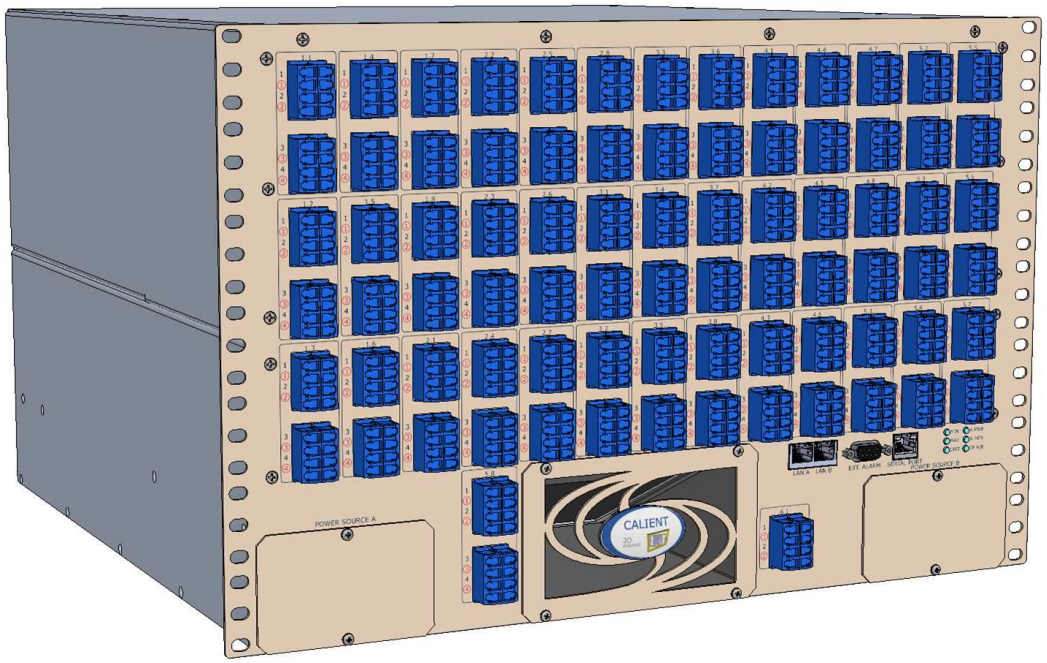
CALIENT

3D MEMS

Move the light, not the fiber

CALIENT Optical Circuit Switch (OCS)
SNMP User Guide



Confidential and Proprietary Information

CALIENT Technologies
25 Castilian Drive
Goleta, CA 93117 USA
Phone: +1.805.562.5500
www.calient.net

Service and Support

CALIENT offers a wide range of product support programs including installation support, repair services, maintenance services and technical training.

If you need technical assistance with CALIENT’s products, please visit our automated customer support portal at http://support.calient.net or email support@calient.net.

If you are experiencing a service-affecting emergency, please contact us on the following numbers:

Within US: 1.877.682.1160
International: International Call Prefix + Country Code + 1.877.682.1160

If your call is not answered immediately, please leave a message. Messages are retrieved continuously.

Document Part Number: 460183-00, Rev. A

Revision History

Date	Version	Description	Author(s)
04/08/2013	0.1	Preliminary draft describing the SNMP feature and configuration	Engineering
04/13/2013	0.2	Incorporated review comments	Engineering
04/29/2013	0.3	Updated Configuration Details and added System Restrictions in Appendix A	Engineering
05/26/2015	0.4	Update content and formatting	T. Schilz
06/18/2015	0.5	Additional content and formatting changes	T. Schilz
06/19/2015	0.6	Incorporate Vijayan's review edits	T. Schilz
06/24/2015	A	Incorporate Deepti's review edits	T. Schilz

Table of Contents

List of Figures

List of Tables

PREFACE

The *CALIENT Optical Circuit Switch (OCS) SNMP User Guide* provides information on how the Simple Network Management Protocol (SNMP) is used on CALIENT's S320 and S160 platforms to monitor and manage devices attached to IP networks.

AUDIENCE

The *CALIENT Optical Circuit Switch (OCS) SNMP User Guide* is written for both the network operations center personnel and field service personnel who configure, provision and monitor the equipment. It is assumed that this audience is familiar with SNMP.

1 ABOUT SNMP

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects.

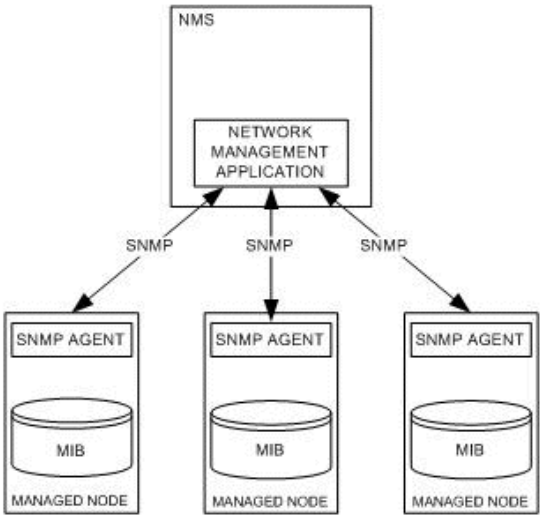


Figure 1 – SNMP Overview

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried, and sometimes set, by managing applications.

SNMP itself does not define which information (i.e., which variables) a managed system should offer. Rather, it uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by Abstract Syntax Notation One (ASN.1). There are two types of MIBs: standard and enterprise. Standard MIBs are definitions of network and hardware events used by many different devices. Enterprise MIBs are used to give information about events that are specific to a single manufacturer.

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and Inform Requests) on port 162 by default.

2 SNMP AGENT SUPPORT FOR THE OCS

The CALIENT SNMP agent supports all the three versions of SNMP—SNMPv1, SNMPv2c and SNMPv3. SNMPv3 support makes the CALIENT SNMP interface highly secure. CALIENT OCS features are defined as part of Enterprise MIBs. The CALIENT OCS SNMP agent supports SNMP Get/Set and GetBulk requests for SNMP MIB-II MIBs and Enterprise-specific MIBs. It also sends traps on alarm/event generation; the trap versions supported are v1 Trap, v2c Trap, v2c Inform, v3 Trap and v3 Inform. The CALIENT OCS agent MIBs can be copied from the installation package located at /opt/calient/GXCP/net-snmp/share/snmp/mibs on the target board.

Table 1 lists enterprise-specific MIBs that describe the functionality and configuration of the CALIENT OCS.

Table 1 – CALIENT MIBs

S. No.	MIB Name	Description
1	CALIENT-SMI	CALIENT SMI and top-level registrations
2	CALIENT-TC	CALIENT textual conventions
3	CALIENT-CHASSIS-MIB	MIB describing the physical elements (primarily shelves and modules) in a chassis
4	CALIENT-PORTS-MIB	MIB describing CALIENT port features
5	CALIENT-CONNECTION-MIB	MIB describing a list of transit connections provisioned in this OCS. This MIB supports CALIENT connection creation using SNMP set functionality as well.
6	CALIENT-PORT-GROUP-MIB	MIB describing a list of the port groups configured in this OCS
7	CALIENT-SW-MGMT-MIB	MIB describing a list of software versions running on various slots in the chassis
8	CALIENT-ALARM-CONF-MIB	MIB defining the various alarms supported by CALIENT devices
9	CALIENT-SERVICE-CONF-MIB	MIB describing the various services running on the CALIENT device
10	CALIENT-SCP-CONF-MIB	MIB describing the SCP configuration for installation/backup
11	CALIENT-NTP-SERVER-CONF-MIB	MIB describing the NTP configuration for the switch
12	CALIENT-USER-MGMT-MIB	MIB describing the list of users configured to access this device

S. No.	MIB Name	Description
13	CALIENT-SESSION-MGMT-MIB	MIB describing a list of configured user sessions
14	CALIENT-SECURITY-MIB	MIB describing support for security profiles and monitoring of access to CALIENT nodes
15	CALIENT-ENV-MIB	MIB monitoring the CALIENT environment

CALIENT-TC and CALIENT-SMI MIBs contain the various CALIENT Textual Conventions and top-level registrations required by the MIB browser to load the CALIENT-specific MIBS successfully. The CALIENT-ENV-MIB contains only Notifications/Traps that monitor the various environmental parameters for the switch and does not contain any OIDs that can be Get/Set. As such, a list of supported OIDs are not are described for these MIBs in Appendix C.

3 BROWSING OCS MIBS

The MIB browser is an indispensable tool for engineers to manage SNMP-enabled network devices and applications. It allows users to load standard and proprietary MIBs, and even some malformed MIBs. It also allows them to issue SNMP requests to retrieve the SNMP agent's data or make changes to the agent. A built-in trap receiver can receive and process SNMP traps according to its rule engine. Most network management systems (NMS) have built-in MIB browsers, although standalone MIB browsers can also be used. iReasoning is a freely available MIB browser that can be downloaded from http://ireasoning.com/mibbrowser.shtml. Figure 2 provides a snapshot of loaded CALIENT MIBs viewed with the iReasoning MIB browser.

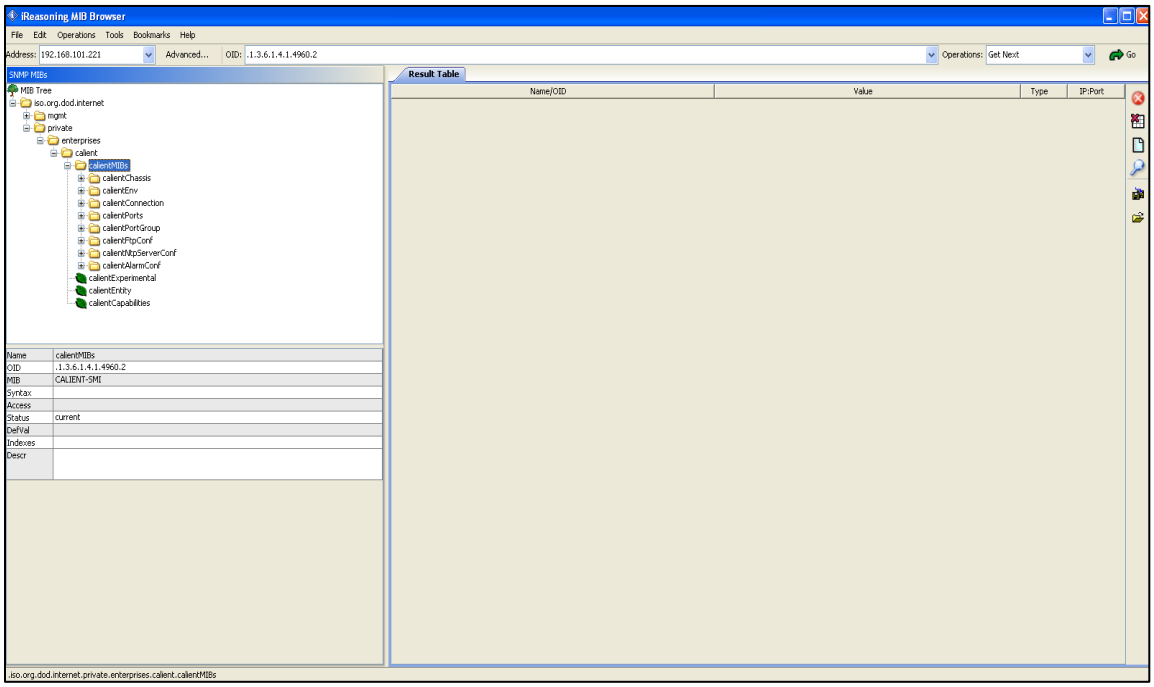


Figure 2 – Viewing MIBs with Standalone Browser

4 OCS SNMP AGENT INSTALLATION AND STARTUP

4.1 Supported Software Releases

SNMP agent installation and startup is supported in CALIENT software release 5.2.7 (GXCP-5.2-7) or later.

4.2 Installing the OCS SNMP Agent

The following procedure describes how to install the SNMP agent on your system:

1. Copy the GXCP image tar ball on the target board.
2. Log in to the target board at the following location:

   ```
   cd /opt/installtemp

   scp <userid>@192.168.120.13:/ws/images/xxx/GXCP-xxx.tar
   ```

3. Untar (open) the .tar file by issuing the following command:

   ```
   tar -xf  GXCP-xxx.tar
   ```

4. Install the GXCP image with the following command:

   ```
   cd /opt/installtemp/GXCP-xxx

   /install-upgrade
   ```

5. Stop services by issuing either of the following commands:

   ```
   gxc-stop OR StopAll.sh
   ```

6. Start services by issuing either of the following commands:

   ```
   gxc-start OR StartAll.sh
   ```

7. Check the status of services by issuing the following command:

   ```
   pl
   ```

   A list of all system services will be displayed. Services that are operational will appear as RUNNING; any that are not will appear as STOPPED.

```
                    Switch Status

      GxcMonitor ------>                    RUNNING
             Dsp ------>                    RUNNING
  NamingService ------>                    RUNNING
```

```
          EventServices ------>                 RUNNING
        EventConsumers ------>                  RUNNING
                CfgReg ------>                  RUNNING
         AlarmServices ------>                  RUNNING
         DeviceManager ------>                  RUNNING
          NodeServices ------>                  RUNNING
        Authentication ------>                  RUNNING
          SwitchMatrix ------>                  RUNNING
  xConnectProvisioner ------>                   RUNNING
           TL1Service ------>                   RUNNING
          PHPServices ------>                   RUNNING
          WebServices ------>                   RUNNING
          SNMPServices ------>                  RUNNING
```

5 CONFIGURING SNMP WITH THE WEB GUI

The OCS SNMP agent can be configured from the CALIENT WebGUI (graphical user interface); however, the user must have the required credentials to access it. Figure 3 provides a snapshot of the WebGUI Login page.

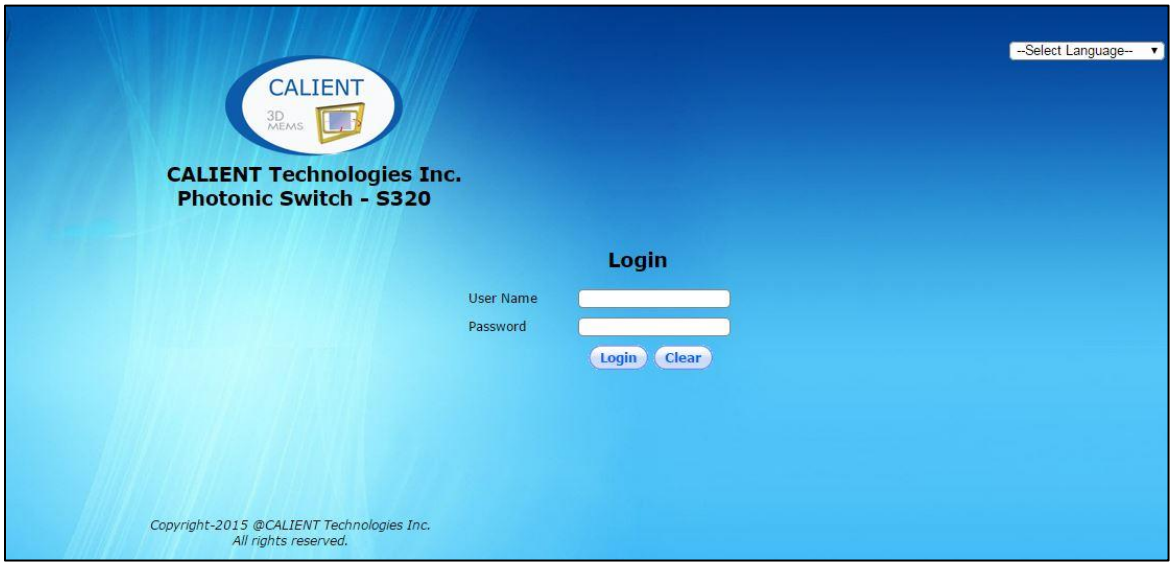


Figure 3 – CALIENT WebGUI Login

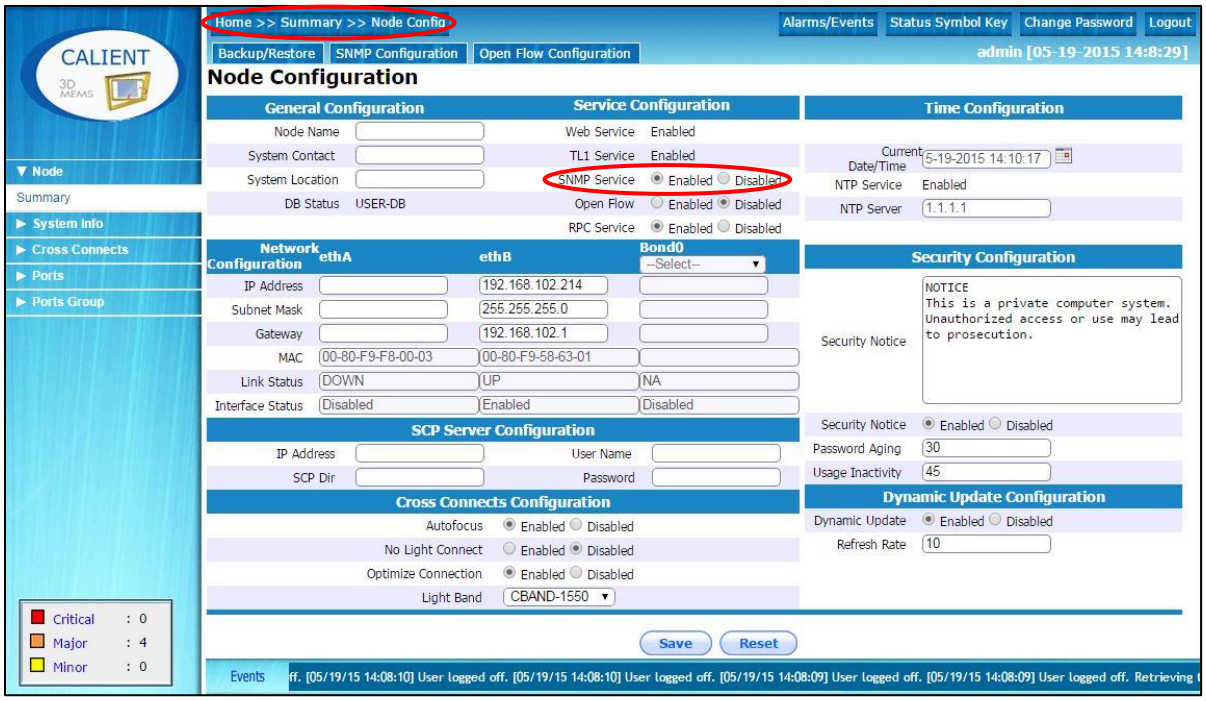
5.1 Enabling and Disabling SNMP

The following procedure describes how to enable and disable SNMP on the CALIENT OCS using the WebGUI:

1. Type in the appropriate information in the **User Name** and **Password** fields on the WebGUI **Login** page.
2. Click the **Login** button. The **Home** page will display.

3. Navigate the following path: **Node** > **Summary** > **Node Config**.

   The **Node Configuration** screen will open.



4. Click the **Enabled** radio button next to **SNMP Service** in the **Service Configuration** section of the **Node Configuration** screen to enable SNMP.

Conversely, clicking the **Disabled** radio button next to **SNMP Service** will disable SNMP on the switch.

5. Once the SNMP service is enabled, click the **SNMP Configuration** tab on the **Node Configuration** screen (Figure 4) to configure additional parameters for the service.

5.2 Configuring SNMP v1/v2c Get/Set Parameters

To access the SNMP v1/v2c agent, the SNMP Community and Type need to be configured. The Type can be configured as RO (Read Only) or RW (Read-Write). The Manager IP Address is an optional parameter that, if configured, restricts usage of the community name to the specified IP Address only. By default, one *public* read-only community and one *private* read-write community are created and added to the configuration. Authorized users can add, delete, and modify the parameters listed in Table 2 and shown in Figure 4.

Table 2 – SNMP v1/v2c Get/Set Parameters

Name Field	Description	Required
Community	SNMP v1/v2c Community Name	Yes
Manager IP Address	SNMP Manager IP Address	No
Type	RO (Read Only), RW (Read-Write)	Yes

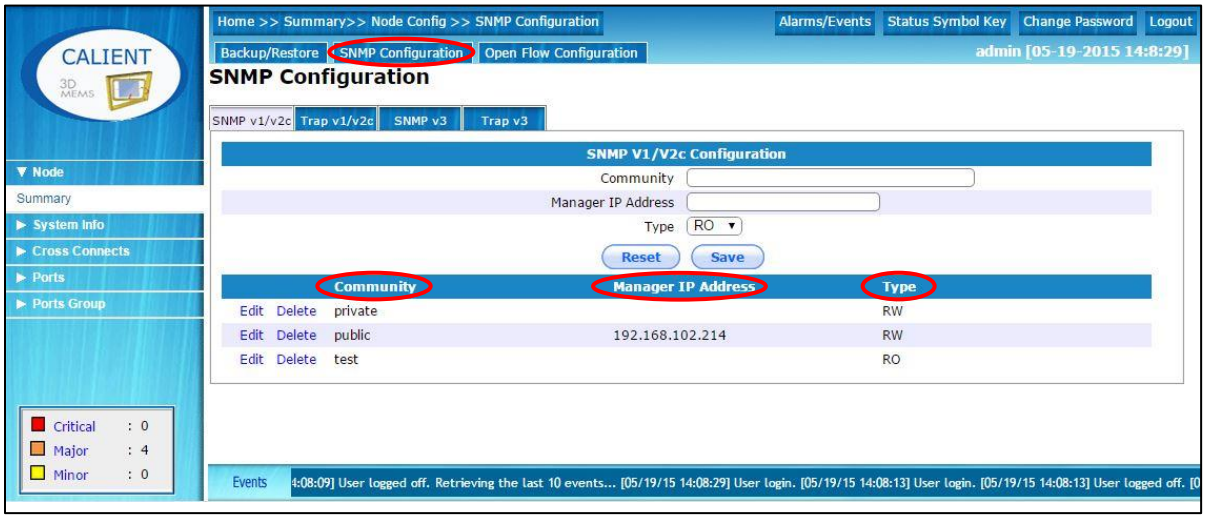


Figure 4 – Configuring SNMP v1/v2c Get/Set Parameters

5.3 Configuring SNMP v1/v2c Trap Parameters

Table 3 lists the trap parameters that need to be configured in order for the SNMP v1/v2c agent to send SNMP v1 Trap, v2c Trap or v2c Inform. Authorized users can add, delete or modify these parameters.

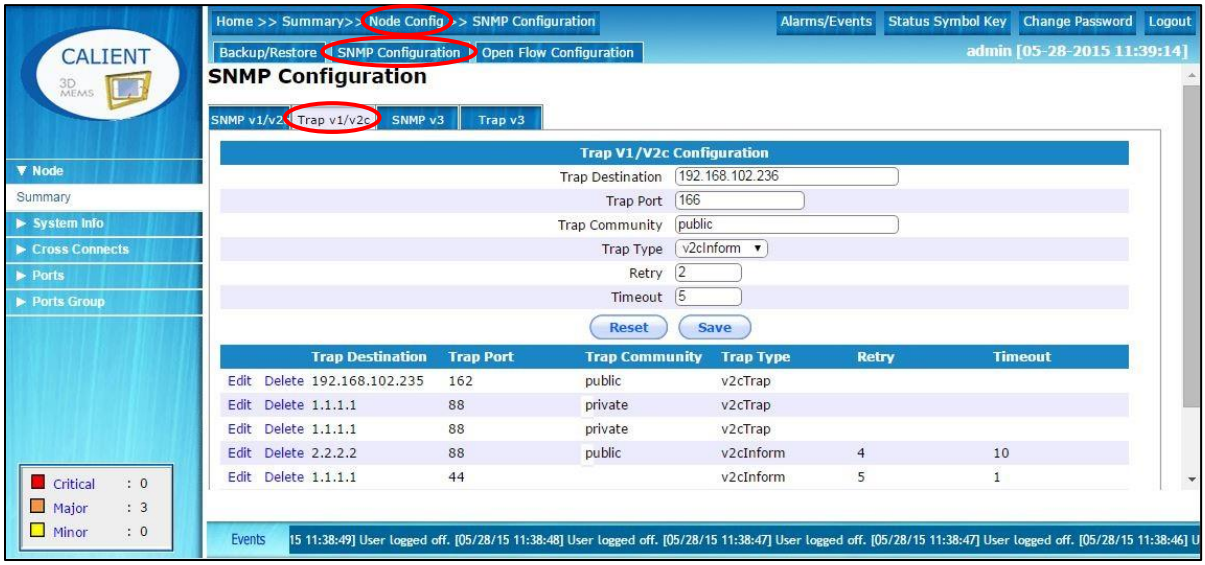
Table 3 – SNMP v1/v2c Trap Parameters

Field Name	Description	Required
Retry	The number of times the agent will resend the Inform message if an acknowledgement is not received.	Yes, if the trap type is v2c Inform
Timeout	The timeout, in seconds, that the agent will wait before resending the Inform message.	Yes, if the trap type is v2c Inform
Trap Community	The community name of the trap being sent	No; the default value is public for v1 Trap and v2 Trap
Trap Destination	The IP Address of the device to which the trap will be sent	Yes
Trap Port	The port number to which the trap will be sent	No; the default value is 162
Trap Type	The type of trap to be sent: v1 Trap, v2 Trap or v2c Inform.	Yes

Authorized users can add, delete or modify these parameters using the WebGUI. The following procedure describes how to do this:

1. Log in to the WebGUI.
2. Navigate the following path: **Node** > **Summary** > **Node Config**.

   The **Node Configuration** screen will open.
3. Click the **SNMP Configuration** tab in the **Node Configuration** screen.
4. Click the **Trap v1/v2c** tab in the **SNMP Configuration** screen to configure the trap parameters.



5.4 Configuring SNMP v3 Get/Set Parameters

To access the SNMP v3 agent, an SNMP v3 user needs to be configured. Table 4 lists the parameters that can be added, deleted or modified by the system administrator to configure a user. Figure 5 shows the parameters as they appear in the WebGUI.

Note

If a user is being utilized in a Trap v3 configuration, the user cannot be modified or deleted unless that specific Trap v3 configuration entry exists.

Table 4 – SNMP v3 Get/Set Parameters

Field Name	Description	Required
User Name	Unique SNMP v3 user name	Yes
User Type	Value can be RO (Read-Only) or RW (Read-Write)	Yes
Security Level	This value can be Auth/NoPriv or Auth/Priv ONLY	Yes
Auth Protocol	Authentication Protocol; value can be MD5 or SHA	Yes, if Security Level is Auth/NoPriv or Auth/Priv ONLY

Field Name	Description	Required
Priv Protocol	Privacy Protocol; value can be AES or DES	Yes, if Security Level is Auth/Priv ONLY
Auth Password	Authentication Password	Yes, if Security Level is Auth/NoPriv or Auth/Priv ONLY
Same Password for Auth & Priv	Flag specifying whether the password is the same for both Authentication and Privacy; values can be Yes or No	Yes
Priv Password	Privacy Password	Yes, if the Security Level is authPriv and Same Password for Auth & Priv is No

The SNMP v3 Engine ID and user parameters are displayed in the **SNMP v3** tab under the **SNMP Configuration** tab of the **SNMP Configuration** screen:

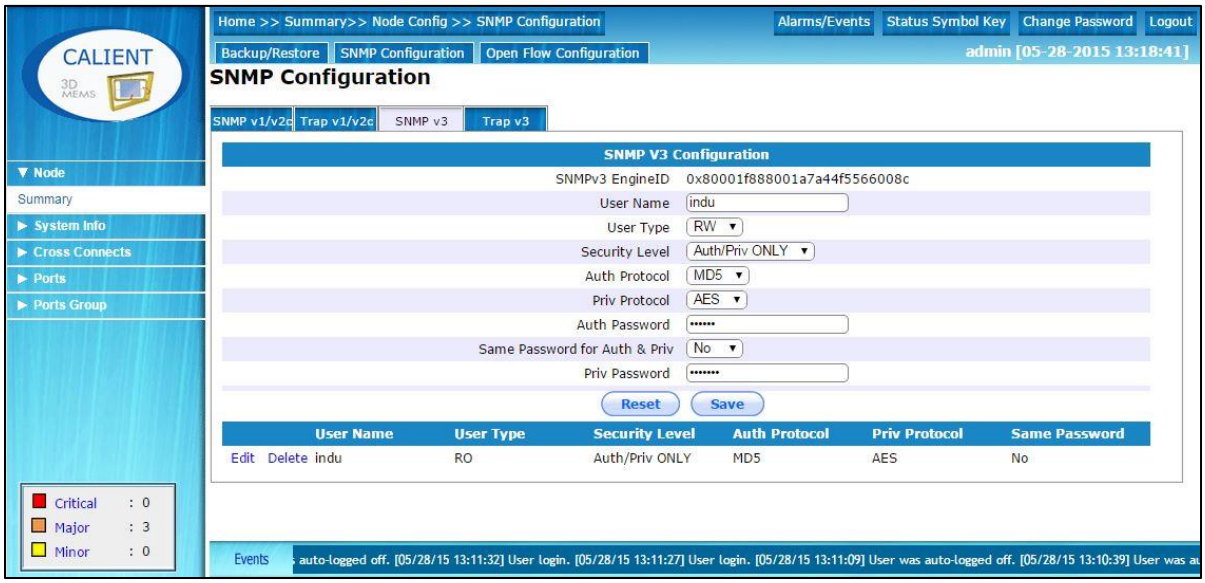


Figure 5 – Configuring SNMP v3 Get/Set Parameters

5.5 Configuring SNMP v3 Trap Parameters

For the SNMP v3 agent to send an SNMP v3 Trap or Inform message, a trap destination and SNMP v3 user need to be configured. The system has a provision to import already-configured SNMP v3 users from the SNMP v3 Get/Set configuration, but an SNMP v3 user needs to be

created before this can be done in the Trap v3 configuration. Table 5 lists the parameters that a system administrator can set to configure the SNMP v3 Trap. Figure 6 shows the parameters as they appear in the WebGUI.

Table 5 – SNMP v3 Trap Parameters

Field Name	Description	Required
Trap Destination	The IP address of the device to which the trap should be sent.	Yes
Trap Port	The port number to which the trap should be sent.	No; the default value is 162
Trap Type	The type of trap to be sent; the value can be v3Trap or v3Inform.	Yes
Retry	The number of times the agent will resend the Inform message if an acknowledgement is not received.	Yes, if the Trap Type is v3Inform
Timeout	The time, in seconds, the agent will wait before resending the Inform message.	Yes, if the Trap Type is v3Inform
User Name	A unique SNMP v3 user name; an SNMP v3 user created in an SNMP v3 Get/Set Configuration can be directly imported to this field.	Yes

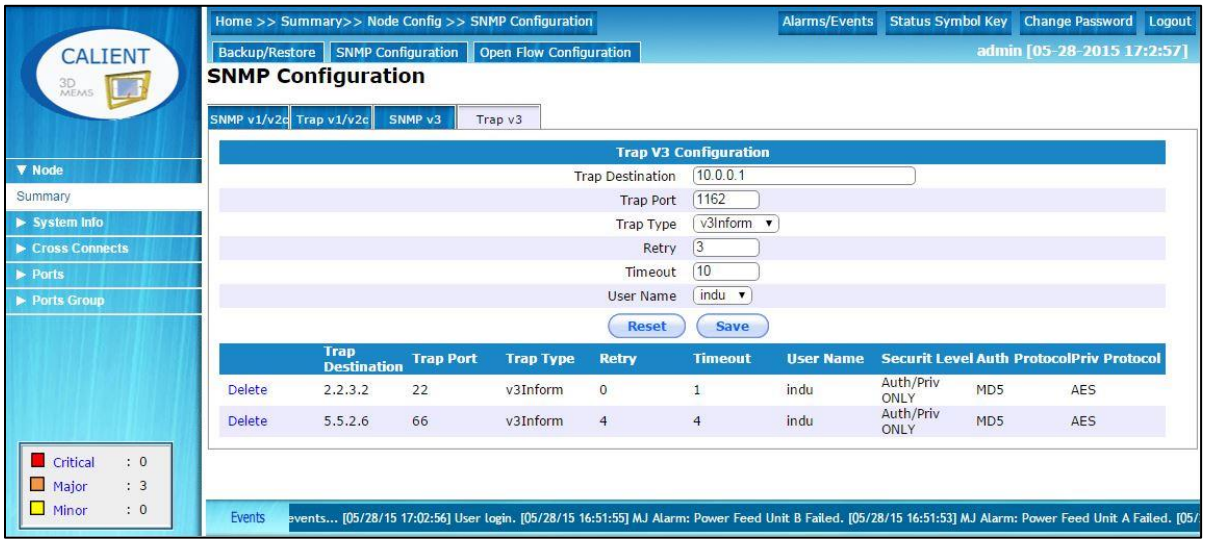


Figure 6 – Configuring SNMP v3 Trap Parameters

A SNMP CONFIGURATION RESTRICTIONS

A.1 Configuring the SNMP Agent

Following is a list of key words that should not be used when configuring the SNMP agent:

- rwcommunity
- rocommunity
- trapsink
- trap2sink
- informsink
- rwuser
- rouser
- trapsess

A.2 Configuring SNMP Users

Following is a list of SNMP v3 users that should not be created:

- defaultUserMD5
- defaultUserSHA
- defaultUserMD5DES
- defaultUserMD5AES
- defaultUserSHADES
- defaultUserSHAAES

B SNMP TEST PROCEDURES

This section describes various SNMP test procedures, including:

- Cross-connect testing
- Connection set table testing
- Port group testing
- Scalar OID testing
- User management testing
- Trap testing

B.1 Required Tools

The following tools are needed to perform SNMP tests:

- Net-SNMP command line utilities for table testing – these utilities are used to test the Create and Delete functionality of cross-connections. If you do not have them, they can be downloaded at http://www.net-snmp.org/download.html.
- iReasoning MIB browser for the snmpget/walk operation

B.1.1 Loading MIBs in SNMP Command Line Utilities

Before testing begins, MIBs need to be loaded into the SNMP command line utilities. The following procedure describes how to do this:

1. Locate the `mibdirs` at either of the following default paths:

   `/usr/local/share/snmp/mibs`

   OR

   `$HOME/.snmp/mibs`

2. Run the following command:

   `net-snmp-config --default-mibdirs`

3. Copy all of the MIBs in `mibdir`. If needed, the MIBs are available on the Caleng server at `//ftpsserver/Calient/mibs.tgz`.

4. Run the following command to verify that the MIBs have loaded successfully:

   ```
   snmptranslate -m +CALIENT-CONNECTION-MIB -IR -On calientTConnPortA
   ```

   The command should return the calientTConnPortA OID (.1.3.6.1.4.1.4960.2.5.1.1.3.1.1).

B.2 Cross-Connect Testing

Create and Delete connection requests will come as `snmpset` requests from NMS/SNMP utilities with multiple OIDs for creating and deleting cross-connections.

The calientTConnRowStatus OID in the `snmpset` request will be used to specify whether the request is for a Create or Delete operation.

B.2.1 Adding a Cross-Connection Using SNMP

The following procedure describes how to add a cross-connection using SNMP:

1. Verify existing connections in the cross-connection table using the `snmptable` binary.

   a. calientTransitConnectionTable:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnectionTable
   ```

   b. calientTransitConnHalfTable:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnHalfTable
   ```

2. Verify existing connections in the cross-connection table using the `snmpwalk` binary.

   a. calientTransitConnectionTable:

   ```
   snmpwalk -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnectionTable
   ```

   b. calientTransitConnHalfTable:

   ```
   snmpwalk -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnHalfTable
   ```

Note

SNMP is based on the User Datagram Protocol (UDP). UDP is inherently unreliable and, as such, sometimes the Manager may not receive a response packet from the SNMP agent. Most UDP-based systems have a timeout-retry mechanism to offset the unreliability of IP/UDP packet delivery. If the SNMP agent response is not received by the Manager, the Manager can be configured to resend the request after a specified timeout using the following command:

```
snmpwalk -v 2c –r 3 -t 20-m +CALIENT-CONNECTION-MIB -c public
192.168.101.221 calientTransitConnectionTable
```

3. Create a new cross-connection using the `snmpset` binary. Following is the command syntax for performing this step:

```
snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c <community> <host>
calientTConnRowStatus.0.0 i <row_status> calientTConnPortA.0.0 s
<src_port> calientTConnPortB.1.1 s <dest_port>
calientTConnDirection.1.1 i <connection_type> calientTConnName.1.1 s
<conn_name> calientTConnLightBand.1.1 s <waveband>
calientTConnAutoFocusState.1.1 s <auto_focus_state>
calientTConnNoLightState.1.1 s <no_light_state>
calientTConnGroupName.1.1 s <group_name>
```

Table 6 describes the parameters used to configure a new cross-connection with SNMP.

Table 6 – Cross-Connection Parameters

Parameter	Description	Required/Optional
row_status	Specifies whether the `snmpset` request is for creating or deleting a connection. Values for the parameter are: 4 – Create cross-connection 6 – Delete cross-connection	Required
src_port	The source port for the transit connection.	Required
dest_port	The destination port for the transit connection.	Required
connection_type	The directionality of the connection. Values for the parameter are: 1 – Bidirectional 2 – Unidirectional	Required

Parameter	Description	Required/Optional
conn_name	The customer or administratively assigned name of the connection.	Optional
waveband	The Light Band of the connection. Values for the parameter are: 0 – WBAND 1 – CBAND 2 – LBAND 3 – XLBAND 4 – OBAND 5 – NM850 6 – LightBandMax	Optional
auto_focus_state	Indicates whether or not Auto Focus has been enabled on the connection. Values for the parameter are: 0 – Disabled 1 – Enabled	Optional
no_light_state	Indicates whether or not No Light Connection has been enabled on the connection. Values for the parameter are: 0 – Disabled 1 – Enabled	Optional
group_name	The assigned group name of the connection.	Optional

4. Verify that the connection has been successfully created with the following command:

```
snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
192.168.101.221 calientTransitConnectionTable
```

B.2.1.1 Sample Cross-Connections

The following examples show how cross-connection parameters may be configured for different types of connections:

- Cross-connection with mandatory parameters specified

```
snmpset -m +CALIENT-CONNECTION-MIB -v 2c -t 30 -c private 192.168.101.221
calientTConnRowStatus.1.1 i 4 calientTConnPortA.1.1 s 1.1.1
calientTConnPortB.1.1 s 1.1.1 calientTConnDirection.1.1 i 2
```

- Cross-connection with optional connection name (conn_name) parameter specified

```
snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
calientTConnRowStatus.1.1 i 4 calientTConnPortA.1.1 s 2.5.7
calientTConnPortB.1.1 s 2.5.7 calientTConnDirection.1.1 i 2
calientTConnName.1.1 s from-Snmp
```

- Cross-connection with all parameters (required and optional) specified

```
snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
calientTConnRowStatus.1.1 i 4 calientTConnPortA.1.1 s 2.4.8
calientTConnPortB.1.1 s 2.4.8 calientTConnDirection.1.1 i 2
calientTConnName.1.1 s "ALL_Parms_Test" calientTConnLightBand.1.1 i 3
calientTConnAutoFocusState.1.1 i 1 calientTConnNoLightState.1.1 i 1
calientTConnGroupName.1.1 s SNMP_Group
```

B.2.2 Activating and Deactivating a Cross-Connection

This section describes the commands used to activate and deactivate a cross-connection using SNMP.

B.2.2.1 Activating a Connection

The following procedure explains how to activate a cross-connection on the CALIENT OCS using SNMP:

1. Issue the following `snmpwalk` command to get `calientTConnPortAEntPhysIndex` and `calientTConnPortBEntPhysIndex` from the `calientTransitConnectionTable`:

   ```
   snmpwalk -v 2c -m +CALIENT-CONNECTION-MIB -t 30 -c public <host-ip>
   calientTransitConnectionTable
   ```

2. Issue the following `snmpset` request to activate the connection:

   ```
   snmpset -v 2c -m +CALIENT-CONNECTION-MIB -c private <host-ip>
   calientTConnAdminState.<calientTConnPortAEntPhysIndex>.<calientTConnPortB
   EntPhysIndex> i 0 (in-service)
   ```

B.2.2.2 Deactivating a Connection

The following procedure explains how to deactivate a cross-connection on the CALIENT OCS using SNMP:

1. Issue the following `snmpwalk` command to get `calientTConnPortAEntPhysIndex` and `calientTConnPortBEntPhysIndex` from the `calientTransitConnectionTable`:

   ```
   snmpwalk -v 2c -m +CALIENT-CONNECTION-MIB -t 30 -c public <host-ip>
   calientTransitConnectionTable
   ```

2. Issue the following `snmpset` request to deactivate the connection:

   ```
   snmpset -v 2c -m +CALIENT-CONNECTION-MIB -c private <host-ip>
   calientTConnAdminState.<calientTConnPortAEntPhysIndex>.<calientTConnPortB
   EntPhysIndex> i 3 (under management)
   ```

B.2.3 Deleting a Cross-Connection

The following procedure describes how to delete a cross-connection on the CALIENT OCS:

1. Verify the existing connections in the cross-connect table using the `snmptable` binary.

   calientTransitConnectionTable:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnectionTable
   ```

   calientTransitConnHalfTable:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnHalfTable
   ```

2. Specify the index (`calientTConnPortAEntPhysIndex` and `calientTConnPortBEntPhysIndex`) of the connection to be deleted:

   ```
   snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c <community> <host>
   calientTConnRowStatus. < calientTConnPortAEntPhysIndex >.
   < calientTConnPortBEntPhysIndex > i <row_status>
   ```

3. Issue an `snmpwalk` request to determine the row index of the connection to be deleted.

   Command:

   ```
   $ snmpwalk -v 2c -m +CALIENT-CONNECTION-MIB -t 30 -c public
   192.168.101.221 calientTConnId
   ```

   Response:

   ```
   CALIENT-CONNECTION-MIB::calientTConnId.101031.101031 = STRING: 1.1.1>1.1.1
   CALIENT-CONNECTION-MIB::calientTConnId.101032.101032 = STRING: 1.1.2>1.1.2
   ```

4. Send an `snmpset` request to delete, specifying the 101032.101032 index, to delete the 1.1.2>1.1.2 connection.

   Command:

   ```
   $ snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
   calientTConnRowStatus.101032.101032 i 6
   ```

   Response:

   ```
   CALIENT-CONNECTION-MIB::calientTConnRowStatus.101032.101032 = INTEGER:
   destroy(6)
   ```

5. Verify that the connection has been successfully deleted with the following command:

```
snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
192.168.101.221 calientTransitConnectionTable
```

B.2.4 Delete All (Bulk Delete) Cross-Connections

The following procedure describes how to delete all (bulk delete) cross-connections on the CALIENT OCS:

1. Verify the existing connections in the cross-connect table using the `snmptable` binary.
2. Set the scalar object `calientDeleteAllConnections` to 1.

   Command Syntax:

   ```
   snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c <community> <host>
   calientDeleteAllConnections.0 i <value>
   ```

   Command:

   ```
   snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
   calientDeleteAllConnections.0 i 1
   ```

3. Verify that all connections have been successfully deleted with the following command:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnectionTable
   ```

B.2.5 Loopback All Cross-Connections

The following procedure describes how to loopback all cross-connections on the CALIENT OCS:

1. Set the scalar object `calientLoopbackAllConnections` to 1.

   Command Syntax:

   ```
   snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c <community> <host>
   calientLoopbackAllConnections.0 i <value>
   ```

   Command:

   ```
   snmpset -m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
   calientLoopbackAllConnections.0 i 1
   ```

2. Verify that the loopback connections have been successfully created with the following command:

   ```
   snmptable -v 2c -t 30 -m +CALIENT-CONNECTION-MIB -c public
   192.168.101.221 calientTransitConnectionTable
   ```

B.2.6 Checking the Status of the Last Operation

The following procedure describes how to check the status of the last operation performed on connection tables:

1. Execute an SNMP Get on the scalar object `calientLastOperationResult`.

   Command Syntax:

   ```
   snmpget -m +CALIENT-CONNECTION-MIB -v 2c -c <community> <host>
   calientLastOperationResult.0
   ```

   Command:

   ```
   snmpget-m +CALIENT-CONNECTION-MIB -v 2c -c private 192.168.101.221
   calientLastOperationResult.0

   snmpget -r 4 -v 2c -c public -t 20 192.168.102.209
   1.3.6.1.4.1.4960.2.5.1.1.8.0
   ```

   Response:

   ```
   Cannot find module (HOST-RESOURCES-MIB): At line 1 in (none)
   Cannot find module (UCD-DLMOD-MIB): At line 1 in (none)
   SNMPv2-SMI::enterprises.4960.2.5.1.1.8.0 = STRING: "Completed"
   ```

B.3 Connection Set Table Testing

B.3.1 Creating a New Connection Set

The following procedure describes how to create a new connection set using SNMP:

1. Verify the existing connection sets with the `snmptable` binary.

   ```
   snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
   192.168.102.175 calientConnectionSetTable
   ```

2. Create new connection set with the following command:

   Command Syntax:

   ```
   snmpset -v 2c -t 30 -m All -c <community> <host>
   calientConnSetRowStatus.1 i <value>  calientTConnSetName.1 s
   <ConnectionSetName>  calientTConnSetDesc.1 s <ConnectionSetDescription>
   ```

   Command:

   ```
   snmpset -v 2c -t 30 -m All -c private 192.168.102.175
   calientConnSetRowStatus.1 i 4  calientTConnSetName.1 s
   snmpTestSave  calientTConnSetDesc.1 s  "TestSaveConnection"
   ```

3. Verify that the connection set has been successfully created with the following command:

```
snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
192.168.102.175 calientConnectionSetTable
```

B.3.2 Deleting a Saved Connection Set

The following procedure describes how to delete a saved connection set using SNMP:

1. Verify existing connection sets with the `snmptable` binary.

```
snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
192.168.102.175 calientConnectionSetTable
```

2. Delete the saved connection set with the following command:

   Command Syntax:

```
snmpset -v 2c -t 30 -m All -c private 192.168.102.175
calientConnSetRowStatus.<calientConnSetIndex> i <value>
```

   Command:

```
snmpset -v 2c -t 30 -m All -c private 192.168.102.175
calientConnSetRowStatus.10002 i 6
```

3. Verify that the connection set has been successfully deleted with the following command:

```
snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
192.168.102.175 calientConnectionSetTable
```

B.3.3 Recalling a Saved Connection Set

The following procedure describes how to recall a saved connection set using SNMP:

1. Verify existing connection sets with the `snmptable` binary.

```
snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
192.168.102.175 calientConnectionSetTable
```

2. Recall the saved connection set with the following command:

   Command Syntax:

```
snmpset -v 2c -t 30 -m All -c private 192.168.102.175
calientTConnSetLoaded.<calientConnSetIndex> i <value>
```

   Command:

```
snmpset -v 2c -t 30 -m All -c private 192.168.102.175
calientTConnSetLoaded.10002 i 1
```

3. Verify that the connection set has been successfully recalled with the following command:

```
snmptable -v 2c -t 30 -m + CALIENT-CONNECTION-MIB -c public
192.168.102.175 calientConnectionTransitTable
```

Recalling a Connection Set will create the connections saved in the Connection Set; hence, a connection table walk needs to be performed.

B.4 Port Group Testing

B.4.1 Creating a New Port Group

The following procedure describes how to create a new port group using SNMP:

1. Verify existing port groups with the `snmptable` binary.

```
snmptable -v 2c -t 30 -m + CALIENT-PORT-GROUP-MIB -c public
192.168.101.221 calientPortGroupTable
```

2. Create new port group with the following command:

   Command Syntax:

```
snmpset -m +CALIENT-PORT-GROUP-MIB -v 2c -c <community> <host>
calientPortGroupRowStatus.1 i <value> calientPortGroupName.1 s
<portGroupName> calientPortGroupMemberPorts.1 s <memberPortList>
```

   Command:

```
snmpset -m +CALIENT-PORT-GROUP-MIB -v 2c -c private 192.168.101.221
calientPortGroupRowStatus.1 i 4 calientPortGroupName.1 s SNMP_PG
calientPortGroupMemberPorts.1 s 1.1.1,1.1.2
```

3. Verify that the port group has been successfully created with the following command:

```
snmptable -v 2c -t 30 -m + CALIENT-PORT-GROUP-MIB -c public
192.168.101.221 calientPortGroupTable
```

B.4.2 Deleting an Existing Port Group

The following procedure describes how to delete an existing port group using SNMP:

1. Verify existing port groups with the `snmptable` binary.

   ```
   snmptable -v 2c -t 30 -m + CALIENT-PORT-GROUP-MIB -c public
   192.168.101.221 calientPortGroupTable
   ```

2. Delete the existing port group with the following command:

   Command Syntax:

   ```
   snmpset -m +CALIENT-PORT-GROUP-MIB -v 2c -c <community> <host>
   calientPortGroupRowStatus.1 i <value>
   ```

   Command:

   ```
   snmpset -m +CALIENT-PORT-GROUP-MIB -v 2c -c private 192.168.101.221
   calientPortGroupRowStatus.1000 i 6
   ```

3. Use the unique index associated with the `calientPortGroupRowStatus` OID to delete the port group.

4. Verify that the port group has been successfully deleted with the following command:

   ```
   snmptable -v 2c -t 30 -m + CALIENT-PORT-GROUP-MIB -c public
   192.168.101.221 calientPortGroupTable
   ```

B.5 Scalar OID Testing

Scalar OIDs are tested using `snmpget`, `snmpset` and `snmpwalk` commands, based on the access type of the object. Examples of these commands are provided below:

- `snmpget`

  Command Syntax:

  ```
  snmpget -m +<mib_name> -v 2c -c <community> <host> <OID>.0
  ```

  Command:

  ```
  snmpget  -m +CALIENT-CHASSIS-MIB -v 2c -c public 192.168.101.221
  calientChassisGenName.0
  ```

- `snmpset`

  Command Syntax:

  ```
  snmpset -m +<mib_name> -v 2c -c <community> <host> <OID>.0 <type> <value>
  ```

  Command:

  ```
  snmpset  -m +CALIENT-CHASSIS-MIB -v 2c -c private 192.168.101.221
  calientChassisGenName.0 s SNMP_Board
  ```

- `snmpwalk`

  Command Syntax:

  ```
  snmpwalk –m +<mib_name> -v 2c -c <community> <host> <OID>
  ```

  Command:

  ```
  snmpwalk –m +CALIENT-CHASSIS-MIB -v 2c -c public 192.168.101.221
  calientChassisGen
  ```

B.6 User Management Testing

This section describes the procedures for testing User Management MIBs, including creating a new user, modifying a user and deleting a user.

B.6.1 Creating a New User

Various parameters—some required, some optional—need to be configured in order to create a new user. Table 7 lists the parameters for creating a new user.

Table 7 – New-User Parameters

Parameter	Description	Required/Optional
Row status	Identifies whether the `snmpset` request is for the create or delete operation. Values for the parameter are: 4 – Create user 6 – Delete user	Required
Username	Name/User ID of the user	Required
Password	Password of user	Required
User role	Specifies the role/privilege level of the user. Values for the parameter are: 0 – No Role 1 – Administrator 2 – Install-Maintenance 3 – Field 4 – Provisioner 5 – Read-Only 6 – Restricted 7 – Expired	Required

Parameter	Description	Required/Optional
TL1Access	Indicates whether the user is allowed to access the device using TL1. Values for the parameter are: 0 – No 1 – Yes	Optional
Web Access	Indicates whether the user is allowed to access the device using the Web. Values for the parameter are: 0 – No 1 – Yes	Optional
Multi Session Allow	Indicates whether the user is allowed to conduct multiple sessions. Values for the parameter are: 0 – Disabled 1 – Enabled	Optional
AssocPortGrp	Indicates the PortGroups the user is associated with.	Optional
UserStatus	Indicates whether the user is enabled or disabled. Values for the parameter are: 0 – Disabled 1 – Enabled	Optional

B.6.1.1 Required Parameters

The following parameters must be specified when creating a new user:

- calientUserName
- calientUserRole
- calientUserPass

B.6.1.2 Optional Parameters

The following parameters may be specified when creating a new user, but are not required:

- calientUserTL1Access
- calientUserWebAccess
- calientUserMultiSessAllow

- calientUserAssocPortGrp
- calientUserStatus

B.6.1.3 Procedure

The following procedure describes how to create a new user with SNMP:

1. Verify existing users in the `calientUserMgmtConfTable` with the `snmptable` binary.

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

2. Create a new user with the `snmpset` binary.

   Command Syntax:

   ```
   snmpset -v 2c -c private  -m CALIENT-USER-MGMT-MIB  192.168.101.221
   calientUserMgmtRowStatus.10 i < Row status > calientUserName.10 s <User
   name> calientUserPass.10 s <password> calientUserRole.10 i <user role>
   calientUserTL1Access.10 i <TL1Access> calientUserWebAccess.10 i <Web
   Access> calientUserMultiSessAllow.10 i <MultiSession Allow>
   calientUserAssocPortGrp.10 s <AssocPortGrp> calientUserStatus.10  i
   <UserStatus>
   ```

   Command:

   ```
   snmpset -v 2c -c private -m CALIENT-USER-MGMT-MIB  192.168.101.221
   calientUserMgmtRowStatus.10 i 4 calientUserName.10 s psl_User
   calientUserPass.10  s  Psl@123 calientUserRole.10 i 2
   calientUserTL1Access.10 i 1 calientUserWebAccess.10 i 0
   calientUserMultiSessAllow.10 i 1 calientUserAssocPortGrp.10 s SYS
   calientUserStatus.10 i 1
   ```

3. Verify that the new user has been successfully created with the following command:

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

B.6.2 Modifying a User

The following procedure describes how to modify a user with SNMP:

1. Verify existing users in the `calientUserMgmtConfTable` with the `snmptable` binary:

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

2. Issue the following commands to modify a user:

   Command Syntax:

   ```
   snmpset  -v 2c -m CALIENT-USER-MGMT-MIB-c private 192.168.101.221 <oid-to
   -be-modified>.<index-of-the-user-record-to-be-modified>  [ObjectType
   (i/s)]  <value>
   ```

   c. Modifying the user password:

   ```
   snmpset -m CALIENT-USER-MGMT-MIB -v 2c -c private 192.168.101.221
   calientUserPass.10001 s Test@12
   ```

   d. Modifying the user role:

   ```
   snmpset -m CALIENT-USER-MGMT-MIB -v 2c -c private 192.168.101.221
   calientUserRole.10002 i 3
   ```

3. Verify that the user record has been modified with the following commands:

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

   ```
   snmpwalk -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.102.201
   calientUserMgmtConfTable
   ```

B.6.3 Deleting a User

The following procedure describes how to delete a user with SNMP:

1. Verify existing users in the `calientUserMgmtConfTable` with the `snmptable` binary.

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

2. Delete the user with the following `snmpset` command:

   Command Syntax:

   ```
   snmpset -v 2c -m CALIENT-USER-MGMT-MIB-c private 192.168.101.221
   calientUserMgmtRowStatus.<index-of-the-user-record-to-be-deleted> i 6
   ```

   Command:

   ```
   snmpset  -m CALIENT-USER-MGMT-MIB  -v 2c -c private 192.168.101.221
   calientUserMgmtRowStatus.10001  i 6
   ```

3. Verify that the user record has been deleted with the following command:

   ```
   snmptable -m CALIENT-USER-MGMT-MIB -v 2c -c public 192.168.101.221
   calientUserMgmtConfTable
   ```

B.7 Trap Testing

The following procedure describes how to perform trap tests with SNMP:

1. Configure the SNMP agent to send traps.
2. Perform the following steps to generate a Connection Input signal-degraded trap:
   a. Log into TL1 service.
   b. Create a connection.

      ```
      ent-crs::1.1.1,1.1.2:::,1way
      ```

   c. Activate the connection.

      ```
      act-crs::1.1.1,1.1.2:::1.1.1>1.1.2
      ```

   d. Degrade the port.

      ```
      ed-port::1.1.1::::inoptdegr=5.0
      ```

3. Run Wireshark (or any other trap-receiver application) on a device that is configured as the trap destination.
4. Verify that the trap has been received.

B.8 Useful SNMP Commands

The following commands are useful tools for managing the CALIENT OCS with SNMP:

- **SNMP Walk Command**

  The `snmpwalk` command can be applied to the entire node.

  Syntax:

  ```
  snmpwalk -v <Version> -c <community> -t <timeout in sec> -m ALL <host>
  <node_name>
  ```

  Example:

  ```
  snmpwalk -v 2c -c public -t 30 -m ALL 192.168.101.221 calient
  ```

- **SNMP Bulk Walk Command**

  Syntax:

  ```
  snmpbulkwalk -v <Version> -c <community> -t <timeout in sec> -m ALL
  <host> <node_name>
  ```

Example:

```
snmpbulkwalk -v 2c -c public -t 30 -m ALL 192.168.101.221 calient
```

C SUPPORTED CALIENT MIB OIDS

This section lists the various CALIENT MIB OIDs supported on the CALIENT OCS. MIBs supported on the switch include:

- Alarm Configuration MIBs
- Chassis MIBs
- Connection MIBs
- Environmental MIBs
- FTP Configuration MIBs
- NTP Server Configuration MIBs
- Port MIBs
- Port Group MIBs
- Security MIBs
- Service Configuration MIBs
- Session Management MIBs
- Software Management MIBs
- User Management MIBs

C.1 Alarm Configuration MIBs

Table 8 lists the CALIENT MIB OIDs for alarms.

Table 8 – CALIENT Alarm Configuration MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.16.1.2	calientAlarmSoakInterval	The soak interval for all alarms.
Table Objects – calientAlarmConfTable		
1.3.6.1.4.1.4960.2.16.1.1.1.1	calientAlarmEntryIndex	The unique index identifying the alarm entry.

OID	Name	Description
1.3.6.1.4.1.4960.2.16.1.1.1.2	calientConfAlarmName	The name of the configured alarm; it can be any of the values enumerated in calientAlarmClass.
1.3.6.1.4.1.4960.2.16.1.1.1.2	calientConfAlarmSev	The severity of the configured alarm.

C.2 Chassis MIBs

Table 9 lists the CALIENT MIB OIDs for the switch chassis.

Table 9 – CALIENT Chassis MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.1.1.1.1	calientChassisGenName	The administratively configured name of the chassis; typically, this name is unique within a given network.
1.3.6.1.4.1.4960.2.1.1.1.2	calientChassisGenSerialNum	The serial number of the chassis.
1.3.6.1.4.1.4960.2.1.1.1.3	calientChassisGenOperState	The current operating state of the chassis.
1.3.6.1.4.1.4960.2.1.1.1.4	calientChassisGenCapState	The capability state of the chassis.
1.3.6.1.4.1.4960.2.1.1.1.5	calientChassisGenTime	The time of the clock set in the chassis.
1.3.6.1.4.1.4960.2.1.1.4.1	calientPortCount	The number of ports installed in this OCS.
1.3.6.1.4.1.4960.2.1.1.4.2	calientConnectedPortCount	The current number of ports connected in this OCS.
Traps		
1.3.6.1.4.1.4960.2.1.2.6.1	calientChassisLogUploadOK	A system log file has been uploaded successfully.
1.3.6.1.4.1.4960.2.1.2.6.2	calientChassisLogUploadFailure	A system log file upload has failed.
1.3.6.1.4.1.4960.2.1.2.6.3	calientChassisLogRemoved	A system log file has been removed.
1.3.6.1.4.1.4960.2.1.2.6.4	calientChassisLogOpenFailure	Attempt to open the system log file has failed.
1.3.6.1.4.1.4960.2.1.2.6.5	calientChassisBackupCompleted	The configuration backup has been completed.

OID	Name	Description
1.3.6.1.4.1.4960.2.1.2.6.6	calientChassisBackupFailure	The configuration backup has failed.
1.3.6.1.4.1.4960.2.1.2.6.7	calientChassisRestoreCompleted	The configuration restoration has been completed.
1.3.6.1.4.1.4960.2.1.2.6.8	calientChassisRestoreFailure	The configuration restoration has failed.
1.3.6.1.4.1.4960.2.1.2.6.9	calientChassisCPRoleChanged	The CP card role has been changed.
1.3.6.1.4.1.4960.2.1.2.6.10	calientChassisLinkSwitchOver	Bond0 primary interface changed.
1.3.6.1.4.1.4960.2.1.2.6.11	calientChassisRTCFailedEvent	RTC access failed.
1.3.6.1.4.1.4960.2.1.2.6.12	calientChassisGxcSrvsUpEvent	GXC services up.
1.3.6.1.4.1.4960.2.1.2.6.13	calientChassisGxcSrvsDownEvent	GXC services down.
1.3.6.1.4.1.4960.2.1.2.6.14	calientChassisPhyIfDownEvent	Physical interface is down.
1.3.6.1.4.1.4960.2.1.2.6.325	calientCPSwitchOverAlarm	Switchover to standby CP alarm.

C.3 Connection MIBs

Table 10 lists the CALIENT MIB OIDs for connections.

Table 10 – CALIENT Connection MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.5.1.1.1	calientTransitConnectionCount	Number of Transit Connections provisioned on this OCS.
1.3.6.1.4.1.4960.2.5.1.1.2	calientTransitFailedConnectionCount	Number of Transit Connections provisioned on this OCS that currently have and operational status of OOS and an operation capability of Failed.
1.3.6.1.4.1.4960.2.5.1.1.6	calientDeleteAllConnections	Provisions the operator to delete all connections.
1.3.6.1.4.1.4960.2.5.1.1.7	calientLoopbackAllConnections	Provisions the operator to create loopback connections on all ports.
1.3.6.1.4.1.4960.2.5.1.1.8	calientLastOperationResult	Provisions the operator to get the result (e.g., completed or in-progress) of the last operation (e.g., recall/create loopback).

OID	Name	Description
Table Objects – calientTransitConnectionTable		
1.3.6.1.4.1.4960.2.5.1.1.3.1.1	calientTConnPortA	One of the ports involved in the transit connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.2	calientTConnPortB	One of the ports involved in the transit connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.3	calientTConnPortAEntPhysIndex	The entPhysicalIndex corresponding to one of the ports involved in the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.4	calientTConnPortBEntPhysIndex	The entPhysicalIndex corresponding to one of the ports involved in the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.5	calientTConnId	The name of the connection. By convention, it has the format <PortIdentifier>-<PortIdentifier> (e.g., 3.2b.1-4.3b.3).
1.3.6.1.4.1.4960.2.5.1.1.3.1.6	calientTConnDirection	Directionality of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.7	calientTConnType	The type of connection; local(1) signifies the connection was configured by a user.
1.3.6.1.4.1.4960.2.5.1.1.3.1.8	calientTConnRowStatus	The Transit Connection Table Row Status for creating/deleting a row
1.3.6.1.4.1.4960.2.5.1.1.3.1.9	calientTConnAdminState	The administrative state of this connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.10	calientTConnOperState	The operating state of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.11	calientTConnCapabilityState	The operational capability of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.12	calientTConnRedundantState	The redundancy state of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.13	calientTConnAlarmState	The alarm state of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.14	calientTConnCustName	The name of the customer/owner of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.15	calientTConnName	The customer/administratively assigned name of the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.16	calientTConnDiagMessage	A summary of the last diagnostics performed on the connection, or additional details on the current operational state.
1.3.6.1.4.1.4960.2.5.1.1.3.1.17	calientTConnLightBand	The light band of the connection.

OID	Name	Description
1.3.6.1.4.1.4960.2.5.1.1.3.1.18	calientTConnAutoFocusState	Indicates whether or not Auto Focus has been enabled on the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.19	calientTConnNoLightState	Indicates whether or not No Light Connection has been enabled on the connection.
1.3.6.1.4.1.4960.2.5.1.1.3.1.20	calientTConnSRRLCktID1	The name of the Shared Resource Risk List for the connection. By convention, it has the format <PortIdentifier>-<PortIdentifier> (e.g., 3.2b.1-4.3b.3).
1.3.6.1.4.1.4960.2.5.1.1.3.1.21	calientTConnSRRLCktID2	The name of the Shared Resource Risk List for the connection. By convention, this has the format <PortIdentifier>-<PortIdentifier> (e.g., 3.2b.1-4.3b.3).
1.3.6.1.4.1.4960.2.5.1.1.3.1.22	calientTConnGroupName	The assigned group name of the connection.
Table Objects – calientTransitConnHalfTable		
1.3.6.1.4.1.4960.2.5.1.1.4.1.1	calientTConnHalfType	The type of connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.2	calientTConnHalfConnId	Connection ID for one half of a connection. The reverse half of a bi-directional connection will have a connection ID that is the reverse of the forward one.
1.3.6.1.4.1.4960.2.5.1.1.4.1.3	calientTConnHalfAdminState	The administrative state of a connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.4	calientTConnHalfOperState	The operating state of a connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.5	calientTConnHalfCapState	The capability state of a connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.6	calientTConnHalfRedState	The redundant state of a connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.7	calientTConnHalfAlarmState	The alarm state of a connection half.
1.3.6.1.4.1.4960.2.5.1.1.4.1.8	calientTConnHalfWorkMatrix	The working matrix in which the connection is used; this is an index to a row in the calientXMatrixTable.

OID	Name	Description
1.3.6.1.4.1.4960.2.5.1.1.4.1.9	calientTConnHalfProtMatrix	The protection matrix that the connection uses; this is an index to a row in the calientXMatrixTable.
1.3.6.1.4.1.4960.2.5.1.1.4.1.10	calientTConnHalfLightBand	The light band of the connection.
1.3.6.1.4.1.4960.2.5.1.1.4.1.11	calientTConnHalfAutoFocusStat e	Indicates whether or not Auto Focus has been enabled on the connection.
1.3.6.1.4.1.4960.2.5.1.1.4.1.12	calientTConnHalfNoLightState	Indicates whether or not No Light Connection has been enabled on the connection.
1.3.6.1.4.1.4960.2.5.1.1.4.1.13	calientTConnHalfSRRLCktID1	The name of the Shared Resource Risk List for the connection. By convention, it has the format <PortIdentifier>-<PortIdentifier> (e.g., 3.2b.1-4.3b.3).
1.3.6.1.4.1.4960.2.5.1.1.4.1.14	calientTConnHalfSRRLCktID2	The name of the Shared Resource Risk List for the connection. By convention, it has the format <PortIdentifier>-<PortIdentifier> (e.g., 3.2b.1-4.3b.3).
1.3.6.1.4.1.4960.2.5.1.1.4.1.15	calientTConnHalfGroupName	The assigned group name of the connection.
1.3.6.1.4.1.4960.2.5.1.1.4.1.16	calientTConnInPower	Connection input power.
1.3.6.1.4.1.4960.2.5.1.1.4.1.17	calientTConnOutPower	Connection output power.
1.3.6.1.4.1.4960.2.5.1.1.4.1.18	calientTConnLoss	Connection power loss.
Table Objects – calientConnectionSetTable		
1.3.6.1.4.1.4960.2.5.1.1.5.1.1	calientTConnSetName	The assigned name of the connection set.
1.3.6.1.4.1.4960.2.5.1.1.5.1.2	calientTConnSetUser	The user who created the set.
1.3.6.1.4.1.4960.2.5.1.1.5.1.3	calientTConnSetCreationDate	The date and time the set was created.
1.3.6.1.4.1.4960.2.5.1.1.5.1.4	calientTConnSetConnCount	The number of connections in the set.
1.3.6.1.4.1.4960.2.5.1.1.5.1.5	calientTConnSetLoaded	Indicates whether or not the set was loaded.
1.3.6.1.4.1.4960.2.5.1.1.5.1.6	calientTConnSetDesc	The set description.
1.3.6.1.4.1.4960.2.5.1.1.5.1.7	calientConnSetRowStatus	The Connection Set Row Status for creating and deleting a row.

OID	Name	Description
Traps		
1.3.6.1.4.1.4960.2.5.2.6.1	calientTranConnRcvHWFail	The Transit Connection has encountered a hardware failure on the receiving end.
1.3.6.1.4.1.4960.2.5.2.6.3	calientTranConnXmtHWFail	The Transit Connection has encountered a hardware failure on the transmitting end.
1.3.6.1.4.1.4960.2.5.2.6.5	calientTranConnRcvSignalDegraded	Receiving end of Transit Connection has signal power below the degrade threshold.
1.3.6.1.4.1.4960.2.5.2.6.6	calientTranConnRcvSignalCritical	Receiving end of Transit Connection has signal power below the critical threshold.
1.3.6.1.4.1.4960.2.5.2.6.8	calientTranConnXmtSignalDegraded	Transmitting end of Transit Connection has signal power below the degrade threshold.
1.3.6.1.4.1.4960.2.5.2.6.9	calientTranConnXmtSignalCritical	Transmitting end of Transit Connection has signal power below the critical threshold.
1.3.6.1.4.1.4960.2.5.2.6.11	calientTranConnUnprotected	A matrix detects no protection on the Transit Connection.
1.3.6.1.4.1.4960.2.5.2.6.13	calientTranConnOK	The Transit Connection is normal.
1.3.6.1.4.1.4960.2.5.2.6.14	calientTranConnAdded	A Transit Connection has been added.
1.3.6.1.4.1.4960.2.5.2.6.15	calientTranConnDeleted	A Transit Connection has been deleted.
1.3.6.1.4.1.4960.2.5.2.6.16	calientTranConnActivated	A Transit Connection has been activated.
1.3.6.1.4.1.4960.2.5.2.6.17	calientTranConnDeactivated	A Transit Connection has been deactivated.
1.3.6.1.4.1.4960.2.5.2.6.18	calientTranConnProtectionSwitchOK	A Transit Connection has been switched to another matrix.
1.3.6.1.4.1.4960.2.5.2.6.19	calientTranConnProtectionSwitchFailed	A Transit Connection has failed to switch to another matrix.
1.3.6.1.4.1.4960.2.5.2.6.20	calientTranConnThresholdDegraded	A Transit Connection power loss in the switch matrix has reached the degraded threshold.

OID	Name	Description
1.3.6.1.4.1.4960.2.5.2.6.21	calientTranConnThresholdCritical	A Transit Connection power loss in the switch matrix has reached the critical threshold.
1.3.6.1.4.1.4960.2.5.2.6.28	calientTranConnPowerControlAlarm	Alarm generated because of an inability to maintain the Transit Connection's output power.
1.3.6.1.4.1.4960.2.5.2.6.29	calientTranConnReceiveSignal	Alarm generated because the Transit Connection's Receive Signal is too high.

C.4 Environment MIBs

Table 11 lists the CALIENT MIB OIDs for environmental factors affecting the switch.

Table 11 – CALIENT Environment MIBs

OID	Name	Description
Traps		
1.3.6.1.4.1.4960.2.3.2.6.51	calientEnvOverTemp	The current ambient temperature of a card has exceeded the configured threshold.
1.3.6.1.4.1.4960.2.3.2.6.53	calientEnvPowerFail	One of the redundant power breakers is not functioning.
1.3.6.1.4.1.4960.2.3.2.6.55	calientEnvFanFailure	One of the fans in the fan tray has failed.
1.3.6.1.4.1.4960.2.3.2.6.57	calientEnvFanTrayFailure	Multiple fans in the fan tray have failed, and the entire fan tray is marked as failed.
1.3.6.1.4.1.4960.2.3.2.6.58	calientEnvFanTrayOK	The fan tray has resumed normal operation.
1.3.6.1.4.1.4960.2.3.2.6.61	calientCardDiskOverUtilized	One or more disks on the card are over-utilized; utilization is above the major threshold.
1.3.6.1.4.1.4960.2.3.2.6.62	calientCardDiskUtilNormal	The disk space on the card is normal.
1.3.6.1.4.1.4960.2.3.2.6.63	calientCardMemOverUtilized	Card memory is over-utilized; utilization is above the major threshold.

OID	Name	Description
1.3.6.1.4.1.4960.2.3.2.6.65	calientCardCpuOverUtilized	The card CPU is over-utilized; utilization is above the major threshold.
1.3.6.1.4.1.4960.2.3.2.6.67	calientCardBusFailure	The shelf supervisory bus has failed; error counts exceed the major threshold.
1.3.6.1.4.1.4960.2.3.2.6.69	calientCardIntCommFailure	Internal communication is degrading; number of transmit packets dropped exceeds the major threshold.
1.3.6.1.4.1.4960.2.3.2.6.71	calientUpgradeFailedAlarm	Upgrade Failed alarm.
1.3.6.1.4.1.4960.2.3.2.6.72	calientSystemRestartedAlarm	Calient System Restarted alarm.
1.3.6.1.4.1.4960.2.3.2.6.73	calientLanThresholdExceededAlarm	LAN Threshold Exceeded alarm.
1.3.6.1.4.1.4960.2.3.2.6.74	calientADCBusErrorAlarm	ADC Bus Error alarm.
1.3.6.1.4.1.4960.2.3.2.6.75	calientLinkADownAlarm	Link A Down alarm.
1.3.6.1.4.1.4960.2.3.2.6.76	calientLinkBDownAlarm	Link B Down alarm.
1.3.6.1.4.1.4960.2.3.2.6.77	calientPowerFeedBAlarm	Power Feed Unit B has failed.
1.3.6.1.4.1.4960.2.3.2.6.78	calientPowerFeedAAlarm	Power Feed Unit A has failed.
1.3.6.1.4.1.4960.2.3.2.6.79	calientFanAccessAlarm	Fan Control Unit Access has failed.
1.3.6.1.4.1.4960.2.3.2.6.80	calientTempAccessAlarm	Temperature Sensor Unit Access has failed.
1.3.6.1.4.1.4960.2.3.2.6.81	calientSWUIBoardAccessAlarm	Switch UI Board Access has failed.

C.5 FTP Configuration MIBs

Table 12 lists the CALIENT MIB OIDs for configuring FTP on the switch.

Table 12 – CALIENT FTP Configuration MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.11.1.1.1	calientFtpHostAddress	IP address of the FTP server onto which the configuration will be uploaded.
1.3.6.1.4.1.4960.2.11.1.1.2	calientFtpUserName	FTP server User Name.
1.3.6.1.4.1.4960.2.11.1.1.3	calientFtpUserPass	FTP server User Password.
1.3.6.1.4.1.4960.2.11.1.1.4	calientFtpBackupDirPAth	FTP server Node Backup Directory Path.

C.6 NTP Server Configuration MIBs

Table 13 lists the CALIENT MIB OIDs for configuring NTP on the switch.

Table 13 – CALIENT NTP Configuration MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.12.1.1	calientNTPServiceStatus	The NTP Service Enable or Disable.
1.3.6.1.4.1.4960.2.12.1.2	calientNtpServerAddress	The NTP Server IP Address.

C.7 Port MIBs

Table 14 lists the CALIENT MIB OIDs for configuring ports on the switch.

Table 14 – CALIENT Port MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.6.1.1.1	calientPortCount	The number of ports installed in this OCS.
1.3.6.1.4.1.4960.2.6.1.1.2	calientFailedPortCount	The current number of ports with an operational status of OOS and an operation capability of failed.
Table Objects – calientPortTable		
1.3.6.1.4.1.4960.2.6.1.1.3.1.1	calientPortShelfNum	The shelf number where the port is located.
1.3.6.1.4.1.4960.2.6.1.1.3.1.2	calientPortSlotNum	The slot number of the card where the port is located.
1.3.6.1.4.1.4960.2.6.1.1.3.1.3	calientPortPosition	The position of the card where the port is located.
1.3.6.1.4.1.4960.2.6.1.1.3.1.4	calientPortNum	The physical number of the port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.5	calientPortType	The type of port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.6	calientPortId	The administratively assigned name of the port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.7	calientInPortOperStatus	The current operational status of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.8	calientInPortAdminStatus	The current administrative status of the input port.

OID	Name	Description
1.3.6.1.4.1.4960.2.6.1.1.3.1.9	calientInPortCapStatus	The current operating capability status of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.10	calientInPortRedStatus	The current redundancy status of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.11	calientInPortProtStatus	The current protection status of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.12	calientInPortAlarmState	The current alarm state of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.13	calientOutPortOperStatus	The current operational status of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.14	calientOutPortAdminStatus	The current administrative status of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.15	calientOutPortCapStatus	The current operating capability status of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.16	calientOutPortRedStatus	The current redundancy status of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.17	calientOutPortProtStatus	The current protection status of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.18	calientOutPortAlarmState	The current alarm state of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.19	calientPortDescr	A text description of the port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.20	calientPortDiagMessage	A description of the last diagnostic results.
1.3.6.1.4.1.4960.2.6.1.1.3.1.21	calientInPortOwner	The owner of the input port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.22	calientOutPortOwner	The owner of the output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.23	calientPortGroupName	The name of the port group to which this port belongs.
1.3.6.1.4.1.4960.2.6.1.1.3.1.24	calientPortAlias	The alias used to identify the port; the alias may contain alphanumeric characters.
1.3.6.1.4.1.4960.2.6.1.1.3.1.25	calientPortInPower	The input power of the port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.26	calientPortConnections	The connection identifiers for the connections in which the port acts as an input port or output port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.27	calientPortInOptPower	The input optical power of the port.
1.3.6.1.4.1.4960.2.6.1.1.3.1.28	calientPortOutOptPower	The output optical power of the port.

C.8 Port Group MIBs

Table 15 lists the CALIENT MIB OIDs for configuring port groups on the switch.

Table 15 – CALIENT Port Group MIBs

OID	Name	Description
Table Objects – calientPortGroupTable		
1.3.6.1.4.1.4960.2.10.1.1.1.1	calientPortGroupName	The name of the port group.
1.3.6.1.4.1.4960.2.10.1.1.1.2	calientGroupPortIndex	The port group index uniquely identifying the port group.
1.3.6.1.4.1.4960.2.10.1.1.1.3	calientPortGroupMemberPorts	The member ports belonging to this port group. It has the format <portID1>,<portID2>...<portIDn>.
1.3.6.1.4.1.4960.2.10.1.1.1.4	calientPortOwner	The owner of this port group.
1.3.6.1.4.1.4960.2.10.1.1.1.5	calientPortType	The port group type.
1.3.6.1.4.1.4960.2.10.1.1.1.6	calientGroupPortCount	The number of member ports belonging to this group.
1.3.6.1.4.1.4960.2.10.1.1.1.7	calientPortGroupRowStatus	The Calient Port Group Table Row Status for creating and deleting a row.
Traps		
1.3.6.1.4.1.4960.2.10.2.6.1	calientPortGroupInputSignalDegraded	Input signal power of the Port Group is below degrade threshold.
1.3.6.1.4.1.4960.2.10.2.6.2	calientPortGroupInputSignalCritical	Input signal power of the Port Group is below critical threshold.
1.3.6.1.4.1.4960.2.10.2.6.3	calientPortGroupInputSignalHigh	Input signal power of the Port Group is above high threshold.
1.3.6.1.4.1.4960.2.10.2.6.4	calientPortGroupOutputSignalDegrade	Output signal power of the Port Group is below degrade threshold.
1.3.6.1.4.1.4960.2.10.2.6.5	calientPortGroupOutputSignalCritical	Output signal power of the Port Group is below critical threshold.

C.9 Security MIBs

Table 16 lists the CALIENT MIB OIDs for configuring security on the switch.

Table 16 – CALIENT Security MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.7.1.1.1	calientLoginName	The user login name.
1.3.6.1.4.1.4960.2.7.1.1.2	calientLoginService	The service through which a user can log into system.
1.3.6.1.4.1.4960.2.7.1.1.3	calientSecurityNotice	Indicates whether or not a user who has logged in should receive a security notice.
1.3.6.1.4.1.4960.2.7.1.1.4	calientSecPassAging	The maximum number of days the user password is valid.
1.3.6.1.4.1.4960.2.7.1.1.5	calientSecUsageInactivity	The max timeout for automatic lockout for the duration in which there is no usage activity in minutes.
Traps		
1.3.6.1.4.1.4960.2.7.2.6.1	calientSecurityLoginOK	An authorized user has logged into the system.
1.3.6.1.4.1.4960.2.7.2.6.2	calientSecurityLoginFailure	An unauthorized user attempted to log in to the system.
1.3.6.1.4.1.4960.2.7.2.6.3	calientSecurityLogoff	A user has logged out of the system.
1.3.6.1.4.1.4960.2.7.2.6.4	calientSecurityUserAdded	A user profile has been added to system.
1.3.6.1.4.1.4960.2.7.2.6.5	calientSecurityUserDeleted	A user profile has been deleted from system.

C.10 Service MIBs

Table 17 lists the CALIENT MIB OIDs for configuring service on the switch.

Table 17 – CALIENT Service MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.13.1.1	calientWebServiceStatus	The Web Service Enable or Disable.
1.3.6.1.4.1.4960.2.13.1.2	calientTL1ServiceStatus	The TL1 Service Enable or Disable.
1.3.6.1.4.1.4960.2.13.1.3	calientSNMPServiceStatus	The SNMP Service Enable or Disable.
1.3.6.1.4.1.4960.2.13.1.4	calientNBCORBAServiceStatus	The NB CORBA Service Enable or Disable.

C.11 Session Management MIBs

Table 18 lists the CALIENT MIB OIDs for configuring session management on the switch.

Table 18 – CALIENT Session Management MIBs

OID	Name	Description
Scalar Objects		
1.3.6.1.4.1.4960.2.15.1.2.2	calientSessionTimeout	The Session Timeout value in mins.
Table Objects – calientSessionMngConfTable		
1.3.6.1.4.1.4960.2.15.1.2.1.1	calientSessionID	This object uniquely identifies a user session.
1.3.6.1.4.1.4960.2.15.1.2.1.2	calientSessUserName	The User Name of the session.
1.3.6.1.4.1.4960.2.15.1.2.1.3	calientSessUserRole	The role of the user. The user can be an Administrator or Provisioner, a Field User, a user allowed to perform Install-Maintenance, or a user with Read-Only access.
1.3.6.1.4.1.4960.2.15.1.2.1.4	calientNodeIPAddress	The IP Address of the node on which the session is running.
1.3.6.1.4.1.4960.2.15.1.2.1.5	calientSessionUserServiceType	The Service Type configured for the user.
1.3.6.1.4.1.4960.2.15.1.2.1.6	calientUserLoginTime	The time at which the user has logged in; the time format is dd/mm/yy HH:MM:SS.
1.3.6.1.4.1.4960.2.15.1.1.1.7	calientTerminateSess	This object enables an admin user to terminate a session.

C.12 Software Management MIBs

Table 19 lists the CALIENT MIB OIDs for configuring software management on the switch.

Table 19 – CALIENT Software Management MIBs

OID	Name	Description
Table Objects – calientSWMngConfTable		
1.3.6.1.4.1.4960.2.14.1.1.1.1	calientSwEntryIndex	The unique index that identifies the software management entry.
1.3.6.1.4.1.4960.2.14.1.1.1.2	calientSlotNo	The position of the card on which the software module is running. The format for this object is <shelfNum>.<slotNum>.
1.3.6.1.4.1.4960.2.14.1.1.1.3	calientSWType	The general type of the software running on the card: • cp – Control Processor Module • wam – Watchdog Processor and Alarm Module • lic – LAN Interface Card • iosc – I/O Shelf Controllers • ooo – All Optical I/O card • oeo – Optical-Electrical-Optical I/O card • adc – A/D Converter bus PCB • sm – Switch Matrix Module • np – Network Processor Module
1.3.6.1.4.1.4960.2.14.1.1.1.4	calientSWVer	The software version running on the card.

C.13 User Management MIBs

Table 20 lists the CALIENT MIB OIDs for configuring user management on the switch.

Table 20 – CALIENT User Management MIBs

OID	Name	Description
Table Objects – calientUserMngConfTable		
1.3.6.1.4.1.4960.2.17.1.2.1.1	calientUserName	The login user name.
1.3.6.1.4.1.4960.2.17.1.2.1.2	calientUserIndex	The index of the user table.
1.3.6.1.4.1.4960.2.17.1.2.1.3	calientUserRole	The role of the user. The user can be an Administrator or Provisioner, a Field User, a user allowed to perform Install-Maintenance, or a user with Read-Only access.
1.3.6.1.4.1.4960.2.17.1.2.1.4	calientUserPass	The password for this user.
1.3.6.1.4.1.4960.2.17.1.2.1.5	calientUserTL1Access	This object indicates whether or not the user is allowed to access the device using TL1.
1.3.6.1.4.1.4960.2.17.1.2.1.6	calientUserWebAccess	This object indicates whether or not the user is allowed to access the device using the Web.
1.3.6.1.4.1.4960.2.17.1.2.1.7	calientUserMultiSessAllow	This object indicates whether or not the user is allowed multiple sessions.
1.3.6.1.4.1.4960.2.17.1.2.1.8	calientUserAssocPortGrp	The port groups associated with the user. This is a list of comma-separated port group names. For example: <PortGrpName1>, <PortGrpName2>.
1.3.6.1.4.1.4960.2.17.1.1.1.9	calientUserStatus	This object indicates whether the user is enabled or disabled.
1.3.6.1.4.1.4960.2.17.1.1.1.10	calientUserMgmtRowStatus	The Calient User Management Table Row Status for creation/deletion of a row.