User Guide for Cisco Configuration Professional for Catalyst, Release 1.1

First Published: 2016-11-26

Last Modified: --

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number:

CONTENTS

PART I

Web User Interface Elements

CHAPTER 1

Using the Web UI

Using the Web UI

The Cisco Configuration Professional for Catalyst provides network administrators with a single solution for configuring, monitoring, and optimizing the device.

System Requirements

You can access the application from a client web browser. Ensure that the following web client requirements are met:

- Hardware - A Mac (OS version 10.9.5) or Windows (OS version 7) laptop or desktop compatible with one of the following tested and supported browsers:
    - Google Chrome 52 or later
    - Mozilla Firefox 48 or later
    - Apple Safari 9 or later
    - Microsoft Internet Explorer 11, or later
- Display resolution - We recommend that you set the screen resolution to 1280 x 800 or higher.

Using the Toolbar

The application pages contain the following static global toolbar:

- Product Information - Displays information such as the device name and version.
- Save Configuration - Saves your configuration.
- Help - Launches the user guide for the Web user interface.

Using the Navigation Menu

The Web user interface allows you to perform the following tasks from the navigation pane:

- **Monitoring** - Monitor your network on a daily basis and perform other ad-hoc operations related to network device inventory and configuration management. View the dashboard for a snapshot of connected client devices, performance information, incidents, and search options.
- **Configuring** - Configure device ports, STP mode and VLANs.
- **General Settings** - Configure device time settings, user administration settings, SNMP and HTTP settings.
- **Help** - Access product support and documentation.

Understanding the Dashboard

The Dashboard displays a snapshot of the overall status and statistics for your device.

- **Switch View** - Displays a snapshot of the ports on the device.
- **CPU and Memory Utilization** - Displays CPU usage on the processors on each core, every 5 minutes, every 1 minute and every 5 seconds. The Memory Utilization section displays a chart of the device memory usage. Hover over the graph to view the processor pool and the I/O pool percentage.
- **System Messages** - Displays high severity, critical alerts that require your attention.
- **System Information** - The **PoE Power Utilization** section displays a pie-chart showing the total Power over Ethernet (PoE) on the device, the power used by the device and the current power available. The **System Temperature** section displays the temperature of the device. If the temperature is yellow or red, your device needs attention.

Obtaining Documentation and Submitting a Service Request

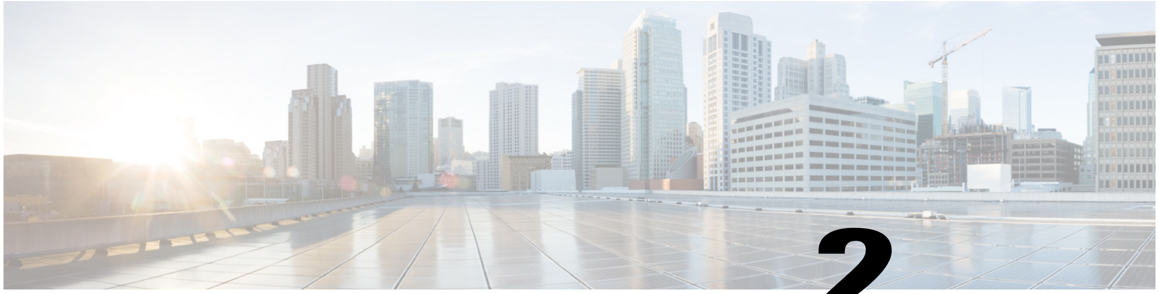
For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

PART II

Quick Setup Tasks



CHAPTER 2

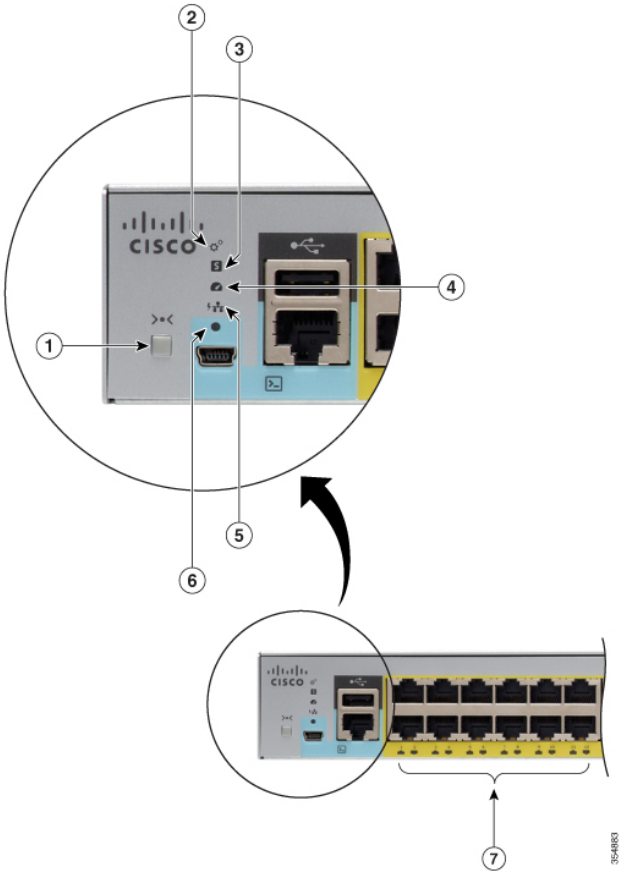
Getting Started with Your Device Configuration

Quick Setup Tasks

On the first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured. The Day 0 wizard allows you to quickly set up your device with the minimum configuration required to enable traffic to pass through the network.

Quick Setup: Accessing the Configuration Setup Wizard

When you first set up the switch, use the Configuration Setup wizard to enter the initial IP information. This enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for further configuration.



1	Mode button	2	SYST LED (system)
3	STAT LED (status)	4	SPEED LED
5	PoE LED [1]	6	Console LED
7	Port LEDs		

[1] Only on switch models that support PoE.

Step 1 Verify that no devices are connected to the switch. Initially, the switch acts as a DHCP server. If your PC has a static IP address, before you begin, you should change your PC settings to temporarily use DHCP.

Step 2 Verify that POST has completed by confirming that the STAT LED is solid green. If the switch fails POST, the STAT LED turns amber.

Step 3 Press and hold the **Mode** button for 3 seconds. When all of the LEDs above the **Mode** button turn green, release the **Mode** button immediately.

Note Continuing to hold the **Mode** button after the LEDs have turned green, exits the Setup mode.

Step 4 Connect a straight-through Category 5 Ethernet cable to a 10/100/1000 Ethernet port on the switch front panel and to the Ethernet port on the PC.

Step 5 Verify that the LEDs on both Ethernet ports are green.

Step 6 Wait 30 seconds.

Step 7 Enter the IP address 10.0.0.1 or 10.0.0.3 in the Web browser, on your PC. On Cisco Catalyst 2960-X and 2960-XR switches, if you have connected to a downlink access port, enter the IP address 10.0.2.1.

Step 8 Enter the following default credentials: username: cisco, password: cisco and press **Enter**.
The Configuration Setup wizard is displayed.

Quick Setup: Configuration Basic Device Settings

Setting a hostname and creating a user account is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Step 1 Log on using the default username and password provided with the device.

Step 2 Enter a hostname to identify your device on the network. The hostname can be alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters.

Step 3 Enter a username that is unique and between 8 and 64 characters long.

Step 4 Set a password of up to 32 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 5 Enter the password again in the **Enable Password** field.

Step 6 Set the device time and date.

Step 7 Click **Interface Configuration**.

Quick Setup: Configuring Interfaces

Next, configure VLANs on your device and assign interfaces to them.

Step 1 In the **Data VLAN** field, enter the VLAN on which to carry IP data traffic. All ports, by default, are associated with data VLAN 1.
Separating voice and data traffic creates a security boundary preventing data applications from accessing voice traffic.

Step 2 In the **Voice VLAN**field, enter the VLAN on which to carry IP voice traffic.

Step 3 Hold the CTRL key down to select multiple access ports, from the **Access Ports** drop-down list. An access port carries traffic for the VLAN configured on the interface. If a VLAN is not configured for the access port, the interface carries traffic on the default VLAN.

Step 4 To enable PortFast on all the specified access ports, select the **Portfast enable** check box. Devices that connect to PortFast enabled ports can connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state. If your device connects to endpoints (for example, to phones and computers and not to other switches or hubs), select to enable PortFast on the interface.

Step 5 Select the uplink port. The uplink port functions as a trunk port connecting to a switch or router. A trunk port carries traffic for all the VLANs that are accessible by a specific device. Trunk ports mark traffic with unique identifying tags (802.1Q tags, when configured), to ensure that traffic is accurately directed to its designated VLAN.

Step 6 Click **Layer 3 Configuration**. To go back and update configuration details, click **Previous**.

Quick Setup: Configuring Layer 3 Settings

Configure Layer 3 settings to enable your device to connect to Layer 3 devices and pass traffic outside of the network.

Step 1 In the **Default Gateway** field, enter the IP address of the default gateway that will allow endpoints and devices on your network to communicate with endpoints on other networks.

Step 2 Assign an IP to an interface or VLAN. You can assign IP addresses to multiple interfaces including data and voice VLANs. You cannot assign an IP address to a GigabitEthernet interface.

Step 3 Click **Advanced Configuration**. To go back and update configuration details, click **Previous**.

Quick Setup: Configuring Advanced Device Settings

Step 1 Select **Enable telnet** check box to enable access to the device using Telnet.

Step 2 Select **Enable SSH** check box to enable access to the device using SSH.

Step 3 Enter a domain name for the device.

Step 4 In the **RSA Key** field, enter the RSA key size. The Rivest, Shamir, and Adelman (RSA) key is based on the RSA algorithm and is used to authenticate SSH access to the device. The recommended minimum RSA key size is 1024.

Step 5 To enable Auto-QoS on access ports connected to Cisco IP phones, select the **Auto-QoS for Cisco Phones** checkbox. This field may not be displayed, if your device does not support Auto-QoS.

Step 6 To enable Auto-QoS on uplink ports connecting to a trusted switch or router, select the **Auto-QoS for Uplinks** checkbox . This field may not be displayed, if your device does not support Auto-QoS.

Step 7 Click **Summary** to verify your configuration on the **Summary** page.

Step 8 Verify your configuration and click **Submit** to save your changes. To go back and update configuration details, click **Previous**.
When you click **Submit**, the device is configured and exits the **Configuration Setup** page. The PC displays a message and then attempts to connect with the new device IP address. If you configured the device with an IP address that is in a different subnet from the PC, connectivity between the PC and the device is lost.

Step 9 Disconnect the device from the PC, and install the device in your network.

PART III

Device Configuration

CHAPTER 3

Configuring Your Device

Configuring Access to the Device

Step 1 Choose **Configuration** > **Switch** > **Switch**.

Step 2 In the **Switch Host Name** field, enter a hostname to identify your device on the network. The hostname can be alphanumeric, is case sensitive, can contain special characters, and can have a maximum of 32 characters.

Step 3 To be able to manage the switch remotely, assign an IP address in the **Switch IP Address** field.

Step 4 Enter a VLAN ID to identify in the **Switch Management VLAN** field. The management VLAN is the VLAN that contains the interface that is used to remotely manage the switch. By default, this is VLAN 1, as all ports are assigned to VLAN 1. We recommend that you not use VLAN 1 or VLANs that are used by client devices such as users and printers.

Step 5 Set the maximum transmission unit is the largest sized packet that your device can send. If the connected router cannot handle a large MTU, packets may be retransmitted. A small MTU may result in a higher number of packets and cause overheads and performance limitations. The default MTU is 1500 bytes. Setting the MTU size sets the system MTU.

Step 6 To control the Ethernet lights connected to your device, ensure that the **CoAP** checkbox remain selected. The connected Ethernet lights must support CoAP. By default, CoAP is already enabled on your device.

Step 7 Click **Apply** to save your changes.

Configuring Stacking

On the **Configuration** > **Switch** > **Switch** screen, on the **Stacking** tab, choose a value from the **Stacking** drop-down list to set your device as a standalone switch, as part of a physical stack, or as part of a cluster. The switch can belong to only one state at a time.

Step 1 To connect your switch to other switches on the stack ports, using a stacking cable, choose *Physical Stacking*. Click **Apply**.

Step 2 To enable clustering on your switch and allow your switch to start a cluster, choose *Virtual Stacking* . Click **Apply**. If your device is physically stacked, you cannot start a virtual cluster.

Step 3 To add a switch to the cluster, when Virtual Stacking is enabled, click **Enable** next to the switch MAC address. Enter the enable password of the cluster member, in the **Enable Password** field, to authenticate your action on the switch. Click **OK**.

Configuring STP

Understanding Spanning Tree Protocol

Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks.

To learn the topology of the network, STP-enabled switches communicate with each other using standardized data messages called BPDUs. Using BPDUs, the switch with the smallest bridge priority number is automatically elected as the root bridge. If the bridge priority is the same on all the switches then the switch with the smaller MAC address is elected as the root bridge. Each switch then elects ports that are designated and that can communicate with the root bridge and forward traffic. Non-designated ports block traffic.

A port normally starts in Blocking state, and then immediately moves through to the Listening state. In the Listening state, the device determines if the port is part of a physical loop. If it is, the port state is changed back to Blocking, and no data is sent or received on the port. If the port is not part of a loop, the port proceeds to the Learning state, and learns the MAC addresses in the frame. The port then moves into Forwarding state ready to send and receive data.

You device supports the following STP modes:

- RPVST
- PVST
- MST

Configuring STP

Step 1 Choose **Configuration** > **Switch** > **STP**.

Step 2 From the **STP Mode** drop-down list, choose the STP mode for your device. Spanning-Tree Protocol (STP) prevents loops when switches are interconnected via multiple paths. STP implements the IEEE 802.1D algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by blocking selected bridge interfaces. This algorithm guarantees that there is only one active path between two network devices. Your device supports MST, PVST, and RPVST STP modes.

Step 3 Ensure that STP is set to *Enable* for the interface.

Step 4 Select a VLAN ID and update the bridge priority number. The bridge priority is a numerical value that is used with the MAC address, to find the switch on the network. The default value is 32768. The priority can only be configured in multiples of 4096.

Step 5 Click **Apply** to save your changes.

Configuring Device Ports

Configuring Port General Settings

Step 1 On the**Configure** > **Ports** > **Port Configuration** page. All the ports on your device are displayed. Choose the port you want to configure, and click the **General** tab.

Step 2 Choose *10 MB*, *100 MB*, or *1000 MB* as the interface speed, from the **Speed** drop-down list. To auto-negotiate the interface speed, and allow communicating ports to decide the optimum speed for transmission, choose *auto*.

Step 3 Choose *full*, *half*, or *auto* from the **Duplex** drop-down list.

- *Auto* auto-negotiates the interface mode, and allows communicating ports to decide the optimum mode for data transmission.
- Half-duplex communication is unidirectional, and the device cannot send and receive data simultaneously. This option can impact the performance of your device.
- Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.

Step 4 To enable the interface on the device, set the **Status** field to *up*.

Step 5 Click **Apply** to save your changes.

Configuring Port Settings

Step 1 On the**Configure** > **Ports** > **Port Configuration** page. All the ports on your device are displayed. Choose the port you want to configure, and click the **Port Settings** tab.

Step 2 Choose a switch mode.
Access ports transport traffic to and from only the VLAN assigned to it.

Trunk ports carry traffic for multiple VLANs, using a process called trunking. Trunk ports mark frames with unique identifying IEEE 802.1Q tags (when configured), to direct each frame to its designated VLAN.

When a port is in *dynamic auto* mode, it passively listens for and receives Dynamic Trunking Protocol (DTP) messages generated by a port in *dynamic desirable* mode, on another switch on the other side. A trunk link is formed between the two interfaces and all frames are tagged.

Step 3 If you choose *access* mode, assign a VLAN to the port, in the **Access VLAN** field. By default, all ports assigned to VLAN 1 are assigned as access ports.

Step 4 If you choose *trunk* as the switch mode, assign a range of VLANs to the port. To assign all VLANs to carry port traffic, select **All VLANs**, or select **VLAN IDs** and specify a range of VLANs that can carry traffic for the port.

Step 5 If you choose *dynamic auto* or *dynamic desirable*, assign a range of VLANs to the port. To assign all VLANs to carry port traffic, select **All VLANs**, or select **VLAN IDs** and specify a range of VLANs that can carry traffic for the port. If DTP negotiation fails, the dynamic auto and dynamic desirable ports become access ports. Assign an access VLAN to the ports, in the **Access VLAN** field.

Step 6 In the **Voice VLAN** field, specify a VLAN to carry voice traffic.

Step 7 For network security reasons, specify a VLAN other than VLAN 1 in the **Native VLAN** field. When your device receives untagged frames on a trunk port, they are sent to the native VLAN. By default, this is VLAN 1.

Step 8 If your device connects to endpoints (for example, to phones and computers and not to other switches or hubs), set the **Port Fast** field to *on*, to enable PortFast on the interface.
Devices that connect to PortFast enabled ports can connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state. For more information on Spanning Tree Protocol modes, see Understanding Spanning Tree Protocol, on page 16.

Step 9 To activate DHCP snooping on the port, set **DHCP Snooping** to *enable*. DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers, validating DHCP messages received from untrusted sources and filtering out invalid messages. The DHCP snooping binding database maintains information about untrusted hosts with leased IP addresses, and validates subsequent requests from untrusted hosts.

Step 10 Click **Apply** to save your changes.

Configuring Advanced Port Settings

Step 1 On the**Configuration** > **Ports** > **Port Configuration** page. All the ports on your device are displayed. Choose the port you want to configure, and click the **Adavanced Settings** tab.

Step 2 Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. From the **Storm Control** drop-down list:

- To error-disable the port during a storm, choose *Shutdown*.
- To generate an SNMP trap when a storm is detected, choose *Trap*.
- To disable storm control choose *None*.

Step 3 Specify thresholds for unicast, broadcast, and multicast traffic entering your device. These values indicates the number of packets allowed per second, as part of your unicast, broadcast, and multicast traffic.

Step 4 In the **Policy Management** section, choose an Auto-QoS policy to apply to the port. The Auto-QoS policy ensures that the traffic on the port receives the selected QoS treatment automatically.

Step 5 Click **Apply** to save your changes.

Troubleshooting Your Device

To troubleshoot network reachability, communication delays, and packet loss, use the **Configuration > Troubleshooting** screens.

On the **Troubleshooting > Ping** screen, choose the interface from which to send ping packets to the specified destination, and click **Ping**.

On the **Troubleshooting > Tracroute** screen, enter the destination address for which you want to run traceroute, and click **Traceroute**. Traceroute discovers the route, and the number of hops that packets take when traveling to their destination and helps you identify potential link bottlenecks throughout the transmission path.

On the **Troubleshooting > Diagnostics** screen, choose the type of tests to run on the switch, and click **Start**. Running some diagnostic tests may be disruptive to the switch.

Rebooting Your Device

Use the **Troubleshooting** > **Switch Reboot** screen, to restart your switch, and its stack members or restore it to factory defaults.

- **Restart Switch** - Click to reboot the switch. The switch restarts with your saved configuration.
- **Factory Reset** - Click to erase the startup configuration in the persistent memory on the switch and all its stack members, and reboot the switches with the initial factory default configuration. After you reset a switch, there is no way to recover the erased configuration.

Configuring VLANs

Understanding VLANs

A VLAN or a virtual LAN is a group of devices on one or more LANs, which are configured to communicate as if they were physically connected, despite being located across LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

Using VLANs you can partition your network based on functional and security requirements within your organization, without investing in new cables and without making major changes to current network infrastructure. For example, VLANs can be created to divide your network into logical groups, and secure traffic to and from departments such as Finance or Marketing. VLANs could also be created to restrict the use of resources such as file servers and printers to a logical group of users on your network.

As defined by the IEEE 802.1Q standard, the VLAN identifier or tag consists of 12 bits in the Ethernet frame, creating an inherent limit of 4,096 VLANs on a LAN.

Configuring Layer 2 VLANs

Step 1 On the**Configure** > **VLANs** page, click the Layer 2 VLANs page. To add a Layer 2 VLAN, click **Add**. To edit a VLAN, select the VLAN ID in the table. Details of the VLAN are displayed below.

Step 2 In the **VLAN ID** field, enter an ID between 2 and 4094, to identify the VLAN on your network. VLAN 1 is the default VLAN on your device.

Step 3 Enter a description for the VLAN.

Step 4 Set the **State** field to *active* to forward traffic through the VLAN. VLANs in *suspended* state cannot forward traffic on your device.

Step 5 Click **Apply** to save your changes.

Configuring VLAN Groups

Step 1 On the **Configure** > **VLAN** page, click the **VLAN Groups** tab. Click **Add**.

Step 2 In the **VLAN Group Name** field, enter a name for the VLAN group that acts like a logical container for your VLANs. A VLAN group allows you to apply a set of common parameters to all the VLANs in the group.

Step 3 In the VLAN List field, enter the range of VLANs, from 2 to 4094, you want to include in the VLAN group. The recommended number of VLANs in a group is 32.

Step 4 Click **Apply** to save your changes.

Configuring DHCP Snooping on VLANs

Step 1 Choose **Configuration** > **VLAN** > **IP DHCP Snooping**.

Step 2 To activate DHCP snooping on a VLAN or a range of VLAN, set the **IP DHCP Snooping** field to *enable*. DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers, validating DHCP messages received from untrusted sources and filtering out invalid messages.

The DHCP snooping binding database maintains information about untrusted hosts with leased IP addresses, and validates subsequent requests from untrusted hosts.

Step 3 In the **VLAN List** field, enter a VLAN ID or a range of VLAN IDs on which you want to enable DHCP snooping.

Step 4 Click **Apply** to save your changes.

Configuring Services

Configuring NetFlow

The **Services > NetFlow** screen is not displayed, if your device does not support NetFlow.

Step 1 Choose **Services** > **Netflow.**

Step 2 From the **Netflow Template** field, choose a pre-defined template to determine what information to monitor in your network traffic. You can choose to monitor application and server usage, network security vulnerabilities, and network capacity and bandwidth usage.

Step 3 In the **Collector IP Address** field, enter the IP address of the designated device on which the exported Netflow data is collected.

Step 4 In the **Switch Export Address** field, choose the IP address to identify the switch interface from which flows will be exported to the collector.

Step 5 From the **Sampling Method** field, choose the method based on which traffic originating from the port is monitored.

- Deterministic – Monitors the first packet in a specified number of packets. For example, to monitor 1 in every 30 packets, specify 30 as the sampling method range.
- Random – Allows packets to be monitored randomly by the device.
- Full NetFlow – Monitors all the traffic on the specified device port. This option is not displayed if your device does not support Full NetFlow.

Step 6 In the **Input Capture Interface** drop-down list, choose the switch interface on which to apply NetFlow.

Step 7 Click **Create** to apply the NetFlow. TheNetFlow Monitor section displays the flow monitor you created.

PART IV

General Settings

CHAPTER 4

Configuring Device General Settings

Configuring SNMP

Understanding Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices. Using SNMP, system administrators can remotely manage network performance, find and solve network problems, and plan for network growth.

SNMP is made up of 3 components — the SNMP manager, the SNMP agent, and Management Information Base (MIBs).The network management software (NMS) uses the Cisco MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can get graphed and analyzed to help you troubleshoot network problems, increase network performance, verify the configuration of devices, and monitor traffic loads. The SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The SNMP agent also can send traps (notifications) of certain events, to the SNMP manager.

SNMPv1 represents the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI) and operates over protocols, such as User Datagram Protocol (UDP) and IP. SNMP Version 1 and SNMP Version 2 use community strings to authenticate access to the device. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device discards the request and does not respond. SNMP Version 3 allows access to the device through a username and password, and an encryption method to improve security. SNMPv3 provides the following security features:

- Authentication—Verifying that the request comes from a genuine source.
- Privacy—Encrypting data.

- Authorization—Verifying that the user allows the requested operation.
- Access control—Verifying that the user has access to the objects that are requested. SNMPv3 prevents packets from being exposed on the network. Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users.

Configuring SNMP General Settings

Step 1 Choose **General Settings** > **Management** > **SNMP** > **General**.

Step 2 To enable SNMP on the device, set **SNMP Status** to *Enable*.

Step 3 Enter the location of the device. Also enter the contact details of the device administrator.

Step 4 To enable traps globally, set **SNMP Global Trap** to *Enable*. An SNMP Trap is an immediate notification sent from your device for an event that might otherwise be discovered only during SNMP polling. Traps might indicate events such as power-up or link-up/down conditions, temperatures exceeding certain thresholds, or high traffic.

Step 5 To configure the device to end SNMP logs to en external server, check the **SNMP Logging** check box.

Step 6 Click **Apply** to save changes.

Configuring SNMP Communities

Use SNMP community strings authenticate access to MIB objects.

Step 1 Choose **General Settings** > **Management** > **SNMP** > **SNMP Communities**.

Step 2 Click **Add**, to add a new community.

Step 3 Enter a community name . A community name acts as a password that is shared, typically, by multiple SNMP agents and one or more SNMP managers. The name must be a unique, case-sensitive, alphanumeric string of up to 16 characters. Embedded spaces are not allowed in SNMP community strings.

Step 4 By default, the access mode is Read-only and supports only SNMP GetRequests and GetNextRequests. In this mode, you can access SNMP information, but cannot modify it. To support SNMP SetRequests to access and modify SNMP information, choose Read-write mode from the **Access Mode** drop-down list.

Step 5 Click **Apply** to save your changes.

Configuring SNMP V3 Users

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users.

Step 1 Choose **General Settings** > **Management** > **SNMP** > **SNMP V3 Users**.

Step 2 Click **Add**.

Step 3 In the **User Name** field, enter a name for the SNMP user. The username is the name of the user on the host (the recipient of an SNMP trap) that connects to the SNMP agent.

Step 4 In the **Group** field, enter a group name for the profile. An SNMP group is an access control policy to which users can be added. Each SNMP group is configured with a security model. A user within an SNMP group should match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique.

Step 5 From the **Auth Protocol** list, choose an algorithm to configure authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms. In the **Auth Password** field, enter a passkey to authenticate user access. Auth Protocol corresponds to the AuthNoPriv security model.

Step 6 To configure Advanced Encryption Standard (AES) or Data Encryption Standard (DES) encryption, choose a Priv Protocol encyption method, from the **Priv Protocol** list. In the **Priv Password** field, enter a passkey to authenticate user access. AES 128, AES 192, and AES 256 use Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits respectively. 3DES uses the Cipher Block Chaining (CBC)-DES (DES-56) standard with a 168-bit key size for encryption. Priv Protocol corresponds to the AuthPriv security model.

Step 7 Click **Apply** to save your changes.

Configuring SNMP Hosts

Step 1 Choose **General Settings** > **Management** > **SNMP** > **SNMP Host**.

Step 2 Click **Add**.

Step 3 In the **IP Address** field, enter the IP address from which this device accepts and sends SNMP packets.

Step 4 In the **Port** field, enter the UDP port number for the remote SNMP agent of the device where the user resides.

Step 5 From the **Version** drop-down list, choose the SNMP version. SNMP V1, V2C, and V3 are supported on your device.

Step 6 Specify the SNMP community string that will act as the password on the host.

Step 7 For SNMP Version 3, from the **Security Level** drop-down list, choose the authentication level.

Step 8 Click **Apply** to save your changes.

Configuring HTTP/HTTPS Settings

Step 1 Choose **General Settings** > **Management** > **HTTP/HTTPS**

Step 2 To sent data using an HTTP connection, set the **HTTP Access** field to *Enable*.

Step 3 In the **HTTP Port** field, enter the designated port to listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

Step 4 To send data over a secure HTTPS connection, set the **HTTPS Access** field to Enable. In the **HTTPS Port** field, enter the designated port to listen for HTTPS requests. The default port is 443. Valid values are 443, and ports between 1025 and 65535. On a secure HTTPS connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow you to connect to your device from a Web browser.

Step 5 To use Certificate Authority (CA) servers as trustpoints, in the **Trust Point Configuration** section, set **Enable Trust Point** to *Enable*. Choose one of the configured trustpoints.
Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. Specific CA servers are referred to as trustpoints. When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate. For secure HTTP connections, we highly recommend that you configure a CA trustpoint.

If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing). If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated. If the device is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned. If the device has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the device or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

Step 6 In the **Timeout Policy Configuration** section, enter the number of minutes of inactivity allowed before the session times out. Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds. Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

Step 7 Click **Apply** to save your changes.

Updating Device Software

Step 1 Choose **General Settings** > **Software Update**.

Step 2 From the **File Type** drop-down list, choose if you want to update only the Web UI software or both the IOS and Web UI bundle, on your device.

Step 3 Browse to the appropriate upgrade file on your computer. This is typically a file you downloaded from the software downloads available to you on http://www.cisco.com/c/en/us/support/index.html.

Step 4 Click **Start Update**. To restart your device with the new software, click **Restart Switch**.

Setting Device Time

Setting Device Time Manually

Step 1 Choose **General Settings** > **System** > **System Time**.

Step 2 In the **Set Date** and **Set Time** fields, set the date and the time for your device. This will override the time and date received from the NTP server (if configured).

Step 3 Choose the time zone associated with the location of the device.

Step 4 Coordinated Universal Time (UTC) is the 24-hour time standard and the basis for civil time today. Based on the time zone you selected, in the **Set Offset Hours** field, enter the number of hours and the number of minutes by which you want it offset from UTC, to arrive at your local time. For example, the offset for PST is -8 hours.

Step 5 Click **Apply** to save your changes.

Setting Device Time Using NTP

An NTP network usually gets its time from an authoritative time source such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient;

no more than one packet per minute is necessary to synchronize two machines to the accuracy of within a millisecond of one another.

Step 1 Choose **General Settings** > **System** > **NTP Server** .

Step 2 Click **Add** to add an NTP server.

Step 3 In the **Host Name Type** field, select **Word** to enter a host name in text. Select **IP** to specify an IPv4 address in the **Host Name** field, or select **IPv6** to enter an IPV6 NTP server address.

Step 4 To indicate that the host name is a VRF with which the NTP server will communicate, select the **VRF** check box.

Step 5 Select **VLAN** to specify a VLAN as the NTP source interface. Choose a VLAN ID from the **VLAN** drop-down list. To specify an interface on your device as the NTP source, select **Interface**.

Step 6 Click **Apply** to save your changes.

Configuring User Accounts and Passwords

Step 1 Choose **General Settings** > **User Administration**.

Step 2 In the **User name** field, enter a username that is unique and between 8 and 64 characters long.

Step 3 From the **Privilege** drop-down list, choose the privilege level to associate with the user. The privilege level defines what commands users can enter using the CLI, after they have logged into the device. Privilege 1 allows access in User Exec mode and privilege 15 allows access in Privileged Exec mode.

Step 4 Enter a password that is between 8 and 127 characters long, using the following guidelines:

- It is recommended that the password is a combination of at least three of the following categories—lowercase letters, uppercase letters, digits, and special characters.
- The new password should not be the same as the associated username or any close variant of the username.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be cisco, ocsic, admin, nimda, or any variant of the order of letters, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".

Step 5 Enter the same password again to confirm.

Step 6 Click **Apply** to save your changes.

PART V

Device Monitoring

CHAPTER 5

Monitoring Your Device

-

Monitoring Ports

The **Monitoring** > **Ports** page displays details of the ports on your device.

For each port, the **Port Monitoring** page displays a snapshot of the configuration details of the port. Each row displays the port status, the type of port, the associated VLAN for the port, the duplex mode, the speed associated with the port, the power, the ingress and egress traffic passing through the port (in bytes), and the number of packets dropped.

The **Port Monitoring** page also displays statistics for the number of packets sent and received on the port. Additionally, the page displays unidirectional links (traffic transmitted but not received by the port), buffer overruns on the port, queue drops, optics connected to the port, and if the interface is a loopback interface.

Monitoring Clients

The **Monitoring** > **Clients** page lists information about the clients connected to the device.

The page displays the name, the manufacturer, and the MAC address of the client, the port to which the client is connected, the operating system running on the client, the VLAN that is handling traffic from the client, and the power drawn by the client over Ethernet.