Configure SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by Cisco NCS 4000 series.

Understand SNMP

SNMP is an application-layer communication protocol that allows Cisco NCS 4000 series network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

NCS 4000 uses SNMP for asynchronous event notification to a network management system (NMS). SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information.

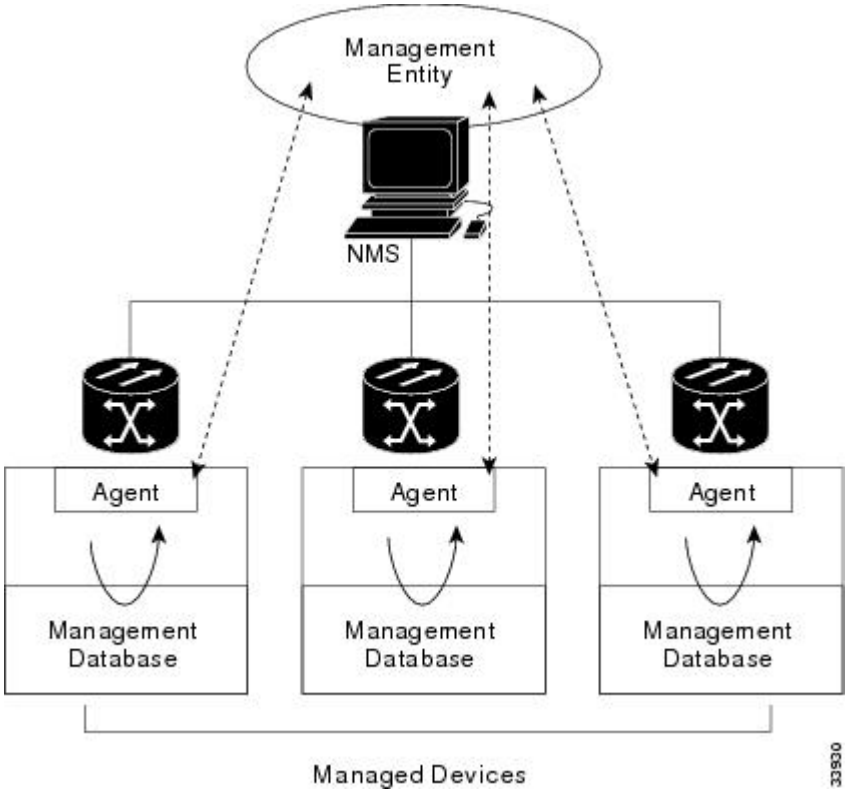
NCS 4000 supports SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2), and SNMP Version 3 (SNMPv3). As compared to SNMPv1, SNMPv2 includes additional protocol operations and 64-bit performance monitoring support. SNMPv3 provides authentication, encryption, and message integrity and is more secure.

Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

A management system executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or several management systems. The following figure illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

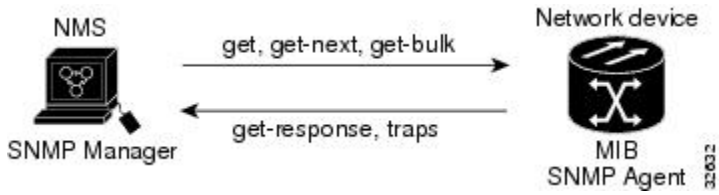
Figure 1: Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data—such as performance information or event and error information—caught in software traps, into a readable form

for the management system. The following figure illustrates SNMP agent get-requests that transport data to the network management software.

Figure 2: Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15454 NCSNCS 4000)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

SNMPv3 Support

Cisco ONS 15454 NCS Software R9.0 and later supports SNMPv3 in addition to SNMPv1 and SNMPv2c. SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authentication and encryption packets over the network based on the User Based Security Model (USM) and the View-Based Access Control Model (VACM).

Cisco NCS 4000 supports SNMPv1, SNMPv2, and SNMPv3. SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authentication and encryption packets over the network based on the User Based Security Model (USM) and the View-Based Access Control Model (VACM).

- **User-Based Security Model—**The User-Based Security Model (USM) uses the HMAC algorithm for generating keys for authentication and privacy. SNMPv3 authenticates data based on its origin, and ensures that the data is received intact. SNMPv1 and v2 authenticate data based on the plain text community string, which is less secure when compared to the user-based authentication model.
- **View-Based Access Control Model—**The view-based access control model controls the access to the managed objects. RFC 3415 defines the following five elements that VACM comprises:
  - Groups—A set of users on whose behalf the MIB objects can be accessed. Each user belongs to a group. The group defines the access policy, notifications that users can receive, and the security model and security level for the users.
  - Security level—The access rights of a group depend on the security level of the request.
  - Contexts—Define a named subset of the object instances in the MIB. MIB objects are grouped into collections with different access policies based on the MIB contexts.
  - MIB views—Define a set of managed objects as subtrees and families. A view is a collection or family of subtrees. Each subtree is included or excluded from the view.

- Access policy—Access is determined by the identity of the user, security level, security model, context, and the type of access (read/write). The access policy defines what SNMP objects can be accessed for reading, writing, and creating.

Access to information can be restricted based on these elements. Each view is created with different access control details. An operation is permitted or denied based on the access control details.

You can configure SNMPv3 on a node to allow SNMP get and set access to management information and configure a node to send SNMPv3 traps to trap destinations in a secure way. SNMPv3 can be configured in secure mode, non-secure mode, or disabled mode.

SNMP, when configured in secure mode, only allows SNMPv3 messages that have the authPriv security level. SNMP messages without authentication or privacy enabled are not allowed. When SNMP is configured in non-secure mode, it allows SNMPv1, SNMPv2, and SNMPv3 message types.

SNMP Traps

The ONS 15454 NCSNCS 4000 uses SNMP traps to generate all alarms and events, such as raises and clears. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

NTP-K8 Configure SNMP Using CTC

Purpose	This procedure configures SNMP using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- DLP-G498 Create Group Access Using CTC, on page 5
- DLP-G496 Creating an SNMPv3 User Using CTC, on page 6
- DLP-G497 Create MIB Views Using CTC, on page 8
- DLP-G499 Configure SNMPv3 Trap Destination Using CTC, on page 8
- DLP-K88 Create SNMP Community Using CTC, on page 10
- DLP-K89 Enabling SNMP Trap Notifications Using CTC, on page 11
- DLP-G502 Manually Configuring the SNMPv3 Proxy Forwarder Table, on page 11
- DLP-G503 Automatically Configuring the SNMPv3 Proxy Forwarder Table, on page 13
- NTP-K8 Configure SNMP Using CTC, on page 4
- DLP-G505 Automatically Configuring the SNMPv3 Proxy Trap Forwarder Table, on page 14

Stop. You have completed this procedure.

DLP-G498 Create Group Access Using CTC

Purpose	This procedure creates a user group and configures the access parameters for the users in the group.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **SNMP** > **Group Access** tabs.

Step 2 Click **Create**.

Step 3 In the Create Group Access dialog box, enter the following information:

- Group Name—The name of the SNMP group, or collection of users, who share a common access policy.
- SNMP Version—Version of SNMP. The possible values are SNMPv1, SNMPv2, and SNMPv3.
- Security Level—The security level for which the access parameters are defined. You can configure the security level only when SNMPv3 is selected. Select from the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.

    If you select authNoPriv or authPriv for a group, the corresponding user must be configured with an authentication protocol and password, with privacy protocol and password, or both.
- Views
  - Read View Name—Read view name for the group.
  - Notify View Name—Notify view name for the group.
  - Write View Name—Write view name for the group.
- Allow SNMP Sets—Select this check box if you want the SNMP agent to accept SNMP SET requests. If this check box is not selected, SET requests are rejected.

Note SNMP SET request access is implemented for very few objects.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-G496 Creating an SNMPv3 User Using CTC

Purpose	This procedure creates an SNMPv3 user.
Tools/Equipment	None

Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* • DLP-G498 Create Group Access Using CTC, on page 5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **SNMP** > **Users** tabs.

Step 2 Click **Create**.

Step 3 In the Create User dialog box, enter the following information:

- User Name— Specify the name of the user on the host that connects to the agent. The user name must be a minimum of 6 and a maximum of 40 characters (up to only 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, "-" (hyphen), and "." (dot) . For TL1 compatibility, the user name must be of 6 to 10 characters.
- Group Name—Specify the group to which the user belongs.

  The SNMP version and security level of the group are displayed as read-only.
- Authentication
  - Protocol—Select the authentication algorithm that you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter a password if you select MD5 or SHA. By default, the password length is set to a minimum of eight characters.
- Privacy—Initiates a privacy authentication level setting session that enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select the privacy authentication algorithm. The available options are None, DES, and AES-256-CFB.
  - Password—Enter a password if you select a protocol other than None.

Step 4 Click **OK** to create an SNMP user.

Step 5 Return to your originating procedure (NTP).

DLP-G497 Create MIB Views Using CTC

Purpose	This procedure creates an SNMPv3 MIB view.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **SNMP** > **MIB views** tabs.

Step 2 Click **Create**.

Step 3 In the Create Views dialog box, enter the following information:

- Name—Name of the view.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Bit Mask—A family of view subtrees. Each bit in the bit mask corresponds to a sub-identifier of the subtree OID.
- Type—Select the view type. Options are Included and Excluded.

  Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-G499 Configure SNMPv3 Trap Destination Using CTC

Purpose	This procedure configures SNMPv3 trap destination.
Tools/Equipment	None

Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **SNMP** > **Trap Destinations (V3)** > **Trap Destinations** tabs.

Step 2 Click **Create**.

Step 3 In the Configure SNMPv3 Trap dialog box, enter the following information:

- Target Address—Target to which the traps should be sent. Use an IPv4 or an IPv6 address.
- UDP Port—UDP port number that the host uses. Default value is 162.
- User Name—Specify the name of the user on the host that connects to the agent.
- Security Level—Select one of the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Filter Profile—Select this check box and enter the filter profile name. Traps are sent only if you provide a filter profile name and create a notification filter. For more information, see DLP-G501 Creating Notification Filters.
- Proxy Traps Only—If selected, forwards only proxy traps from the ENE. Traps from this node are not sent to the trap destination identified by this entry.
- Proxy Tags—Specify a list of tags. The tag list is needed on a GNE only if an ENE needs to send traps to the trap destination identified by this entry, and wants to use the GNE as the proxy.

Step 4 In the Create SNMP Trap dialog box, enter the IP address of your network management system (NMS).

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-K88 Create SNMP Community Using CTC

Purpose	This procedure creates SNMP community.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* • DLP-G496 Creating an SNMPv3 User Using CTC, on page 6 • DLP-G499 Configure SNMPv3 Trap Destination Using CTC, on page 8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Trap Destinations** tabs.

Step 2 In the Communities area, click **Create**.
The Create SNMP Community dialog box appears.

Step 3 In the Destination area, the Destination Address field displays the trap destination address configured in DLP-G499 Configure SNMPv3 Trap Destination Using CTC, on page 8.

Step 4 Enter the User Datagram Protocol (UDP) port on which you want to create a community in the UDP Port field.
The default UDP port for SNMP is 162.

Step 5 In the User area, choose the user from the User Name droop-down list.
The SNMP version and the security level of the selected user are displayed.

Step 6 In the Notification area, check the required basic trap types. The available options are BGP, Config, Syslog, and SNMP.

Step 7 From the Advance Trap Types drop-down list, choose **None** or **Copy Complete**.

Step 8 Click **OK** to create SNMP community.

Step 9 Return to your originating procedure (NTP).

DLP-K89 Enabling SNMP Trap Notifications Using CTC

Purpose	This procedure enables SNMP trap notifications that are sent to a MIB tree.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Notifications** tabs.

Step 2 In the Notifications area, enable the following notifications as required by checking the **Enable** check box next to each notification.

- BGP—Border Gateway Protocol (BGP) trap notifications
- Config—Configuration trap notifications
- SNMP—SNMP trap notifications
- Syslog—Trap notifications in the system log file

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-G502 Manually Configuring the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3**.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.
- Check the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Target Address—Target to which the request should be forwarded. Use an IPv4 or an IPv6 address.
- Context Engine ID—The context engine ID of the ENE to which the request is to be forwarded. The context engine ID should be the same as the context engine ID of the incoming request.
- Proxy Type—Type of SNMP request that needs to be forwarded. The options are Read and Write.
- Local User Details—The details of the local user who proxies on behalf of the ENE user.
  - User Name—Specify the name of the user on the host that connects to the agent.
  - Local Security Level—Select the security level of the incoming requests that are to be forwarded. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Remote User Details—User to which the request is forwarded.
  - User Name—Specify the user name of the remote user.
  - Remote Security Level—Select the security level of the outgoing requests. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE, DES, or AES-256-CFB as the privacy authentication algorithm.
  - Password—Enter the password if you select protocol other than None. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-G503 Automatically Configuring the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Proxy Type—Select the type of proxies to be forwarded. The options are Read and Write.
- Security Level—Select the security level for the incoming requests that are to be forwarded. The options are:
  - noAuthNoPriv—Uses a username match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Target Address List—Select the proxy destination.

- Local User Name—Select the user name from the list of users.

Note When you configure SNMPv3 Proxy Forwarder Table automatically, the default_group is used on the ENE. The default_group does not have write access. To enable write access and allow SNMP sets, you need to edit the default_group on ENE.

Step 5 Click **OK** to save the settings.

Step 6 Return to your originating procedure (NTP).

DLP-G505 Automatically Configuring the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.
- Check the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the **SNMPv3 Proxy Trap Forwarder Table** area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. All GNE Trap destinations that have this tag in their proxy tags list are chosen.
- Source of Trap—The list of ENEs whose traps are forwarded to the SNMPv3 Trap destinations that are identified by the Target Tag.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).