CHAPTER 19

DLPs F401 to F499

DLP-F401 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task connects the CTC Launcher to ONS nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Start the CTC Launcher:

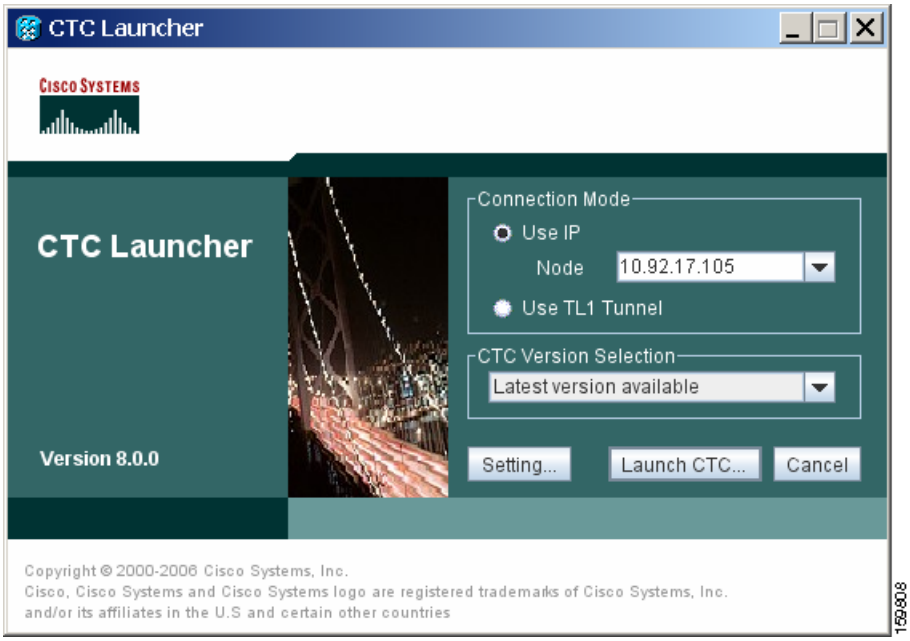
- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the StartCTC.exe file and type:

  % java -jar StartCTC.exe

Step 2 In the CTC Launcher dialog box, choose **Use IP**.

Figure 19-1 shows the CTC Launcher window.

Figure 19-1 CTC Launcher Window



Step 3 In the Login Node box, enter the ONS NE node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)

Step 4 Select the CTC version you want to launch from the following choices in the drop-down menu:

- Same version as the login node: Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.
- Latest version available: Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.
- Version x.xx: Select if you want to launch a specific CTC version.

Note Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is needed (for example, when CTC must manage a network containing mixed version NEs).

Step 5 Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS node.

Note Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory.

After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.

Step 7 Return to your originating procedure (NTP).

DLP-F402 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Double-click the StartCTC.exe file.

Step 2 Click **Use TL1 Tunnel**.

Step 3 In the Open CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the default TL1 port 3081 and 3082.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 When the CTC Login dialog box appears, complete the CTC login.

Step 7 Return to your originating procedure (NTP).

DLP-F403 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click **Create**.

Step 3 In the Create CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.

- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 After the CTC Login dialog box appears, log into CTC.

Step 7 Return to your originating procedure (NTP).

DLP-F404 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Log into CTC.

Step 2 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 3 In the TL1 Tunnels window, view the information shown in Table 19-1.

Table 19-1 TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS NE. It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
Port	The TCP port number where the GNE accepts TL1 connections coming from the DCN. These port numbers are standard (such as 3081 and 3082) unless custom port numbers are provisioned on the GNE.

Table 19-1 TL1 Tunnels Window (continued)

Item	Description
TL1 Encoding	Defines the TL1 encoding used for the tunnel: • LV + Binary Payload— TL1 messages are delimited by an LV (length value) header. TCP traffic is encapsulated in binary form. • LV + Base64 Payload— TL1 messages are delimited by an LV header. TCP traffic is encapsulated using the base 64 encoding. • Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
GNE TID	The GNE TID is shown when the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs. If present, CTC asks the user for the ACT-USER user ID and password when the tunnel is opened.
State	Indicates the tunnel state: OPEN—A tunnel is currently open and carrying TCP traffic. RETRY PENDING—The TL1 connection carrying the tunnel has been disconnected and a retry to reconnect it is pending. (CTC automatically attempts to reconnect the tunnel at regular intervals. During that time all ENEs behind the tunnel are unreachable.) (empty)—No tunnel is currently open.
Far End IP	The IP address of the ONS NE that is at the far end of the TL1 tunnel. This information is retrieved from the NE when the tunnel is established.
Sockets	The number of active TCP sockets that are multiplexed in the tunnel. This information is automatically updated in real time.
Retries	Indicates the number of times CTC tried to reopen a tunnel. If a network problem causes a tunnel to go down, CTC automatically tries to reopen it at regular intervals. This information is automatically updated in real time.
Rx Bytes	Shows the number of bytes of management traffic that were received over the tunnel. This information is automatically updated in real time.
Tx Bytes	Shows the number of bytes of management traffic that were transmitted over the tunnel. This information is automatically updated in real time.

Step 4 Return to your originating procedure (NTP).

DLP-F405 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit CTC TL1 Tunnel dialog box, edit the following:

- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
- Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click **OK**.

Step 6 If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue Step 6.

a. In the UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Step 8 Return to your originating procedure (NTP).

DLP-F406 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F407 Create an SNMPv3 User

Purpose	This procedure creates an SNMPv3 user.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > User** 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 six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters.
- Group Name—Specify the group to which the user belongs.
- 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 NONE or DES as the privacy authentication algorithm.
  - Password—Enter a password if you select DES.

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

Step 5 Return to your originating procedure (NTP).

DLP-F408 Create MIB Views

Purpose	This procedure creates an SNMPv3 MIB view.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > 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 Include and Exclude. 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-F409 Create Group Access

Purpose	This procedure creates a user group and configures the access parameters for the users in the group.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

- Security Level—The security level for which the access parameters are defined. 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.
- 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-F410 Configure SNMPv3 Trap Destination

Purpose	This procedure provisions SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > Trap Destinations (V3)** 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. This field is optional and traps can also be sent without providing a filter profile and create a notification filter. For more information, see "DLP-F412 Create Notification Filters" task on page 19-12.
- 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 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F411 Delete SNMPv3 Trap Destination

Purpose	This procedure deletes an SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP> SNMPv3 > Trap Destination** tabs.

Step 2 In the Trap Destinations area, select the trap destination you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F412 Create Notification Filters

Purpose	This procedure creates SNMPv3 notification filters. The notification filters are used to filter the notifications or traps, which should or should not be transmitted to the management target.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 2 Click **Create**.

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

- Filter Profile Name—Specify a name for the filter.
- 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.
- View Type—Select the view type. Options are Include and Exclude. 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-F413 Manually Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- 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 **Manual Create**.

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

- Target IP 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 or DES as the privacy authentication algorithm.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

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

Step 6 Return to your originating procedure (NTP).

DLP-F414 Automatically Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.

- 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-F415 Manually Configure the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- 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 Trap Forwarder Table area, click **Manual Create**.

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

- Remote Trap Source—Select the IP address from which the traps are sent. If the IP address is not listed, enter the IP address manually.
- Context Engine ID—Specify the context engine ID of the ENE from which traps need to be forwarded. This field is automatically populated if the source of trap is selected. If the source of trap is not specified, you need to manually enter the context engine ID.
- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. Traps are forwarded to all GNE Trap destinations whose proxy tags list contains this tag.
- Remote User Details
  - User Name—Specify the user name.
  - Security Level—Select the security level for the user. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication—Select the authentication algorithm.
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA. Default is None.
  - 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 or DES as the privacy authentication algorithm. Encryption is disabled if NONE is selected.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

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

Step 6 Return to your originating procedure (NTP).

DLP-F416 Automatically Configure 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-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.

- 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 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).