Infinera Cloud Xpress

SNMP Agent Reference Guide

Release 17.1
Version 001

Document ID 1900-001887

Infinera Corporation
140 Caspian Court
Sunnyvale, California 94089
www.infinera.com

Copyright

Trademarks

Infinera DTN-X, DTN, FlexILS, Cloud Xpress, XT, and ATN Regulatory Compliance

FCC Class A

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Modifying the equipment without Infinera's written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

DOC Class A

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard titled “Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le Ministère des Communications.

Class A

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。

この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FDA

This product complies with the DHHS Rules 21CFR 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

Contents

List of Figures

List of Tables

About this Document

This chapter provides an overview of the *Infinera Cloud Xpress SNMP Reference Guide*.

Objective

This document describes the user interface for the Infinera® Cloud-Xpress Simple Network Management Protocol (SNMP) Agent. It provides detailed instructions to configure the Infinera Cloud-Xpress SNMP Agent.

Audience

The primary audience for this manual includes network operations and maintenance engineers who are responsible for deploying, monitoring and administering Infinera Intelligent Transport Network. This guide assumes that the reader is familiar with the basic internet working terminology and concepts.

Document Organization

The following table describes each chapter in this guide.

Chapter	Description
Infinera SNMP Overview	Provides an introduction to the Infinera Cloud-Xpress SNMP Agent.
SNMP Support on Cloud Xpress	Describes the procedures to setup SNMP support on the Infinera Cloud Xpress network element. The Infinera Cloud Xpress network element, referred to as CX, is a 500G transport network element deployed as part of a point-to-point network configuration.

Chapter	Description
SNMP Traps	Provides the list of alarms, TCAs and events supported. Additionally, the list of all attributes displayed as part of alarms, TCAs and events.
NU Design MIB Browser Settings	Describes the Infinera recommended settings and procedure to load Infinera MIBs and modify event configuration from Nu Design MIB Browser.

Documents for Release 17.1

The following documents are available for Infinera Cloud Xpress.

Document Name	Document ID	Description
Infinera Cloud Xpress Hardware Installation and Configuration Guide	1900-001882	Describes the procedures for initial installation and configuration of the Infinera Cloud Xpress at any given site. Includes procedures and requirements for safety, site preparation and site testing, chassis installation, system cabling, and initial commissioning of the chassis.
Infinera Cloud Xpress Hardware Description Guide	1900-001883	Provides the hardware description of the Infinera Cloud Xpress which includes the description of chassis, common modules and circuit packs. It provides hardware block diagrams, functional descriptions, mechanical and electrical specifications for each module.
Infinera Cloud Xpress System Description Guide	1900-001884	Provides an overview of the Cloud Xpress functionality.
Infinera Cloud Xpress CLI User Guide	1900-001885	Describes the Command Line Interface (CLI) supported by the Infinera Cloud Xpress. It includes the description of the supported CLI commands and the procedures for the commonly performed OAM&P functions.
Infinera Cloud Xpress NETCONF Agent Reference Guide	1900-001886	Describes the Infinera® Cloud Xpress Network Configuration (NETCONF) Agent.
Infinera Cloud Xpress SNMP Agent Reference Guide	1900-001887	Provides the user interface for the Infinera® Cloud Xpress Simple Network Management Protocol (SNMP) Agent. It provides detailed instructions to configure the Infinera Cloud Xpress SNMP Agent.
Infinera Cloud Xpress Task Oriented Procedures Guide	1900-001888	Provides the routine task oriented procedures (TOPs) used in support of the Infinera Cloud Xpress network elements.
Infinera Cloud Xpress Operations and Maintenance Guide	1900-001889	Provides the Infinera Cloud Xpress Alarms and Configurations for RADIUS and TACACS+ files Server.

Document Name	Document ID	Description
Infinera Cloud Xpress Acronyms	1900-001604	Lists the acronyms used in Cloud Xpress Infinera documentation.
Infinera License Manager User Guide	1900-001890	Describes the Infinera License Manager standalone application used to perform instant bandwidth licensing operations on Cloud Xpress nodes.
Infinera Cloud Xpress RESTCONF Agent Reference Guide	1900-001952	Describes the Infinera® Cloud Xpress REpresentational State Transfer Configuration Protocol (RESTCONF) Agent.

Conventions

The table below lists the conventions used in this guide.

Convention	Item	Example
bold default font	Menu command paths	Select **Fault Management-> Alarm Manager**
	Button names	Click **Apply**
	User interface labels	Click **Summary** panel
	Window/dialog box titles	In the **Dial-Up Networking** window
`courier font`	User-entered text	In the **Label** enter EastBMM
	Command output	Database restore from local or remote machine?
	Directory path	/DNA/EMS **Note:** If the directory path or command is spanning across two lines, copy the directory path or command to notepad and execute in editor.
default font, italic	Document titles	Refer to the *CLI User Guide*
Default font	Icon names	Click Node icon

Convention	Item	Example
	Window names not in the user interface	In the DNA Main View
Note:	Helpful suggestions	**Note:** The window is refreshed only after making all the changes.

Technical Assistance

Customer Support for Infinera products is available, 24 hours a day, 7 days a week (24x7). For information or assistance with Infinera products, please contact the Infinera Technical Assistance Center (TAC) using any of the methods listed below:

- Email: techsupport@infinera.com
- Telephone:
  - Direct within United States: 1-408-572-5288
  - Outside North America: +1-408-572-5288
  - Toll-free within United States: +1-877-INF-5288 (+1-877-463-5288)
  - Toll-free within Germany/France/Benelux/United Kingdom: 00-800-4634-6372
  - Toll-free within Japan: 010-800-4634-6372
- Infinera corporate website: http://www.infinera.com
- Infinera Customer Web Portal: https://support.infinera.com

  Please see the Infinera Customer Web Portal to view technical support policies and procedures, to download software updates and product documentation, or to create/update incident reports and RMA requests.

Documentation Feedback

Infinera strives to constantly improve the quality of its products and documentation. Please submit comments or suggestions regarding Infinera Technical Product Documentation using any of the following methods:

- Submit a service request using the Infinera Customer Web Portal
- Send email to: techpubs@infinera.com
- Send mail to the following address:

  Attention: Infinera Technical Documentation and Technical Training

  Infinera Corporation

  140 Caspian Court

Sunnyvale, CA 94089

When submitting comments, please include the following information:

- Document name and document ID written on the document cover page
- Document release number and version written on the document cover page
- Page number(s) in the document on which there are comments

CHAPTER 1

Infinera SNMP Agent Overview

This chapter provides an introduction to the Infinera SNMP Agent. It includes the following sections:

Infinera SNMP Agent Overview

The SNMP protocol is an application layer protocol in the OSI protocol suite. The Infinera SNMP Agent running on the Cloud Xpress network element supports the SNMP protocol operations between the SNMP Manager and the SNMP Agent. The SNMP Manager is a network management station and the Cloud Xpress SNMP Agent resides on the Infinera network element.

Infinera SNMP Agent is a multi-lingual agent as defined in RFC 3584 and can handle SNMPv2c and SNMPv3 messages seamlessly.

The main components of a SNMP managed network are:

- **SNMP Manager**—The SNMP managed network supports three types of SNMP managers:
  - SNMP Managers configured to perform request operations. These managers are labeled as Allowed Managers in the graphic user interface.
  - SNMP managers configured to receive traps. These managers are labeled as Trap Destinations in the graphic user interface.
  - SNMP Managers configured to process requests and receive SNMP traps.
- **SNMP Agent**—The Infinera SNMP Agent is a software module residing on the Infinera network element. The SNMP agent:
  - Processes requests made by the SNMP Manager and returns response to the SNMP Manager.
  - Generates autonomous traps for any events, alarms and threshold crossing alerts raised by the network element and forwards it to the appropriate SNMP Manager that is registered to receive traps.

The SNMP Manager(s) and the SNMP Agent maintain a copy of the management information base (MIB) that is kept in sync at all times.

The SNMP Agent provides the following benefits:

- Ability to integrate the Infinera network elements with third party network management system based on SNMP.
- Ease of integration with third party off-the-shelf value added tool-kits spanning various applications.

The SNMP Agent provides the following capabilities:

- Processes requests received from SNMP Managers to the Infinera network elements and returns the response to the SNMP Manager.
- Ability to configure a list of SNMP Managers that can access the Infinera SNMP Agent. Only requests from any of the configured SNMP Managers are processed. All other requests received from any other SNMP Managers are dropped.
- Ability to configure community strings. A community string is an authenticator for a SNMPv2c request process. The network element performs the authentication for each SNMP request made to the SNMP agent. Community strings are configured on the SNMP Manager and the network element. Only if both of them match, the requests are processed.

- Provides the capability to configure the list of SNMP Managers to which the traps can be forwarded. These SNMP Managers are called Trap Destinations.
- Provides an ability to raise an authentication failure trap if the community string is invalid or a USM authentication fails.
- Provides the user to select a policy to forward traps from a network element to the SNMP Manager.
- Supports the standard User Based Security Model for authentication and privacy mechanisms as defined in RFC 3414.
- Supports the standard View Based Access Control Model for access control as defined in RFC 3415
- Supports the standard set of SNMP Applications as defined in RFC 3413. The Notification Generation application does not support INFORM notification type at the time of this release. Only TRAP Notification type is supported.

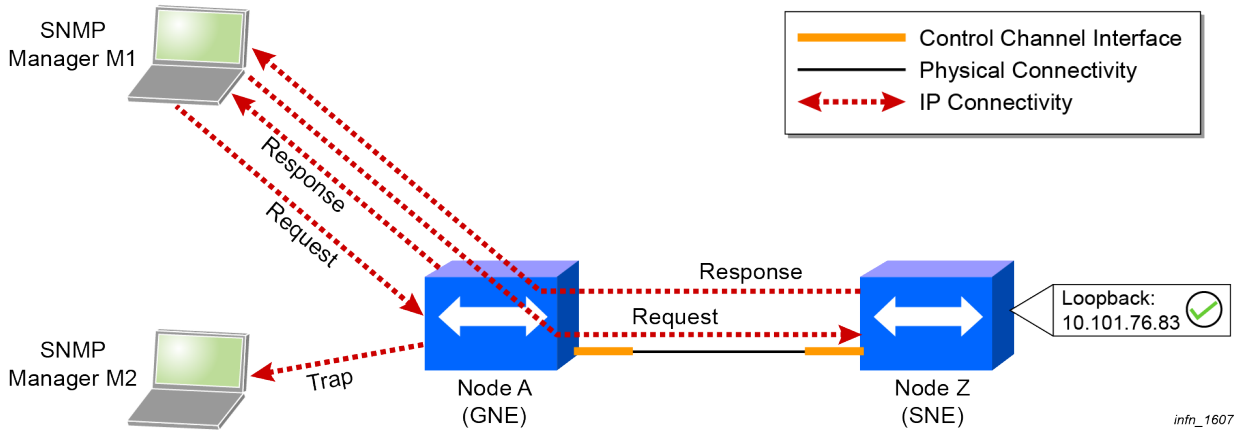
The SNMP Agent complies with the following RFC standards:

- RFC-2578 SMI
- RFC-2579 SMIv2 Textual Conventions
- RFC-2580 SMIv2 Conformance statement
- RFC-3416 SNMPv2 protocol operations (INFORM-Requests not supported)

The SNMP Agent supports the following RFCs for the SNMPv3 protocol:

- RFC3411
- RFC3412
- RFC3413
- RFC3414
- RFC3415
- RFC3584

Figure 1-1 SNMP Management Scenario



In Figure 1-1: SNMP Management Scenario on page 1-4 the SNMP Manager M1 is registered to perform request operations. The SNMP Manager M2 is registered to receive traps from the network element and to perform request operations.

The GNE is a network element that is directly IP addressable from the DCN. The GNE provides management proxy services to any network element within the same routing domain as the GNE. The GNE provides management proxy service to any management traffic received via its DCN. The SNE is a network element that does not have physical connectivity to the DCN and is not directly IP addressable from the DCN. In-Band communication is enabled between GNE and SNE.

- Any request operation from the SNMP Manager to SNE is IP tunneled through GNE.
- Any response operation from SNE to the requesting SNMP Manager is IP tunneled through GNE

SNMP Versions Supported

The Infinera network elements supports the following SNMP protocol versions:

- SNMPv2c
- SNMPv3

SNMP Features

This section describes the features of the Infinera SNMP Agent supported on the Infinera network elements. It covers the following:

SNMP Request Configuration

The SNMP Agent supports the retrieval of MIB data from a network element with or without DCN connectivity. This feature is helpful to monitor remote network elements in a large network where not all network elements have IP connectivity.

The network element provides the capability to configure a list of SNMP Managers that can access the network element. A maximum of 10 SNMP Managers can be configured to be accessible by each network element. Only requests from any of the valid SNMP Managers configured on the network element are processed. All other requests received from any other SNMP Managers are dropped. The list of SNMP Managers configured is validated only when the parameter for validation is enabled. If the parameter for validation is not enabled, then no authentication for the list of SNMP Managers is performed and request from all SNMP Managers are processed. If it is a SNMPv2C request, the community string is validated. If the request is SNMPv3, the USM user is validated.

The network element performs the following levels of validation in the order SNMP requests are received from the SNMP Managers:

- Checks if the network element is enabled for validation based on a list of allowed SNMP Managers
- Checks if the request received is from any of the configured SNMP Managers and the above condition is met
- Checks if the community string matches on the network element and the SNMP Manager. For SNMPv3, checks if the USM user ‘s credentials are authenticated by the network element

If all above conditions are met, the SNMP request is processed.

The network element communicates with the SNMP Manager using the following SNMP Operations:

- `get-request`
- `get-next-request`

Figure 1-2 SNMP Management Scenario

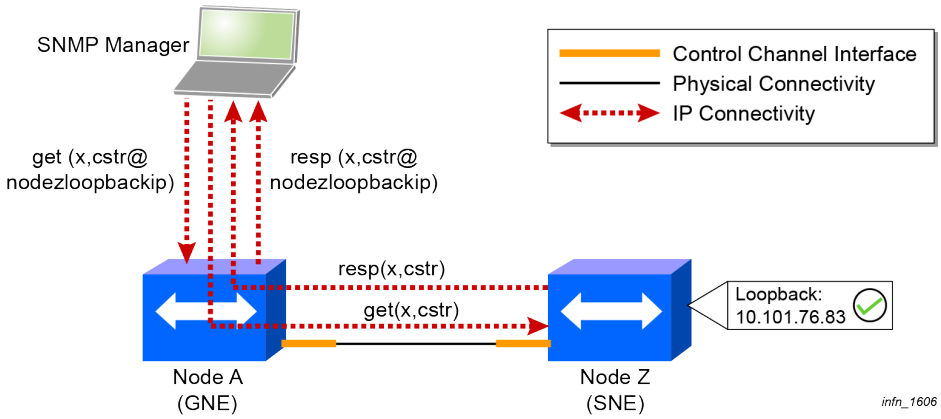


Figure 1-2: SNMP Management Scenario on page 1-7 describes the interaction between the SNMP Manager and the SNMP Agent. The SNMP Manager M1 is registered to perform request operations on GNE. The SNMP Manager M2 is registered to receive traps from all network elements. The functionality is as follows:

- Any request operation from M1 to the GNE is processed and the response is sent to the SNMP Manager M1
- Any alarms, events or TCAs raised by the GNE are forwarded as TRAPS to the SNMP Manager M2
- Any request operation from M1 to the SNE is IP tunneled through GNE.
- Any response from SNE to M1 is IP tunneled through GNE.

Allowed SNMP Managers

The network element provides the capability to configure a list of SNMP Managers that can be accessible by the network element. A maximum of 10 SNMP Managers can be configured to be accessible by each network element. Only requests from any of the SNMP Managers configured on the network element are processed. All other requests received from any other SNMP Managers are dropped. The network element provides the ability to enable or disable the authentication based on the IP address of the SNMP Manager. This feature is enabled by selecting the checkbox **Enable IP Access List** in the NE SNMP Configuration window. See Configure Allowed Manager in CX on page 2-3 for the detailed procedure. If the parameter for validation is not enabled, then no authentication for the list of SNMP Managers is performed and request from any SNMP Manager is processed.

Authentication Failure Traps

As described in Community Strings on page 1-10, the first level of authentication by the network element is performed on the list of configured SNMP Managers (if configured and enabled for validation). If both the IP address and the community string are valid, the SNMP request is processed.

- If the network element is enabled for SNMP Managers and the request received from one of the allowed managers and the community string is invalid, an Authentication Failure Trap is raised.
- If the network element is not enabled for validation on the list of configured SNMP Managers, the first and only level of the authentication is performed on the community string. If the community string is invalid an Authentication Failure Trap is raised.
- If the network element is enabled for validation and the SNMP Manager is not in the list of configured manager, no Authentication Failure Trap is raised.

The Authentication Failure Trap is raised if the Authentication Failed Trap checkbox is enabled in the NE SNMP Configuration window. See Enable Authentication Failure Trap on page 2-10 for detailed procedure. By default, the network element is not configured to raise an Authentication Failure Trap.

The authentication failure trap can be configured via CLI/DNA.

Enterprise specific authentication failure traps and cold start trap

An additional trap is received for every standard trap like Authentication Failure and Cold Start. As the standard SNMPv2 trap has no var-bind indicating the SNMP Agent that sent the trap, the TRAP manager cannot differentiate such traps (such as cold start trap). To enable this differentiation an additional Enterprise Specific TRAP is sent, (`infnAdminEventNotification`) which specifies the Node Id (and more) of the Node generating the TRAP in the var-bind in the TRAP PDU.

The SNMP Agent can be configured in the following methods:

- Using one of the management interfaces like CLI or DNA. See SNMP Agent Configuration using Infinera Management Interfaces on page 1-9.
- Using any standard third-party SNMP Manager. See SNMP Agent Configuration using Standard Third-Party SNMP Managers on page 1-11.

Note: It is recommended that any *one* of the methods should be used. Do not attempt to use both simultaneously.

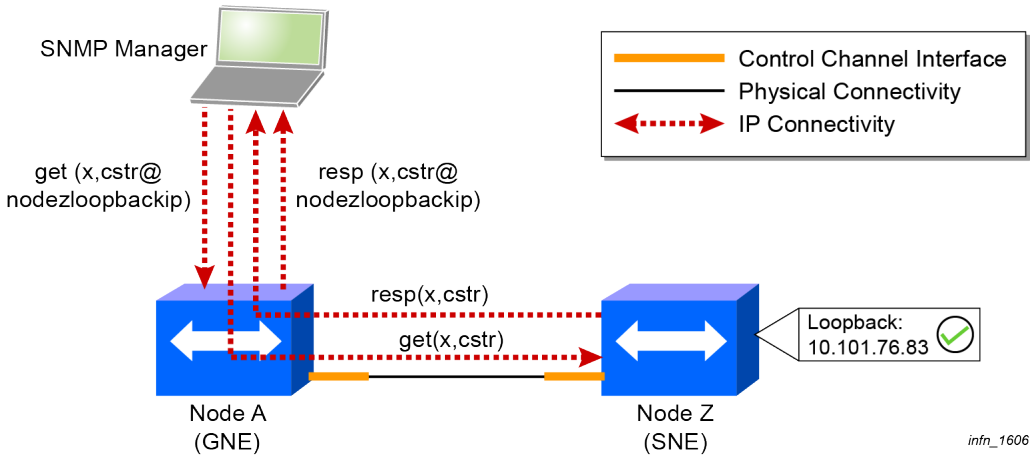
SNMP Agent Configuration using Infinera Management Interfaces

This section describes the behavior and configuration of the SNMP agent when it is managed by one of the Infinera Management interfaces such as CLI or DNA. For procedural details, see Setting up SNMP Support in CX on page 2-2.

Request-Response behavior in GNE-SNE configuration

In Figure 1-3: Request-Response behavior in GNE-SNE configuration on page 1-9, the SNMP Manager requests to SNE are IP forwarded through GNE. The community string sent by the manager should include the Loopback IP address of the SNE to which the access request is required.

Figure 1-3 Request-Response behavior in GNE-SNE configuration



In Figure 1-3: Request-Response behavior in GNE-SNE configuration on page 1-9, `cstr` is the community string configured on the SNE, `sneloopbackip` is the loopback IP address of the SNE.

- The communication between the SNMP Manager, GNE and the SNE is as follows:
  - The SNMP Manager sends requests to the SNE by including the loopback IP address of the SNE in the community string. The format of the community string will be *<community string as configured on the Node2>@<Loopback IP address of Node2>.* See Configure SNMP Community Strings in CX *on page 2-4* to configure community strings.
  - The SNE processes the request and sends back the result to the SNMP Manager.

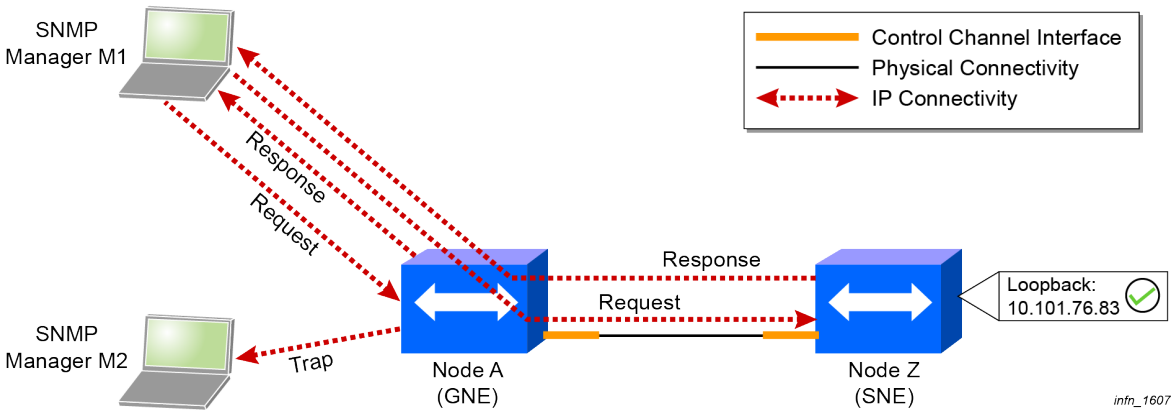
Trap Generation

The network element provides the capability to configure the list of SNMP Managers to which the traps can be forwarded. These SNMP Managers are called Trap Destinations. A maximum of 10 SNMP Managers can be configured per network element as Trap Destinations. The network element also

provides the capability to decide on a policy to forward traps from a network element to the SNMP Manager. The following options are provided:

- **Disabled**—If the trap proxy forwarding is disabled and there is no DCN connectivity to the SNMP Manager, no traps are received from this network element. If DCN connectivity is available, the traps are sent directly via DCN. This is the default option set by the network element.

Figure 1-4 SNMP Management Scenario



As displayed in Figure 1-4: SNMP Management Scenario on page 1-10, any alarms, events or TCAs raised by the GNE are forwarded as traps to the SNMP Manager M2.

The TRAP sent out by the network element conforms to SNMPv2-Trap format as mentioned in RFC 3416.

Community Strings

The SNMP community string is a form of authentication and access control for the SNMP Manager to access the network element. The network element provides the ability to configure a list of community strings using which the network element verifies the authentication of the request from the SNMP Manager. A maximum of 10 community strings can be configured on a network element. The network element performs the authentication for each request made to the Cloud Xpress SNMP agent. See Configure SNMP Community Strings in CX on page 2-4 for detailed procedures.

SNMP Agent Configuration using Standard Third-Party SNMP Managers

In order to enable any standard third-party SNMP Managers to configure the SNMP Agent, the agent supports some of the standard SNMP Configuration MIBs.Table 1-1: SNMP MIB and RFC compliance on page 1-11 lists the SNMP MIBs and RFC compliance.

The SNMP Agent is enhanced to support SNMPv3 and the ability to use GET to retrieve network element inventory information. The GET function is supported on all the supported MIBs. The SET function is supported on configuration MIBs. See Supported MIBs on page 1-16.

Table 1-1 SNMP MIB and RFC compliance

SNMP MIB Name	RFC	Standard SNMP Tables
SNMP-TARGET-MIB	RFC 3413	■ snmpTargetAddrTable ■ snmpTargetParamsTable
SNMP-NOTIFICATION-MIB	RFC 3413	■ snmpNotifyTable ■ snmpNotifyFilterProfileTable ■ snmpNotifyFilterTable
SNMP-PROXY-MIB	RFC 3413	snmpProxyTable
SNMP-USER-BASED-SM-MIB	RFC 3414	usmUserTable
SNMP-VIEW-BASED-ACM-MIB	RFC 3415	■ vacmContextTable ■ vacmSecurityToGroupTable ■ vacmAccessTable ■ vacmViewTreeFamilyTable
SNMP-COMMUNITY-MIB	RFC 3584	snmpCommunityTable
SNMP-FRAMEWORK-MIB	RFC3411	Defines snmpEngine related scalars like snmpEngineID, snmpEngineBoots

To enable remote configuration, Release 5.1, introduces the support for SET operations on the standard SNMP tables listed in Table 1-1: SNMP MIB and RFC compliance on page 1-11. Third party SNMP Managers can issue SNMP SET operations to create, modify or delete rows in the standard SNMP tables. The Cloud Xpress SNMP Agent provides a default USM user called `snmpadmin` to enable SNMP Managers to configure the network element through SNMP SET requests. For security reasons on the network element, the default user `snmpadmin` is not enabled by default. The user can be activated with required authentication and privacy parameters from the NE SNMP Configuration window. Once the user is enabled, it can be used to configure SNMP tables. See SNMPv3 User Administration on page 2-12.

Every Cloud Xpress SNMP Agent has an administratively unique identifier called SNMP Engine ID constructed as defined in the SNMP-FRAMEWORK-MIB. The SNMP Engine ID of the Cloud Xpress SNMP Agent can be retrieved by issuing a GET request for the OID 1.3.6.1.6.3.10.2.1.1.0. This OID is defined in the SNMP-FRAMEWORK-MIB. The semantic for the Engine ID is as follows:

- The first bit is 1, which indicates that the rest of the data is composed as defined by the Infinera.
- The first four octets are set to the binary equivalent of the SNMP Agent assigned by Internet Assigned Numbers Authority (IANA) which is 21296 for Infinera.
- The fifth octet indicates how the remaining octets are formatted. The value 5 indicates that the octets are administratively assigned having maximum remaining length 27.
- All octects from the 6th are binary equivalent of the Backplane ID of the chassis.

Alternatively, it can send an SNMPv3 request without any SNMP Engine ID in the request and the agent will send back a Report-PDU with the SNMP Engine ID and the timeliness parameters, `snmpEngineBoots` and `snmpEngineTime`.

`Ifindex` is a unique positive integer generated by the network element when a managed object is created. The index will be associated with the managed object for the lifetime of the object. The value of `ifindex` cannot be modified. Ifindex is persistent and will not get changed when the network element is rebooted. It is unique in the MIB groups.

Request-Response Configuration

In order to configure the Cloud Xpress SNMP Agent for SNMP requests, the SNMP Manager issues SET requests with `snmpadmin` user to the Cloud Xpress SNMP Agent to create/modify rows in the following tables

- `snmpCommunityTable` (for community based authentication) or `usmUserTable` (for user based authentication)
- `snmpTargetParamsTable`
- `vacmSecurityToGroupTable`
- `vacmAccessTable`
- `vacmViewTreeFamilyTable`

Interoperability with external SNMP Managers

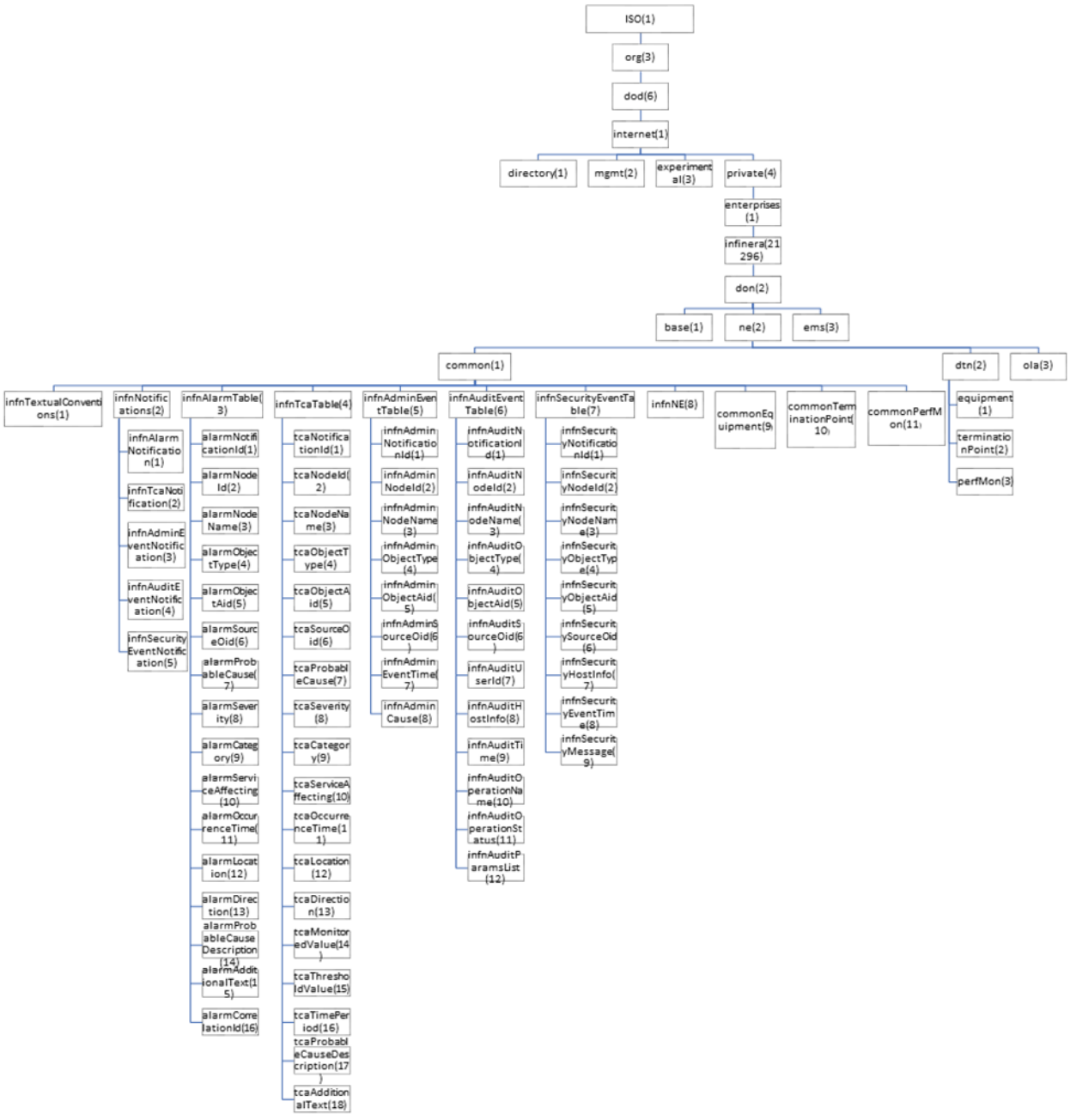
At the time of this release the Cloud Xpress SNMP Agent is tested with:

- NuDesign version 7.2.

SNMP MIB Tree

This section depicts the managed objects defined in the Infinera MIB files tree structure. A specific instance of a managed object is known as object instance. A MIB file contains the description of the object hierarchy on the managed device, also as an Object ID, syntax, and access privileges for each variable in the MIB. Objects are arranged in a hierarchical, inverted tree structure. Object Identifiers (Object IDs or OIDs) are series of numbers that uniquely identify a managed object.

Figure 1-5 SNMP MIB Tree Structure



Supported MIBs

MIB rules define the object ID and provide them a valid name. Typically, objects that can be managed by SNMP are defined in MIBs, which are ASCII text files in a structured format.

The CX SNMP Agent supports the Infinera enterprise MIBs that can be obtained from the following locations:

- The Infinera IQ NOS CD.
- The Infinera ftp website ftp.infinera.com. Contact Infinera Technical Assistance.

Note: Refer to the corresponding NU Design documentation for detailed procedures on how to load the MIBs. Additionally, refer to NU Design MIB Browser Settings on page A-1.

MIBs	Description
Common MIBs	
INFINERA-REG-MIB	This module defines the Infinera Registration for SNMP enterprise hierarchy."
INFINERA-TC-MIB	Textual conventions used by Infinera Network Elements MIBs
INFINERA-SYSTEMS	Infinera systems MIBs; Information of a Network element
INFINERA-DHCP-MIB	DHCP MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-ZTP-MIB	Zero Touch Provisioning MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SYSLOG-MIB	System Log MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-STATICROUTE-MIB	Static Route MIB. Each entry is uniquely identified by the value of ifIndex.
Trap MIB	
INFINERA-NOTIFICATION-MIB	Module representing trap notifications generated by Infinera Network Elements. Retrieval is supported only alarms and TCAs. It is not supported for events.
PM MIBs	
INFINERA-PM-XOCGPTP	PM information pertaining to Infinera cxOcgPtp interfaces. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type cxOcgPtp. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
INFINERA-PM-GIGECLIENTCTP	This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type GigeClientCtp. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration
INFINERA-PM-OCHCTP	OCHCTP PM MIB. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type GigeClientCtp. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.

MIBs	Description
INFINERA-PM-TRIBPTP	TRIBPTP PM MIB. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type GigeClientCtp. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
RMON-MIB	Standard RMON MIB.
INFINERA-PM-PEM	PEM PM MIB.
INFINERA-PM-FAN	FAN PM MIB.
INFINERA-PM-SECYTXSCSTATS	PM information pertaining to Infinera MACSEC Secy Tx Secure Channel objects. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type Secy Tx Secure Channel objects. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
INFINERA-PM-SECYRXSCSTATS	PM information pertaining to Infinera MACSEC Secy Rx Secure Channel objects. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type Secy Rx Secure Channel objects. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
INFINERA-PM-SECYSTATS	PM information pertaining to Infinera MACSEC Secy Secure Entity Objects. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type SecyStats. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
INFINERA-PM-XSCGPTP	PM information pertaining to Infinera cxScgPtp interfaces. This table is a subclass of IfCommon. Entries will exist in this table only for interfaces of type cxScgPtp. Each interface may have a number of entries in this table, each with a different combination of timestamp and sample duration.
Facilities MIB	
INFINERA-TP-CXOCGPTP	CX OCG PTP MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-GBECLIENTCTP	GbE MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-IFCOMMON	Common MIB applicable to all facilities. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-NCTGIGE	NCT GIGE MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-OCHCTP	OCH MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-TRIBPTP	TRIB MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-TP-LLDPPTP	LLDP MIB. Each entry is uniquely identified by the value of ifIndex.
INFN-RFC2863	Interface MIB. Each entry is uniquely identified by the value of ifIndex.
Equipment MIB	
INFINERA-ENTITY-CHASSIS	Chassis MIB, Each entry is uniquely identified by the value of entPhysicalIndex.
INFINERA-ENTITY-EQPT	EQPT MIB is common attributes; Each entry is uniquely identified by the value of entPhysicalIndex.

MIBs	Description
INFINERA-ENTITY-FAN	FAN MIB. Each entry is uniquely identified by the value of entPhysicalIndex.
INFINERA-ENTITY-PEM	PEM MIB. Each entry is uniquely identified by the value of entPhysicalIndex
INFINERA-ENTITY-RFC-4133	Entity MIB. Each entry is uniquely identified by the value of entPhysicalIndex
INFINERA-ENTITY-TOM	TOM MIB. Each entry is uniquely identified by the value of entPhysicalIndex
INFINERA-ENTITY-XMM	XMM MIB. Each entry is uniquely identified by the value of entPhysicalIndex
Security MIB	
INFINERA-CERT-LOCALCERT	LOCAL CERTIFICATE MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-CERT-PEERCERT	PEER CERTIFICATE MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SECURITY-IKE	IKE MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SECURITY-SECYCTRL	SECURITY CONTROL MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SECY-SECUREENTITY	SECURE ENTITY MIB. Each entry is uniquely identified by the value of ifIndex.
IEEE8021-SECY-MIB (IEEE 8021 SECY RFC)	1EEE 8021 SECY RFC MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SECURITY-BESECYCTRL-MIB	SECURITY BESECYCTRL MIB. Each entry is uniquely identified by the value of ifIndex.
INFINERA-SECURITY-ACF-MIB	SECURITY ACF MIB. Each entry is uniquely identified by the value of ifIndex.

CHAPTER 2

SNMP Support on Cloud Xpress

This chapter describes the procedures to setup SNMP support on the Infinera Cloud Xpress network element. The Infinera Cloud Xpress network element, referred to as CX, is a 500G transport network element deployed as part of a point-to-point network configuration. It covers the following topics:

Setting up SNMP Support in CX

Configuring the CX SNMP Agent involves the following steps:

- Configure SNMP Requests. See SNMP Request Configuration in CX on page 2-3.
- Configure Trap Destination. See Configuring SNMP Trap Destinations on page 2-7.
- Configure Authentication Failure Trap. See Enable Authentication Failure Trap on page 2-10.
- Configure Trap Proxy Forwarding. See Trap Proxy Forwarding on page 2-11.

  To configure SNMP Agent on multiple network elements simultaneously, see the *Infinera DNA Administrator Guide*.

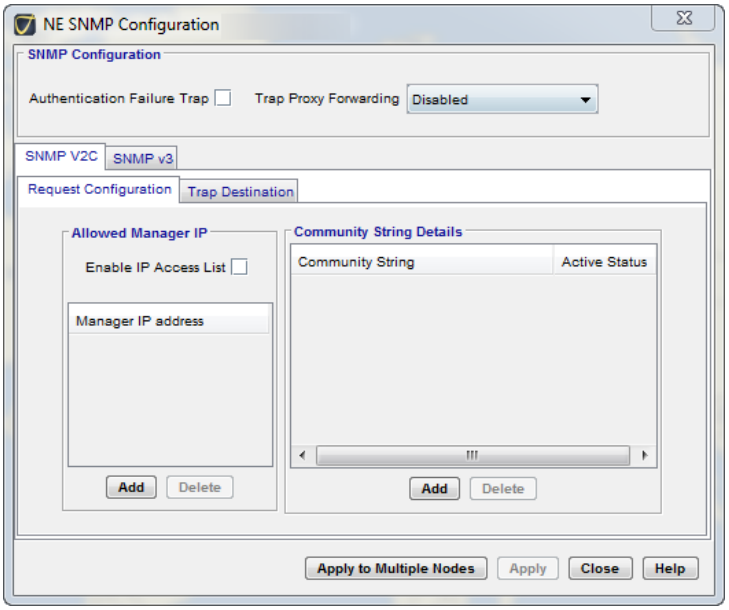
To invoke the NE SNMP Configuration window from DNA

Step 1 Log into the Infinera DNA with security administrator privilege.

Step 2 In the Infinera DNA tree view, select the administrative domain to which the network element belongs. The physical view of the administrative domain is displayed.

Step 3 In the Physical View, right-click the network element and choose **Tools > NE SNMP Configuration**. The NE SNMP Configuration window is displayed.

Figure 2-1 NE SNMP Configuration window



SNMP Request Configuration in CX

Configuring the SNMP Request Configuration involves the following steps:

- Configure Allowed Manager. See Configure Allowed Manager in CX on page 2-3.
- Configure the Community Strings. See Configure SNMP Community Strings in CX on page 2-4.

To configure SNMP Request across all network elements, see the *Infinera DNA Administrator Guide*.

Configure Allowed Manager in CX

The network element provides the ability to configure a list of acceptable SNMP Managers that can access the network element. In Release 8.2, the maximum number of SNMP Managers that can access a network element is 30. The SNMP Manager is configured by providing the IP address of the SNMP Manager and is configured from the NE SNMP Configuration window. See Add Allowed Manager IP in CX on page 2-3. Once the IP address has been added, it can be deleted at any time. See Delete Allowed Manager on page 2-4 if you do not want the network element to be accessible from the SNMP Manager.

The network element supports a mechanism by which the network element can be accessed by all or no SNMP Managers configured as Allowed Managers. This is supported by enabling the checkbox Enable IP Access List in the NE SNMP Configuration window. See To invoke the NE SNMP Configuration window from DNA on page 2-2.

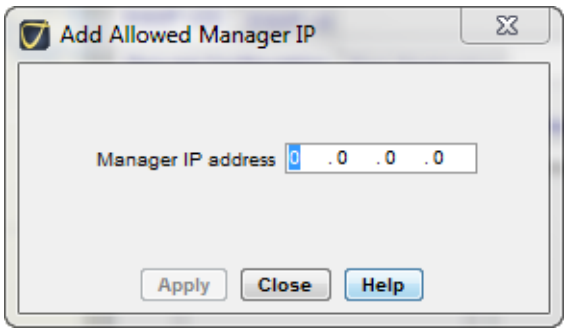
Add Allowed Manager IP in CX

To Add Allowed Manager in CX

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the SNMP request configuration panel, Allowed Manager IP panel, click **Add**. The **Add Allowed Manager IP** window is displayed.

Figure 2-2 Add Allowed Manager



Step 3 In the Add Allowed Manager IP window, enter the IP address of the SNMP Manager that is to access the network element.

Step 4 Click **Apply**.

Step 5 Click **Close**. The IP address of the machine is displayed in the Manager IP address list in the Allowed Manager IP panel.

Step 6 To add more SNMP Managers to the list, repeat Step2 to Step5.

Step 7 If the list of allowed SNMP Managers should be accessible to the network element, check the Enable IP Access List.

> **Note:** By checking the Enable IP Access List all the configured SNMP Managers will be able to access the network element. If the Enable IP Access List is not checked, any of the SNMP Managers can access the network element. However, if no SNMP Managers are configured and the Enable IP Access List checkbox is checked, all SNMP Managers will be accessible by the network element.

Step 8 Click **Close** to close the NE SNMP Configuration window.

Delete Allowed Manager

To delete Allowed Manager

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the SNMP request configuration panel, select the IP address of the SNMP Management station to be removed from the Manager IP address list.

Step 3 Click **Delete**. The IP address is removed from the list.

Step 4 Click **Close** to close the NE SNMP Configuration window.

Configure SNMP Community Strings in CX

The SNMP community string is a form of authentication and access control for the SNMP Manager to access the network element. The network element provides the ability to configure a list of community strings using which the network element access is authenticated on the list of allowed SNMP Managers. A maximum of 10 community strings can be configured on a network element. Once the community string is created, only the status of the community can be edited. To edit the community string, it should be deleted and created with a new name. The following operations can be performed:

- Add Community Strings in CX on page 2-4
- Modify Community String Status on page 2-5
- Delete Community Strings on page 2-6

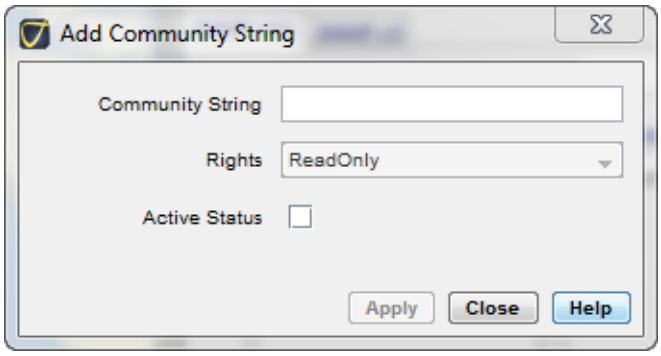
Add Community Strings in CX

To add Community Strings

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, Community String Details panel, click **Add**. The Add Community String window is displayed.

Figure 2-3 Add Community String window



Step 3 In the Add Community String specify following:

- **Community String**—The Community String is a authenticator during access request process. The network element performs the authentication for each SNMP request made to the SNMP agent. If the attribute Enable IP Access List in the Allowed Manager IP panel is also enabled, a combination of the IP address and the community string will be used to validate the access request. Community String must meet the following requirements:
  - The community string is case-sensitive
  - The community string may contain up to 64 alphanumeric characters
  - The community string may contain the following special character: _ + - * .
  - The community string must not contain any blank spaces
- **Rights**—The rights assigned to the community string. This is not applicable for CX nodes.
- **Active Status**—Flag that indicates if the community string is active or inactive. The Active Status flag is checked by default. If the community string status is active, it indicates that authentication can be performed on this community string. If the status is inactive, any request to this community string is rejected and a authentication failure trap is raised.

  Note: Once the community string details are added, the community string cannot be edited; only the status of the community string can changed.

Step 4 Click **Apply**. The community string details are added to the Community String Details table.

Step 5 Click **Close** to close the Add Community String window.

Step 6 To add more community strings repeat Step 2 to Step5.

Step 7 Click **Close** to close the NE SNMP Configuration window.

Modify Community String Status

Once the Community String details is entered, the community string cannot be edited, only the status of the community string can be enabled or disabled.

To modify Community Strings Details

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, in the Community String Details panel, select the Community String for which the status is to be changed.

Step 3 Select/de-select the checkbox as required.

Step 4 Click **Apply**.

Step 5 Click **Close** to close the NE SNMP Configuration.

Delete Community Strings

1. Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.
2. In the NE SNMP Configuration window, in the Community String Details panel, select the Community String to be deleted.
3. Click **Delete**. The Community String is deleted from the Community String Details table.
4. Click **Close** to close the NE SNMP Configuration window.

Configuring SNMP Trap Destinations

The network element provides the ability to configure the SNMP Manager to which the traps can be sent. The trap destination is configured from the NE SNMP Configuration window. A maximum of 10 managers can be configured per network element. The following operations can be performed on the trap destination:

- Add Trap Destination in CX on page 2-7
- Modify Trap Destination on page 2-8
- Delete Trap Destination on page 2-9

Add Trap Destination in CX

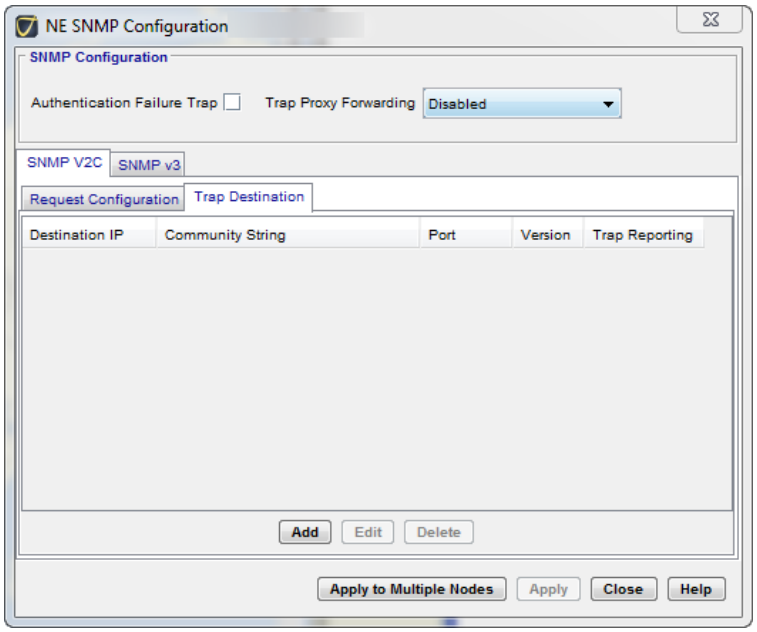
A maximum of 10 SNMP Managers can be provisioned to receive traps from a network element. The SNMP Manager is identified with it's IP address and the community string registered with the SNMP agent.

To add Trap Destination

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, select the **Trap Destination** tab. A list of configured trap destinations is displayed.

Figure 2-4 NE SNMP Configuration Trap Destination



Step 3 Click **Add**. The Add Trap Destination window is displayed.

Step 4 In the Add Trap Destination window, specify the following:

- **Destination IP**—The IP address of the SNMP Manager which is registered to receive SNMP Traps from the network element.
- **Community String**—The Community String is a authenticator during access request process. Community String must meet the following requirements:
  - The community string may contain up to 64 alphanumeric characters
  - The community string may contain the following special character: `_ + - * .`
  - The community string must not contain any blank spaces
- **Port**—The port number to which the trap needs to be sent by the network element. The port number can vary from 1-65535. By default, the port number is 162.
- **Version**—The SNMP trap version to be used while sending traps to the trap destination. At the time of this release, only SNMP v2c is supported.
- **Trap Reporting**—Flag to enable or disable traps to be reported for a given trap destination. If checked, the traps are reported for a given trap destination.

Step 5 Click **Apply**.

Step 6 Click **Close** to close the Add Trap Destination window. The trap destination is added to the trap destination list in the NE SNMP Configuration window.

Step 7 Click **Close** to close the NE SNMP Configuration window.

Modify Trap Destination

Once the Trap Destination details are entered, only the Trap Port and the Reporting Status can be changed.

To modify the Trap Destination

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, select the Trap Destination tab. A list of configured trap destinations is displayed.

Step 3 Select the Trap Destination from the list of configured trap destinations.

Step 4 Click **Edit**. The Edit Trap Destination window is displayed.

Step 5 Edit the Trap Port and select/de-select the Reporting Status as you did while creating the Trap Destination.

Step 6 Click **Apply** to close the Edit Trap Destination. The edited value is displayed in the list of trap destinations in the NE SNMP Configuration window.

Step 7 Click **Close** to close the NE SNMP Configuration window.

Delete Trap Destination

To delete Trap Destination

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, select the Trap Destination tab. A list of configured trap destinations is displayed.

Step 3 In the Trap Destination table, select the trap destination to be deleted.

Step 4 Click **Delete**. The trap destination is removed from the table.

Step 5 Click **Close** to close the NE SNMP Configuration window.

Enable Authentication Failure Trap

The network element authenticates the SNMP request made to the SNMP agent. The network element provides the ability to enable or disable the authentication based on the IP address of the SNMP Manager. by default, the network element is not configured to raise an Authentication Failure Trap. See Authentication Failure Traps on page 1-7.

To enable authentication failed trap to be raised

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, check the **Authentication Failed Trap** checkbox.

Step 3 Click **Close** to close the NE SNMP Configuration window.

Trap Proxy Forwarding

The network element provides the capability to decide on a policy to forward traps from a network element to the SNMP Manager. See Trap Generation on page 1-9.

To enable trap proxy forwarding

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, SNMP Configuration panel, select the trap proxy forwarding policy from the Trap Proxy Forwarding drop-box. The values can be one of the following:

- **Disabled**—If the trap proxy forwarding is disabled and there is no DCN connectivity to the SNMP Manager, no traps are received from this network element. If DCN connectivity is available, the traps are sent directly via DCN. This is the default option set by the network element.
- **Primary GNE**—The traps are sent via the primary GNE and DCN (if connectivity is available).This option is not applicable for Cloud Xpress.
- **Secondary GNE** —The traps are sent via the secondary GNE and DCN (if connectivity is available). This option is not applicable for Cloud Xpress.
- **Both**—The traps are sent via the primary GNE and secondary GNE. If DCN connectivity is available, traps are sent via DCN as well.This option is not applicable for Cloud Xpress.

Step 3 Click **Apply**.

Step 4 Click **Close** to close the NE SNMP Configuration window.

SNMPv3 User Administration

Release 5.1 introduces the support for SNMPv3 traps. The management interfaces namely, DNA, CLI support the configuration of the SNMP agent. SNMPv3 protocol is mainly used when high level of security is required for managing the Infinera network element using SNMP. The SNMPv3 protocol provides three major enhancements compared to the SNMPv2c:

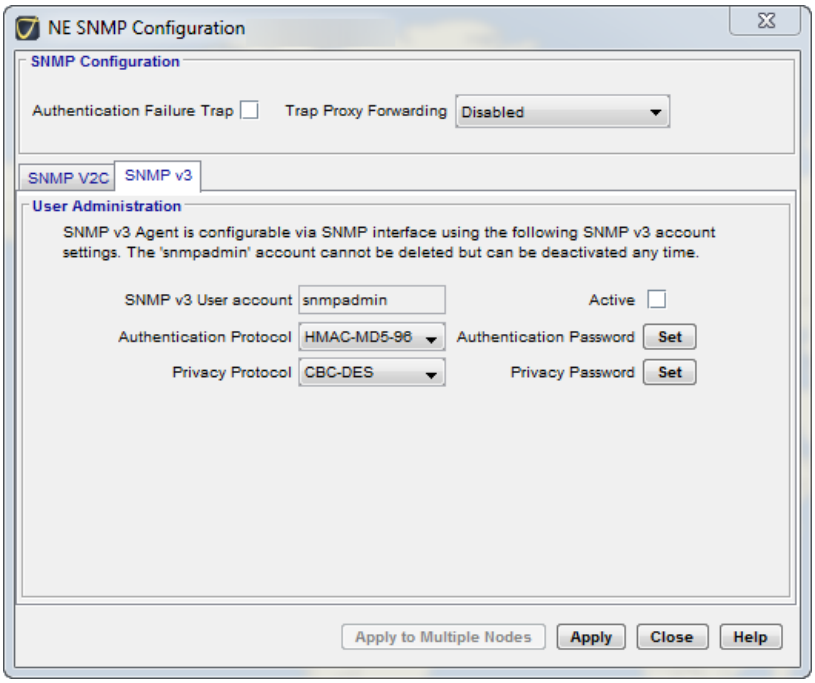
- Authentication of messages (commands) that are invoked by the manager to the agent.
- Privacy of messages between the manager and the agent.
- Access Control of data on the agent.

To enable SNMPv3 user administration

Step 1 Invoke the NE SNMP Configuration window as described in To invoke the NE SNMP Configuration window from DNA on page 2-2.

Step 2 In the NE SNMP Configuration window, select the SNMPv3 tab.

Figure 2-5 SNMPv3 User Administration



Step 3 Check the **Active** checkbox to make the `snmpadmin` user account active.

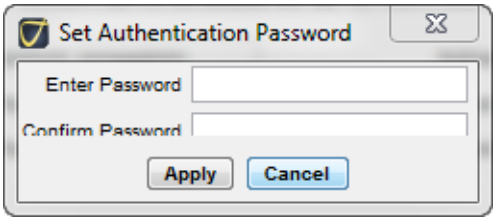
Step 4 From the **Authentication Protocol** drop-down, select the Authentication protocol. The supported configurations are:

- None
- HMAC-MD5-96
- HMAC-SHA-96

Step 5 Click **Set** to change the system default password. The **Set Authentication Password** window is displayed.

Note: If the Authentication Protocol is selected as None, the Set Authentication Password button is disabled.

Figure 2-6 Set Authentication Password



Step 6 In the **Set Authentication Password** window, specify:

- **Enter Password**—User password which meets these requirements:
  - The password must contain 8 to 20 alphanumeric characters and at least one alphabetic and one numeric or one special character
  - The password may contain these special characters: _ - . * + -
  - The password must not contain the associated blank spaces
  - The password is case-sensitive
- **Confirm Password**—Re-enter the password.

Step 7 To save your changes, click **Apply**.

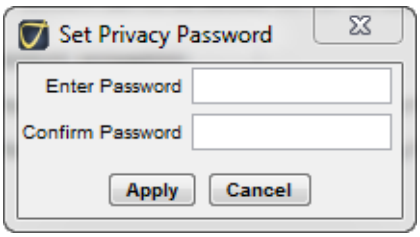
Step 8 From the **Privacy Protocol** drop-down, select the privacy protocol. The supported configurations are:

- None
- CBC-DES
- AES128-CFB

Step 9 Click **Set** to change the system default password. The **Set Privacy Password** window is displayed.

Note: If the Authentication Password is selected as None, the Set Authentication Password button is disabled.

Figure 2-7 Set Privacy Password



Step 10 In the **Set Privacy Password** window, specify:

- **Enter New Password**—User password which meets these requirements:
  - The password must contain 8 to 20 alphanumeric characters and at least one alphabetic and one numeric or one special character
  - The password may contain these special characters: _ - . * + -
  - The password must not contain the associated blank spaces
  - The password is case-sensitive
- **Confirm New Password**—Re-enter the password.

Step 11 To save your changes, click **Apply**.

Step 12 Click **Apply** in the NE SNMP Configuration window.

Step 13 Click Close to close the NE SNMP Configuration window.

CHAPTER 3

SNMP Traps

This chapter describes the alarms, events and TCAs supported by the Infinera Cloud Xpress SNMP Agent. It includes the following sections:

Alarm

An alarm is an indication of a failure condition. Alarms are assigned severities such as critical, major, minor and warning, depending on the degree of service degradation or disruption.

Attributes List

An alarm is an indication of a failure condition. Alarms are assigned severities such as critical, major, minor and warning, depending on the degree of service degradation or disruption.

Table 3-1: Parameters of an alarm on page 3-2 lists the attributes sent as part of the alarm and Table 3-2 Alarm Notification Details lists the Alarm notification details.For more details on the lists of managed objects and probable causes of alarms refer to the *Infinera GNM Fault Management and Diagnostics Guide*.

Table 3-1 Parameters of an alarm

Attributes	Description	OID	Type/Valid Range
InfnAlarmTable: 1.3.6.1.4.1.21296.2.2.1.3			
alarmNotificationId	1.3.6.1.4.1.21296.2.2.1.3.1	A unique identifier assigned to each alarm generated by the network element.	alarmNotificationId
alarmNodeId	1.3.6.1.4.1.21296.2.2.1.3.2	The node ID of the network element.	alarmNodeId
alarmNodeName	1.3.6.1.4.1.21296.2.2.1.3.3	The name of the network element that raised the alarm.	alarmNodeName
alarmObjectType	1.3.6.1.4.1.21296.2.2.1.3.4	Object with which the alarm is associated.	alarmObjectType
alarmObjectAid	1.3.6.1.4.1.21296.2.2.1.3.5	Represents the object name of the facility in the access identifier format.	alarmObjectAid
alarmSourceOid	1.3.6.1.4.1.21296.2.2.1.3.6	Represents the object ID instance of the managed object on which the alarm is reported.	alarmSourceOid
alarmProbableCause	1.3.6.1.4.1.21296.2.2.1.3.7	Network element probable cause. For a list of all alarms raised by the network element.	alarmProbableCause

Table 3-1 Parameters of an alarm (continued)

Attributes	Description	OID	Type/Valid Range
alarmSeverity	1.3.6.1.4.1.21296.2.2.1.3.8	Perceived severity is a classification of alarms depending on the degree of perceived degradations disruption of service or product.	alarmSeverity
alarmCategory	1.3.6.1.4.1.21296.2.2.1.3.9	The category specifies the class to which this alarm is associated.	alarmCategory
alarmServiceAffecting	1.3.6.1.4.1.21296.2.2.1.3.10	The category specifies the class to which this alarm is associated.	alarmServiceAffecting
alarmOccurrenceTime	1.3.6.1.4.1.21296.2.2.1.3.11	The time at which the alarm was raised.	alarmOccurrenceTime
alarmLocation	1.3.6.1.4.1.21296.2.2.1.3.12	The location where the alarm has been raised.	alarmLocation
alarmDirection	1.3.6.1.4.1.21296.2.2.1.3.13	The direction from which the alarm has been received.	alarmDirection
alarmProbableCauseDescription	1.3.6.1.4.1.21296.2.2.1.3.14	Descriptive text for the probable cause attribute.	alarmProbableCauseDescription
alarmAdditionalText	1.3.6.1.4.1.21296.2.2.1.3.15	Additional text describing the alarm.	alarmAdditionalText
alarmCorrelationId	1.3.6.1.4.1.21296.2.2.1.3.16	Represents the correlation ID generated by the network element.	alarmCorrelationId

Alarm Notification Details

The table below lists the Alarm Notification details as described in the Alarm Notification MIB. All identifiers are enclosed in ( ) for every attribute.

Table 3-2 Alarm Notification Details

Description	Severity	Direction	Location	Category
Chassis - Object ID : alarmObjectType (11)				
EQPTFAIL (42)	CR (2)	NA (3)	NA (3)	Equipment (5)
EQPTCOMFAIL(537)	MJ (3)	NA (3)	NA (3)	Equipment (5)
EQPT-PARTFAIL (34)	MN (4)	NA (3)	NA (3)	Equipment (5)
TEMP-OORH (104)	MJ (3)	NA (3)	NA (3)	Equipment (5)
EQPTDEGRADE (41)	MJ (3)	NA (3)	NA (3)	Equipment (5)
REGISTRATION-REQUIRED (705)	MN (4)	NA (3)	NA (3)	Equipment (5)
REGISTRATION-REQUIRED (707)	MJ (3)	NA (3)	NA (3)	Equipment (5)
REGISTRATION-EXPIRED (706)	CR (2)	NA (3)	NA (3)	Equipment (5)
LOCKOUTOFPR (55)	MN (4)	RCV(1)	NEND (1)	Facility (7)
LOCKOUTOFWK (56)	MN (4)	RCV(1)	NEND(1)	Facility (7)
WKSWPR (329)	Event(7)	RCV(1)	NEND(1)	Facility (7)
MANWKSWPR(330)	Event(7)	RCV(1)	NEND(1)	Facility (7)
WKSWBK (131)	Event(7)	RCV(1)	NEND(1)	Facility (7)
MANWKSWBK (132)	Event(7)	RCV(1)	NEND(1)	Facility (7)
DCN-ENET-LOLINK-CTRLRA (24)	MJ (3)	NA (3)	NA (3)	Communication (2)
NCT1-ENET-LOLINK-CTRLRA (65)	MJ (3)	NA (3)	NA (3)	Communication (2)
NCT1-ENET-LOLINK-CTRLRB (66)	MJ (3)	NA (3)	NA (3)	Communication (2)
NTP-SERVER-LOSS-OF-CONTACT (599)	MN(4)	NA(3)	NA(3)	Communication (2)
NTP-SERVER-UNAVAILABLE (600)	NR(7)	NA(3)	NA(3)	Communication (2)
PEER-AUTHENTICATION-FAIL(592)	MJ (3)	NA (3)	NA (3)	Communication (2)
PEER-UNREACHABLE(591)	MJ (3)	NA (3)	NA (3)	Communication (2)
IKE-MIS-CONFIG(594)	MJ (3)	NA (3)	NA (3)	Communication (2)
REKEY-SA-FAIL(593)	MJ (3)	NA (3)	NA (3)	Communication (2)
OCG - Object ID : alarmObjectType (149)				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)

Table 3-2 Alarm Notification Details (continued)

Description	Severity	Direction	Location	Category
OLOS (74)	CR (2)	RCV (1)	NA (3)	Facility (7)
OPR-OORL (76)	MN (4)	RCV(1)	NEND (1)	Facility (7)
OPR-OORH (75)	MN (4)	RCV (1)	NEND (1)	Facility (7)
OCG-MSMT (123)	MJ (3)	NA (3)	NA (3)	Facility (7)
RXEDFASPLIM (533)	MJ (3)	RCV (1)	NEND (1)	Facility (7)
REACH-LTH-EX(701)	Warning(5)	RCV (1)	NEND (1)	Facility (7)
REACH-UTH-EX (702)	CR (2)	RCV (1)	NEND (1)	Facility (7)
TIM-OCG (700)	MN (4)	RCV (1)	NEND (1)	Facility (7)
IGCCFAIL(556)	MN(4)	NA(3)	NA (3)	Communication (2)
OPR-OOL(597)	MJ(3)	RCV(1)	NA(3)	Communication(2)
OPR-OOH(598)	MN(4)	RCV(1)	NA(3)	Communication(2)
OCH - Object ID : alarmObjectType (118)				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)
ADMIN-MAINT (2)	NR (7)	NA (3)	NA (3)	Equipment (5)
OLOS (74)	CR (2)	RCV (1)	NA (3)	Facility (7)
PMD-OORH (562)	MN (4)	RCV (1)	NEND (1)	Facility (7)
PRE-FEC-Q-SIGNAL-DEGRADE (564)	MN (4)	RCV (1)	NEND (1)	Facility (7)
POST-FEC-BER-SF (85)	CR (2)	RCV (1)	NEND (1)	Facility (7)
LPBKTERM (61)	Warning (5)	NA (3)	NEND (1)	Facility (7)
LIC-ASSIGN-MISMATCH(546)	MN (4)	NA (3)	NA (3)	Software Processing
LIC-INSUFFICIENCY(547)	MN (4)	NA (3)	NA (3)	Software Processing
GIGE Client - Object ID : alarmObjectType (25)				
LOSYNC (59)	CR (2)	RCV (1)	NEND (1)	Facility (7)
LOS (58)	CR(2)	RCV(1)	NEND(1)	Facility(7)
RF (340)	MN (4)	RCV (1)	FEND	Facility (7)
LF (341)	MN (4)	RCV (1)	NEND (1)	Facility (7)
LOA(only for 40G) (53)	MJ (3)	RCV (1)	NEND (1)	Facility (7)
LBKFACILITY(60)	Warning (5)	NA (3)	NA (3)	Facility(7)
LOLM (127)	MJ(3)	RCV(1)	NA (3)	Facility (7)
PEM - Object ID : alarmObjectType (46)				
BRKROPEN48V (18)	MN (4)	NA (3)	NA (3)	Equipment (5)

Table 3-2 Alarm Notification Details (continued)

Description	Severity	Direction	Location	Category
IMPROPRMVL (47)	CR (2)	NA (3)	NA (3)	Equipment (5)
EQPTFAIL (42)	CR (2)	NA (3)	NA (3)	Equipment (5)
EQPTCOMFAIL (537)	MJ (3)	NA (3)	NA (3)	Equipment (5)
EQPT-PARTFAIL (34)	CR (2)	NA (3)	NA (3)	Equipment (5)
PWRUV(518)	MN (4)	NA (3)	NA (3)	Equipment (5)
PWROV(517)	CR (2)	NA (3)	NA (3)	Equipment (5)
GLNA	Warning (5)	NA (3)	NA (3)	Equipment (5)
FAN - Object ID : alarmObjectType (21)				
IMPROPRMVL (47)	CR (2)	NA (3)	NA (3)	Equipment (5)
EQPTCOMFAIL (537)	MJ (3)	NA (3)	NA (3)	Equipment (5)
EQPT-PARTFAIL (34)	CR (2)	NA (3)	NA (3)	Equipment (5)
TRIBPTP - Object ID : alarmObjectType (62)				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)
ADMIN-MAINT (2)	NR (7)	NA (3)	NA (3)	Equipment (5)
LOL(310)	CR (2)	RCV (1)	NA (3)	Facility (7)
LS-ACTIVE (247)	NR (7)	TRMT(2)	NEND (1)	Facility (7)
OPR-OORL (76)	MN (4)	RCV (1)	NEND (1)	Facility (7)
OPR-OORH (75)	MN (4)	RCV (1)	NEND (1)	Facility (7)
XFR - Object ID : alarmObjectType				
TXFR-PRI-FAIL (113)	Warning (5)	NA (3)	NA (3)	Communication (2)
TXFR-PRI-FAIL-SNA (114)	MJ (3)	NA (3)	NA (3)	Communication (2)
TXFRSFAIL (115)	MJ (3)	NA (3)	NA (3)	Communication (2)
AUPFAIL (10)	MJ (3)	NA (3)	NA (3)	Communication (2)
ADMIN-XFR-FAILED-ON-SECONDARY	MJ(3)	NA(3)	NA(3)	Communication (2)
Managed Element - Object ID : alarmObjectType				
DBRESTOREFAIL (22)	CR (2)	NA (3)	NA (3)	Software Processing
DBRESTOREFAIL-RBT (23)	MJ (3)	NA (3)	NA (3)	Software Processing
SWUPGRDFAIL (99)	Warning (5)	NA (3)	NA (3)	Software Processing
SWUPGRDFAIL-BOOTUP (100)	MJ (3)	NA (3)	NA (3)	Software Processing
BKUPMEM-LOW (15)	MN (4)	NA (3)	NA (3)	Software Processing
BKUPMEM-VERYLOW (16)	MJ (3)	NA (3)	NA (3)	Software Processing

Table 3-2 Alarm Notification Details (continued)

Description	Severity	Direction	Location	Category
LIC-NW-AUDIT-MISM (549)	MN (4)	NA (3)	NA (3)	Software Processing
SWINSTALLFAIL (98)	MJ (3)	NA (3)	NA (3)	Software Processing
SCH - Object ID : alarmObjectType				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)
ADMIN-MAINT (2)	NR (7)	NA (3)	NA (3)	Equipment (5)
SCH-MSMT (123)	MJ (3)	NA (3)	NA (3)	Facility (7)
OPR-OORL (76)	MN (4)	RCV (1)	NEND (1)	Facility (7)
OPR-OORH (75)	MN (4)	RCV (1)	NEND (1)	Facility (7)
TTI-MISMATCH-SCH (163)	MJ (3)	RCV (1)	NEND (1)	Facility (7)
SCG - Object ID : alarmObjectType				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)
ADMIN-MAINT (2)	NR (7)	NA (3)	NA (3)	Equipment (5)
OTDR-TEST (595)	CR(2)	RCV (1)	NEND(1)	Equipment (6)
SCG-MSMT (123)	MJ (3)	NA (3)	NA (3)	Facility (7)
OPR-OORL (76)	MN (4)	RCV (1)	NEND (1)	Facility (7)
OPR-OORH (75)	MN (4)	RCV (1)	NEND (1)	Facility (7)
IGCC-FAIL (596)	MN (4)	NA (3)	NA (3)	Communication(2)
Carrier CTP - Object ID : alarmObjectType				
ADMIN-LOCK (1)	NR (7)	NA (3)	NA (3)	Equipment (5)
ADMIN-MAINT (2)	NR (7)	NA (3)	NA (3)	Equipment (5)
OLOS (74)	CR (2)	RCV (1)	NA (3)	Facility (7)
LOS (58)	CR (2)	RCV (1)	NEND (1)	Facility (7)
PRE-FEC-Q-SIG-DEGRADE (564)	MN (4)	RCV (1)	NEND (1)	Facility (7)
PMD-OORH (562)	MN (4)	RCV (1)	NEND (1)	Facility (7)
POST-FEC-BER-SF (85)	CR (2)	RCV (1)	NEND (1)	Facility (7)

TCAs

The Threshold Crossing Alert represents some of the significant threshold changes in the system that needs user attention. Table 3-3: Parameters of a TCA on page 3-8 lists the attributes of a TCA and Table 3-4: List of threshold crossing alerts for Cloud Xpress on page 3-10 lists the TCAs probable cause.

Table 3-3 Parameters of a TCA

Attributes	Description	OID	Type/Valid Range
tcaNotificationId	A unique ID generated by the network element for every TCA.	1.3.6.1.4.1.21296.2.2.1.4.1.1	Integer and can vary from 0-2147483647
tcaNodeId	The Node ID of the network element.	1.3.6.1.4.1.21296.2.2.1.4.1.2	String of 1-128 characters
tcaNodeName	The name of the network element that raised the TCA.	1.3.6.1.4.1.21296.2.2.1.4.1.3	String of 1-20 characters
tcaObjectType	The object type specifies the object to which this TCA is associated.	1.3.6.1.4.1.21296.2.2.1.4.1.4	String
tcaObjectAid	The AID of the object that raised the TCA.	1.3.6.1.4.1.21296.2.2.1.4.1.5	Object type
tcaSourceAid	Represents the object ID instance of the managed object on which the TCA is reported.	1.3.6.1.4.1.21296.2.2.1.4.1.6	Object type
tcaProbableCause	The probable cause of the TCA.	1.3.6.1.4.1.21296.2.2.1.4.1.7	String. See Table 3-4: List of threshold crossing alerts for Cloud Xpress on page 3-10

Table 3-3 Parameters of a TCA (continued)

Attributes	Description	OID	Type/Valid Range
tcaSeverity	The severity of the clearable TCA when it was asserted. For example, if a TCA is raised with severity critical and a corresponding clear is raised, the perceived severity of the current TCA will be Clear and the asserted severity is critical.	1.3.6.1.4.1.21296.2.2.1.4.1.8	Integer can take any one of the following values: ■ 1-Indeterminate ■ 2-Critical ■ 3-Major ■ 4-Minor ■ 5-Warning ■ 6-Cleared ■ 7-Event ■ 8-NotReported
tcaCategory	The category specifies the class to which this TCA is associated.	1.3.6.1.4.1.21296.2.2.1.4.1.9	Category can be anyone of the following: ■ Facility ■ Communication ■ Software Processing ■ Equipment ■ Environmental
tcaServiceAffecting	Flag indicating if the alarm is service-affecting or non-service-affecting.	1.3.6.1.4.1.21296.2.2.1.4.1.10	Integer and can take any one of the following values: ■ 1-saunknown ■ 2-saServiceAffecting ■ 3-saNonServiceAffecting
tcaOccurenceTime	The time at which the TCA was raised.	1.3.6.1.4.1.21296.2.2.1.4.1.11	The Network Element Time format YYYY-MMDD<space>hh:mm:ss<Z>

Table 3-3 Parameters of a TCA (continued)

Attributes	Description	OID	Type/Valid Range
tcsLocation	Represents the location of the source.	1.3.6.1.4.1.21296.2.2.1.4.1.12	String of 0-255 characters and can be one of the following: ■ nearEnd ■ farEnd ■ notApplicable
tcaDirection	The direction from which the alarm has been received.	1.3.6.1.4.1.21296.2.2.1.4.1.13	Integer and can table of the following: ■ 1-receive ■ 2-transmit ■ 3-notApplicable
tcaMonitoredValue	Represents the current threshold value.	1.3.6.1.4.1.21296.2.2.1.4.1.14	String
tcaThresholdValue	Represents the configured threshold value.	1.3.6.1.4.1.21296.2.2.1.4.1.15	String
tcaTimePeriod	Represents the time period (e.g. for which the TCA has been raised.	1.3.6.1.4.1.21296.2.2.1.4.1.16	DisplayString ■ 15-MIN ■ 24-HR
tcaProbableCause Description	Represents the TCA probable cause description.	1.3.6.1.4.1.21296.2.2.1.4.1.17	String. See Table 3-4: List of threshold crossing alerts for Cloud Xpress on page 3-10
tcaAdditionalText	Represents the additional text describing the TCA	1.3.6.1.4.1.21296.2.2.1.4.1.18	String

Table 3-4 List of threshold crossing alerts for Cloud Xpress

Managed Objects/ Payload types	Alarm ID	Condition Type	Probable Cause	Severity	SA/NSA	Loc.	Dir	Chassis LED
GbE Client	FAC0187	RXMACCRCALIGNED15MINEV	MAC CRC Aligned, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0195	RXMACCRCALIGNEDDAYEV	MAC CRC Aligned, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False

Table 3-4 List of threshold crossing alerts for Cloud Xpress (continued)

Managed Objects/ Payload types	Alarm ID	Condition Type	Probable Cause	Severity	SA/NSA	Loc.	Dir	Chassis LED
	FAC0184	RXMACERROCTET15MINEV	MAC Error Octets, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0192	RXMACERROCTETDAYEV	MAC Error Octets, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0186	RXMACFRAGMENT15MINEV	MAC Fragment, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0194	RXMACFRAGMENTDAYEV	MAC Fragment, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0185	RXMACJABBER15MINEV	MAC Jabber, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0193	RXMACJABBERDAYEV	MAC Jabber, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0183	RXMACSES15MINEV	MAC Severely Errored Seconds, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0191	RXMACSESDAYEV	MAC Severely Errored Seconds, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
GbE Client [Continued]	FAC0175	RXPCSES15MINEV	PCS Errored Seconds, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0179	RXPCSESDAYEV	PCS Errored Seconds, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0176	RXPCSSES15MINEV	PCS Severely Errored Seconds, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0180	RXPCSSESDAYEV	PCS Severely Errored Seconds, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0177	RXPCSSESS15MINEV	PCS Severely Errored Sync Seconds, 15-Minutes, Rx TCA	EVT	SA	NEnd	Rx	False
	FAC0181	RXPCSSESSDAYEV	PCS Severely Errored Sync Seconds, 24-Hours, Rx TCA	EVT	SA	NEnd	Rx	False

Table 3-4 List of threshold crossing alerts for Cloud Xpress (continued)

Managed Objects/ Payload types	Alarm ID	Condition Type	Probable Cause	Severity	SA/NSA	Loc.	Dir	Chassis LED
	FAC0211	TXMACCRCALIGNED15MINEV	MAC CRC Aligned, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0219	TXMACCRCALIGNEDDAYEV	MAC CRC Aligned, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0208	TXMACERROCTET15MINEV	MAC Error Octets, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0216	TXMACERROCTETDAYEV	MAC Error Octets, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0210	TXMACFRAGMENT15MINEV	MAC Fragment, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
GbE Client [Continued]	FAC0218	TXMACFRAGMENTDAYEV	MAC Fragment, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0209	TXMACJABBER15MINEV	MAC Jabber, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0217	TXMACJABBERDAYEV	MAC Jabber, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0207	TXMACSES15MINEV	MAC Severely Errored Seconds, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0215	TXMACSESDAYEV	MAC Severely Errored Seconds, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0199	TXPCSES15MINEV	PCS Errored Seconds, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0203	TXPCSESDAYEV	PCS Errored Seconds, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0200	TXPCSSES15MINEV	PCS Severely Errored Seconds, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0204	TXPCSSESDAYEV	PCS Severely Errored Seconds, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False

Table 3-4 List of threshold crossing alerts for Cloud Xpress (continued)

Managed Objects/ Payload types	Alarm ID	Condition Type	Probable Cause	Severity	SA/NSA	Loc.	Dir	Chassis LED
	FAC0201	TXPCSSESS15MINEV	PCS Severely Errored Sync Seconds, 15-Minutes, Tx TCA	EVT	SA	NEnd	Tx	False
	FAC0205	TXPCSSESSDAYEV	PCS Severely Errored Sync Seconds, 24-Hours, Tx TCA	EVT	SA	NEnd	Tx	False

Audit Events

The audit event represents all the user-actions that are performed in the system. Table 3-5: Parameters for an audit event on page 3-14 lists the parameters for an audit event.

Table 3-5 Parameters for an audit event

Attributes	Description	OID	Access
infnAuditNotificationId	A unique identifier assigned to each audit event by the network element.	1.3.6.1.4.1.21296.2.2.1.6.1.1	Interger and can vary from 0-2147483647
infnAuditNodeId	A unique identifier generated by the network element.	1.3.6.1.4.1.21296.2.2.1.6.1.2	Interger and can vary from 0-128 characters
infnAuditNodeName	The name of the network element.	1.3.6.1.4.1.21296.2.2.1.6.1.3	String of 1-20 characters
infnAuditObjectType	Represents the managed object type.	1.3.6.1.4.1.21296.2.2.1.6.1.4	String
infnAuditObjectAid	Represents the object name of the facility in the access identifier format.	1.3.6.1.4.1.21296.2.2.1.6.1.5	String
infnAuditSourceOid	Represents the object identifier instance of the managed object on which the audit is reported.	1.3.6.1.4.1.21296.2.2.1.6.1.6	Object type
infnAuditUserId	The name of the user that issued this operation.	1.3.6.1.4.1.21296.2.2.1.6.1.7	String
infnAuditHostInfo	Hostname or IP address from where this operation was issued.	1.3.6.1.4.1.21296.2.2.1.6.1.8	String
infnAuditTime	Represents the event occurrence date and time.	1.3.6.1.4.1.21296.2.2.1.6.1.9	YYYY-MM-DD<space>hh:mm:ss
infnAuditOperationName	The operation name which resulted in this audit event.	1.3.6.1.4.1.21296.2.2.1.6.1.10	String of 0-255 characters
infnAuditOperationStatus	The status of the operation for this audit event.	1.3.6.1.4.1.21296.2.2.1.6.1.11	String of 0-255 characters
infnAuditParamsList	This attribute contains display string data in comma separated format. The data represents the attributes and their values that got affected by the operation which resulted in this Audit event.	1.3.6.1.4.1.21296.2.2.1.6.1.2	DisplayString

Table 3-6 List of Audit Events

ApplyOcg Failed	ApplyOcg Successful
ApplyOch Failed	ApplyOch Successful
Creation Failed	Creation Successful
Delete Failed	Delete Successful
InitiateManualXfr Failed	InitiateManualXfr Successful
Install Failed	Install Successful
InstallWithEmptyDB Failed	InstallWithEmptyDB Successful
LocalBackup Failed	LocalBackup Successful
Login Failed	Login Successful
Logout Failed	Logout Successful
PasswordChange Failed	PasswordChange Successful
PasswordReset Failed	PasswordReset Successful
ResetCard Failed	ResetCard Successful
Restore Failed	Restore Successful
Revert Failed	Revert Successful
SessionTermination Failed	SessionTermination Successful
Update Failed	Update Successful
Upgrade Failed	Upgrade Successful

Admin Events

Administrative events are internal communication events between the network element and management clients such as GNM and DNA. These events are used to communicate the event queue status and processor activities (reboot, switchover, active). Table 3-7: Parameters of an admin event on page 3-16 lists the parameters for an admin event.

Table 3-7 Parameters of an admin event

Attributes	Description	OID	Valid Range
infnAdminNotificationId	A unique identifier assigned to each admin event by the network element.	1.3.6.1.4.1.21296.2.2.1.5.1.1	Integer which varies from 0-2147483647
infnAdminNodeId	The identifier for the network element.	1.3.6.1.4.1.21296.2.2.1.5.1.2	String of 1-128 characters
infnAdminNodeName	The name of the network element.	1.3.6.1.4.1.21296.2.2.1.5.1.3	String of 1-20 characters
adminObjectType	Represents the managed object type on Infinera Information Model.	1.3.6.1.4.1.21296.2.2.1.5.1.4	String
infnAdminObjectAid	Represents the object name of the facility in the access identifier format	1.3.6.1.4.1.21296.2.2.1.5.1.5	Object type
infnAdminSourceOid	Represents the object identifier instance of the managed object on which the admin event is reported.	1.3.6.1.4.1.21296.2.2.1.5.1.6	Object identifier
infnAdminEventTime	Time when the trap is generated by network element.	1.3.6.1.4.1.21296.2.2.1.5.1.7	YYYY-MM-DD<space>hh:mm:ss<Z>
infnAdminCause	Descriptive text for the cause attribute. The term is mapped to the cause field of admin events raised by Infinera Network Elements.	1.3.6.1.4.1.21296.2.2.1.5.1.8	String of 0-255 characters

Table 3-8 List of Adminstrative Events

File Transfer Failed	File Transfer Failed Because of MCM/Controller Card Reboot
File transfer partially succeeded	File Transferred Process Started
File transferred successfully	Install Failed
Install in Progress...Unpacking the Tar File	Install: Done Unpacking the Tar File...Rebooting…
Local Backup Done	Local Backup Failed Because of Reboot
Migrate Completed Successfully	Database Migrate Failed
NC System is Active Now	Restore Completed Successfully
Revert Failed	Revert in Progress
WTRCANCEL	AUTOREVERT

Table 3-8 List of Adminstrative Events (continued)

OWA Automation Done	OWA Automation Failed
Revert: Done Unpacking the Tar File...Rebooting…	Scheduled Transfer Request Dropped
Software Install Failed Because of Reboot	Software Revert Failed Because of Reboot
Software Uncompress Failed Because of Reboot	Transfer Request Dropped
Upgrade Completed Successfully	Upgrade in Progress...Unpacking the Tar File
REKEY-SA-SUCCESS	AUTHENTICATION-SUCCESS
TX-SA-HARDTIMEOUT	RX-SA-HARDTIMEOUT
CertExpiredEvent	

Security Events

The security event represents the information related to system's security. Table 3-9: Parameters of a security event on page 3-18 lists the parameters for a security event.

Table 3-9 Parameters of a security event

Attributes	Description	OID	Access
infnSecurityNotificationId	A unique identifier assigned to each security event by the network element.	1.3.6.1.4.1.21296.2.2.1.7.1.1	Integer and varies from 0-2147483647
infnSecurityNodeId	A unique identifier generated by the network element.	1.3.6.1.4.1.21296.2.2.1.7.1.2	Integer and varies from 0-2147483647
infnsecurityNodeName	The name of the network element. This maps to the managed element name of the Info Model.	1.3.6.1.4.1.21296.2.2.1.7.1.3	String of 1-128 characters
infnsecurityObjectType	Represents the object type. (For Example: USER).	1.3.6.1.4.1.21296.2.2.1.7.1.4	String
infnSecurityObjectAid	Represents the user name.	1.3.6.1.4.1.21296.2.2.1.7.1.5	String
infnSecuritySourceOid	Represents the object identifier instance of the user on which security event is reported.	1.3.6.1.4.1.21296.2.2.1.7.1.6	Object type
infnSecurityHostInfo	IP address or host name from which the operation was performed.	1.3.6.1.4.1.21296.2.2.1.7.1.7	String of 0-255 characters
infnSecurityEventTime	Time when trap is generated by network element in ISO 8601 format.	1.3.6.1.4.1.21296.2.2.1.7.1.8	YYYY-MM-DD<space>hh:mm:ss<Z>
infnSecurityMessage	Represents the security event description	1.3.6.1.4.1.21296.2.2.1.7.1.9	

Table 3-10 List of Security Events

Security Cause Description
Intrusion Detected
Session limit reached
Reserved session limit reached

Sample Traps

Sample Trap for Raise

```
Notification(s)
Trap (V2), 01-14-2015 13:47:35, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 503
sysUpTime.0 = 1-5:55:25.58
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12551 = 12551
alarmNodeId.12551 = 504133333134323931373136
alarmNodeName.12551 = 4e45313435
alarmObjectType.12551 = pem (46)
alarmObjectAid.12551 = 312d494f5348454c462d50454d41
alarmSourceOid.12551 = pemMoId
alarmProbableCause.12551 = impropRmvl (47)
alarmSeverity.12551 = psMajor (3)
alarmCategory.12551 = equipment (5)
alarmServiceAffecting.12551 = saServiceAffecting (2)
alarmOccurrenceTime.12551 = 323030392d31302d32362032322d31332d3430
alarmLocation.12551 = notApplicable (3)
alarmDirection.12551 = notApplicable (3)
alarmProbableCauseDescription.12551 =
45717569706d656e7420696d70726f7065722072656d6f76616c
alarmAdditionalText.12551 =
alarmCorrelationId.12551 = 12551
```

Sample Trap for Clear

```
Trap (V2), 01-14-2015 13:47:55, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 523
```

```
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12563 = 12563
alarmNodeId.12563 = 504133333134323931373136
alarmNodeName.12563 = 4e45313435
alarmObjectType.12563 = pem (46)
alarmObjectAid.12563 = 312d494f5348454c462d50454d41
alarmSourceOid.12563 = pemMoId
alarmProbableCause.12563 = impropRmvl (47)
alarmSeverity.12563 = psCleared (6)
alarmCategory.12563 = equipment (5)
alarmServiceAffecting.12563 = saServiceAffecting (2)
alarmOccurrenceTime.12563 = 323030392d31302d32362032322d31332d3539
alarmLocation.12563 = notApplicable (3)
alarmDirection.12563 = notApplicable (3)
alarmProbableCauseDescription.12563 =
45717569706d656e7420696d70726f7065722072656d6f76616c
alarmAdditionalText.12563 =
alarmCorrelationId.12563 = 12551
```

Sample Trap for CXOCGPTP with OIDs

```
[Port#]
162
Notification(s)
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 439
1.3.6.1.2.1.1.3.0 = 1-4:15:49.4
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12511 = 12511
1.3.6.1.4.1.21296.2.2.1.3.1.2.12511 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12511 = NE145
```

```
1.3.6.1.4.1.21296.2.2.1.3.1.4.12511 = ocgPtp (149)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12511 = 1-A-2
1.3.6.1.4.1.21296.2.2.1.3.1.6.12511 = 1.3.6.1.4.1.21296.2.2.2.2.51.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12511 = ocgMismatch (123)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12511 = psMajor (3)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12511 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12511 = saNonServiceAffecting (3)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12511 = 2009-10-26 20-34-04
1.3.6.1.4.1.21296.2.2.1.3.1.12.12511 = notApplicable (3)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12511 = notApplicable (3)
1.3.6.1.4.1.21296.2.2.1.3.1.14.12511 = OCG Mismatch
1.3.6.1.4.1.21296.2.2.1.3.1.15.12511 =
1.3.6.1.4.1.21296.2.2.1.3.1.16.12511 = 12511
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 441
1.3.6.1.2.1.1.3.0 = 1-4:15:49.5
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12512 = 12512
1.3.6.1.4.1.21296.2.2.1.3.1.2.12512 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12512 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12512 = ocgPtp (149)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12512 = 1-A-2
1.3.6.1.4.1.21296.2.2.1.3.1.6.12512 = 1.3.6.1.4.1.21296.2.2.2.2.51.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12512 = olOorh (73)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12512 = psMinor (4)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12512 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12512 = saNonServiceAffecting (3)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12512 = 2009-10-26 20-34-04
1.3.6.1.4.1.21296.2.2.1.3.1.12.12512 = notApplicable (3)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12512 = transmit (2)
```

```
1.3.6.1.4.1.21296.2.2.1.3.1.14.12512 = OCG Loss Out of Range - High
1.3.6.1.4.1.21296.2.2.1.3.1.15.12512 =
1.3.6.1.4.1.21296.2.2.1.3.1.16.12512 = 12512
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 443
1.3.6.1.2.1.1.3.0 = 1-4:15:49.5
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12513 = 12513
1.3.6.1.4.1.21296.2.2.1.3.1.2.12513 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12513 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12513 = ocgPtp (149)
```

Sample Trap for CXOCGPTP

```
[Port#]
162
Notification(s)
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 439
sysUpTime.0 = 1-4:15:49.4
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12511 = 12511
alarmNodeId.12511 = 504133333134323931373136
alarmNodeName.12511 = 4e45313435
alarmObjectType.12511 = ocgPtp (149)
alarmObjectAid.12511 = 312d412d32
alarmSourceOid.12511 = terminationPoint.51.1.1.1
alarmProbableCause.12511 = ocgMismatch (123)
alarmSeverity.12511 = psMajor (3)
alarmCategory.12511 = facility (7)
```

```
alarmServiceAffecting.12511 = saNonServiceAffecting (3)
alarmOccurrenceTime.12511 = 323030392d31302d32362032302d33342d3034
alarmLocation.12511 = notApplicable (3)
alarmDirection.12511 = notApplicable (3)
alarmProbableCauseDescription.12511 = 4f4347204d69736d61746368
alarmAdditionalText.12511 =
alarmCorrelationId.12511 = 12511
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 441
sysUpTime.0 = 1-4:15:49.5
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12512 = 12512
alarmNodeId.12512 = 504133333134323931373136
alarmNodeName.12512 = 4e45313435
alarmObjectType.12512 = ocgPtp (149)
alarmObjectAid.12512 = 312d412d32
alarmSourceOid.12512 = terminationPoint.51.1.1.1
alarmProbableCause.12512 = olOorh (73)
alarmSeverity.12512 = psMinor (4)
alarmCategory.12512 = facility (7)
alarmServiceAffecting.12512 = saNonServiceAffecting (3)
alarmOccurrenceTime.12512 = 323030392d31302d32362032302d33342d3034
alarmLocation.12512 = notApplicable (3)
alarmDirection.12512 = transmit (2)
alarmProbableCauseDescription.12512 =
4f4347204c6f7373204f7574206f662052616e6765202d2048696768
alarmAdditionalText.12512 =
alarmCorrelationId.12512 = 12512
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 443
```

```
sysUpTime.0 = 1-4:15:49.5
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12513 = 12513
alarmNodeId.12513 = 504133333134323931373136
alarmNodeName.12513 = 4e45313435
alarmObjectType.12513 = ocgPtp (149)
alarmObjectAid.12513 = 312d412d32
alarmSourceOid.12513 = terminationPoint.51.1.1.1
alarmProbableCause.12513 = olos (74)
alarmSeverity.12513 = psCritical (2)
alarmCategory.12513 = facility (7)
alarmServiceAffecting.12513 = saServiceAffecting (2)
alarmOccurrenceTime.12513 = 323030392d31302d32362032302d33342d3034
alarmLocation.12513 = nearEnd (1)
alarmDirection.12513 = receive (1)
alarmProbableCauseDescription.12513 =
4f70746963616c204c6f7373204f66205369676e616c202d205061796c6f6164
alarmAdditionalText.12513 =
alarmCorrelationId.12513 = 12513
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 445
sysUpTime.0 = 1-4:15:49.10
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12514 = 12514
alarmNodeId.12514 = 504133333134323931373136
alarmNodeName.12514 = 4e45313435
alarmObjectType.12514 = ocgPtp (149)
alarmObjectAid.12514 = 312d412d32
alarmSourceOid.12514 = terminationPoint.51.1.1.1
alarmProbableCause.12514 = oprOorh (75)
alarmSeverity.12514 = psMinor (4)
```

```
alarmCategory.12514 = facility (7)
alarmServiceAffecting.12514 = saNonServiceAffecting (3)
alarmOccurrenceTime.12514 = 323030392d31302d32362032302d33342d3034
alarmLocation.12514 = nearEnd (1)
alarmDirection.12514 = receive (1)
alarmProbableCauseDescription.12514 =
4f5052204f7574206f662052616e6765202d2048696768
alarmAdditionalText.12514 =
alarmCorrelationId.12514 = 12514
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 447
sysUpTime.0 = 1-4:15:49.10
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12515 = 12515
alarmNodeId.12515 = 504133333134323931373136
alarmNodeName.12515 = 4e45313435
alarmObjectType.12515 = ocgPtp (149)
alarmObjectAid.12515 = 312d412d32
alarmSourceOid.12515 = terminationPoint.51.1.1.1
alarmProbableCause.12515 = oprOorl (76)
alarmSeverity.12515 = psMinor (4)
alarmCategory.12515 = facility (7)
alarmServiceAffecting.12515 = saNonServiceAffecting (3)
alarmOccurrenceTime.12515 = 323030392d31302d32362032302d33342d3034
alarmLocation.12515 = nearEnd (1)
alarmDirection.12515 = receive (1)
alarmProbableCauseDescription.12515 =
4f5052204f7574206f662052616e6765202d204c6f77
alarmAdditionalText.12515 =
alarmCorrelationId.12515 = 12515
Trap (V2), 01-14-2015 12:08:00, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
```

```
Request = 449
sysUpTime.0 = 1-4:15:49.10
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12516 = 12516
alarmNodeId.12516 = 504133333134323931373136
```

Sample Trap for TRIBPTP with OIDs

```
[Port#]
162
Notification(s)
Trap (V2), 01-14-2015 12:11:32, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 487
1.3.6.1.2.1.1.3.0 = 1-4:19:21.98
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12537 = 12537
1.3.6.1.4.1.21296.2.2.1.3.1.2.12537 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12537 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12537 = tribPtp (62)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12537 = 1-A-4-T1-4
1.3.6.1.4.1.21296.2.2.1.3.1.6.12537 = 1.3.6.1.4.1.21296.2.2.2.2.17.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12537 = oprOorh (75)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12537 = psMinor (4)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12537 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12537 = saNonServiceAffecting (3)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12537 = 2009-10-26 20-37-37
1.3.6.1.4.1.21296.2.2.1.3.1.12.12537 = nearEnd (1)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12537 = receive (1)
1.3.6.1.4.1.21296.2.2.1.3.1.14.12537 = OPR Out of Range - High
1.3.6.1.4.1.21296.2.2.1.3.1.15.12537 =
1.3.6.1.4.1.21296.2.2.1.3.1.16.12537 = 12537
```

```
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 489
1.3.6.1.2.1.1.3.0 = 1-4:19:21.98
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12538 = 12538
1.3.6.1.4.1.21296.2.2.1.3.1.2.12538 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12538 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12538 = tribPtp (62)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12538 = 1-A-4-T1-4
1.3.6.1.4.1.21296.2.2.1.3.1.6.12538 = 1.3.6.1.4.1.21296.2.2.2.2.17.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12538 = oprOorl (76)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12538 = psMinor (4)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12538 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12538 = saNonServiceAffecting (3)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12538 = 2009-10-26 20-37-37
1.3.6.1.4.1.21296.2.2.1.3.1.12.12538 = nearEnd (1)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12538 = receive (1)
1.3.6.1.4.1.21296.2.2.1.3.1.14.12538 = OPR Out of Range - Low
1.3.6.1.4.1.21296.2.2.1.3.1.15.12538 =
1.3.6.1.4.1.21296.2.2.1.3.1.16.12538 = 12538
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 485
1.3.6.1.2.1.1.3.0 = 1-4:19:21.98
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12536 = 12536
1.3.6.1.4.1.21296.2.2.1.3.1.2.12536 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12536 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12536 = tribPtp (62)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12536 = 1-A-4-T1-4
```

```
1.3.6.1.4.1.21296.2.2.1.3.1.6.12536 = 1.3.6.1.4.1.21296.2.2.2.2.17.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12536 = misConn (62)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12536 = psMajor (3)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12536 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12536 = saNonServiceAffecting (3)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12536 = 2009-10-26 20-37-37
1.3.6.1.4.1.21296.2.2.1.3.1.12.12536 = notApplicable (3)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12536 = notApplicable (3)
1.3.6.1.4.1.21296.2.2.1.3.1.14.12536 = Inter-module mis-connection
1.3.6.1.4.1.21296.2.2.1.3.1.15.12536 =
1.3.6.1.4.1.21296.2.2.1.3.1.16.12536 = 12536
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145],
1.3.6.1.4.1.21296.2.2.1.2.1
Community String = public
Request = 483
1.3.6.1.2.1.1.3.0 = 1-4:19:21.98
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.21296.2.2.1.2.1
1.3.6.1.4.1.21296.2.2.1.3.1.1.12535 = 12535
1.3.6.1.4.1.21296.2.2.1.3.1.2.12535 = PA3314291716
1.3.6.1.4.1.21296.2.2.1.3.1.3.12535 = NE145
1.3.6.1.4.1.21296.2.2.1.3.1.4.12535 = tribPtp (62)
1.3.6.1.4.1.21296.2.2.1.3.1.5.12535 = 1-A-4-T1-4
1.3.6.1.4.1.21296.2.2.1.3.1.6.12535 = 1.3.6.1.4.1.21296.2.2.2.2.17.1.1.1
1.3.6.1.4.1.21296.2.2.1.3.1.7.12535 = olos (74)
1.3.6.1.4.1.21296.2.2.1.3.1.8.12535 = psCritical (2)
1.3.6.1.4.1.21296.2.2.1.3.1.9.12535 = facility (7)
1.3.6.1.4.1.21296.2.2.1.3.1.10.12535 = saServiceAffecting (2)
1.3.6.1.4.1.21296.2.2.1.3.1.11.12535 = 2009-10-26 20-37-37
1.3.6.1.4.1.21296.2.2.1.3.1.12.12535 = nearEnd (1)
1.3.6.1.4.1.21296.2.2.1.3.1.13.12535 = receive (1)
1.3.6.1.4.1.21296.2.2.1.3.1.14.12535 = Optical Loss Of Signal
1.3.6.1.4.1.21296.2.2.1.3.1.15.12535 =
```

```
1.3.6.1.4.1.21296.2.2.1.3.1.16.12535 = 12535
```

Sample Trap for TRIBPTP

```
[Port#]
162
Notification(s)
Trap (V2), 01-14-2015 12:11:32, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 487
sysUpTime.0 = 1-4:19:21.98
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12537 = 12537
alarmNodeId.12537 = 504133333134323931373136
alarmNodeName.12537 = 4e45313435
alarmObjectType.12537 = tribPtp (62)
alarmObjectAid.12537 = 312d412d342d54312d34
alarmSourceOid.12537 = terminationPoint.17.1.1.1
alarmProbableCause.12537 = oprOorh (75)
alarmSeverity.12537 = psMinor (4)
alarmCategory.12537 = facility (7)
alarmServiceAffecting.12537 = saNonServiceAffecting (3)
alarmOccurrenceTime.12537 = 323030392d31302d32362032302d33372d3337
alarmLocation.12537 = nearEnd (1)
alarmDirection.12537 = receive (1)
alarmProbableCauseDescription.12537 =
4f5052204f7574206f662052616e6765202d2048696768
alarmAdditionalText.12537 =
alarmCorrelationId.12537 = 12537
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 489
sysUpTime.0 = 1-4:19:21.98
```

```
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12538 = 12538
alarmNodeId.12538 = 504133333134323931373136
alarmNodeName.12538 = 4e45313435
alarmObjectType.12538 = tribPtp (62)
alarmObjectAid.12538 = 312d412d342d54312d34
alarmSourceOid.12538 = terminationPoint.17.1.1.1
alarmProbableCause.12538 = oprOorl (76)
alarmSeverity.12538 = psMinor (4)
alarmCategory.12538 = facility (7)
alarmServiceAffecting.12538 = saNonServiceAffecting (3)
alarmOccurrenceTime.12538 = 323030392d31302d32362032302d33372d3337
alarmLocation.12538 = nearEnd (1)
alarmDirection.12538 = receive (1)
alarmProbableCauseDescription.12538 =
4f5052204f7574206f662052616e6765202d204c6f77
alarmAdditionalText.12538 =
alarmCorrelationId.12538 = 12538
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 485
sysUpTime.0 = 1-4:19:21.98
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12536 = 12536
alarmNodeId.12536 = 504133333134323931373136
alarmNodeName.12536 = 4e45313435
alarmObjectType.12536 = tribPtp (62)
alarmObjectAid.12536 = 312d412d342d54312d34
alarmSourceOid.12536 = terminationPoint.17.1.1.1
alarmProbableCause.12536 = misConn (62)
alarmSeverity.12536 = psMajor (3)
alarmCategory.12536 = facility (7)
```

```
alarmServiceAffecting.12536 = saNonServiceAffecting (3)
alarmOccurrenceTime.12536 = 323030392d31302d32362032302d33372d3337
alarmLocation.12536 = notApplicable (3)
alarmDirection.12536 = notApplicable (3)
alarmProbableCauseDescription.12536 =
496e7465722d6d6f64756c65206d69732d636f6e6e656374696f6e
alarmAdditionalText.12536 =
alarmCorrelationId.12536 = 12536
Trap (V2), 01-14-2015 12:11:33, [::ffff:10.100.89.145], infnAlarmNotification
Community String = public
Request = 483
sysUpTime.0 = 1-4:19:21.98
snmpTrapOID.0 = infnAlarmNotification
alarmNotificationId.12535 = 12535
alarmNodeId.12535 = 504133333134323931373136
alarmNodeName.12535 = 4e45313435
alarmObjectType.12535 = tribPtp (62)
alarmObjectAid.12535 = 312d412d342d54312d34
alarmSourceOid.12535 = terminationPoint.17.1.1.1
alarmProbableCause.12535 = olos (74)
alarmSeverity.12535 = psCritical (2)
alarmCategory.12535 = facility (7)
alarmServiceAffecting.12535 = saServiceAffecting (2)
alarmOccurrenceTime.12535 = 323030392d31302d32362032302d33372d3337
alarmLocation.12535 = nearEnd (1)
alarmDirection.12535 = receive (1)
alarmProbableCauseDescription.12535 =
4f70746963616c204c6f7373204f66205369676e616c
alarmAdditionalText.12535 =
alarmCorrelationId.12535 = 12535
```

APPENDIX A:

NU Design MIB Browser Settings

This chapter describes Infinera recommended settings and procedures to load Infinera MIBs and modify event configuration from NuDesign MIB browser.

Recommended Settings and Procedures for NU Design MIB Browser Version 7.2 on page A-2

Recommended Settings and Procedures for NU Design MIB Browser Version 7.2

This section describes the procedure to configure NuDesign to enable it to receive Infinera traps and process them without errors.

Note: Refer to the NuDesign Version 7.2 document for detailed procedures.

1. Copy the Infinera MIBs (INFINERA-REG-MIB, INFINERA-TC-MIB and INFINERA-NOTIFICATION-MIB) from the IQ NOS CD to the machine on which NuDesign is installed. The Infinera MIBs can be copied to any directory of your choice. For example, `c:/snmp_mibs/Vendor/Infinera.`
   a. On the machine where NuDesign is installed, change directory to `c:/snmp_mibs/Vendor`
   b. Create directory Infinera. Type,

      ```
      mkdir Infinera
      ```

   c. Copy the Infinera MIBs obtained from the DNA server to this directory.
2. Start NuDesign MIB browser.
3. Close the **Alarm Categories** and **All Alarms Browser** windows if they are open.
4. Select **Load MIB button** button .
5. Browse to the directory that contains the Infinera MIBs (`etc/snmp_mibs/Vendor/Infinera`.)
6. Select INFINERA-REG-MIB.
7. Click **Open**. The Loaded SNMP MIBs list is updated with the INFINERA-REG-MIB.
8. Click **Load**. The **Load** dialog box is displayed.
9. Select **Load MIB button** button .
10. Browse to the directory that contains the Infinera MIBs (`etc/snmp_mibs/Vendor/Infinera.).`
11. Select INFINERA-TC-MIB.
12. Click **Open**. The Loaded SNMP MIBs list is updated with the INFINERA-TC-MIB.
13. Now load the remaining MIBs in the `etc/snmp_mibs/Vendor/Infinera` directory.
14. Configure the SNMP Agent using the **Edit > Add/Edit SNMP Agent** menu. In the **Configuration** window, enter the following values:
    - Protocol Version= SNMP Protocol version. SNMPV2c or SNMPV3.
    - IP Address= IP Address of the network element.
    - Port= Port used to connect to the network element.
    - Number of Retries= The maximum number of retires allowed to connect to the network element.
    - Timeout Interval = The timeout interval (in seconds) after which the connection to the network element is terminated.

- Read community= Specifies the community string configured using the CLI interface. For more information about configuring community string, see *Infinera Cloud Xpress CLI User Guide*.
- Write community= This should not be configured.
- Number of Polls = Use the default value provided by the browser.
- Poll Period =Use the default value provided by the browser.

15. To receive the traps from the network element, click **Trap Rx** tab in the NuDesign MIB browser.

:.