSE

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium Networks in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium

Networks, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

GOVERNING LAW

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

ASSIGNMENT

This agreement may not be assigned by you without Cambium's prior written consent.

SURVIVAL OF PROVISIONS

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

ENTIRE AGREEMENT

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium Networks may modify this Agreement as necessary to comply with applicable laws.

THIRD PARTY SOFTWARE

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

6.1.3 Source Code

6.1.3.1 Source Code

OpenSSL 1.1.0	OpenSSL License ==========

	Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ========== This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). Original SSLeay License ---------- Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be

	given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Libwebsockets v1.3-chrome37-firefox30	Copyright (C) 2010-2014 Andy Green andy@warmcat.com Libwebsockets and included programs are provided under the terms of the GNU Library General Public License (LGPL) 2.1 (available in Appendix A), with the following exceptions: 1) Static linking of programs with the libwebsockets library does not constitute a derivative work and does not require the author to provide source code for the program, use the shared libwebsockets libraries, or link their program against a user-supplied version of libwebsockets. If you link the program to a modified version of libwebsockets, then the changes to libwebsockets must be provided under the terms of the LGPL in sections 1, 2, and 4. 2) You do not have to provide a copy of the libwebsockets license with programs that are linked to the libwebsockets library, nor do you have to identify the libwebsockets license in your program or documentation as required by section 6 of the LGPL. However, programs must still identify their use of libwebsockets. The following example statement can be included in user documentation to satisfy this requirement: "[program] is based in part on the work of the libwebsockets project (http://libwebsockets.org)"

Jansson 2.11	Copyright (c) 2009-2016 Petri Lehtinen

	<petri@digip.org> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Zlib 1.2.11	(C) 1995-2017 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any 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 licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.

Open SSH 5.1	1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name 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 licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto";.

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR 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.

2)
The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>
<">http://www.core-sdi.com>;

3)
ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4)
The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)
One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)
Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjölä
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42):

<phk@login.dknet.dk> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995
This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the

openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] Preamble The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below. When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things. To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

	For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights. We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library. To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others. Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license. Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs. When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library. We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances. For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

	Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library. The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you". A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".) "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does. 1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee. 2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.
This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.
If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.
You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies

the executable.
It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original

copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.
NO WARRANTY
15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES 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!

6.1.4 Hardware Warranty

Hardware Warranty

cnMatrix™ switch family (“Covered Product”) hardware is covered with a 5 - year Limited Lifetime Warranty. “Lifetime” is defined as the period beginning on the date of original purchase by the first end user of the Product and ending five (5) years thereafter. Under this Limited Lifetime Warranty, Cambium warrants to its end users for the Lifetime (as defined) that the Covered Product purchased by such end user, when used under normal conditions and consistent with applicable Covered Product documentation supplied with the Covered Product, will be free from defects in material and workmanship, and will perform in accordance with the documentation supplied for such Covered Product.

Except as otherwise prescribed by applicable law, in the event of a breach of this Hardware Limited Lifetime Warranty, the sole and exclusive remedy, and Cambium’s sole and exclusive liability, will be for Cambium to use commercially reasonable efforts to repair or replace the Covered Product that caused the breach of this warranty. If Cambium cannot, or determines that it is not practical to, repair or replace the Covered Product, then the sole and exclusive remedy and the limit of Cambium’s obligation will be to refund the amount received by Cambium for purchase of such Covered Product. The Hardware Limited Lifetime Warranty is provided to the original end user only and is not transferrable.

6.1.5 LIMITATION OF LIABILITY

LIMITATION OF LIABILITY

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING,
WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.)

IN NO CASE SHALL CAMBIUM’S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT

6.1.6 Compliance with Safety Standards

Intended Use: The Cambium Networks cnMatrix next-generation switching platform offers a cloud-managed, high-performance, feature-rich enterprise-grade ethernet switching solution. This equipment is intended for professional applications for fixed indoor installations only.

Installation and Operation: Installation and operation of this product are complex and Cambium Networks therefore recommends professional installation and management of the system. Please follow the instructions in this leaflet. Further

guidance on cnMatrix installation and operation is available in the accompanying *Quick Start Guide*, which can also be found online at the link below

The installer must have sufficient skills, knowledge, and experience to perform the installation task and is responsible for:

- Familiarity with current applicable national regulations, including electrical installation and surge protection
- Installation in accordance with Cambium Networks' instructions

Product Safety Information:

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product *User Guide, web link below,* for more details. Please observe the following safety rules:

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e., touch grounded bare metal) before touching the product. Ensure that the product is properly grounded.

Ensure that the equipment is not powered during installation. Always disconnect equipment from its power source before servicing.

Always use a qualified electrician to install cabling.

Use outdoor-rated cables for connections that will be exposed to the outdoor environment.

Operation in the EU – Restrictions:

- This equipment is for indoor use only.
- CE EMI Class A Warning: This equipment is compliant with Class A of CISPR32. In a residential environment, this equipment may cause radio interference.

Waste Electrical and Electronic Equipment (WEEE) Directive:

Please do not dispose of electronic and electric equipment or electronic and electric accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. If you reside in European Union countries, please contact your local equipment supplier representative or the Cambium Networks Support Center for information about the waste collection system in your country

Useful Web Links:

- User Guide: https://www.cambiumnetworks.com/guides
- Technical Training: https://learning.cambiumnetworks.com
- Cambium Support Center: https://support.cambiumnetworks.com/
- EU Declaration of Conformity: http://www.cambiumnetworks.com/eu_dofc

Equipment Manufacturer:

Cambium Networks Ltd, Unit B2 Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP, United Kingdom

7 Appendix: Parameters and Commands

7.1 Appendix: Parameters and Commands

7.1.1 LLDP-MED Parameters and Commands

7.1.1.1 LLDP-MED

Commands	Description	**CLI Mode**
lldp med-tlv-select { med-capability | networkpolicy | inventory-management | location-id | expower-via-	Enables thetransmission of aspecific LLDP-MEDTLV on a given port.	Interface Configuration

mdi } [mac-address] Available options: med-capability ■ Configures the Med Capability TLVtransmission for the LLDP module. network-policy - Configures the Network-policy ■ TLVrelated transmission for the LLDP module. inventory-management - Configures the Inventorymanagement ■ TLV related transmission for the LLDPmodule. location-id ■ Configures the Location identificationTLV related transmission for the LLDP module. ex-power-via-mdi ■ Configures the Extended power viaMDI TLV related transmission for the LLDP module. mac-address ■ Configures the basic TLVtransmission to use the MAC address as destination MACaddress by the LLDP agent on the specified switch port.		
lldp med-location elin-location location-id Available options: location-id ■ Configures the location identification	Configures theEmergency LocationInformation Number(ELIN) location subtypeinformation advertisedby the endpoint	Interface Configuration
lldp med-app-type {voice | voiceSignaling |guestVoice | guestVoiceSignaling | softPhoneVoice| videoconferencing | streamingVideo |videoSignaling} {vlan {untagged | vlan-id priority } dscp | none} Available options: voice ■ Sets the Network-policy TLV as VoiceApplication for indicating that the media type defining aprimary function of the application for the policy advertisedon the local port is voice. voiceSignaling ■ Sets the Network-policy TLV asVoiceSignaling Application for indicating that the mediatype defining a primary function of the application for thepolicy advertised on the local port is VoiceSignaling. guestVoice ■ Sets the Network-policy TLV asguestVoice Application for indicating that the media	Enables the propertiesof Network-policy TLV	Interface Configuration

typedefining a primary function of the application for the policyadvertised on the local port is guestVoice.

`guestVoiceSignaling`

- Sets the Network-policy TLVas guestVoiceSignaling Application for indicating that themedia type defining a primary function of the applicationfor the policy advertised on the local port isguestVoiceSignaling

`softPhoneVoice`

- Sets the Network-policy TLV assoftPhoneVoice Application for indicating that the mediatype defining a primary function of the application for thepolicy advertised on the local port is softPhoneVoice.

`videoconferencing`

- Sets the Network-policy TLV asvideoconferencing Application for indicating that the mediatype defining a primary function of the application for thepolicy advertised on the local port is videoconferencing

`streamingVideo`

- Configures the location identificationEnables the propertiesof Network-policy TLVInterfaceConfigurationLLDP-MED Parameters and Commands2

`videoSignaling`

- Sets the Network-policy TLV asvideoSignaling Application for indicating that the mediatype defining a primary function of the application for thepolicy advertised on the local port is videoSignaling.

`vlan`

- Configures the advertised VLAN properties.Options are:
  - untagged - Configures the ports that should beused for the VLAN to transmit egress packets asuntagged packets
  - priority - Configures the priority value forthe VLAN
  - vlan-id - VLAN ID is a unique value thatrepresents the specific VLAN

`dscp`

- Sets the DSCP value

`none`

- Sets the MED policy unknown flag, causing theswitch not to advertise this policy

7.1.2 Save Restore Erase Download Configurations Parameters and Commands in CLI

7.1.2.1 Introduction

Commands	Description	CLI Mode
write { flash:filename | startup-config |tftp://server/filename | sftp://<user-name>:<pass-word>@server/filename} Available options: flash:filename ■ Configures the name of the file to whichthe configuration is to be saved. This file is present in theflash. startup-config ■ Starts the switch with the savedconfiguration on reboot. tftp ■ Configures the TFTP related details for writing theconfiguration to a file in TFTP server. server ■ The IP address or host name of the server inwhich configuration should be maintained. filename ■ The name of the file in which theconfiguration should be written. sftp ■ Configures the SFTP related details for writing theconfiguration to a file in SFTP server. user-name ■ The user name of remote host or server. pass-word ■ The password for the corresponding username of remote host or server. server ■ The IP address or host name of the server inwhich configuration should be maintained. filename ■ The name of the file in which theconfiguration should be written.	This command writes the running-config to a flash file, startup configuration file or to a remote site.	Privileged EXEC Mode
copy { tftp://server/filename startup-config | sftp://<user-name>:<pass-word>@server/filename startup-config |	This command copies the configuration from a remote site to flash.	Privileged EXEC Mode

flash: filename} startup-config Available options: tftp://server/filename startup-config ■ Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details. sftp://<user-name>:<pass-word>@server/filename ■ Configures the name of the file in remote location to be copied (downloaded) into configuration file. This option configures the SFTP server details. flash: filename startup-config ■ Configures the name of the file in flash. The configuration in the flash file are used.		
copy running-config startup-config	This command copies the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the switch and the startup config is the configuration that is loaded when the router boots up.	Privileged EXEC Mode
copy startup-config {flash: filename | tftp://server/filename | sftp://<user-name>:<password>@ server/filename} Available options: flash: filename ■ Configures the name of the file in which the initial configuration should be stored. This file is available in the Flash. tftp://server/filename ■ Configures the TFTP details for taking back up of initial configuration in TFTP server. server ■ The IP address or host name of the server. filename ■ The name of the file in which the initial configuration should be stored. sftp://<user-name>:<password>@ server/filename ■ Configures the SFTP details for taking back up of initial configuration in SFTP server.	This command takes a backup of the initial configuration in flash to a remote location.	Privileged EXEC Mode

user-name ■ The user name of remote host or server. pass-word ■ The password for the corresponding user name of remote host or server. server ■ The IP address or host name of the server. filename ■ The name of the file in which the initial configuration should be stored.		
incremental-save { enable | disable } Available options: enable ■ Enables the incremental save feature. disable ■ Disables the incremental save feature.	Enables/Disables the auto save trigger function feature.	GlobalConfiguration
auto-save trigger { enable | disable } Available options: enable ■ Enables the auto save trigger function. disable ■ Disables the auto save trigger function.	Enables/Disables the auto save trigger function feature.	GlobalConfiguration
config-restore {flash | norestore} Available options: flash ■ Enables configuration restore from flash start-up configuration file. norestore ■ Specifies that the switch configurations need not be restored when the system is restarted.	Configures the startup configuration restore option.	Privileged EXEC Mode
erase startup-config	Clears the startup configuration file.	Privileged EXEC Mode
show nvram	Displays the current information stored in the NVRAM.	Privileged EXEC Mode
show system information	Displays the system information.	Privileged EXEC Mode
clear config[default-config-restore	All configurations will be cleared and default configurations will	Privileged EXEC Mode

<filename>]	berestored.	

7.1.3 Auto Attach Parameters and Commands

7.1.3.1 Auto Attach Parameters and Commands

Commands	Description	CLI Mode
debug auto-attach [trace { error | warning | info | debug }] [dump { rule | action | policy | prec | ifc }]	Enables debug options for the Auto-Attach module.	Privileged EXEC
no debug auto-attach	Disable trace option for the Auto-Attach module.	Privileged EXEC
no debug auto-attach	Displays Auto-Attach global configuration details.	Privileged EXEC
show auto-attach interface [<iftype> <ifnum>]	Displays Auto-Attach per-interface configuration details.	Privileged EXEC
show auto-attach action [name <string(20)>]	Displays Auto-Attach per-interface configuration details.	Privileged EXEC
show auto-attach rule [name <string(20)>]	Displays Auto-Attach per-interface configuration details.	Privileged EXEC
show auto-attach policy [name <string(20)>] [{detail | interface | statistics}]	Displays Auto-Attach per-interface configuration details.	Privileged EXEC
show auto-attach script [{cnPilot}]	Displays Auto-Attach per-interface configuration details.	Privileged EXEC

Commands	Description	CLI Mode
auto-attach	Enables Auto-Attach on the system.	Global Configuration
no auto-attach	Disables Auto-Attach on the system.	Global Configuration
auto-attach default	Resets all Auto-Attach settings to default values.	Global Configuration
auto-attach string-comparison { casesensitive | ignore-case } Available options: case-sensitive ■ Perform case-sensitive device data comparisons. ignore-case ■ Ignore case for device data	Configures the device data string comparison mode.	Global Configuration

comparisons.		
auto-attach action <action-name(20)> ([vlan <vlan-list(99)>] [pvid <vlan(1-4094)>] [switch-port-mode hybrid]) Available options: <action-name(20)> ■ Unique action set name. vlan ■ Specify list of VLANs. <vlan-list(99)> ■ List of 1..20 commaseparated VLANs. pvid ■ Specify default port VLAN. <vlan> ■ Default VLAN from VLAN list. switch-port-mode ■ Update switch port mode for the interface. hybrid ■ Update switch port mode to Hybrid.	Configures Auto-Attach action entries.	Global Configuration
no auto-attach action <string(20)>	Deletes Auto-Attach action entries	Global Configuration
auto-attach rule <string(20)> { LLDP-ANY | LLDP-CAP | LLDP-SYS-NAME | LLDP-SYS-DESC | LLDP-CHASSIS | LLDP-PORT | LLDP-PORT-DESC } <string(60)> Available options: <rule-name(20)> ■ Unique rule name. LLDP-ANY ■ Search multiple LLDP TLVs for device ID data. LLDP-CAP ■ Match LLDP Capabilities TLV data (comma-separated combination of 'bridge', 'wlan', 'router', 'phone', 'station', 'repeater', 'docsis', 'other').	Configures Auto-Attach rule entries.	Global Configuration

LLDP-SYS-NAME ■ Search LLDP System Name TLV for device ID data. LLDP-SYS-DESC ■ Search LLDP System Description TLV for device ID data. LLDP-CHASSIS ■ Search LLDP Chassis ID TLV for device ID data. LLDP-PORT ■ Search LLDP Port ID TLV for device ID data. LLDP-PORT-DESC ■ Search LLDP Port Description TLV for device ID data. <device-desc(60)> ■ Target device identification data.		
no auto-attach rule <rule-name(20)>	Deletes Auto-Attach rule entries.	Global Configuration
auto-attach policy <string(20)> match { rule <string(20)> | { LLDP-ANY | LLDP-CAP | LLDP-SYS-NAME | LLDP-SYS-DESC | LLDP-CHASSIS | LLDP-PORT | LLDP-PORT-DESC } <string(60)> } set { action <string(20)> | vlan <string(99)> [pvid <integer(1-4094)>] [switch-port-mode hybrid] | switch-port-mode hybrid } [precedence <integer(1-100)>] [{ enable | disable }] Available options: policy ■ Configure Auto-Attach policy data. <policy-name(20)> ■ Unique policy name. match ■ Specify device match criteria. rule ■ Specify rule table entry. <rule-name(20)> ■ Unique rule name. LLDP-ANY ■ Search multiple LLDP TLVs for device ID data.	Configures Auto-Attach policy entries.	Global Configuration

LLDP-CAP ■ Match LLDP Capabilities TLV data (comma-separated combination of 'bridge', 'wlan', 'router', 'phone', 'station', 'repeater', 'docsis', 'other'). LLDP-SYS-NAME ■ Search LLDP System Name TLV for device ID data. LLDP-SYS-DESC ■ Search LLDP System Description TLV for device ID data. LLDP-CHASSIS ■ Search LLDP Chassis ID TLV for device ID data. LLDP-PORT ■ Search LLDP Port ID TLV for device ID data. LLDP-PORT-DESC ■ Search LLDP Port Description TLV for device ID data. <device-desc(60)> ■ Target device identification data. set ■ Specify action criteria. action ■ Specify action table entry. <action-name(20)> ■ Unique action name vlan ■ Specify list of VLANs. <vlan-list(99)> ■ List of 1..20 commaseparated VLANs. pvid ■ Specify default port VLAN. <vlan> ■ Default VLAN from VLAN list. switch-port-mode ■ Update switch port mode for the interface. switch-port-mode ■ Update switch port mode for the interface. hybrid ■ Update switch port mode to Hybrid.		

precedence ■ Policy precedence value. <value(1-100)> ■ Precedence. enable ■ Enable policy. disable ■ Disable policy		
auto-attach policy <string(20)> ([precedence <integer(1-100)>] [{ enable | disable }]) Available options: <policy-name(20)> ■ Unique policy name. precedence ■ Policy precedence value. <value(1-100)> ■ Precedence. enable ■ Enable policy. disable ■ Disable policy.	Updates Auto-Attach policy information.	Global Configuration
no auto-attach policy <string(20)>	Deletes Auto-Attach policy entries.	Global Configuration
clear auto-attach policy statistics [<string(20)>] Available options: <policy-name(20)> ■ Unique policy name	Clears Auto-Attach policy-related statistics.	Global Configuration
auto-attach script {cnPilot} vlan <vlanlist(99)> [pvid <vlan(1-4094)>] Available options: cnPilot ■ Configure cnPilot device detection.	Creates Auto-Attach device script configuration.	Global Configuration

vlan ■ Specify list of VLANs. <vlan-list(99)> ■ List of 1..20 commaseparated VLANs. pvid ■ Specify default port VLAN. <vlan> ■ Default VLAN from VLAN list.		
no auto-attach script {cnPilot}	Deletes Auto-Attach script configuration data.	Global Configuration

Commands	Description	CLI Mode
auto-attach	Enables Auto-Attach on the target interface.	Interface Configuration
no auto-attach	Disables Auto-Attach on the target interface.	Interface Configuration
clear auto-attach statistics	Clears Auto-Attach interface-related statistics.	Interface Configuration

7.1.4 VLAN Parameters and Commands

7.1.4.1 VLAN Parameters and Commands

Command	Description	CLI Mode
vlan <vlan-id>	Creates a VLAN and enters into the config - VLAN mode in which VLAN specific configurations are done and sets the VLAN in active mode.	Global Configuration
protocol-vlan	Enables protocol-VLAN based membership classification on all ports of the switch.	Global Configuration
map protocol {ip | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther} protocols-group <Group id integer(0-2147483647)> TBD	Creates a protocol group with a specific protocol and encapsulation frame type combination.	Global Configuration
clear mac-address-table dynamic [interface {port-channel <port-channel-id (1-65535)> | <interface-type> <interface-id>}] [vlan	Clears the dynamically learnt MAC Addresses.	Global Configuration

<vlan_>] Available options: port-channel <port-channel-id (1-65535)> ■ Clears the FDB entries for the specified port channel interface. <interface-type> ■ Clears the FDB entries for the specified type of interface. gigabitethernet <vlan –id> ■ VLAN ID is a unique value that represents the specific VLAN.		

Command	Description	CLI Mode
name <vlan name string>	Configures name for the VLAN.	Config-VLAN
ports [add] [(gigabitethernet/extremeethernet/ port-channel)]	Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.	Config-VLAN
ports [add] ([<interface-type> <0/ab, 0/c,...>] [<interface-type> <0/ab, 0/c,...>] [port-channel <a,b,c-d>]) [untagged <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [portchannel <a,b,c-d>][all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [portchannel <a,b,c-d>] <interface-type> parameter can have the following values: ■ gigabitethernet ■ extreme-ethernet ■ port-channel	Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.	Config-VLAN
vlan active	Activates a VLAN in the switch.	Config-VLAN

Command	Description	CLI Mode
switchport access vlan <vlanid (1-4094)>	Configures the PVID (Port VLAN Identifier) on a port.	Interface Configuration

switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged } Available options: all ■ configures the acceptable frame type as all. tagged ■ configures the acceptable frame type as tagged. untaggedAndPrioritytagged ■ configures the acceptable frame type as untagged and priority tagged.	Configures the type of VLAN dependent BPDU frames such as GMRP BPDU that the port should accept during the VLAN membership configuration.	Interface Configuration
switchport ingress-filter	Enables ingress filtering feature on the port.	Interface Configuration
port protocol-vlan	Enables protocol-VLAN based membership classification in a port.	Interface Configuration
switchport map protocols-group <Group id integer(0-2147483647)> vlan <vlan-id> Available options: <Group id integer(0-2147483647)> ■ configures a unique group ID that is already created with the specified protocol type and encapsulation frame type.	Maps the configured protocol group to a particular VLAN ID for an interface.	Interface Configuration
switchport mode { access | trunk | hybrid | {private-vlan {promiscuous | host }} |{dynamic {auto | desirable}} } Available options: access ■ configures the port as access port that accepts and sends only untagged. trunk ■ configures the port as trunk port that accepts and sends only tagged frames. hybrid ■ configures the port as hybrid port that accepts and sends both tagged and untagged frames.	Configures the mode of operation for a switch port.	Interface Configuration

Command	Description	CLI Mode

`debug vlan { [{fwd | priority | redundancy}([initshut] [mgmt] [data] [ctpl][dump] [os] [failall] [buffer] [all])][switch <context_name>] }[{ <short (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings }]`
 	
Available options:
`fwd`
■ sets the submodule as VLAN forward module, for which the tracing is to be done as per the configured debug levels.
`priority`
■ sets the submodule as VLAN priority module, for which the tracing is to be done as per the configured debug levels.
`redundancy`
■ sets the submodule as VLAN redundancy module, for which the tracing is to be done as per the configured debug levels.
`initshut`
■ generates debug statements for init and shutdown traces.
`switch <context_name>`
■ configures the tracing of the VLAN submodule for the specified context.
`mgmt`
■ generates debug statements for management traces.
`dump`
■ Generates debug statements for packet dump traces.
`failall`
■ generates debug statements for all kind of failure traces.
`buffer`
■ generates debug statements for VLAN buffer related traces.
`ctpl`
■ generates debug statements for control path traces.
	Enables the tracing of the VLAN sub module as per the configured debug levels.	Privileged Exec

os ■ generates debug statements for OS resource related traces. data ■ generates debug statements for data path traces.		
show vlan [brief | id <vlan-range> | summary | ascending]	Displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.	Privileged Exec
show vlan device info	Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.	Privileged Exec
show vlan protocols-group	Displays all entries in the protocol group table.	Privileged Exec
show protocol-vlan	Displays all entries in the port protocol table.	Privileged Exec
show mac-address-table [vlan <vlan-range>]	Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone.	Privileged Exec
how mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> Available options: vlan <vlan-range> ■ displays all static unicast MAC address entries created in the FDB table for the specified VLANs alone. address <aa:aa:aa:aa:aa:aa> ■ displays all static unicast MAC address entries created in the FDB table for the specified unicast MAC address. interface ■ displays all static unicast MAC address entries for the specified interface.	Displays all static unicast MAC address entries created in the FDB table.	Privileged Exec
show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id>	Displays all dynamically learnt unicast entries from the MAC address table.	Privileged Exec

Available options:
`vlan <vlan-range>`
■ displays all dynamically learnt unicast entries from the MAC address table for the specified VLANs alone.
`address <aa:aa:aa:aa:aa:aa>`
■ displays all dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address.
`interface`
■ displays all dynamically learnt unicast entries from the MAC address table for the specified interface.		

show mac-address-table dynamic multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id>}]
 	
Available options:
`vlan <vlan-range>`
■ displays all dynamically learnt multicast entries from the MAC address table for the specified VLANs alone.
`address <aa:aa:aa:aa:aa:aa>`
■ displays all dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address.
`interface`
■ displays all dynamically learnt multicast entries from the MAC address table for the specified interface.
	Displays all dynamically learnt multicast entries from the MAC address table.	Privileged Exec

`show mac-address-table aging-time`	Displays the ageing time configured for the MAC address table.	Privileged Exec
`debug vlan global`	Enables tracing in VLAN sub module and generates debug statements for global traces for the specified severity levels.	Privileged Exec