

Configuring SNMP

The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use SNMP to modify a role that was created using the CLI and vice versa.

Users, passwords, and roles for all CLI and SNMP users are the same. A user configured through the CLI can access the switch using SNMP (for example, the Cisco DCNM-SAN or the Device Manager) and vice versa.

- Information About SNMP Security, on page 1
- Default Settings, on page 6
- Configuring SNMP, on page 6
- Verifying SNMP Configuration, on page 22
- Additional References, on page 27

Information About SNMP Security

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3 (see #unique_388 unique_388_Connect_42_fig_sjx_bwq_sz).

SNMP Version 1 and Version 2c

SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c) use a community string match for user authentication. Community strings provided a weak form of access control in earlier versions of SNMP. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported.

SNMP Version 3

Note Starting with Cisco MDS NX-OS Release 9.4(4), the AES-256 privacy encryption algorithm is supported. It is the recommended privacy encryption algorithm due to its stronger security. However, AES-128 remains the default privacy encryption algorithm. DES privacy encryption algorithm is still supported.

SNMP Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SNMPv3 CLI User Management and AAA Integration

The Cisco NX-OS software implements RFC 3414 and RFC 3415, including user-based security model (USM) and role-based access control. While SNMP and the CLI have common role management and share the same credentials and access privileges, the local user database was not synchronized in earlier releases.

SNMPv3 user management can be centralized at the AAA server level. This centralized user management allows the SNMP agent running on the Cisco MDS switch to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. The AAA server also is used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

CLI and SNMP User Synchronization

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

To create an SNMP or CLI user, use either the **username** or **snmp-server user** commands.

Users are synchronized as follows:

- Deleting a user using either command results in the user being deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Existing SNMP users continue to retain the auth and priv passphrases without any changes.
- If the management station creates an SNMP user in the usmUserTable, the corresponding CLI user is created without any password (login is disabled) and will have the network-operator role.

AAA Exclusive Behavior in SNMPv3 Servers

The AAA exclusive behavior feature enables you to authenticate users based on location.

A unique SNMPv3 user is not authenticated if the user is not a local user or a remote AAA user. If the user exists in both the local and remote database, the user will be authenticated or rejected based on whether AAA exclusive behavior is enabled or not.

Table 1: AAA Exclusive Behavior Scenarios

User Location	AAA Server	AAA Exclusive Behavior	User Authentication
Local user database	Disabled	Enabled	User is authenticated.
Local user database	Enabled	Enabled	User is not authenticated.
Local user database	Enabled	Disabled	User is authenticated.
Local user database	Disabled	Disabled	User is authenticated.
Remote and local user databases (same username)	Enabled	Enabled	Remote user is authenticated, but the local user is not authenticated.
Remote and local user databases (same username)	Disabled	Enabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Disabled	Disabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Enabled	Disabled	Local user is authenticated, but the remote user is not authenticated.



Note When AAA servers are unreachable, a fallback option can be configured on the server so that a user is validated against the local user database. The SNMPv3 server returns an error if the user is not available in the local database or in the remote user database. The SNMPv3 server returns an "Unknown user" message without checking the availability of AAA servers when a user is not available in the remote user database.

Restricting Switch Access

You can restrict access to a Cisco MDS 9000 Family switch using IP access control lists (IP-ACLs).

Group-Based SNMP Access



Note Because *group* is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

You can begin communicating with the agent once your user name is created, your roles are set up by your administrator, and you are added to the roles.

Creating and Modifying Users

You can create users or modify existing users using SNMP, DCNM-SAN, or the CLI.

- SNMP—Create a user as a clone of an existing user in the usmUserTable on the switch. Once you have created the user, change the cloned secret key before activating the user. Refer to RFC 2574.
- DCNM-SAN.
- CLI—Create a user or modify an existing user using the **snmp-server user** command.

A network-operator and network-admin roles are available in a Cisco MDS 9000 Family switch. There is also a default-role if you want to use the GUI (DCNM-SAN and Device Manager). You can also use any role that is configured in the Common Roles database.



Tip All updates to the CLI security database and the SNMP user database are synchronized. You can use the SNMP password to log into either DCNM-SAN or Device Manager. However, after you use the CLI password to log into DCNM-SAN or Device Manager, you must use the CLI password for all future logins. If a user exists in both the SNMP database and the CLI database before upgrading to Cisco MDS SAN-OS Release 2.0(1b), then the set of roles assigned to the user becomes the union of both sets of roles after the upgrade.

AES Encryption-Based Privacy

The Advanced Encryption Standard (AES) is the most secure symmetric cipher algorithm used by SNMP. The Cisco NX-OS software uses AES as one of the privacy protocols for SNMP message encryption and conforms with RFC 3826.

The priv option offers a choice of DES, 128-bit or 256-bit AES encryption for SNMP security encryption. The priv option along with the aes-128 parameter indicates that this privacy password is for generating a 128-bit AES key. AES-128 is made the default privacy option from Cisco MDS NX-OS Release 8.5(1). This indicates that any SNMP server users configured or modified from Cisco MDS NX-OS Release 8.5(1) will use aes-128 as the privacy option. The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters. If you use the localized key, you can specify a maximum of 130 characters.

Starting from Cisco MDS NX-OS Release 9.4(4), aes-256 is supported increasing maximum encryption key size to 256 bits.



Note For an SNMPv3 operation using the external AAA server, user configurations in the external AAA server require AES to be the privacy protocol to use SNMP PDU encryption.

Traps, Notifications, and Informs

A trap is an unacknowledged message sent from an SNMP agent to SNMP managers in SNMPv1. It is known as a notification in SNMPv2 and SNMPv3. An inform is an acknowledged message sent from an SNMP agent to an SNMP manager. If the response is not received by the agent, it sends the inform request again.

An inform consumes more resources in the agent and in the network. Unlike a trap or notification, which is discarded by the agent as soon as it is sent, an inform request must be held in memory until a response is received, or the request times out. Traps and notifications can be sent only once, while informs can be sent multiple times. Resending informs increases traffic and contributes to a higher overhead on the network. The same traps, notifications, and informs can be sent to multiple host receivers.



Note For SNMPv3 informs to work, you must configure the Network Management Server (NMS) engineID with the SNMP user using the **snmp-server user***name* **engineID** command.

To get a Linux engineID from an NMS, start the **snmptrapd** and look for the **lcd_set_enginetime** string in the output.

```
#snmptrapd -f -D -Le 3162
lcd_set_enginetime: engineID 80 00 1F 88 80 14 D4 89 07 46 D5 74 5A 00 00 00
00 : boots=96, time=0
```

EngineID

An SNMP engineID is used to identify an entity independent of its source address. The entity consists of an SNMP engine and SNMP applications. The engineID is important when protocol data units (PDUs) must traverse proxies or Network Address Translator (NAT), or when the source entity itself has a dynamically assigned transport address or multiple source addresses.

In SNMPv3, engineIDs are also used for encoding and decoding secure PDUs. This is a requirement of the SNMPv3 user-based security model (USM).

There are two types of engineIDs, local and remote. On Cisco MDS 9000 Series switches, only remote engineIDs can be configured. The local engineID is automatically generated by the switch based on the MAC address and does not change.

LinkUp/LinkDown Notifications for Switches

You can configure which LinkUp/LinkDown notifications to enable on switches. You can enable the following types of LinkUp/LinkDown notifications:

- Cisco—Only notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Only notifications (LinkUp, LinkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the notification definition are sent with the notifications.
- IEFT extended—Only notifications (LinkUp, LinkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the notification definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent. This is the default setting.

- IEFT Cisco—Only notifications (LinkUp, LinkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the notification definition are sent with the linkUp and linkDown notifications.
- IEFT extended Cisco—Only notifications (LinkUp, LinkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in linkUp and linkDown notification definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent with the LinkUp and LinkDown notifications.



Note For more information on the varbinds defined in the IF-MIB specific to the Cisco Systems implementation, refer to the *Cisco MDS 9000 Family MIB Quick Reference*.

Scope of LinkUp and LinkDown Trap Settings

The LinkUp and LinkDown trap settings for the interfaces generate traps based on the following scope:

Switch-level Trap Setting	Interface-level Trap Setting	Trap Generated for Interface Links?
Enabled (default)	Enabled (default)	Yes
Enabled	Disabled	No
Disabled	Enabled	No
Disabled	Disabled	No

Default Settings

Table 2: Default SNMP Settings , on page 6 lists the default settings for all SNMP features in any switch.

Table 2: Default SNMP Settings

Parameters	Default
User account	No expiry (unless configured)
Password	None

Configuring SNMP

SNMP is an application layer protocol that facilitates the exchange of management information between network devices.

Assigning SNMP Switch Contact and Location Informations

You can assign the switch contact information, which is limited to 32 characters (without spaces), and the switch location.

To configure contact and location information, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server contact NewUser**

Assigns the contact name for the switch.

Step 3 switch(config)# **no snmp-server contact NewUser**

Deletes the contact name for the switch.

Step 4 switch(config)# **snmp-server location SanJose**

Assigns the switch location.

Step 5 switch(config)# **no snmp-server location SanJose**

Deletes the switch location.

Configuring SNMP Users from the CLI

The passphrase specified in the **snmp-server user** command and the **username** command are synchronized.

Starting from Cisco MDS NX-OS Release 8.5(1), DES encryption is no longer considered a secure privacy protocol and AES-128 is the default privacy protocol for SNMPv3 users.

Starting from Cisco MDS NX-OS Release 8.5(1), an In-Service System Downgrade (ISSD) using the **install all** command fails if SNMPv3 users are configured with DES privacy protocol. Users must be reconfigured using AES-128 privacy protocol or deleted. If the switch cold reboots, SNMPv3 users with DES privacy protocol are automatically deleted. The admin SNMPv3 user, which cannot be deleted, must be reconfigured with a non-DES privacy protocol.

Starting from Cisco MDS NX-OS Release 9.4(4), AES-256 privacy protocol is supported for SNMPv3 users. The maximum encryption key size is increased to 256 bits and is the recommended encryption type.



Note When the passphrase or password is specified in the **localizedkey** or encrypted format, the password is not synchronized. If a configuration file is copied to the device, the passwords will not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device.

To create or modify SNMP users from the CLI, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server user joe network-admin auth sha abcd1234**

Creates or modifies the settings for a user (joe) in the network-admin role using the HMAC-SHA-96 authentication password (abcd1234).

Note
From Cisco MDS NX-OS Release 8.5(1), AES-128 is the default privacy protocol for SNMPv3.

Step 3 switch(config)# **snmp-server user sam network-admin auth md5 abcdefgh**

Creates or modifies the settings for a user (sam) in the network-admin role using the HMAC-MD5-96 authentication password (abcdefgh).

Step 4 switch(config)# **snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh**

Creates or modifies the settings for a user (Bill) in the network-admin role using the HMAC-SHA-96 authentication level. AES-128 is used as the privacy encryption parameter from Cisco MDS NX-OS Release 8.5(1). Prior to Cisco MDS NX-OS Release 8.5(1), DES was used as the privacy protocol.

Step 5 switch(config)# **no snmp-server user usernameA**

Deletes the user (usernameA) and all associated parameters.

Step 6 switch(config)# **no snmp-server usam role vsan-admin**

Deletes the specified user (usam) from the vsan-admin role.

Step 7 switch(config)# **snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey**

Specifies the password to be in localized key format (RFC 2574). The localized key is provided in hexadecimal format (for example, 0xacbdef).

Step 8 switch(config)# **snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj**

Configures the user2 with the MD5 authentication protocol and AES-128 privacy protocol. This command is supported in releases prior to Cisco MDS NX-OS Release 8.5(1). AES-128 is the default privacy option from Cisco MDS NX-OS Release 8.5(1).

Step 9 (Optional) switch(config)# **snmp-server user user2 auth md5 Cisc0123 priv aes-256 Cisc0123**

Configures the user *user2* with the MD5 authentication protocol and the AES-256 privacy protocol. Starting from Cisco MDS NX-OS Release 9.4(4), the AES-256 encryption algorithm is supported increasing the key size to 256 bits. If aes-128 or no encryption protocol is specified in step 8 then aes-128 will be used.

Step 10 switch(config)# **snmp-server user joe sangroup**

Adds the specified user (joe) to the sangroup role.

Step 11 switch(config)# **snmp-server user joe techdocs**

Adds the specified user (joe) to the techdocs role.

Creating or Modifying Passwords

To create or modify passwords for SNMP users from the CLI, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey**

Specifies the password to be in localized key format using the DES option for security encryption.

Note
From Cisco MDS NX-OS Release 8.5(1), AES-128 is the default privacy protocol for SNMPv3.

Step 3 switch(config)# **snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey**

Specifies the password to be in localized key format using the 128-bit AES option for security encryption

Note
This command is supported in releases prior to Cisco MDS NX-OS Release 8.5(1). AES-128 is the default privacy option from Cisco MDS NX-OS Release 8.5(1).

The **snmp-server user** command takes the engineID as an additional parameter. The engineID creates the notification target user (see the Configuring the Notification Target User , on page 18). If the engineID is not specified, the local user is created.

Enforcing SNMPv3 Message Encryption

By default the SNMP agent allows the securityLevel parameters of authNoPriv and authPriv for the SNMPv3 messages that use user-configured SNMPv3 message encryption with auth and priv keys.

To enforce the message encryption for a user, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server user testUser enforcePriv**

Enforces the message encryption for SNMPv3 messages using this user.

Note
You can only use this command for previously existing users configured with both auth and priv keys. When the user is configured to enforce privacy, for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv, the SNMP agent responds with authorizationError.

Step 3 switch(config)# **no snmp-server user testUser enforcePriv**

Disables SNMPv3 message encryption enforcement.

Enforcing SNMPv3 Message Encryption Globally

Alternatively, you can enforce the SNMPv3 message encryption globally on all the users using the following commands:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server globalEnforcePriv**

Enforces the SNMPv3 message encryption for all the users on the switch.

Step 3 switch(config)# **no snmp-server globalEnforcePriv**

Disables global SNMPv3 message encryption enforcement.

Assigning SNMPv3 Users to Multiple Roles

The SNMP server user configuration is enhanced to accommodate multiple roles (groups) for SNMPv3 users. After the initial SNMPv3 user creation, you can map additional roles for the user.

Note Only users belonging to a network-admin role can assign roles to other users.

To configure multiple roles for SNMPv3 users from the CLI, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server user NewUser role1**

Creates or modifies the settings for an SNMPv3 user (NewUser) for the role1 role.

Step 3 switch(config)# **snmp-server user NewUser role2**

Creates or modifies the settings for an SNMPv3 user (NewUser) for the role2 role.

Step 4 switch(config)# **no snmp-server user User5 role2**

Removes role2 for the specified user (User5).

Adding Communities

You can configure read-only or read-write access for SNMPv1 and SNMPv2 users. Refer to RFC 2576.

To create an SNMPv1 or SNMPv2c community, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server community snmp_Community ro**

Adds read-only access for the specified SNMP community.

Step 3 switch(config)# **snmp-server community snmp_Community rw**

Adds read-write access for the specified SNMP community.

Step 4 switch(config)# **no snmp-server community snmp_Community**

Deletes access for the specified SNMP community (default).

Configuring SNMP Trap and Inform Notifications

You can configure the Cisco MDS switch to send notifications to SNMP managers when particular events occur.



Note Switches can forward events (SNMP traps and informs) up to 10 destinations. When you try to configure the eleventh target host for SNMP, the following message is displayed:

```
switch(config)# snmp-server host 10.4.200.173 traps version 2c noauth
reached maximum allowed targets limit
```

- You must enable the RMON traps in the SNMP configuration. For more information, refer to Configuring RMON.
- Use the SNMP-TARGET-MIB to obtain more information on the destinations to which notifications are to be sent either as traps or as informs. Refer to the Cisco MDS 9000 Family MIB Quick Reference.

Tip The SNMPv1 option is not available with the **snmp-server host** *ip-address* **informs** command.

Note SNMP hostname using DSN server name starting with 0. or 127. is not supported.

Configuring SNMPv2c Notifications

Configuring SNMPv2c Notifications using IPv4

To configure SNMPv2c notifications using IPv4, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host 171.71.187.101 traps version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).

Step 3 switch(config)# **no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).

Step 4 switch(config)# **snmp-server host 171.71.187.101 informs version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).

Step 5 switch(config)# **no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private).

Configuring SNMPv2c Notifications using IPv6

To configure SNMPv2c notifications using IPv6, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).

Step 3 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).

Step 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).

Step 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private).

Configuring SNMPv2c Notifications using DNS Name

To configure SNMPv2c notifications using the DNS Name of the SNMP notification host myhost.cisco.com, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host myhost.cisco.com traps version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).

Step 3 switch(config)# **no snmp-server host myhost.cisco.com traps version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).

Step 4 switch(config)# **snmp-server host myhost.cisco.com informs version 2c private udp-port 1163**

Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).

Step 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 2c private udp-port 2162**

Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private).

Note
Switches can forward events (SNMP traps and informs) up to 10 destinations.

Configuring SNMPv3 Notifications

Configuring SNMPv3 Notifications using IPv4

To configure SNMPv3 notifications using IPv4, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 traps using SNMPv3 user (testuser) and securityLevel of noAuthNoPriv.

Step 3 switch(config)# **snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthNoPriv.

Step 4 switch(config)# **snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthPriv.

Step 5 switch(config)# **no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162**

Prevents the specified host from receiving SNMPv3 informs.

Configuring SNMPv3 Notifications using IPv6

To configure SNMPv3 notifications using IPv6, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 traps using SNMPv3 user (testuser) and securityLevel of noAuthNoPriv.

Step 3 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthNoPriv.

Step 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthPriv.

Step 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162**

Prevents the specified host from receiving SNMPv3 informs.

Configuring SNMPv3 Notifications using DNS Name

To configure SNMPv3 notifications using the DNS Name of the SNMP notification host myhost.cisco.com, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server host myhost.cisco.com traps version 3 noauth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 traps using SNMPv3 user (testuser) and securityLevel of noAuthNoPriv.

Step 3 switch(config)# **snmp-server host myhost.cisco.com informs version 3 auth testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthNoPriv.

Step 4 switch(config)# **snmp-server host myhost.cisco.com informs version 3 priv testuser udp-port 1163**

Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthPriv.

Step 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 3 testuser noauth udp-port 2162**

Prevents the specified host from receiving SNMPv3 informs.

Authenticating SNMPv3 Users Based on Location

You can authenticate local or remote SNMPv3 users based on their location.

Use the following command in global configuration mode to enable AAA exclusive behavior in SNMPv3 servers:

Command	Purpose
snmp-server aaa exclusive-behavior enable	Enables the AAA exclusive behavior in SNMPv3 servers to authenticate users based on location. Depending on the location of the user and whether the AAA server is enabled, the exclusive behavior is as follows: • If the user is a local user and the AAA server is enabled, queries for the user will fail with an "Unknown user" message. • If the user is a remote AAA user and the AAA server is disabled, queries for the user will fail with an "Unknown user" message. • If the user is both a local user and a remote AAA user and the AAA server is enabled, the queries with remote credentials will succeed, and queries with local credentials will fail with an "Incorrect password" message. If the AAA server is disabled, queries with local remote credentials will succeed, and queries with remote credentials will fail with an "Incorrect password" message.

Enabling SNMP Notifications

Table 3: Enabling SNMP Notifications , on page 16 lists the CLI commands that enable the notifications for Cisco NX-OS MIBs.

Table 3: Enabling SNMP Notifications

MIB	DCNM-SAN Check Boxes
CISCO-ENTITY-FRU-CONTROL-MIB	**Click the Other tab and check FRU Changes.**
CISCO-FCC-MIB	**Click the Other tab and check FCC.**
CISCO-DM-MIB	**Click the FC tab and check Domain Mgr RCF.**
CISCO-NS-MIB	**Click the FC tab and check Name Server.**
CISCO-FCS-MIB	**Click the Other tab and check FCS Rejects.**
CISCO-FDMI-MIB	**Click the Other tab and check FDMI.**

MIB	DCNM-SAN Check Boxes
CISCO-FSPF-MIB	**Click the FC tab and check FSPF Neighbor Change.**
CISCO-LICENSE-MGR-MIB	**Click the Other tab and check License Manager.**
CISCO-IPSEC-SIGNALLING-MIB	**Click the Other tab and check IPSEC.**
CISCO-PSM-MIB	**Click the Other tab and check Port Security.**
CISCO-RSCN-MIB	**Click the FC tab and check RSCN ILS, and RCSN ELS.**
SNMPv2-MIB	**Click the Other tab and check SNMP AuthFailure.**
VRRP-MIB, CISCO-IETF-VRRP-MIB	**Click the Other tab and check VRRP.**
CISCO-ZS-MIB	**Click the FC tab and check Zone Rejects, Zone Merge Failures, Zone Merge Successes, Zone Default Policy Change, and Zone Unsuppd Mode.**

The following notifications are enabled by default:

- entity fru
- license
- link ietf-extended

All other notifications are disabled by default.

You can enable or disable the supported traps at the following levels:

- Switch level—You can use snmp-server enable traps command to enable all the traps in the supported MIBs at the switch level.
- Feature level—You can use snmp-server enable traps command with the feature name to enable traps at the feature level.

```
switch =>snmp-server enable traps callhome ?
event-notify    Callhome External Event Notification
smtp-send-fail  SMTP Message Send Fail notification
```

- Individual traps - You can use snmp-server enable traps command with the feature name to enable traps at the individual level.

```
switch =>snmp-server enable traps callhome event-notify ?
```

Note The snmp-server enable traps CLI command enables both traps and informs, depending on how you configured SNMP. See the notifications displayed with the snmp-server host CLI command.

To enable individual notifications, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server enable traps fcdomain**

Enables the specified SNMP (fcdomain) notification.

Step 3 switch(config)# **no snmp-server enable traps**

Disables the specified SNMP notification. If a notification name is not specified, all notifications are disabled.

Configuring the Notification Target User

You must configure a notification target user on the switch for sending SNMPv3 inform notifications to the SNMP manager.

For authenticating and decrypting the received INFORM PDU, the SNMP manager should have the same user credentials in its local configuration data store of users.

To configure the notification target user, use the following command:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

Configures the notification target user with the specified credentials for the SNMP manager with the specified engine ID.

Note
From Cisco MDS NX-OS Release 8.5(1), AES-128 is the default privacy protocol for SNMPv3.

Step 3 switch(config)# **no snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

Removes the notification target user.

The credentials of the notification target user are used for encrypting the SNMPv3 inform notification messages to the configured SNMPmanager (as in the **snmp-server host** command).

Configuring LinkUp/LinkDown Notifications for Switches

To configure the LinkUp/LinkDown notification for a switch using NX-OS Release 4.2(1) and later, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **snmp-server enable traps link extended-link**

Enables only IETF extended linkUp notifications.

Step 3 switch(config)# **snmp-server enable traps link extended-linkDown**

Enables only IETF extended linkDown notifications.

Step 4 switch(config)# **snmp-server enable traps link cieLinkDown**

Enables Cisco extended link state down notification.

Step 5 switch(config)# **snmp-server enable traps link cieLinkUp**

Enables Cisco extended link state up notification.

Step 6 switch(config)# **snmp-server enable traps link connUnitPortStatusChange**

Enables FCMGMT The overall status of the connectivity unit Notification.

Step 7 switch(config)# **snmp-server enable traps link delayed-link-state-change**

Enables Delayed link state change.

Disable the delayed link state traps to allow the device to generate port down SNMP alerts immediately.

- Use the **no system delayed-traps enable mode FX** command on NX-OS versions 6.2(5) or lower.
- Use the **no snmp-server enable traps link delayed-link-state-change** command on NX-OS version 6.2(7) and above.

Note
For upgrade between specific NX-OS release versions, ensure that delayed link state traps are disabled. When migrating from an earlier release like 5.(x) or 6.1(x) or 6.2(x) to a release 6.2(7) and above, ensure that you explicitly disable the delayed link state traps using **no snmp-server enable traps link delayed-link-state-change** command.

Step 8 switch(config)# **snmp-server enable traps link extended-linkDown**

Enables IETF extended link state down notification.

Step 9 switch(config)# **snmp-server enable traps link extended-linkUp**

Enables IETF extended link state down notification.

Step 10 switch(config)# **snmp-server enable traps link fcTrunkIfDownNotify**

Enables FCFE Link state down notification.

Step 11 switch(config)# **snmp-server enable traps link fcTrunkIfUpNotify**

Enables FCFE Link state up notification.

Step 12 switch(config)# **snmp-server enable traps link fcot-inserted**

Enables FCOT info trap.

Step 13 switch(config)# **snmp-server enable traps link fcot-removed**

Enables FCOT info trap.

Step 14 switch(config)# **snmp-server enable traps link linkDown**

Enables IETF Link state down notification.

Step 15 switch(config)# **snmp-server enable traps link linkUp**

Enables IETF Link state up notification.

Step 16 switch(config)# **no snmp-server enable traps link**

Reverts to the default setting (IETF extended).

Configuring Up/Down SNMP Link-State Traps for Interfaces

By default, SNMP link-state traps are enabled for all interfaces. Whenever a link toggles its state from Up to Down or vice versa, an SNMP trap is generated.

In some instances, you may find that you have numerous switches with hundreds of interfaces, many of which do not require monitoring of the link state. In such cases, you may elect to disable link-state traps.

To disable SNMP link-state traps for specific interfaces, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **interface fc** *slot/port*

Specifies the interface on which to disable SNMP link-state traps.

Step 3 switch(config-if)# **no link-state-trap**

Disables SNMP link-state traps for the interface.

Step 4 switch(config-if)# **link-state-trap**

Enables SNMP link-state traps for the interface.

Configuring Entity (FRU) Traps

To enable individual SNMP trap control, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 **switch(config)# snmp-server enable traps entity**

Enables individual SNMP trap control.

Step 3 **switch(config)# snmp-server enable entity_fan_status_change**

Enables entity fan status change.

Step 4 **switch(config)# snmp-server enable entity_mib_change**

Enables entity MIB change.

Step 5 **switch(config)# snmp-server enable entity_module_inserted**

Enables entity module to be inserted.

Step 6 **switch(config)# snmp-server enable entity_module_removed**

Enables entity module to be removed.

Step 7 **switch(config)# snmp-server enable entity_module_status_change**

Enables entity module status change.

Step 8 **switch(config)# snmp-server enable entity_power_out_change**

Enables entity power out change.

Step 9 **switch(config)# snmp-server enable entity_power_status_change**

Enables entity power status change.

Step 10 **switch(config)# snmp-server enable entity_unrecognised_module**

Enables entity unrecognized module.

Note
All these traps have to do with legacy FRU traps.

Modifying the AAA Synchronization Time

You can modify how long Cisco NX-OS holds the synchronized user configuration.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server aaa-user cache-timeout** *seconds* **Example:** `switch(config)# snmp-server aaa-user cache-timeout 1200`	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 60000.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying SNMP Configuration

To display the SNMP configuration information, perform one of the following tasks:

Command	Purpose
show running-config	Displays the running configuration **Note** From Cisco MDS NX-OS Release 8.5(1), SNMP users with the configured privacy protocol, AES-128 or DES, are displayed in the running configuration. This is unlike releases prior to Cisco MDS NX-OS Release 8.5(1) where only AES-128 users were displayed the **aes-128** option in the running configuration. From Cisco MDS NX-OS Release 8.5(1), users are configured with AES-128 protocol, by default.
show interface	Displays the SNMP link-state trap configuration for a particular interface
show snmp trap	Displays all the notifications and their status
show snmp	Displays configured SNMP information, counter information for SNMP contact, location, and packet settings.

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

Viewing the Up/Down SNMP Link-State Traps for Interfaces

Whenever you disable an SNMP link-state trap for an interface, the command is also added to the running configuration of the system.

To view the running configuration, use the **show running-config** command for the interface.

```
switch# no link-state-trap
switch# show running-config interface fc2/25

!Command: show running-config interface fc2/25
!Running configuration last done at: Fri Sep 20 11:28:19 2019
!Time: Fri Sep 20 11:28:22 2019

version 8.4(1)

interface fc2/25
  no link-state-trap
  no shutdown
```

To view the SNMP link-state trap configuration for a particular interface, enter the **show interface** command.

```
switch# show interface fc2/25

fc2/25 is trunking
    Hardware is Fibre Channel, SFP is long wave laser cost reduced
    Port WWN is 20:59:54:7f:ee:ea:c0:00
    Peer port WWN is 20:1d:00:de:fb:b1:7b:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Admin Speed is auto max 32 Gbps
    Operating Speed is 32 Gbps
    Rate mode is dedicated
    Port flow-control is ER_RDY
.
.
.
```

Displaying SNMP Traps

You can use the **show snmp trap** command to display all the notifications and their status.

```
switch# show snmp trap
--------------------------------------------------------------------------------
Trap type                                                              Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                              Yes
entity               : entity_module_status_change                    Yes
entity               : entity_power_status_change                     Yes
entity               : entity_module_inserted                         Yes
entity               : entity_module_removed                          Yes
entity               : entity_unrecognised_module                     Yes
entity               : entity_fan_status_change                       Yes
entity               : entity_power_out_change                        Yes
link                 : linkDown                                       Yes
link                 : linkUp                                         Yes
link                 : extended-linkDown                              Yes
link                 : extended-linkUp                                Yes
link                 : cieLinkDown                                    Yes
link                 : cieLinkUp                                      Yes
link                 : connUnitPortStatusChange                       Yes
link                 : fcTrunkIfUpNotify                              Yes
```

```
link                : fcTrunkIfDownNotify                       Yes
link                : delayed-link-state-change                 Yes
link                : fcot-inserted                             Yes
link                : fcot-removed                              Yes
callhome            : event-notify                              No
callhome            : smtp-send-fail                            No
cfs                 : state-change-notif                        No
cfs                 : merge-failure                             No
fcdomain            : dmNewPrincipalSwitchNotify                No
fcdomain            : dmDomainIdNotAssignedNotify               No
fcdomain            : dmFabricChangeNotify                      No
rf                  : redundancy_framework                      Yes
aaa                 : server-state-change                       No
license             : notify-license-expiry                     Yes
license             : notify-no-license-for-feature             Yes
license             : notify-licensefile-missing                Yes
license             : notify-license-expiry-warning             Yes
scsi                : scsi-disc-complete                        No
fcns                : reject-reg-req                            No
fcns                : local-entry-change                        No
fcns                : db-full                                   No
fcns                : remote-entry-change                       No
rscn                : rscnElsRejectReqNotify                    No
rscn                : rscnIlsRejectReqNotify                    No
rscn                : rscnElsRxRejectReqNotify                  No
rscn                : rscnIlsRxRejectReqNotify                  No
fcs                 : request-reject                            No
fcs                 : discovery-complete                        No
fctrace             : route                                     No
zone                : request-reject1                           No
zone                : merge-success                             No
zone                : merge-failure                             No
zone                : default-zone-behavior-change              No
zone                : unsupp-mem                                No
port-security       : fport-violation                           No
port-security       : eport-violation                           No
port-security       : fabric-binding-violation                  No
vni                 : virtual-interface-created                 No
vni                 : virtual-interface-removed                 No
vsan                : vsanStatusChange                          No
vsan                : vsanPortMembershipChange                  No
fspf                : fspfNbrStateChangeNotify                  No
upgrade             : UpgradeOpNotifyOnCompletion               No
upgrade             : UpgradeJobStatusNotify                    No
feature-control     : FeatureOpStatusChange                     No
vrrp                : cVrrpNotificationNewMaster                No
fdmi                : cfdmiRejectRegNotify                      No
snmp                : authentication                            No
```

Displaying SNMP Security Information

Use the **show snmp** commands to display configured SNMP information (see the following examples):

SNMP User Details

The following example SNMP user details:

```
switch# show snmp user
_____________________________________________________________
                    SNMP USERS
```

```
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  ____________  ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                    role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv

____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

SNMP Community Information

The following example displays SNMP community information:

```
switch# show snmp community

Community             Group / Access      context
_________             ______________      _______
dcnm_user             network-admin
admin                 network-admin
```

SNMP Host Information

The following example displays SNMP host information:

```
switch# show snmp host
Host                            Port Version  Level  Type   SecName
____                            ____ _______  ______ ____   ______
171.16.126.34                   2162 v2c      noauth trap   public
171.16.75.106                   2162 v2c      noauth trap   public
...
171.31.58.97                    2162 v2c      auth   trap   public
...
```

The **show snmp** command displays counter information for SNMP contact, location, and packet settings. This command provides information that is used entirely by the Cisco MDS 9000 Family DCNM-SAN (refer to the System Management Configuration Guide, Cisco DCNM for SAN). See the following example:

SNMP Information

The following example displays SNMP information:

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
```

```
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                       Group / Access
---------                       ------
public                           rw

_____________________________________________________________________
                  SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  _____________ ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                    role222

_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

Displays SNMP Engine IDs

The following example displays SNMP engine IDs:

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DEC2CF180
                     [Dec] 128:000:000:009:003:000:013:236:044:241:128
```

Information on SNMP Security Groups

The following example displays information on SNMP Security groups:

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-operator
```

```
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

Additional References

For additional information related to implementing SNMP, see the following sections:

MIBs

MIBs	MIBs Link
• CISCO-SNMP-TARGET-EXT-MIB • CISCO-SNMP-VACM-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html