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.