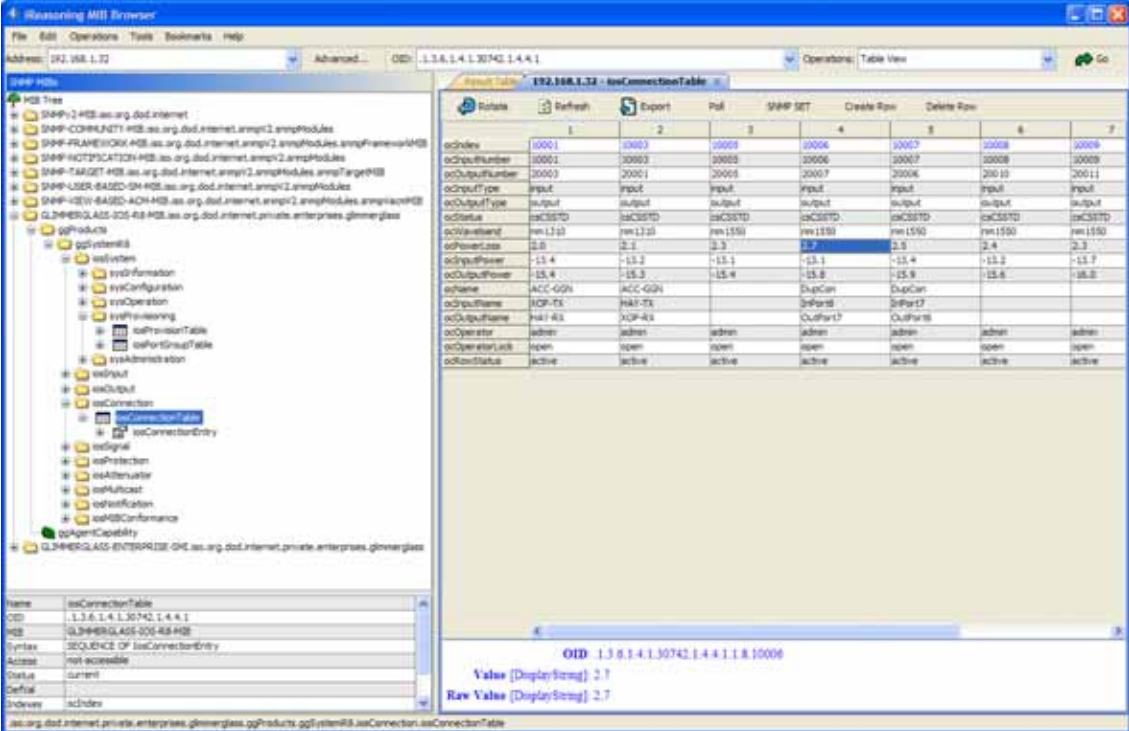


# Intelligent Optical Systems SNMP User Manual

Product Release 8.0  
Part Number 901-0105  
Revision A



1	2	3	4	5	6	7
oidIndex	10001	10002	10003	10004	10005	10006
oidOutputNumber	10001	10002	10003	10004	10005	10006
oidOutputType	input	input	input	input	input	input
oidStatus	input	input	input	input	input	input
oidWaveband	nm 1310	nm 1310	nm 1550	nm 1550	nm 1550	nm 1550
oidPowerLoss	-13.4	-13.2	-13.1	-13.1	-13.4	-13.2
oidOutputPower	-15.4	-15.3	-15.4	-15.8	-15.8	-15.8
oidName	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH
oidOutputName	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH	ACC-GGH
oidOperator	admin	admin	admin	admin	admin	admin
oidOperatorLock	open	open	open	open	open	open
oidConnStatus	active	active	active	active	active	active

Last updated: July 8, 2013

The Glimmerglass Intelligent Optical Systems are non-blocking photonic cross-connects that support configuration, operation, and monitoring via web browser, SNMP, and TL1 interfaces.

The Glimmerglass Intelligent Optical Switch System SNMP Agent supports alarm reporting to SNMP-based Network Management Systems and uses SNMP v3, v2c, and v1 security models.

# Release Notice

Glimmerglass has released the SNMP feature in the following Glimmerglass products and associated user documentation:

Software Release Date	Glimmerglass Intelligent Optical Systems Product Software Release Number	Most Recent Document Version
July 2013	R08.00p000	A

***Author and Copy Requests:***

Glimmerglass Networks, Inc.  
26142 Eden Landing Road  
Hayward, CA 94545  
Tel +1 510 723 1900  
Fax +1 510 780 9851

# Contents

## Introduction

Glimmerglass Intelligent Optical System SNMP Agent.....	1
Document Overview .....	2
IOS Installation and Operation Documents .....	3

## IOS SNMP Agent Access

Overview .....	5
SNMP Management Information Bases (MIBs) .....	6
Installation Default Access .....	7
IOS SNMP Engine ID .....	8
SNMP v3 Access .....	9
SNMP v3 User-based Security Module (USM) User Table .....	10
SNMP v3 View-based Access Control Model (VACM) Tables .....	10
SNMP v3 User Management .....	13
Change an SNMP v3 Authentication/Privacy Password .....	13
Add an SNMP v3 User .....	14
Delete/Disable an SNMP v3 User—Security Name .....	14
Delete/Disable an SNMP v3 User—Security Group .....	15
SNMP v1/v2c Access .....	15
Change the Default SNMP v1/v2c Community Names via ClickFlow/TL1 .....	17
Change an SNMP v1/v2c Community Name .....	18
Add an SNMP v1/v2c Community Name .....	19
Disable SNMP v1/v2c Write Access .....	19
Disable SNMP v1/v2c Access .....	20
Restrict SNMP v1/v2c Access to an SNMP Manager IP Address .....	21

## IOS SNMP Traps

Overview .....	23
IOS SNMP Traps .....	23
IOS SNMP Trap Example—iosComponentStateTrap .....	24
IOS SNMP Trap Example—iosInputSignalTrap .....	25
IOS SNMP Trap Example—iosOutputSignalTrap .....	27
IOS SNMP Trap Example—iosConnectionStateTrap .....	29
IOS System Administration Trap Example—iosSystemAdminTrap .....	32
Configure the SNMP Target Address Table .....	33

SNMP Target Address Format .....	34
Adding/Deleting an SNMP v2c Target Address via ClickFlow/TL1.....	34
Revising an SNMP Target Address .....	35
Adding an SNMP Target Address .....	36
Deleting an SNMP Target Address .....	36

## IOS SNMP MIB

Overview .....	39
System Information—sysInformation .....	42
System Configuration—sysConfiguration .....	45
System Operation Options—sysOperation .....	47
System Provisioning Table—iosProvisionTable.....	48
System Provisioning Port List Formats.....	53
Making Multiple Connections.....	54
Making All Connections .....	55
Breaking Multiple Connections .....	56
Breaking All Connections .....	57
Naming Multiple Connections.....	58
Backing Up the System Configuration .....	59
Restoring the System Configuration.....	60
Saving the System Configuration .....	62
Upgrading System Software .....	63
Rolling Back System Software .....	66
Rebooting/Shutting Down/Restarting System .....	68
Resetting System Configuration to Factory Defaults .....	69
Assigning a Port Group to a list of Ports.....	70
Assigning a Signal Threshold to a List of Ports .....	71
Assigning a Waveband to a List of Ports.....	72
Assigning an Alarm Severity to a List of Ports.....	73
Reissuing a Prior Operation .....	75
Port Grouping - iosPortGroupTable .....	75
Adding a Port Group .....	77
Revising an Existing Port Group.....	77
Deleting an Existing Port Group .....	78
System Clock - sysClock.....	78
System Network - sysNetwork .....	80
System Log (SYSLOG) - sysLog .....	83
Changing the Syslog Notification Level .....	84
Adding a Syslog Server .....	84
Deleting a Syslog Server .....	85
System Alarm—sysAlarm .....	85
Security Tables—ClickFlow/TL1 Users.....	86
ClickFlow/TL1 User “snmpuser” .....	86
ClickFlow/TL1 Port Privileges—Virtual Private Switch .....	87
SNMP Port Privileges—VACM .....	87

---

Input Port Table—iosInputPortTable.....	87
Configuring an Input Port.....	90
Output Port Table—iosOutputPortTable .....	91
Configuring an Output Port.....	93
Connection Table—iosConnectionTable .....	94
Viewing Connections.....	97
Making a New Connection.....	97
Revising an Existing Connection .....	97
Breaking an Existing Connection.....	98
Signal Threshold Table—iosSigThresholdTable .....	98
Viewing Signal Thresholds .....	100
Creating a New Signal Threshold.....	101
Revising an Existing Signal Threshold .....	101
Deleting an Existing Signal Threshold.....	102
Protection Rule Table—iosProtectionRuleTable .....	102
Viewing Protection Rules.....	105
Creating a New Protection Rule .....	105
Deleting an Existing Protection Rule .....	106
Attenuator (VOA) Tables.....	106
VOA Unit Table—VOA Operation Configuration .....	107
Configuring a VOA (Power/Attenuation).....	108
VOA Port Table—VOA Port Configuration .....	109
Configuring a VOA Port (Name/Description) .....	111
Multicast (PMU) Tables.....	112
Multicast Unit Table—List of installed PMUs.....	112
Multicast Port Table—PMU Port Configuration .....	113
Configuring a PMU Port (Name/Description).....	116

THIS PAGE INTENTIONALLY LEFT BLANK

The Glimmerglass Intelligent Optical Systems (IOS) are non-blocking photonic cross-connects that support configuration, operation, and monitoring via web browser, SNMP, and TL1 interfaces. This manual describes access to the Glimmerglass IOS SNMP Agent which supports the SNMP v3, v2c, and v1 security models.

## Glimmerglass Intelligent Optical System SNMP Agent

The embedded Glimmerglass IOS SNMP Agent supports configuration, operation, and monitoring of the Glimmerglass IOS by SNMP Management Information Base (MIB) Browsers and by NMS SNMP Managers, such as HP OpenView.

Some features of the Glimmerglass IOS SNMP Agent are described below:

- **User interface parity**—The majority of the IOS features that are configurable via the ClickFlow web browser graphical interface and the TL1 textual interface are also configurable via SNMP.
- **SNMP v3 security/access**—The IOS SNMP Agent complies with the SNMP v3 User-based Security Module (USM) and the SNMP v3 View-based Access Control Model (VACM). SNMP access privileges are configured solely via the SNMP USM and VACM MIB tables.
  - USM supports configuration of user/security names, passwords, user authentication protocol (none, MD5, and SHA), and payload privacy protocol/encryption (none or DES).
  - VACM supports configuration of what may be viewed (read), modified (write), or in a trap payload (notification).
- **SNMP v1 and v2c access**—Under the control of the SNMP v3 USM/VACM MIBs, the SNMP Agent's access is extended to the SNMP v1 and v2c security models via the COMMUNITY MIB. SNMP v1/v2c security is limited: authentication consists of an unencrypted user/community name; the SNMP payload is unencrypted. The COMMUNITY MIB supports restricting SNMP v1/v2c access by IP address. If the traffic between the SNMP Manager and IOS SNMP Agent passes over a non-secure net-

work, or the IOS SNMP Agent can be reached from a non-secure network, it is recommended that SNMP v1 and v2c access be disabled or restricted by IP address.

- **SNMP access logging**—Configuration changes are logged to the TL1 autonomous message log and the syslog. The log entry includes the SNMP user name.
- **Disable SNMP access**—SNMP access may be totally disabled via ClickFlow System Startup Options or the Maintenance Console by setting the SNMP port (snmpPort) to 0 and then restarting/rebooting the IOS application.
- **SNMP traps**—The SNMP Agent may be configured to send traps (optical power threshold crossing alarms, etc.) to multiple SNMP Managers (trap targets) via the v1, v2c, or v3 security models. Trap events are logged to the TL1 autonomous message log and the syslog.
- **ClickFlow GUI (web browser) and TL1 access**—There is no correlation between SNMP v3 users (usmUserName) and ClickFlow/TL1 users; adding an SNMP usmUserName does not add a ClickFlow/TL1 user and vice-versa. For a description of ClickFlow/TL1 user management see the IOS *ClickFlow Graphical User Interface Manual*. The IOS SNMP Agent does not support configuration of ClickFlow/TL1 users and their privileges via SNMP.
- **Limited SNMP v2c configuration via ClickFlow/TL1**—For quick-start operation using the SNMP v2c model, the ClickFlow and TL1 interfaces support the following:
  - Revision of the installation default read and read/write community names
  - Configuring one or more SNMP trap destination addresses

## Document Overview

The *Glimmerglass SNMP User Manual* describes configuration, operation, and monitoring of Glimmerglass Intelligent Optical Systems via SNMP (v3, v2c, and v1).

This manual contains the following chapters:

Chapter	Description
Chapter 1: Introduction	Introduces the IOS SNMP Agent, this document, and other Glimmerglass IOS user manuals.
Chapter 2: IOS SNMP Agent Access	Describes initial access to the IOS SNMP Agent via SNMP v1/v2c/v3 and initial revision of community/user names and passwords.
Chapter 3: IOS SNMP Traps	Describes the IOS SNMP traps and configuration of the SNMP trap target table (SNMP Manager IP addresses).



Chapter	Description
Chapter 4: IOS SNMP MIB	Describes the IOS SNMP Management Information Base (MIB).

## IOS Installation and Operation Documents

The following documents describe installation of Glimmerglass Intelligent Optical Systems and the configuration, operation and monitoring of the IOS via its web browser, TL1 and SNMP interfaces:

Document Name	Document Part Number	Description
<i>IOS System Installation and Maintenance Guide</i>	901-0101	Describes Intelligent Optical Systems features, installation, system configuration, and maintenance.
<i>IOS ClickFlow Graphical User Interface Manual</i>	901-0102	Describes configuration, operation, and monitoring of the IOS via a web browser GUI.
<i>IOS Transaction Language 1 (TL1) User Manual</i>	901-0103	Describes textual configuration, operation, and monitoring of the IOS via TL1, a management protocol defined in Bellcore GR-831-CORE.
<i>IOS TL1 Quick Reference Guide</i>	901-0104	Examples of commonly-used TL1 commands used to administer and provision Glimmerglass Intelligent Optical Systems.
<i>IOS SNMP User Manual</i>	901-0105	(This document) Describes configuration, operation, and monitoring of the IOS via SNMP (v3, v2c, and v1).

THIS PAGE INTENTIONALLY LEFT BLANK

## Overview

This section describes access to the IOS SNMP Agent from an SNMP Manager (an SNMP NMS or an SNMP MIB Browser). The following are the possible levels of access to the IOS SNMP Agent:

- **Disable SNMP Access**—SNMP access may be totally disabled via ClickFlow or the Maintenance Console by setting the SNMP port (snmpPort) to 0 and then restarting/rebooting the IOS application:
  - For ClickFlow: **System > System Configuration > Startup Options**, set snmpPort to 0, then **System Maintenance > Restart**.
  - For Maintenance Console: **Configure start-up options**, set snmpPort to 0, then **Restart** (see the *Glimmerglass IOS System Installation and Maintenance Guide*).
- **SNMP v3 security/access**—The IOS SNMP Agent complies with the SNMP v3 User-based Security Module (USM) and the SNMP v3 View-based Access Control Model (VACM). SNMP access privileges are configured solely via the SNMP USM and VACM MIB tables.
  - USM supports configuration of user/security names, passwords, user authentication protocol (none, MD5, and SHA), and payload privacy protocol/encryption (none or DES).
  - VACM supports configuration of what may be viewed (read), modified (write), or in a trap payload (notification).
- **SNMP v1 and v2c access**—Under the control of the SNMP v3 USM/VACM MIBs, the SNMP Agent's access is extended to the SNMP v1 and v2c security models via the COMMUNITY MIB. SNMP v1/v2c security is limited: authentication consists of an unencrypted user/community name; the SNMP payload is unencrypted. The COMMUNITY MIB supports restricting SNMP v1/v2c access by IP address. If the traffic between the SNMP Manager and IOS SNMP Agent passes over a non-secure network, or the IOS SNMP Agent can be reached from a non-secure network, it is recommended that SNMP v1 and v2c access be disabled or restricted by IP address.
- **Factory default access tables**—Initial SNMP access is enabled via installation default USM, VACM, and COMMUNITY MIB table entries. For security, the SNMP administrator should minimally revise the community names and passwords, and may

optionally disable/restrict SNMP v1/v2c access. The SNMP access tables may be returned to installation defaults by Maintenance Console selection **Reset SNMP to Factory Default** (see the *Glimmerglass IOS Installation and Maintenance Guide*).

The following sections further describe access to the SNMP Agent:

- "SNMP Management Information Bases (MIBs)" on page 6
- "Installation Default Access" on page 7
- "IOS SNMP Engine ID" on page 8
- "SNMP v3 Access" on page 9
- "SNMP v1/v2c Access" on page 15

## SNMP Management Information Bases (MIBs)

The following MIBs should be loaded in the SNMP Manager for interpretation of the Glimmerglass IOS traps and for MIB browser access to the SNMP MIB objects:

MIB	Standard/Proprietary	Description
SNMPv2-MIB	Standard (RFCs 1902, 1903, 1904, 3418)	The IOS supports standard objects in the systemGroup and the snmpGroup.
SNMP-COMMUNITY-MIB	Standard (RFC 2576, 3584)	Extend access to the v1 and v2c security models; configure community names; restrict access to selected SNMP Managers.
SNMP-FRAMEWORK-MIB	Standard (RFC 3411)	Management architecture MIB.
SNMP-NOTIFICATION-MIB	Standard (RFC 3413)	Configure trap security models and levels.
SNMP-TARGET-MIB	Standard (RFC 3413)	Configure trap destination addresses, using above security models and levels.
SNMP-USER-BASED-SM-MIB	Standard (RFC 3414)	Configure users, security models and levels.
SNMP-VIEW-BASED-ACM-MIB	Standard (RFC 3415)	Configure object access (none, read, write).
GLIMMERGLASS-ENTERPRISE-SMI	Proprietary	Imported by Glimmerglass product MIBs, defines the enterprise product root.

MIB	Standard/Proprietary	Description
GLIMMERGLASS-IOS-R8-MIB	Proprietary	Configure IOS objects; define traps.

**NOTE:** The above MIB files may be downloaded from the Glimmerglass Customer website; the standard MIBs are most likely loaded on the SNMP Manager by default.

## Installation Default Access

This section describes the default users, passwords, security models, authentication, and privacy protocols that are present on the IOS at installation.

Glimmerglass IOS SNMP Agent access from an SNMP Manager requires:

Parameter	Description
IOS IP Address	Configured at IOS installation
IOS SNMP Port	161 (installation default)
IOS SNMP Security Name	Community/security name (see the default security names and passwords in the table on page 7).
IOS SNMP Password(s)	For SNMP v3 access (see the default security names and passwords in the table on page 7).
IOS SNMP Engine ID	Required for SNMP v3 access, this ID is usually auto-discovered by the SNMP Manager (see "IOS SNMP Engine ID" on page 8).

**NOTE:** The IOS SNMP port (snmpPort) may be revised via ClickFlow **System > System Configuration > Startup Options** or the IOS Maintenance Console (see the *Glimmerglass IOS System Installation and Maintenance Guide*).

To enable initial SNMP access, the installation includes default access MIB table entries that establish six user security names with different security models and security protocols. The default security names and passwords are shown in the following table:

**NOTE:** The "Access to 1.3.6..." column indicates that all object identifiers (OIDs) under 1.3.6 are accessible (i.e., all SNMP objects).

Default Security Names and Passwords	Security Model	Authentication Protocol	Privacy Protocol	Access to 1.3.6...
Security Name: glimmerPublic Community Name: glimmerPublic	v1 and v2c	None	None	read, notify
Security Name: glimmerPrivate Community Name: glimmerPrivate	v1 and v2c	None	None	read, write, notify
Security Name: glimmerPublic	v3	None	None	read, notify
Security Name: glimmerAuthOnlyMD5 UserAuthKey: glimmerMD5AuthPassword	v3	MD5	None	read, write, notify
Security Name: glimmerAuthOnlySHA UserAuthKey: glimmerSHAAuthPassword	v3	SHA	None	read, write, notify
Security Name: glimmerPrivacyMD5DES UserAuthKey: glimmerMD5DESAuthPassword UserPrivKey: glimmerMD5DESPrivPassword	v3	MD5	DES	read, write, notify
Security Name: glimmerPrivacySHADES UserAuthKey: glimmerSHADESAuthPassword UserPrivKey: glimmerSHADESPrivPassword	v3	SHA	DES	read, write, notify

For security, the SNMP administrator should minimally revise the community names and passwords, and may optionally disable or restrict SNMP v1/v2c access. The SNMP access tables may be returned to installation defaults by the Maintenance Console selection **Reset SNMP to Factory Default** (see the *Glimmerglass IOS System Installation and Maintenance Guide*).

## IOS SNMP Engine ID

SNMP v3 USM uses snmpEngineID as part of the authentication process. The IOS SNMP Agent snmpEngineID is composed of an RFC compliant 5-byte header 0x8000781605 ("0x" indicates hexadecimal), followed by the 12 ASCII character IOS system serial number. For example:

IOS serial number: 04BD4PC10020  
snmpEngineID: 0x8000781605303442443450433130303230

The IOS SNMP Agent supports snmpEngineID discovery per RFC 3411. SNMP Managers will usually automatically discover the IOS snmpEngineID on the first access to the IOS, and then use that snmpEngineID as part of the authentication process for subsequent access.

## SNMP v3 Access

For SNMP v3 access, configure the SNMP Manager with the IOS IP address, IOS SNMP port, a user name, an authorization protocol value (none, MD5 or SHA), and an authorization password. In addition if a privacy protocol of DES has been specified for the user name in the usmUserTable, then configure the SNMP Manager with a privacy protocol of DES and a privacy password.

As shown in the table on page 8, the IOS installation defaults are:

- IOS IP Address: 192.168.2.200, revised at IOS installation
- IOS SNMP Port: 161, optionally revised at IOS installation

Use one of the five default SNMP v3 USM User Names, security protocols and passwords:

- USM User Name: glimmerPublic
  - Authentication Protocol: None
  - Privacy Protocol: None
- USM User Name: glimmerAuthOnlyMD5
  - Authentication Protocol and Password: MD5, glimmerMD5AuthPassword
  - Privacy Protocol: None
- USM User Name: glimmerAuthOnlySHA
  - Authentication Protocol and Password: SHA, glimmerSHAAuthPassword
  - Privacy Protocol: None
- USM User Name: glimmerPrivacyMD5DES
  - Authentication Protocol and Password: MD5, glimmerMD5DESAuthPassword
  - Privacy Protocol and Password: DES, glimmerMD5DESPrivPassword
- USM User Name: glimmerPrivacySHADES
  - Authentication Protocol and Password: SHA, glimmerSHADESAuthPassword
  - Privacy Protocol and Password: DES, glimmerSHADESPrivPassword

---

**NOTE:** The SNMP Manager should automatically discover the IOS agent's unique snmpEngineID (see "IOS SNMP Engine ID" on page 8).

---

## SNMP v3 User-based Security Module (USM) User Table

The SNMP v3 usmUserTable defines user names (usmUserName), their authentication protocol (none, MD5 or SHA), and their privacy protocol (none, DES).

Figure 1 IOS Installation Default usmUserTable

	1	2	3	4	5	6
usmUserEngineID	..x..04BD4PC10020	..x..04BD4PC10020	..x..04BD4PC10020	..x..04BD4PC10020	..x..04BD4PC10020	..x..04BD4PC10020
usmUserName	glimmerPublic	glimmerPrivate	glimmerAuthOnlyMD5	glimmerAuthOnlySHA	glimmerPrivacyMD5DES	glimmerPrivacySHADES
usmUserSecurityName	glimmerPublic	glimmerPrivate	glimmerAuthOnlyMD5	glimmerAuthOnlySHA	glimmerPrivacyMD5DES	glimmerPrivacySHADES
usmUserCloneFrom	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0
usmUserAuthProtocol	usmNoAuthProtocol	usmNoAuthProtocol	usmHMACMD5AuthProtocol	usmHMACSHAAuthProtocol	usmHMACMD5AuthProtocol	usmHMACSHAAuthProtocol
usmUserAuthKeyChange						
usmUserOwnAuthKeyChange						
usmUserPrivProtocol	usmNoPrivProtocol	usmNoPrivProtocol	usmNoPrivProtocol	usmNoPrivProtocol	usmDESPrivProtocol	usmDESPrivProtocol
usmUserPrivKeyChange						
usmUserOwnPrivKeyChange						
usmUserPublic						
usmUserStorageType	nonVolatile	nonVolatile	nonVolatile	nonVolatile	nonVolatile	nonVolatile
usmUserStatus	active	active	active	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

## SNMP v3 View-based Access Control Model (VACM) Tables

Once a user is authenticated, the four SNMP v3 VACM tables (vacmSecurityToGroupTable, vacmContextTable, vacmAccessTable, and vacmViewTreeFamilyTable) control what the user may view (read), modify (write), or receive in a trap payload (notification). Figure 2 through Figure 5 show the IOS installation default SNMP v3 VACM tables, and Figure 6 is a flow chart that shows the inputs and outputs to each of the four VACM tables.



Figure 2 IOS Installation Default vacmSecurityToGroupTable

OID: .1.3.6.1.6.3.16.1.2

Result Table 192.168.2.43 - vacmSecurityToGroupTable X

Rotate Refresh Export Poll SNMP SET Create Row

	vacmSecurityModel	vacmSecurityName	vacmGroupName	vacmSec...	vac...
1	1	glimmerPublic	SNMPv3PublicGroup	nonVolatile	active
2	1	glimmerPrivate	SNMPv3AuthOnlyGroup	nonVolatile	active
3	2	glimmerPublic	SNMPv3PublicGroup	nonVolatile	active
4	2	glimmerPrivate	SNMPv3AuthOnlyGroup	nonVolatile	active
5	3	glimmerPublic	SNMPv3PublicGroup	nonVolatile	active
6	3	glimmerAuthOnlyMD5	SNMPv3AuthOnlyGroup	nonVolatile	active
7	3	glimmerAuthOnlySHA	SNMPv3AuthOnlyGroup	nonVolatile	active
8	3	glimmerPrivacyMD5DES	SNMPv3PrivacyGroup	nonVolatile	active
9	3	glimmerPrivacySHADES	SNMPv3PrivacyGroup	nonVolatile	active

Figure 3 IOS Installation Default vacmContextTable

OID: .1.3.6.1.6.3.16.1.1

Result Table 192.168.2.43 - vacmContextTable X

Rotate Refresh Export Poll

vacmContextName	1
-----------------	---

**NOTE:** The context name is a null string; hence a context name is not required for access

Figure 4 IOS Installation Default vacmAccessTable

OID: .1.3.6.1.6.3.16.1.4 Operations: Table View Go

Result Table 192.168.2.43 - vacmAccessTable X

Rotate Refresh Export Poll SNMP SET Create Row Delete Row

	1	2	3	4	5	6	7
vacmAccessContextPrefix							
vacmAccessSecurityModel	1	2	3	3	1	2	3
vacmAccessSecurityLevel	noAuthNoPriv	noAuthNoPriv	noAuthNoPriv	authPriv	noAuthNoPriv	noAuthNoPriv	authNoPriv
vacmAccessContextMatch	exact	exact	exact	exact	exact	exact	exact
vacmAccessReadViewName	SNMPv3PublicReadScope	SNMPv3PublicReadScope	SNMPv3PublicReadScope	SNMPv3AuthReadScope	SNMPv3AuthReadScope	SNMPv3AuthReadScope	SNMPv3AuthReadScope
vacmAccessWriteViewName				SNMPv3AuthWriteScope	SNMPv3AuthWriteScope	SNMPv3AuthWriteScope	SNMPv3AuthWriteScope
vacmAccessNotifyViewName	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope	SNMPv3AuthNotifyScope
vacmAccessStorageType	nonVolatile	nonVolatile	nonVolatile	nonVolatile	nonVolatile	nonVolatile	nonVolatile
vacmAccessStatus	active	active	active	active	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

Figure 5 IOS Installation Default vacmViewTreeFamilyTable

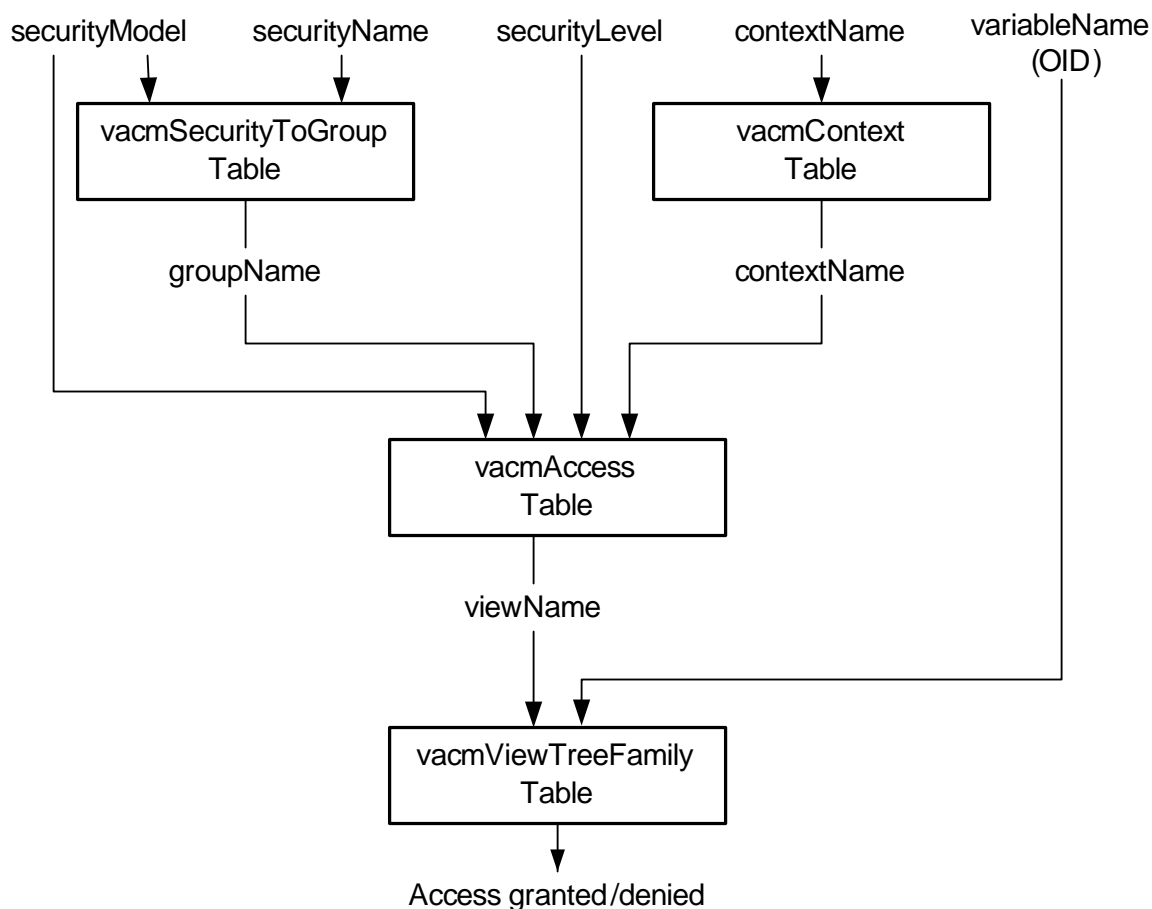
OID: .1.3.6.1.6.3.16.1.5.2 Operations: Table View

Result Table 192.168.2.43 - vacmViewTreeFamilyTable

	1	2	3	4
vacmViewTreeFamilyViewName	SNMPv3AuthReadScope	SNMPv3AuthWriteScope	SNMPv3AuthNotifyScope	SNMPv3PublicReadScope
vacmViewTreeFamilySubtree	3.1.3.6	3.1.3.6	3.1.3.6	3.1.3.6
vacmViewTreeFamilyMask				
vacmViewTreeFamilyType	included	included	included	included
vacmViewTreeFamilyStorageType	nonVolatile	nonVolatile	nonVolatile	nonVolatile
vacmViewTreeFamilyStatus	active	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

Figure 6 SNMP v3 View-based Access Control Model (VACM)



## SNMP v3 User Management

The usmUserTable (Figure 1 on page 10) cannot be directly modified via normal MIB Browser table operations, hence SNMP v3 Managers and MIB Browsers usually provide a Manage SNMPv3 Users facility which typically includes:

- Change a User Password
- Disable/Enable a User
- Create (Clone) a User
- Delete a User

A usmUserTable row cannot be directly added; an existing row must be cloned and then modified. When a new user security name has been added, it will have no access privileges until a corresponding vacmSecurityToGroupTable row has been added. If the vacmSecurityToGroupTable row specifies a new vacmGroupName then one or more corresponding vacmAccessTable rows must be added. Similarly if the new vacmAccessTable rows specify new viewNames, then one or more corresponding vacmViewTreeFamilyTable rows must be added.

The following sections provide simple procedure outlines for revising the SNMP v3 user access:

- "Change an SNMP v3 Authentication/Privacy Password" (below)
- "Add an SNMP v3 User" on page 14
- "Delete/Disable an SNMP v3 User—Security Name" on page 14
- "Delete/Disable an SNMP v3 User—Security Group" on page 15

---

**NOTE:** The procedures are only outlines, as the specific procedures vary by SNMP Manager or MIB Browser.

---

### Change an SNMP v3 Authentication/Privacy Password

SNMP v3 USM provides a secure user authentication, however it isn't secure if the IOS installation default authentication passwords are not changed from those openly published in the table on page 8.

Per "SNMP v3 User Management" on page 13, changing a user password requires use of the SNMP Manager's Manage SNMPv3 Users facility, for example:

1. Select the SNMP Manager's User Management facility.
2. Specify access to the IOS via one of the four authenticated users listed on page 9.

3. Select one of the other users and change the password.
4. Verify IOS SNMP access under the modified user's password.
5. Repeat until all four users are changed.

## Add an SNMP v3 User

As described in "SNMP v3 User Management" on page 13, adding a new SNMP v3 user requires use of the SNMP Manager's Manage SNMPv3 Users facility, for example:

1. Select the SNMP Manager's User Management facility.
2. Specify access to the IOS via an existing user (for example one of the four authenticated users listed on page 9).
3. Select a user security name to be cloned.
4. Specify the new user security name.
5. Modify the cloned user as desired. For example, create a new password.
6. Enable the new user.

---

**NOTE:** A maximum of 30 USM user names (usmUserTable rows) are supported.

---

When a new user security name has been added, it will have no access privileges until a corresponding vacmSecurityToGroupTable row has been added. If the vacmSecurityToGroupTable row specifies a new vacmGroupName then one or more corresponding vacmAccessTable rows must be added. Similarly, if the new vacmAccessTable rows specify new viewNames then one or more corresponding vacmViewTreeFamilyTable rows must be added.

## Delete/Disable an SNMP v3 User—Security Name

Per "SNMP v3 User Management" on page 13, deleting or disabling an SNMP v3 user requires use of the SNMP Manager's Manage SNMPv3 Users facility, for example:

1. Select the SNMP Manager's User Management facility.

2. Specify access to the IOS via an existing user (for example one of the four authenticated users listed on page 9).
3. Select a different user security name to be deleted/disabled.
4. Confirm the operation.

---

**NOTE:** A user can also be disabled by disabling/deleting the user's row(s) in the vacmSecurityToGroupTable (see "Delete/Disable an SNMP v3 User—Security Group" on page 15).

---

### Delete/Disable an SNMP v3 User—Security Group

An SNMP user may be disabled by disabling or deleting the user's row(s) in the VACM Security to Group Table (see Figure 2 on page 11). This table is indexed by both the SNMP Security Model and the Security Name.

For example, to disable or delete unauthenticated SNMP v3 access via the security name glimmerPublic:

1. Using SNMP v3 access, browse to and view the vacmSecurityToGroupTable:  
snmpModules > snmpVacmMIB > vacmSecurityToGroupTable
2. For the row whose Security Model value is 3 and whose Security Name value is glimmerPublic, set the row's vacmSecurityToGroupStatus to one of the following:
  - notInService(2)—To disable the row; this may subsequently be reversed by changing the row status back to active(1)
  - destroy(6)—To delete the row

### SNMP v1/v2c Access

For SNMP v1/v2c access, configure the SNMP Manager with the IOS IP address, IOS SNMP port, read community name, and write community name.

As shown in the table on page 8, the IOS installation defaults are:

- IOS IP Address 192.168.2.200, revised at IOS installation
- IOS SNMP Port 161, optionally revised at IOS installation

- Read community name      glimmerPublic (read-only) or glimmerPrivate (read/write)
- Write community name      glimmerPrivate

Under the control of the SNMP v3 USM/VACM MIBs, the SNMP Agent's access is extended to the SNMP v1 and v2c security models via the COMMUNITY MIB. SNMP v1/v2c security is limited: authentication consists of an unencrypted user/community name and the SNMP payload is unencrypted.

Figure 7      IOS Installation Default snmpCommunityTable

	1	2
snmpCommunityIndex	glimmerPrivate	glimmerPublic
snmpCommunityName	glimmerPrivate	glimmerPublic
snmpCommunitySecurityName	glimmerPrivate	glimmerPublic
snmpCommunityContextEngineID	0x80 00 78 16 05 30 34 42 44 34 50 43 31 30 30 32 30	0x80 00 78 16 05 30 34 42 44 34 50 43 31 30 30 32 30
snmpCommunityContextName		
snmpCommunityTransportTag		
snmpCommunityStorageType	nonVolatile	nonVolatile
snmpCommunityStatus	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The snmpCommunityTable supports multiple community names (opposed to supporting only two community names). The privileges of each community name are specified in the row's Security Name and optional Transport Tag. In the IOS installation default snmpCommunityTable, the snmpCommunityIndex (unique table row name) and the snmpCommunityName have been set to the row's snmpCommunitySecurityName; this is for simplicity, but they do not have to be the same. The snmpCommunityName entry defines the community name, and its privileges are established through the security name specified in corresponding snmpCommunitySecurityName entry. The security name must correspond to a usmUserSecurityName entry in the usmUserTable. The snmpCommunityTransportTag entry may optionally be used as a link to the snmpTargetAddressTable and restrict access to a one or more SNMP Manager IP addresses or their IP subnets.

The following sections provide some simple examples of revising the SNMP v1/v2c access configuration:

- "Change the Default SNMP v1/v2c Community Names via ClickFlow/TL1" on page 17
- "Change an SNMP v1/v2c Community Name" on page 18
- "Add an SNMP v1/v2c Community Name" on page 19

- "Disable SNMP v1/v2c Write Access" on page 19
- "Disable SNMP v1/v2c Access" on page 20
- "Restrict SNMP v1/v2c Access to an SNMP Manager IP Address" on page 21

---

**NOTE:** Since SNMP v1/v2c access is under the auspices of SNMP v3 USM security names and their associated VACM tables, it is possible to create new security names and restrict access by OID trees. For example, exclude access to user management (USM, VACM).

---

## Change the Default SNMP v1/v2c Community Names via ClickFlow/TL1

The IOS installation default snmpCommunityTable (Figure 7 on page 16) defines the community name "glimmerPrivate" (with read/write access) and "glimmerPublic" (with read-only access). The ClickFlow and TL1 interfaces support revision of the two installation default community name rows, such as:

- Displaying the current community names
- Revision of a row's community name
- Deletion of a row, thereby disabling access via that community name
- Recreation of a row, thereby restoring access via that community name

To display the community names in the glimmerPublic and glimmerPrivate rows, use the following TL1 command:

```
rtrv-snmp-community:::<ctag>;
```

To change the community names, use the following TL1 command:

```
set-snmp-community:::<ctag>::READ=<read>,WRITE=<write>;
```

To delete the glimmerPrivate row and hence disable write access via v1/v2c, use the following TL1 command:

```
dlt-snmp-community:::<ctag>::WRITE=glimmerPrivate;
```

To restore the deleted glimmerPrivate row and hence write access via v1/v2c, use the following TL1 command:

```
set-snmp-community:::<ctag>::WRITE=glimmerPrivate;
```

In the above TL1 commands:

Parameter	Description	Example Input
<ctag>	Arbitrary correlation tag	1
<read>	New read-only community name	public
<write>	New read/write community name	private

**NOTE:** For further information, please see the *IOS ClickFlow Graphical User Interface Manual*, and/or the *IOS Transaction Language 1 (TL1) User Manual*.

## Change an SNMP v1/v2c Community Name

The IOS installation default snmpCommunityTable (Figure 7 on page 16) defines the community names “glimmerPrivate” (with read/write access) and “glimmerPublic” (with read-only access).

A community name may be revised by either of the following methods:

- Directly revising the selected snmpCommunityName in the snmpCommunityTable—This method is recommended if managing the snmpCommunityTable table via an SNMP v3 user name.
- Adding a new community name row to the snmpCommunityTable and then deleting the original row—This method is recommended if managing the snmpCommunityTable table via an SNMP v1/v2c community name.

To directly revise the selected snmpCommunityName in the snmpCommunityTable:

1. Using SNMP v3 access, browse to and view the snmpCommunityTable:  
snmpModules > snmpCommunityMIB > snmpCommunityTable
2. For the row whose community name is to be changed:
  - a. Set the row's snmpCommunityStatus to notInService(2)
  - b. Set the row's snmpCommunityName to the new community name
  - c. Set the row's snmpCommunityStatus to active(1)

To add a new community name row to the snmpCommunityTable and then delete the original row:

1. Add a new community name (see “Add an SNMP v1/v2c Community Name” on page 19).
2. Verify SNMP v1/V2c access to the IOS using the new community name.



3. For the row whose community name is to be deleted, set the row's snmpCommunityStatus to destroy(6).

## Add an SNMP v1/v2c Community Name

The IOS installation default snmpCommunityTable (Figure 7 on page 16) defines the community names "glimmerPrivate" (with read/write access) and "glimmerPublic" (with read-only access). The snmpCommunityTable supports multiple community names (not just the two default community names).

To add a new community name row to the snmpCommunityTable:

1. Using SNMP v2c/v3 access, browse to and view the snmpCommunityTable:  
snmpModules > snmpCommunityMIB > snmpCommunityTable
2. Select the MIB Browser's Create Row facility, then Create and Wait, and enter the new community name as the snmpCommunityIndex.
3. Set the new row's snmpCommunityName to the new community name.
4. Set the new row's snmpCommunitySecurityName to one of the following:
  - "glimmerPublic" for read-only access
  - "glimmerPrivate" for read/write access
5. Set the new row's snmpCommunityStatus to active(1).

## Disable SNMP v1/v2c Write Access

The IOS installation default snmpCommunityTable (Figure 7 on page 16) defines the community names "glimmerPrivate" (with read/write access) and "glimmerPublic" (with read-only access).

SNMP v1/v2c write access may be disabled by either disabling (notInService) or deleting (destroy) the snmpCommunityTable row(s) whose snmpCommunitySecurityName is glimmerPrivate.

To disable SNMP v1/v2c write access:

1. Using SNMP v3 access, browse to and view the snmpCommunityTable:  
snmpModules > snmpCommunityMIB > snmpCommunityTable

2. For rows whose `snmpCommunitySecurityName` is `glimmerPrivate`, set the `snmpCommunityStatus` to one of the following:
  - `notInService(2)`—To disable the row; this may subsequently be reversed by changing the row status back to `active(1)`
  - `destroy(6)`—To delete the row

---

**WARNING:** This operation can only be reversed by SNMP v3 access since SNMP v2 write access has been disabled.

---

---

**NOTE:** SNMP v1/v2 write access can also be disabled by disabling/deleting rows in the `vacmAccessTable` that have `vacmAccessSecurityModel` of 1 or 2, and a non-blank `vacmAccessWriteViewName`.

---

## Disable SNMP v1/v2c Access

The IOS installation default `snmpCommunityTable` (Figure 7 on page 16) defines the community names “`glimmerPrivate`” (with read/write access) and “`glimmerPublic`” (with read-only access).

SNMP v1/v2c access may be disabled by either disabling (`notInService`) or deleting (`destroy`) all `snmpCommunityTable` rows.

To disable SNMP v1/v2c access:

1. Using SNMP v3 access, browse to and view the `snmpCommunityTable`:  
`snmpModules > snmpCommunityMIB > snmpCommunityTable`
2. For all rows, set the `snmpCommunityStatus` to one of the following:
  - `notInService(2)`—To disable the row; this may subsequently be reversed by changing the row status back to `active(1)`
  - `destroy(6)`—To delete the row

---

**WARNING:** This operation can only be reversed by SNMP v3 access since SNMP v2 write access has been disabled.

---

---

**NOTE:** SNMP v1/v2c write access can also be disabled by disabling/deleting rows in the `vacmAccessTable` that have `vacmAccessSecurityModel` of 1 or 2, and a non-blank `vacmAccessReadViewName` or `vacmAccessWriteViewName`.

---

## Restrict SNMP v1/v2c Access to an SNMP Manager IP Address

The IOS installation default `snmpCommunityTable` (Figure 7 on page 16) defines the community names “glimmerPrivate” (with read/write access) and “glimmerPublic” (with read-only access). Both community names may be accessed from any IP address.

SNMP v1/v2c access may be restricted to one or more SNMP Manager IP addresses or their IP subnets. If the `snmpCommunityTransportTag` in a `snmpCommunityTable` row contains a tag, then access via the row's corresponding community name is restricted to SNMP target addresses (SNMP Manager IP addresses) specified in the `snmpTargetAddrTable` whose `snmpTargetAddrTagList` entry includes the same tag. A tag is an arbitrary user-specified character string (excluding space, carriage-return, line feed, and tab).

The COMMUNITY MIB's `snmpTargetAddrExtTable` may be used to expand the IP address match to any IP address on the target's IP subnet. `snmpTargetAddrExtTable` rows are automatically created/deleted when creating/deleting `snmpTargetAddrTable` rows; they have the same index value as its corresponding `snmpTargetAddrTable` row. The `snmpTargetAddrExtTable` `snmpTargetAddrTMask` entry defines an ip:port mask whose hexadecimal octet string value of “FF FF FF FF 00 00” specifies and exact IP address match, while “FF FF FF 00 00 00” corresponds to a Class C subnet mask of 255.255.255.0.

---

**WARNING:** Before following this procedure, the IOS installation default SNMP Trap Target Table must be configured to send traps to one or more SNMP Managers (see “Configure the SNMP Target Address Table” on page 33).

---

To restrict SNMP v1/v2c access to one or more SNMP Manager IP addresses:

1. Using SNMP v3 access, browse to and view the `snmpTargetAddrTable`:  
`snmpModules > snmpTargetObjects > snmpTargetAddrTable`
2. For each target (SNMP Manager IP address) that you want to access via SNMP v1/v2c:
  - a. Set the row's `snmpTargetAddrRowStatus` to `notInService(2)`.
  - b. View the row's `snmpTargetAddrTagList` value(s). For example, “ggV2NotifyProfile”.
  - c. Set the row's `snmpTargetAddrTagList` to the current value(s) plus a tag value. For example, “ggV2NotifyProfile myV2TransportTag”.
  - d. Set the row's `snmpTargetAddrRowStatus` to `active(1)`.

---

**WARNING:** Do not delete the row's default tag value (ggV1NotifyProfile, ggV2NotifyProfile, or ggV3NotifyProfile): it is used as a link to the `snmpNotifyTable`.

---

3. Using SNMP v3 access, browse to and view the `snmpCommunityTable`:  
`snmpModules > snmpCommunityMIB > snmpCommunityTable`
4. For each community name that you want to access via SNMP v1/v2c:

- a. Set the row's snmpCommunityStatus to notInService(2).
- b. Set the row's snmpCommunityTransportTag to a tag value. For example, "myV2TransportTag".
- c. Set the row's snmpCommunityStatus to active(1).

---

**NOTE:** To set the snmpTargetAddrExtTable snmpTargetAddrTMask, the corresponding snmpTargetAddrTable row snmpTargetAddrRowStatus must be notInService(2).

---

## Overview

The Glimmerglass IOS SNMP Agent may be configured via the SNMP Target Address Table (snmpTargetAddrTable) to send SNMP traps to multiple SNMP target addresses (SNMP Managers and/or SNMP Trap Forwarders) using the v1, v2c, or v3 security model.

The generated SNMP traps do not require acknowledgment from the SNMP Manager(s) receiving them. The IOS SNMP Agent sends out the trap to each SNMP target address and then discards the trap. The trap includes an incrementing trap sequence number to allow the manager/user to verify receipt of all traps. The event reported via the trap is logged in the IOS AUTO log or the SECU log and may be retrieved by TL1 command RTRV-LOG.

## IOS SNMP Traps

This section summarizes the Glimmerglass IOS SNMP traps.

The SNMP traps include objects to define the alarm/event and its context. The listed page gives an example of each trap type.

SNMP Trap Type	Included SNMP Objects	Page
iosComponentStateTrap <ul style="list-style-type: none"><li>• Loss of redundant DC Power</li><li>• Fan failure</li><li>• Over temperature</li><li>• Electronics failure</li><li>• System Clock NTP sync</li><li>• Intrusion Attempt</li></ul>	iosSystemName, sysLocation, iosNetworkAddress, iosTrapSeverity, iosTrapSequence, iosTrapTime, iosTrapDescr, iosComponentType, iosComponentCondition	24
iosInputSignalTrap <ul style="list-style-type: none"><li>• Input port optical power threshold crossing alarm</li></ul>	iosSystemName, sysLocation, iosNetworkAddress, iosTrapSeverity, iosTrapSequence, iosTrapTime, iosTrapDescr, inPortNumber, inPortStatus, inPortThreshold, inPortPower, inPortName, inPortDescr, inPortPeerPort, ocName, inPortGroup	25

SNMP Trap Type	Included SNMP Objects	Page
<b>iosOutputSignalTrap</b> <ul style="list-style-type: none"> <li>Output port optical power threshold crossing alarm</li> </ul>	iosSystemName, sysLocation, iosNetworkAddress, iosTrapSeverity, iosTrapSequence, iosTrapTime, iosTrapDescr, outPortNumber, outPortStatus, outPortThreshold, outPortPower, outPortName, outPortDescr, outPortPeerPort, ocName, outPortGroup	27
<b>iosConnectionStateTrap</b> <ul style="list-style-type: none"> <li>Connection fault</li> <li>Protection switch notification</li> </ul>	iosSystemName, sysLocation, iosNetworkAddress, iosTrapSeverity, iosTrapSequence, iosTrapTime, iosTrapDescr, ocIndex, ocStatus, ocPowerLoss, ocWaveband, ocName, ocInputNumber, ocInputPower, ocInputName, ocOutputNumber, ocOutputPower, ocOutputName	29
<b>iosSystemAdminTrap</b> <ul style="list-style-type: none"> <li>System shutdown/startup</li> <li>System upgrade/rollback</li> <li>System reset/restore</li> </ul>	iosSystemName, sysLocation, iosNetworkAddress, iosTrapSeverity, iosTrapSequence, iosTrapTime, iosTrapDescr, iosSysAdminTask, iosSysAdminTaskStatus	32

## IOS SNMP Trap Example—iosComponentStateTrap

The following is an example of a fan alarm (fanRear) and the clearing of the alarm.

```

sysUpTime = 21:24:59.37
snmpTrapOID = iosComponentStateTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = minor(3)
iosTrapSequence = 1664
iosTrapTime = 2010-9-28,21:28:4.105,+0:0
iosTrapDescr =
iosComponentType = fanRear(1)
iosComponentCondition = ccFANFLT(8)

sysUpTime = 21:25:43.41
snmpTrapOID = iosComponentStateTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = clear(6)
iosTrapSequence = 1665
iosTrapTime = 2010-9-28,21:28:48.10,+0:0
iosTrapDescr =
iosComponentType = fanRear(1)
iosComponentCondition = ccFANFLT(8)

```

iosComponentStateTrap traps include:

Category	Severity	Component Type	Component Condition
Fan Single	minor(3)	fanLocation(1-13)	ccFANFLT(8)
Fan Multiple	major(2)	fanMultiple(14)	ccFANFLT(8)
Electronics	critical(1)	sysHVPS(15)	ccVBBLO(2), ccVBBHI(3) ccVFBLO(4), ccVFBHI(5)
Temperature	critical(1)	sysTemperature(16)	ccTEMPHI(6)
48VDC Fuse	major(2)	sysPowerFeedA(17) sysPowerFeedB(18)	ccFUSEFLT(9)
48VDC Power	major(2)	sysPowerFeedA(17) sysPowerFeedB(18)	cc48VFLT(10)
NTP Sync	minor(3)	sysClock(19)	ccNTPFLT(7)
Intrusion	minor(3)	sysSecurity(20)	ccINTRUSION(11)

## IOS SNMP Trap Example—iosInputSignalTrap

The following are examples of the input port alarm traps generated when an STMAX alarm condition (psSTMAX) is detected then cleared. In this example, the inPortSTMAX severity for the port is set to minor (3). This alarm is posted when the measured power at the port exceeds the sigThreshPowerMax (5dBm) value plus the sigThreshHysteresis (1dB) value defined in the port's signal threshold (1550). The alarm clear is posted when the power falls below sigThreshPowerMax value minus the sigThreshHysteresis. So in this example, the psSTMAX alarm is generated when the optical power exceeds 6dBm and is cleared when the optical power falls below 4dBm.

```

sysUpTime = 0:14:07.49
snmpTrapOID = iosInputSignalTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = minor(3)
iosTrapSequence = 168
iosTrapTime = 2012-1-22,22:2:4.100,+0:0
iosTrapDescr =
inPortNumber.10001 = 10001
inPortStatus.10001 = psSTMAX(3)
inPortThreshold.10001 = 1550
inPortPower.10001 = 6.1
inPortName.10001 = C1000EastPrimary
inPortDescr.10001 = Panel-01-02-03
inPortPeerPort.10001 = 0
ocName =
inPortGroup.10.10001 = "OpenGroup"

sysUpTime = 0:14:25.09
snmpTrapOID = iosInputSignalTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = clear(6)
iosTrapSequence = 169
iosTrapTime = 2012-1-22,22:2:22.86,+0:0
iosTrapDescr =
inPortNumber.10001 = 10001
inPortStatus.10001 = psSTMAX(3)
inPortThreshold.10001 = 1550
inPortPower.10001 = 3.9
inPortName.10001 = C1000EastPrimary
inPortDescr.10001 = Panel-01-02-03
inPortPeerPort.10001 = 0
ocName =
inPortGroup.10.10001 = "OpenGroup"

```

**NOTES:** Input port traps are reported based upon the severity assigned in the iosInputPortTable. Traps for input ports may be disabled. See “Input Port Table—iosInputPortTable” on page 87.

The trap payload inPort OIDs are those from the corresponding iosInputPortTable row hence they include the table row index (the input port number).

If the input port is not connected to an output port then the inPortPeerPort is 0 and the ocName (connection name) is null.



The iosInputSignalTrap trap conditions are shown below.

Port Status	Trap Condition
psDAMAGE(9)	Optical power at port exceeds 20.5dBm Severity = critical(1) This condition can only be cleared by Glimmerglass Support.
psSTMAX(3)	Alarm: Optical power rises above sigThreshPowerMax + sigThreshHysteresis Clear: Optical power falls below sigThreshPowerMax – sigThreshHysteresis Alarm Severity: Derived from port's inPortSTMAX setting (iosInputPortTable)
psSTMIN(2)	Alarm: Optical power falls below sigThreshPowerMin – sigThreshHysteresis Clear: Optical rises above sigThreshPowerMin + sigThreshHysteresis Alarm Severity: Derived from port's inPortSTMIN setting (iosInputPortTable)

The supported inPortSTMAX and inPortSTMIN severity settings are: critical(1), major(2), minor(3), notice(4), disable(5). Traps are issued only when the severity is critical, major, or minor. Traps reporting the alarm condition is cleared will always have the severity of clear(6).

By default, the severity setting for both inPortSTMIN and inPortSTMAX is disable(5). This means that the psSTMAX and psSTMIN alarms/traps are not reported by default. The psDamage trap condition is always enabled and is coded with a severity of critical.

## IOS SNMP Trap Example—iosOutputSignalTrap

The following are examples of the output port alarm traps generated when an STMIN alarm condition (psSTMIN) is detected then cleared. In this example, the outPortSTMIN severity for the port is set to major(2). This alarm is posted when the measured power at the port falls below the sigThreshPowerMin (-20dBm) value minus the sigThreshHysteresis (1dB) value defined in the port's Signal Threshold (1550). The alarm clear is posted when the power rises above the sigThreshPowerMin value plus the sigThreshHysteresis. So, in this example, the psSTMIN alarm is generated when the optical power falls below -21dBm and is cleared when the optical power rises above -19dBm.

```

sysUpTime = 0:22:28.54
snmpTrapOID = iosOutputSignalTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = major(2)
iosTrapSequence = 170
iosTrapTime = 2012-1-22,22:10:25.20,+0:0
iosTrapDescr =
outPortNumber.20001 = 20001
outPortStatus.20001 = psSTMIN(2)
outPortSignalType.20001 = 1550
outPortPower.20001 = -21.1
outPortName.20001 = C1000WestPrimary
outPortDescr.20001 = Panel-02-03-04
outPortPeerPort.20001 = 10001
ocName.10001 = C1000
outPortGroup.20001 = "OpenGroup"

sysUpTime = 0:22:54.49
snmpTrapOID = iosOutputSignalTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = clear(6)
iosTrapSequence = 171
iosTrapTime = 2012-1-22,22:10:51.30,+0:0
iosTrapDescr =
outPortNumber.20001 = 20001
outPortStatus.20001 = psSTMIN(2)
outPortSignalType.20001 = 1550
outPortPower.20001 = -18.9
outPortName.20001 = C1000WestPrimary
outPortDescr.20001 = Panel-02-03-04
outPortPeerPort.20001 = 10001
ocName.10001 = C1000
outPortGroup.20001 = "OpenGroup"

```

**NOTES:** STMIN and STMAX output port traps are reported based upon the severity assigned in the iosOutputPortTable. STMIN/STMAX output traps for output ports may be disabled. See “Output Port Table—iosOutputPortTable” on page 91.

The trap payload outPort OIDs are those for the corresponding iosOutputPortTable row hence they include the table row index (the output port number).

The ocName (connection name) OID is that from the corresponding iosConnectionTable row hence it contains the table row index (the input port number).

The iosOutputSignalTrap trap conditions are shown below.

Port Status	Trap Condition
psDAMAGE(9)	Optical power at port exceeds 20.5dBm Severity = critical(1) This condition can only be cleared by Glimmerglass Support.
psSTMAX(3)	Alarm: Optical power rises above sigThreshPowerMax + sigThreshHysteresis Clear: Optical power falls below sigThreshPowerMax – sigThreshHysteresis Alarm Severity: Derived from port's outPortSTMAX setting (iosOutputPortTable)
psSTMIN(2)	Alarm: Optical power falls below sigThreshPowerMin – sigThreshHysteresis Clear: Optical rises above sigThreshPowerMin – sigThreshHysteresis Alarm Severity: Derived from port's outPortSTMIN setting (iosOutputPortTable)
psLGTRVRS(8)	Alarm: Optical power (above -40dBm) measured at unconnected output port, or Output port power higher than input port power for connected ports Clear: Optical power below -40dBm at unconnected output or loss is normal Alarm Severity = critical(1)

The supported outPortSTMAX and outPortSTMIN severity settings are: critical(1), major(2), minor(3), notice(4), disable(5). Traps are only issued when the severity is critical, major, or minor. Traps reporting the alarm condition is cleared will always have the severity = clear(6).

By default, the severity setting for both outPortSTMIN and outPortSTMAX is disable(5). This means that the psSTMAX and psSTMIN alarms/traps are not reported by default. The psDamage and psLGTRVRS trap conditions are always enabled and are coded with a severity of critical.

## IOS SNMP Trap Example—iosConnectionStateTrap

The following are examples of the connection state traps generated when a connection fault alarm condition (csCSFLT) is detected then cleared. In this example, the outPortCSFLT severity for the port is set to critical(1). This alarm is posted when the incoming power is too low for full connection optimi-

zation. Depending on factory settings, this will occur below -27dBm or -30dBm on standard systems. This will occur below -37dBm on low power systems.

```
sysUpTime = 4:03:14.41
snmpTrapOID = iosConnectionStateTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = critical(1)
iosTrapSequence = 11
iosTrapTime = 2011-6-23,22:23:12.88,+0:0
iosTrapDescr =
ocIndex.10001 = 10001
ocStatus.10001 = csCSFLT(2)
ocPowerLoss.10001 = NA
ocWaveband.10001 = nm1550(2)
ocName.10001 = C1000
ocInputNumber.10001 = 10001
ocInputPower.10001 = -49.7
ocInputName.10001 = C1000EastPrimary
ocOutputNumber.10001 = 20001
ocOutputPower.10001 = -50.3
ocOutputName.10001 = C1000WestPrimary

sysUpTime = 4:03:42.57
snmpTrapOID = iosConnectionStateTrap
iosSystemName = LosAngeles
sysLocation = DownTown
iosNetworkAddress = 192.168.2.98
iosTrapSeverity = clear(6)
iosTrapSequence = 12
iosTrapTime = 2011-6-23,22:23:40.98,+0:0
iosTrapDescr =
ocIndex.10001 = 10001
ocStatus.10001 = csCSFLT(2)
ocPowerLoss.10001 = 2.0
ocWaveband.10001 = nm1550(2)
ocName.10001 = C1000
ocInputNumber.10001 = 10001
ocInputPower.10001 = -5.0
ocInputName.10001 = C1000EastPrimary
ocOutputNumber.10001 = 20001
ocOutputPower.10001 = -7.0
ocOutputName.10001 = C1000WestPrimary
```

**NOTES:** The csCSFLT connection trap may be enabled or disabled via the iosOutputPortTable, see “Output Port Table—iosOutputPortTable ” on page 91.

The trap payload OIDs are those for the corresponding iosConnectionTable row hence they include the table row index (the input port number), see “Connection Table—iosConnectionTable ” on page 94.

The iosConnectionStateTrap trap conditions are shown below.

Status	Trap Condition
csCSFLT(2)	Alarm: Optical power at output too low for connection optimization Clear: Optical power at output is again sufficient for connection optimization Alarm Severity: Derived from port's outPortCSFLT setting (iosOutputPortTable)
csPROTS(4)	Protection Switch has occurred Severity: notice(4)

The supported outPortCSFLT severity settings are: critical(1), major(2), minor(3), notice(4), disable(5). Traps are only issued when the severity is critical, major, or minor. Traps reporting the alarm condition is cleared will always have the severity = clear(6).

By default, the severity setting for both outPortCSFLT is critical(1).

The csPROTS trap reports a protection switch has occurred. See "Protection Rule Table—iosProtectionRuleTable" on page 102.

## IOS System Administration Trap Example—iosSystemAdminTrap

The following is an example of the system traps that occur on system restart/reboot.

```
sysUpTime = 0:06:03.33
snmpTrapOID = iosSystemAdminTrap
iosSystemName = BD0020
sysLocation =
iosNetworkAddress = 192.168.2.43
iosTrapSeverity = notice(4)
iosTrapSequence = 6
iosTrapTime = 2011-4-7,19:43:51.100,+0:0
iosTrapDescr = System Shutdown Initiated
iosSysAdminTask = sysShutdown(1)
iosSysAdminTaskStatus = taskInitiated(1)

sysUpTime = 0:00:00.50
snmpTrapOID = warmStart

sysUpTime = 0:00:00.50
snmpTrapOID = iosSystemAdminTrap
iosSystemName = BD0020
sysLocation =
iosNetworkAddress = 192.168.2.43
iosTrapSeverity = notice(4)
iosTrapSequence = 7
iosTrapTime = 2011-4-7,19:44:11.50,+0:0
iosTrapDescr = System Startup Completed
iosSysAdminTask = sysStartup(2)
iosSysAdminTaskStatus = taskCompleted(2)
```

iosSystemAdminTrap traps include:

Category	Severity	Component Type
sysShutdown(1) taskInitiated(1)	notice(4)	Occurs on IOS application shutdown due to system restart/reboot/shutdown.
sysStartup(2) taskCompleted(2)	notice(4)	Occurs on conclusion of system restart/reboot or power-on. It is accompanied by a warmStart trap for MIB-2 compliance.
sysResetFactory(3) taskInitiated(1)	notice(4)	Occurs on reset system configuration to factory defaults, see "Resetting System Configuration to Factory Defaults" on page 69.
sysRestore(4) taskCompleted(2)	notice(4)	Occurs on completion of restore system configuration, see "Restoring the System Configuration" on page 60.
sysUpgrade(5) taskInitiated(1) taskCompleted(2)	notice(4)	Occurs on completion of system software upgrade, see "Upgrading System Software" on page 63.

Category	Severity	Component Type
sysRollback(6) taskInitiated(1)	major(2)	Occurs on start of system software rollback, see "Rolling Back System Software" on page 66.
sysClockRTC(7) taskCompleted(2)	notice(4)	Occurs when NTP is disabled, see "System Clock - sysClock" on page 78.
sysClockNTP(8) taskCompleted(2)	notice(4)	Occurs when NTP is enabled/revised, an iosComponentStateTrap will occur if the system fails to synchronize with the NTP server(s), see "System Clock - sysClock" on page 78.

## Configure the SNMP Target Address Table

The IOS SNMP Agent may be configured via the SNMP Target Address Table (snmpTargetAddrTable) to send SNMP traps to multiple SNMP target addresses (SNMP Managers and/or SNMP Trap Forwarders) using the v1, v2c, or v3 security model.

The IOS installation default snmpTargetAddrTable contains three rows, one example for each of the three SNMP security models. The row status is notInService(2) because these entries are just examples/prototypes.


Figure 8 IOS Installation Default snmpTargetAddrTable


OID: .1.3.6.1.6.3.12.1.2


Operations: Table View

Result Table

192.168.2.43 - snmpTargetAddrTable

 Rotate

 Refresh

 Export

Poll

SNMP SET

Create Row

	1	2	3
snmpTargetAddrName	127.0.0.1/162	127.0.0.1/163	127.0.0.1/164
snmpTargetAddrTDomain	.1.3.6.1.6.1.1	.1.3.6.1.6.1.1	.1.3.6.1.6.1.1
snmpTargetAddrTAddress	7F-00-00-01-00-A2	7F-00-00-01-00-A3	7F-00-00-01-00-A4
snmpTargetAddrTimeout	1500	1500	1500
snmpTargetAddrRetryCount	3	3	3
snmpTargetAddrTagList	ggV3NotifyProfile	ggV1NotifyProfile	ggV2NotifyProfile
snmpTargetAddrParams	ggV3TargetProfile	ggV1TargetProfile	ggV2TargetProfile
snmpTargetAddrStorageType	3	3	3
snmpTargetAddrRowStatus	2	2	2

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The arbitrary but unique row index (snmpTargetAddrName) text string in the installation defaults is based on the target IP address and port ('<ip>/<port>'). The following sections provide some simple examples of revising the SNMP Target Address Table:

- "SNMP Target Address Format " on page 34
- "Adding/Deleting an SNMP v2c Target Address via ClickFlow/TL1" on page 34
- "Revising an SNMP Target Address" on page 35
- "Adding an SNMP Target Address " on page 36
- "Deleting an SNMP Target Address" on page 36

## SNMP Target Address Format

The snmpTargetAddrTAddress encodes the SNMP Manager IP address and port as 12 hexadecimal digits (8 for the IP address and 4 for the port). For example:

Manager IP:Port	snmpTargetAddrTAddress
127.0.0.1:162	7F 00 00 01 00 A2
192.168.1.100:162	C0 A8 01 64 00 A2
192.168.1.100:10162	C0 A8 01 64 27 B2

The IOS installation default snmpTargetAddrTable IP address is 127.0.0.1 (IPv4 localhost). The hexadecimal digit string display and entry formats are MIB Browser vendor dependent.

## Adding/Deleting an SNMP v2c Target Address via ClickFlow/TL1

The IOS installation default snmpTargetAddrTable (Figure 8 on page 33) contains three rows, one for each of the three SNMP security models (v1, v2c, and v3). The installation default target address IP:Port is "127.0.0.1:164"; the IOS SNMP Agent does not send traps if the IP address is 127.0.0.1 (localhost). The ClickFlow and TL1 interfaces support operations on SNMP Target Address table rows with the following attributes:

- snmpTargetAddrName                      <ip>/<port> (for example, "192.168.1.100/162")
- snmpTargetAddrTagList                  ggV2NotifyProfile
- snmpTargetAddrParams                  ggV2TargetProfile

Hence, the ClickFlow and TL1 interfaces may be used to manage target addresses for traps to be transmitted using the SNMP v2c model.



To display the current SNMP v2c target addresses, use the following TL1 command:

```
rtrv-snmp-server:::<ctag>;
```

To add a new target address, use the following TL1 command:

```
set-snmp-server::<ip>:<ctag>:::PORT=<port>;
```

To delete an existing target address, use the following TL1 command:

```
dlt-snmp-server::<ip>:<ctag>:::PORT=<port>;
```

In the above TL1 commands:

Parameter	Description	Example Input
<ctag>	Arbitrary correlation tag	1
<ip>	IP address	192.168.1.100
<port>	Port number	162

**NOTE:** For further information please see the *IOS ClickFlow Graphical User Interface Manual*, and/or the *IOS Transaction Language 1 (TL1) User Manual*.

## Revising an SNMP Target Address

The IOS installation default snmpTargetAddrTable (Figure 8 on page 33) contains three rows, one for each of the three SNMP security models (v1, v2c, and v3). The installation default target IP address is "127.0.0.1"; the IOS SNMP Agent does not send traps if the IP address is 127.0.0.1 (localhost).

To revise a snmpTargetAddrTable row's IP:Port:

- Using SNMP v2c/v3 access, browse to and view the snmpTargetAddrTable:  
snmpModules > snmpTargetObjects > snmpTargetAddrTable
- For the row whose target address is to be changed (for example the installation default "127.0.0.1/162" row for SNMP v3 format traps):
  - Set the row's snmpTargetAddrRowStatus to notInService(2).
  - Set the row's snmpTargetAddrTAddress to the SNMP Manager's IP:Port using the hexadecimal format (see "SNMP Target Address Format" on page 34).
  - Set the row's snmpTargetAddrRowStatus to **active(1)**.

## Adding an SNMP Target Address

The IOS installation default `snmpTargetAddrTable` (Figure 8 on page 33) contains three rows, one for each of the three SNMP security models (v1, v2c, and v3). The IOS SNMP Agent supports a maximum of ten `snmpTargetAddrTable` rows.

To add a new Trap Target (SNMP Manager) row to the `snmpTargetAddrTable`:

1. Using SNMP v2c/v3 access, browse to and view the `snmpTargetAddrTable`:  
`snmpModules > snmpTargetObjects > snmpTargetAddrTable`
2. Select the MIB Browser's Create Row facility, then Create and Wait, and enter the new unique `snmpTargetAddrName` (row index). For v2 format trap targets, it is recommended that the string be '`<ip>/<port>`' (for example, '192.168.1.100/162'), so that ClickFlow/TL1 may display/delete the entry.

---

**NOTE:** The Create and Wait will be rejected with "Resource Unavailable" if the `snmpTargetAddrTable` already has ten rows.

---

3. Set the new row's `snmpTargetAddrTDomain` to OID ".1.3.6.1.6.1.1".
4. Set the row's `snmpTargetAddrTAddress` to the SNMP Manager's IP:Port using the hexadecimal format (see "SNMP Target Address Format" on page 34).
5. Optionally set the row's `snmpTargetAddrTimeout` (the default value is 1500 centiseconds or 15 seconds).
6. Set the new row's `snmpTargetAddrTagList` to one of the following:
  - "ggV1NotifyProfile" for SNMP v1 format trap targets
  - "ggV2NotifyProfile" for SNMP v2c format trap targets
  - "ggV3NotifyProfile" for SNMP v3 format trap targets
7. Set the new row's `snmpTargetAddrParams` to one of the following:
  - "ggV1TargetProfile" for SNMP v1 format trap targets
  - "ggV2TargetProfile" for SNMP v2c format trap targets
  - "ggV3TargetProfile" for SNMP v3 format trap targets
8. Set the new row's `snmpTargetAddrRowStatus` to **active(1)**.

## Deleting an SNMP Target Address

The IOS installation default `snmpTargetAddrTable` (Figure 8 on page 33) contains three rows, one for each of the three SNMP security models (v1, v2c, and v3).

To delete a row from the snmpTargetAddrTable (for example the “127.0.0.1/163” row):

1. Using SNMP v2c/v3 access, browse to and view the snmpTargetAddrTable:  
snmpModules > snmpTargetObjects > snmpTargetAddrTable
2. Set the row’s snmpTargetAddrRowStatus to one of the following:
  - notInService(2)—To disable the row; this may subsequently be reversed by changing the row status back to **active(1)**
  - destroy(6)—To delete the row

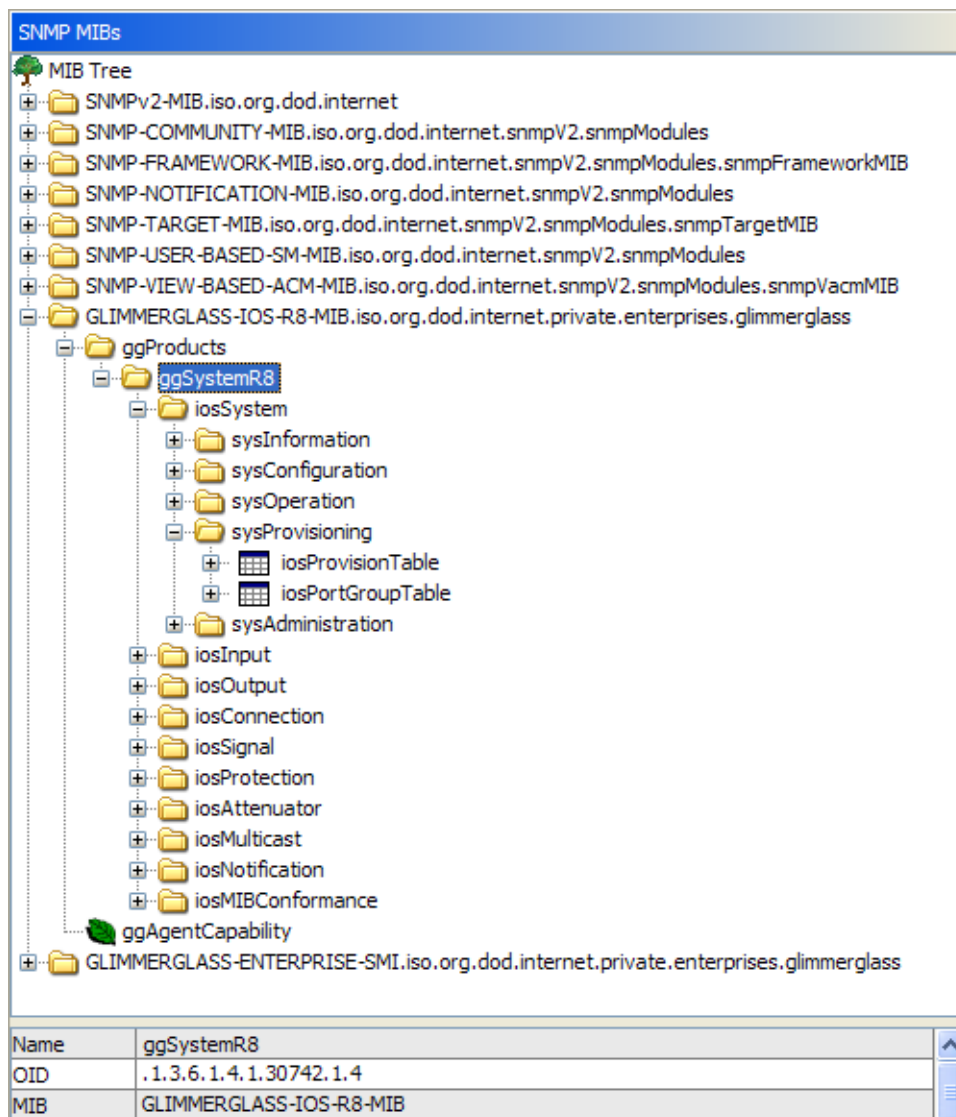
THIS PAGE INTENTIONALLY LEFT BLANK

## Overview

The Glimmerglass IOS SNMP MIB provides a tabular view of the IOS database which allows viewing of the current state, and configuration/provisioning of the IOS system. The majority of IOS features configurable via the ClickFlow web browser graphical interface and the TL1 textual interface are configurable via SNMP. For a more complete understanding of the IOS, it is recommended that the reader become familiar with the IOS concepts and operations by reading the *Glimmerglass IOS Installation and Maintenance Guide* that describes IOS standard and optional features, the *IOS ClickFlow Graphical User Interface Manual*, and that the reader has hands-on experience operating an IOS via ClickFlow and has walked the IOS SNMP MIB with a MIB Browser. MIB files include self-documentation, so when walking the MIB be sure to view the tables, the table descriptions, the table indices, the individual objects descriptions, and their access (read-only, read-write). Additionally, the SNMPv2 system group may be used to view/set the IOS sysName, sysLocation, and sysContact.

Figure 9 shows a MIB Browser view of the IOS private MIB tree expanded to the first branch.

Figure 9 IOS SNMP MIB Tree



The following table describes the branches and gives the page number where the branch's tables are further described.

IOS SNMP MIB Tables	Description	Page
iosSystem sysInformation	A sub-tree listing system information: System name, description, network address, module type and number, serial number, etc.	42
iosSystem sysConfiguration	A sub-tree listing system hardware and software features: Input Power Detection, PMU, VOA, port counts, connector types, software licenses, etc.	45

IOS SNMP MIB Tables	Description	Page
iosSystem sysOperation	A sub-tree listing system operation options: Autosave configuration, Connection Restore, etc. per ClickFlow Runtime Options.	47
iosSystem sysProvisioning iosProvisionTable	A table for asynchronous operations, which include multiple port operations and system maintenance operations.	48
iosSystem sysProvisioning iosPortGroupTable	A table with one row for each configured port group: Configure group name, allowed group names, and description.	75
iosSystem sysAdministration sysClock	A subtree listing system clock/NTP configuration: date-time, clock source (RTC/NTP), clock NTP sync status, NTP server IP addresses per ClickFlow System Date/Time Configuration.	78
iosSystem sysAdministration sysNetwork	A subtree listing system network configuration: host name, Ethernet port IP addresses, masks, TCP ports, etc. per ClickFlow System Name/IP Configuration and Startup Options.	80
iosSystem sysAdministration sysLog	A subtree and table listing the SYSLOG configuration: logging/notification level and syslog server IP addresses per ClickFlow System Syslog Configuration.	83
iosSystem sysAdministration sysAlarm	A subtree listing standing alarms (highest severity) for system HW/SW alarm types: Engine Temperature, NTP, Intrusion, Fans, High Voltage Power Supplies, and DC input power/fuses	85
iosSystem sysSecurity	Tables for configuration of ClickFlow/TL1 users and their privileges. <b>NOTE:</b> These tables are not supported or included in this initial release of the IOS SNMP Agent.	86
iosInput iosInputPortTable	A table with one row for each installed “normal” input port: configure port name, description, group, waveband, threshold, and alarm severities; retrieve port power and state. See iosAttenuator and iosMulticast below for configuration of SVOA/PMU ports.	87
iosOutput iosOutputPortTable	A table with one row for each installed “normal” output port: Configure port name, description, group, threshold, and alarm severities; Retrieve port power and state. See iosAttenuator and iosMulticast below for configuration of SVOA/PMU ports.	91
iosConnection iosConnectionTable	A table with one row for each configured connection: make/break connections, configure connection name; retrieve connection state, connection port powers and connection power loss.	94

IOS SNMP MIB Tables	Description	Page
iosSignal iosSigThresholdTable	A table with one row for each configured signal threshold: configure power thresholds and hysteresis.	98
iosProtection iosProtectionRuleTable	A table with one row for each configured protection rule: configure protection rules; retrieve status.	102
iosAttenuator iosVOAUnitTable	A table with one row for each installed Dedicated VOA and Switched VOA: configure VOA mode and power/attenuation.	107
iosVOAPortTable	A table with one row for each installed Dedicated VOA output port, Switched VOA input port, and Switched VOA output port: configure port name, description; retrieve port power and state.	109
iosMulticast iosPMCUnitTable	A read-only table with one row for each installed PMU: retrieve PMU type and PMU input port (switch output port).	112
iosPMCPortTable	A table with one row for each installed PMU input port and for each installed PMU output port: configure port name, description/comment; retrieve port power and state.	113
iosNotification	MIB definitions defining trap contents, and the above tables.	N/A

## System Information—sysInformation

A sub-tree listing system information (Figure 10) per that in the following ClickFlow windows:

- System Name/IP: ClickFlow menu selection **System > System Configuration > Name/IP**
- System Info: ClickFlow menu selection **Reports > System Info**



Figure 10 IOS System Information—sysInformation

OID: .1.3.6.1.4.1.30742.1.4.1.1 Operations: Get Subtree

Name/OID	Value	Type
iosSystemName.0	BD0466	OctetString
iosSystemDescr.0	Glimmerglass IOS Optical Switch System	OctetString
iosNetworkAddress.0	192.168.1.32	IpAddress
iosHostName.0	BD0466	OctetString
iosModelType.0	600	OctetString
iosModelNumber.0	GG514	OctetString
iosModelRevision.0	C	OctetString
iosSerialNumber.0	138D6PC10466	OctetString
iosSystemBuildDate.0	05/Jun/2013	OctetString
iosLastBootTime.0	2013-6-21, 19:57:12.0, +0:0	OctetString
iosBootPartition.0	1	Gauge
iosBootVersion.0	R08.00p000	OctetString
iosRollbackPartition.0	0	Gauge
iosRollbackVersion.0	R07.03p001	OctetString

The table below describes the System Information sub-tree elements:

Element	Read/Write	Description
iosSystemName	R/W	System Name: 1-20 characters, alphanumeric plus the following special characters: period ("."), dash ("-"), and under-score ("_"). The installation default is derived from the system's serial number.
iosSystemDescr	R/W	System Description. 0-64 characters.
iosNetworkAddress	RO	System IP Address—Ethernet 1 IP address. The system IP address may be revised via netEther1Address (see "System Network - sysNetwork" on page 80).
iosHostName	RO	System Host Name. 1-63 characters, alphanumeric and dash ("-") only. The system host name may be revised via netHostName (see "System Network - sysNetwork" on page 80) or via SNMPv2 mib-2 system sysName.
iosModelType	RO	System type: • <b>100/500/600</b>
iosModelNumber	RO	Model Number: • <b>GG112/GG528/GG524</b>
iosModelRevision	RO	Model Revision


Element	Read/ Write	Description
iosSerialNumber	RO	System Serial Number (12 characters)
iosSystemBuildDate	RO	System Build Date • <b>dd/mmm/yyyy</b>
iosLastBootTime	RO	Last Boot Time (UTC): • <b>yyyy-mm-dd,hh:mm:ss.sss,+0.0</b>
iosBootPartition	RO	Boot Partition: • <b>0/1</b>
iosBootVersion	RO	Boot Version: • <b>Rxx.xxpxxx</b>
iosRollbackPartition	RO	Rollback Partition: • <b>0/1</b>
iosRollbackVersion	RO	Rollback Version: • <b>Rxx.xxpxxx</b>

**NOTE:** See "System Network - sysNetwork" on page 80 for changing the iosNetworkAddress and iosHostName.

## System Configuration—sysConfiguration

A sub-tree listing system hardware and software features (Figure 11) per those in the ClickFlow System Info window (ClickFlow menu selection **Reports > System Info**).

Figure 11 IOS System Configuration sub-tree—sysConfiguration

OID: .1.3.6.1.4.1.30742.1.4.1.2	Operations: Get Subtree	
Result Table		
Name/OID	Value	Type
iosInputPowerDetection.0	yes (1)	Integer
iosPhotonicMulticast.0	no (0)	Integer
iosDedicatedVOA.0	no (0)	Integer
iosSwitchedVOA.0	no (0)	Integer
iosLowPowerOperation.0	no (0)	Integer
iosMulticastMatrixSize.0	0	OctetString
iosTotalDVoaPorts.0	0	Gauge
iosTotalSVoaPorts.0	0	Gauge
iosLicenseConnectionRestore.0	licensed (1)	Integer
iosLicensePortProtection.0	nolicense (0)	Integer
iosLicenseVirtualSwitch.0	licensed (1)	Integer
iosPortMatrixLicensed.0	192x192	OctetString
iosPortMatrixUpgradeable.0	0x0	OctetString
iosPortMatrixReference.0	0x0	OctetString
iosInputConnectorType.0	MTP-12F	OctetString
iosOutputConnectorType.0	MTP-12M	OctetString
iosTotalFans.0	5	Gauge
iosMaxSignalPower.0	20.0	OctetString
iosMinSignalPower.0	-30.0	OctetString
iosLicensePortGrouping.0	licensed (1)	Integer
iosLicensePortPairing.0	nolicense (0)	Integer

The table below describes the System Configuration sub-tree elements:

Element	Read/Write	Description
iosInputPowerDetection	RO	Input Power Detection optional hardware feature installed: • <b>no(0)</b> or <b>yes(1)</b>
iosPhotonicMulticast	RO	Photonic Multicast Unit optional hardware feature installed: • <b>no(0)</b> or <b>yes(1)</b>
iosDedicatedVOA	RO	Dedicated VOA (DVOA) optional hardware feature installed: • <b>no(0)</b> or <b>yes(1)</b>

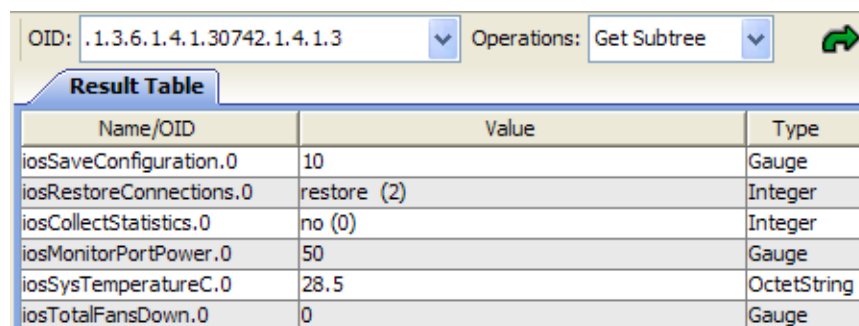
Element	Read/Write	Description
iosSwitchedVOA	RO	Switched VOA (SVOA) optional hardware feature installed: • <b>no(0)</b> or <b>yes(1)</b>
iosLowPowerOperation	RO	Low Power Operation optional hardware feature installed: • <b>no(0)</b> or <b>yes(1)</b>
iosMulticastMatrixSize	RO	Photonic Multicast Unit optional hardware feature configuration: • <b>0</b> —No PMUs installed • <b>1:n[,1:n ...]</b> —“1:n” for each PMU, <i>n</i> = number of outputs
iosTotalDVoaPorts	RO	Dedicated VOA optional hardware feature configuration: • <b>0-32</b> —Number DVOAs installed
iosTotalSVoaPorts	RO	Switched VOA optional hardware feature configuration: • <b>0-32</b> —Number SVOAs installed
iosLicenseConnectionRestore	RO	Connection Restore standard software feature: • <b>licensed(1)</b>
iosLicensePortProtection	RO	Port Protection Switching optional software feature: • <b>nolicense(0)</b> , <b>licensed(1)</b> or <b>expired(2)</b>
iosLicenseVirtualSwitch	RO	Virtual Switch (port privileges) optional software feature: • <b>nolicense(0)</b> , <b>licensed(1)</b> or <b>expired(2)</b>
iosPortMatrixLicensed	RO	Switch “normal” port count (excludes PMU/SVOA): • <b>input x output</b>
iosPortMatrixUpgradeable	RO	Switch spare port count (additional “normal” ports that can be enabled by a license update versus return to factory for upgrade): • <b>input x output</b>
iosPortMatrixReference	RO	Switch “reference” port count (PMU/SVOA ports): • <b>input x output</b>
iosInputConnectorType	RO	Input Port Connector type: • <b>Unknown, LC/UPC, LC/APC, SC/UPC, SC/APC, FC/UPC, FC/APC, ST/UPC, E2000/APC, F3000/UPC, MTP-12F, MTP-12M, MTP-8F, MTP-8M</b>
iosOutputConnectorType	RO	Output port connector type: • <b>Unknown, LC/UPC, LC/APC, SC/UPC, SC/APC, FC/UPC, FC/APC, ST/UPC, E2000/APC, F3000/UPC, MTP-12F, MTP-12M, MTP-8F, MTP-8M</b>

Element	Read/Write	Description
iosTotalFans	RO	Number of fans: <ul style="list-style-type: none"> <li>• <b>2</b>—Model 500 fan tray</li> <li>• <b>3</b>—Model 100</li> <li>• <b>4</b>—Model 600</li> </ul>
iosMaxSignalPower	RO	Maximum valid Signal Threshold Power Max value: <ul style="list-style-type: none"> <li>• <b>15.0</b>—Low Power Operation System</li> <li>• <b>20.0</b>—Normal Power Operation System</li> <li>• <b>25.0</b>—High Power Operation System</li> </ul>
iosMinSignalPower	RO	Minimum valid Signal Threshold Power Minimum value: <ul style="list-style-type: none"> <li>• <b>-25.0</b>—Normal/High Power Operation System</li> <li>• <b>-35.0</b>—Low Power Operation System</li> </ul>
iosLicensePortGrouping	RO	Port Grouping optional software feature: <ul style="list-style-type: none"> <li>• <b>nolicense(0), licensed(1) or expired(2)</b></li> </ul>
iosLicensePortPairing	RO	Port Pairing optional software feature: <ul style="list-style-type: none"> <li>• <b>nolicense(0), licensed(1) or expired(2)</b></li> </ul>

## System Operation Options—sysOperation

A sub-tree listing system operation options (Figure 12) per those in the ClickFlow Runtime Options window (menu selection **System > System Configuration > Runtime Options**).

Figure 12 IOS System Operation Sub-tree—sysOperation



Result Table		
Name/OID	Value	Type
iosSaveConfiguration.0	10	Gauge
iosRestoreConnections.0	restore (2)	Integer
iosCollectStatistics.0	no (0)	Integer
iosMonitorPortPower.0	50	Gauge
iosSysTemperatureC.0	28.5	OctetString
iosTotalFansDown.0	0	Gauge

The table below describes the IOS System Operation sub-tree elements:

Element	Read/Write	Description
iosPersistConfiguration	R/W	Configuration Autosave Delay (secs): <ul style="list-style-type: none"> <li>• <b>0</b>—Autosave Disabled</li> <li>• <b>10 - 86400</b>—10 secs to 1 day, installation default 60 secs</li> </ul>
iosRestoreConnections	R/W	Reset/Restore Connections on power-on: <ul style="list-style-type: none"> <li>• <b>reset(1)</b>—Reset connections (no connections)</li> <li>• <b>restore(2)</b>—Restore connections</li> </ul>
iosCollectStatistics	R/W	Slow multiple connection rate to collect switching time data: <ul style="list-style-type: none"> <li>• <b>no(0)</b></li> <li>• <b>yes(1)</b></li> </ul>
iosMonitorPortPower	R/W	Port threshold crossing power monitoring rate (mS): <ul style="list-style-type: none"> <li>• <b>0</b>—Threshold crossing power monitoring disabled</li> <li>• <b>10 - xxxx</b>—10 minimum value, installation default 50</li> </ul>
iosSysTemperatureC	RO	Switching Engine Temperature °C
iosTotalFansDown	RO	Number of failed fans

**NOTE:** If Configuration Autosave is disabled, a system power cycle will delete any configuration changes made since the last restart, reboot, shut-down, or user-initiated system configuration save (via the ClickFlow Save Configuration operation or via the TL1 command WRT-DB). Configuration changes are saved on system restart, reboot, and shutdown.

## System Provisioning Table—iosProvisionTable

A table (shown in Figure 13) that supports the asynchronous multi-port provisioning operations and system maintenance operations described below:

Operation	Description	Page
Connect ports	Connect a list of input ports to a list of output ports, and optionally name the connections.	54
Connect all ports	Connect all “normal” input ports to all “normal” output ports.	55

Operation	Description	Page
Disconnect ports	Disconnect a list of input/output ports.	56
Disconnect all ports	Disconnect all (both “normal” and “reference”) input and output ports.	57
Name connections	Set the connection name of existing connections for the listed input/output ports.	58
Backup System Configuration	Backup the system configuration to a system configuration XML file.	59
Restore System Configuration	Restore the system configuration from a system configuration XML (backup) file.	60
Save System Configuration	Save configuration changes to persist memory (non-volatile memory)	62
Upgrade System Software	Upgrade the system software release	63
Rollback System Software	Rollback the system software to the prior release	66
Reboot System	System Reboot/Shutdown/Restart	68
Reset System Configuration	Reset system configuration to factory defaults	69
Set Port Group	Assign a port group to a list of ports	70
Set Port Signal Threshold	Assign a signal threshold to a list of ports	71
Set Port Waveband	Assign a waveband to a list of input ports	72
Set Port STMIN Alarm Severity	Assign the severity for STMIN alarms for a list of ports	73
Set Port STMAX Alarm Severity	Assign the severity for STMAX alarms for a list of ports	73
Set Port CSFLT Alarm Severity	Assign the severity for CSFLT alarms for a list of output ports	73
Reissue operation	Reissue a prior provisioning operation.	75

- NOTES:**
- “Normal” input ports are switch input ports that are either connected directly to a switch panel input connector or via an input splitter (optional hardware feature).
  - “Normal” output ports are switch output ports that are either connected directly to a switch panel output connector or via an output splitter (optional hardware feature).
  - “Reference” ports are switch ports connected to non-dedicated internal optional hardware features (PMUs and SVOAs).

Figure 13 IOS System Provisioning Table—iosProvisionTable

OID: .1.3.6.1.4.1.30742.1.4.1.4.1		Operations: Table View		Go
Result Table 192.168.1.32 - iosProvisionTable x				
Rotate	Refresh	Export	Poll	SNMP SET
Create Row	Delete Row			
	1	2	3	
prIndex	1	2	3	
prInputPorts	1-24	1-24	0x00 01 02 03 04 05 06 07 08	
prOutputPorts	1-24	25-48	0x00 29 2A 2B 2C 2D 2E 2F 30	
prValue	primary	backup		
prCommand	connect	connect	connect	
prStatus	pass	pass	pass	
prDescr	Primary circuits	Backup circuits	1-8 to 41-48	
prOwner	glimmerPrivate	glimmerPrivate	glimmerPrivate	
prDateTime	2013-6-24, 15:4:34.76, +0:0	2013-6-24, 15:0:50.46, +0:0	2013-6-24, 15:3:9.16, +0:0	
prConfirm	yes	yes	yes	
prRowStatus	active	active	active	

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the System Provisioning Table elements:

Element	Read/Write	Description
prIndex	idx	Table row index: • 1, 2, ...(Unique integer entered when creating the row)
prInputPorts	R/W	Input port list (0-255 characters/octet): • A list of input ports for connect, disconnect and setConnectionName See "System Provisioning Port List Formats" on page 53.
prOutputPorts	R/W	Output port list (0-255 characters/octet): • A list of output ports for connect, disconnect and setConnectionName. See "System Provisioning Port List Formats" on page 53.
prValue	R/W	Command specific text parameter (0-64 characters): • Connection Name (0-32 characters) for connect and setConnectionName



Element	Read/ Write	Description
prCommand	R/W	<p>Provisioning command:</p> <ul style="list-style-type: none"> <li>• <b>none(0)</b>—Initial value after row creation</li> <li>• <b>connect(1)</b>—Connect input list to output list and name connection</li> <li>• <b>connectFull(2)</b>—Connect all normal inputs to all normal outputs</li> <li>• <b>disconnect(3)</b>—Disconnect listed input/output ports</li> <li>• <b>disconnectFull(4)</b>—Disconnect all ports</li> <li>• <b>setConnectionName(5)</b>—Set connection name for listed input/output ports</li> <li>• <b>sysBackup(6)</b>—Backup the system configuration to a system configuration XML file</li> <li>• <b>sysRestore(7)</b>—Restore the system configuration from a system configuration XML (backup) file</li> <li>• <b>sysCheckpoint(8)</b>—Save configuration changes to persist memory (non-volatile memory)</li> <li>• <b>sysUpgrade(9)</b>—Upgrade system software release</li> <li>• <b>sysRollback(10)</b>—Rollback system software to the prior release</li> <li>• <b>sysReboot(11)</b>—Reboot the system</li> <li>• <b>sysShutdown(12)</b>—Shutdown the system (all connections are broken)</li> <li>• <b>sysRestart(13)</b>—Restart the switch control application</li> <li>• <b>sysResetFactory(14)</b>—Reset the system configuration to factory defaults (all connections are broken)</li> <li>• <b>setPortGroup(15)</b>—Assign a port group name to a list of ports</li> <li>• <b>setPortThreshold(16)</b>—Assign a signal threshold name to a list of input ports</li> <li>• <b>setPortWaveband(17)</b>—Assign a waveband to a list of ports</li> <li>• <b>setPortSTMIN(18)</b>—Assign a STMIN alarm severity to a list of ports</li> <li>• <b>setPortSTMAX(19)</b>—Assign a STMAX alarm severity to a list of ports</li> <li>• <b>setPortCSFLT(20)</b>—Assign a CSFLT alarm severity to a list of output ports</li> </ul>

Element	Read/Write	Description
prStatus	RO	Provisioning command completion status <ul style="list-style-type: none"> <li>• <b>fail(0)</b>—Command rejected</li> <li>• <b>pass(1)</b>—Command executed</li> <li>• <b>partial(2)</b>—Command executed with exceptions</li> <li>• <b>notReady(3)</b>—Initial value after row creation</li> <li>• <b>pending(4)</b>—Command (sysRestore, sysUpgrade) is in progress</li> </ul>
prDescr	R/W	Optional description (0-128 characters)
prOwner	RO	SNMP USM user name (0-32 characters) of the user that created or last activated the row.
prDateTime	RO	Date time (UTC) when the row was created or last activated: <ul style="list-style-type: none"> <li>• <b>yyyy-mm-dd,hh:mm:ss.sss,+0.0</b></li> </ul>
prConfirm	R/W	Command confirmation: <ul style="list-style-type: none"> <li>• <b>no(0)</b>—Value defaulted on row creation and when prRowStatus is changed to notInService in order to change other row values</li> <li>• <b>yes(1)</b>—Value required for row activation (command execution)</li> </ul> <p>The requirement to change a row's prConfirm from no to yes reduces the probability of accidentally re-executing a provisioning command.</p>
prRowStatus	R/W	Table row status: <ul style="list-style-type: none"> <li>• <b>active(1)</b>—Normal row state</li> <li>• <b>notInService(2)</b>—Row disabled for editing</li> <li>• <b>notReady(3)</b>—One or more required row entries are not set</li> <li>• <b>createAndWait(5)</b>—Create then edit row</li> <li>• <b>destroy(6)</b>—Delete row</li> </ul>

## System Provisioning Port List Formats

The prInputPorts and prOutputPorts objects accept two entry formats: port text list and port hex octets.

Port List Format	Description
Input Port Text List (0-255 characters)	<p>The ports are specified by a comma separated value text string that may include ranges. The ports may be specified by their short port number (1 ... 192) or their full 5-digit port number (10001 ... 10192). For example, both of the following input port list strings:</p> <pre>"1,3-5,10,192"</pre> <pre>"10001,10003-10005,10010,10192"</pre> <p>specify the following input ports:</p> <pre>10001 10003 10004 10005 10010 10192</pre>
Output Port Text List (0-255 characters)	<p>The ports are specified by a comma separated value text string that may include ranges. The ports may be specified by a short port number (1 ... 192) or their full 5-digit port number (20001 ... 20192). For example, both of the following output port list strings:</p> <pre>"1,3-5,10,192"</pre> <pre>"20001,20003-20005,20010,20192"</pre> <p>specify the following output ports:</p> <pre>20001 20003 20004 20005 20010 20192</pre>
Input Port Hex Octets (0-193 octets)	<p>The ports are specified by one hexadecimal octet (byte) for each port. The first octet must be x'00', it indicates that the hex octet format is being used. This format does not support ranges. For example, the following octet list:</p> <pre>x'00 01 03 04 05 0A C0'</pre> <p>specifies these ports:</p> <pre>10001 10003 10004 10005 10010 10192</pre>
Output Port Hex Octets (0-193 octets)	<p>The ports are specified by one hexadecimal octet (byte) for each port. The first octet must be x'00', it indicates that the hex octet format is being used. This format does not support ranges. For example, the following octet list:</p> <pre>x'00 01 03 04 05 0A C0'</pre> <p>specifies these ports:</p> <pre>20001 20003 20004 20005 20010 20192</pre>

---

**NOTE:** The port text list format is convenient for direct “human” entry via an SNMP browser. However, due to the SNMP 255 character limit on octet strings, it is not possible to list all ports individually. The hex octet format supports specification of all 192 ports individually in any order and is simple to implement on automated/scripted interfaces. Port text list ranges must be increasing (e.g., “1-10” is supported, while “10-1” is not).

---

## Making Multiple Connections

This operation is analogous to the TL1 command ENT-CRS-FIBER listed below; the input list and output lists are expanded and connections are initiated concurrently from the first input port to the first output port, the second input port to the second output port, etc. The operation is asynchronous, meaning that the SNMP response occurs after the set values have been validated and the connects are initiated, but before the connections are complete and the iosConnectionTable is updated (see “Connection Table—iosConnectionTable ” on page 94).

```
ENT-CRS-FIBER::<inputlist>,<outputlist>:<ctag>:::OPMODE=async
[ ,CONNNAME=<connname> ] ;
```

Per TL1 ENT-CRS-FIBER command operation:

- Existing connections that are in conflict with the specified connections will be automatically disconnected.
- Existing connections that are also in the specified connections will not be affected (they will not be disconnected and reconnected).
- Existing connections that are not in conflict with the specified connections will not be affected (this operation does not behave like the ClickFlow “Connect topology and disconnect all other ports” operation).

To connect a list of input ports to a list of output ports, and optionally name the connections:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser’s Create Row facility, select Create and Wait, and set the prIndex (table index) to an unsigned integer value that is not already present in the table. For example, “4” would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with “Resource Unavailable” if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets)
  - b. Set the row's prOutputPorts (output port list, 1-255 characters / 2-193 octets)
  - c. Set the row's prCommand to **connect(1)**
  - d. Optionally set the row's prValue (connection name, 0-32 characters)
  - e. Optionally set the row's prDescr (description, 0-128 characters)
  - f. Set the row's prConfirm to **yes(1)**
  - g. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr value is used only to document the table row; it may provide value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful:
  - a. Optionally get and check the row's prStatus:
    - **fail(0)**—The connection request was rejected. For example, the input port list and output lists are different length, or all specified connections were prohibited because their ports were not installed or their connection is prohibited by the user's VACM configuration.
    - **pass(1)**—The connection command was issued.
  - b. Optionally check connection status for each input port in the connection table, see Figure 22 on page 95.
5. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted, it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Making All Connections

This operation is analogous to the TL1 command ENT-CRS-FIBER listed below; all "normal" inputs are connected to all "normal" outputs (e.g., 10001 to 20001, 10002 to 20002, etc.). If there are more input ports than output ports, or vice-versa, then only the common ports are connected. The operation is asynchronous, meaning that the SNMP response occurs after connects are initiated, but before the connections are complete and the iosConnectionTable (Figure 22 on page 95) is updated.

```
ENT-CRS-FIBER::input,output:<ctag>::OPMODE=async,PCAT=nor;
```

To connect all "normal" input ports to all "normal" output ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).

2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the prIndex (table index) to an unsigned integer value that is not already present in the table. For example, "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **connectFull(2)**
  - b. Optionally set the row's prValue (connection name, 0-32 characters)
  - c. Optionally set the row's prDescr (description, 0-128 characters)
  - d. Set the row's prConfirm to **yes(1)**
  - e. Set the row's prRowStatus to **active(1)**
4. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted, it may be subsequently reused (see "Reissuing a Prior Operation" on page 75).

---

## Breaking Multiple Connections

This operation is analogous to the TL1 command DLT-CRS-FIBER listed below; the port list is expanded and those ports that are involved in a connection are concurrently disconnected. If both an input list and output list are defined, then the output list takes precedence. The operation is asynchronous: the SNMP response occurs after the set values have been validated and disconnects are initiated, but before the disconnects are complete and the iosConnectionTable (Figure 22 on page 95) is updated.

```
DLT-CRS-FIBER::<portlist>:<ctag>::OPMODE=async;
```

To disconnect a list of input/output ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the prIndex (table index) to an unsigned integer value that is not already present in the table. For example, "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Either set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets), or set the row's prOutputPorts (output port list, 1-255 characters / 2-193 octets)
  - b. Set the row's prCommand to **disconnect(3)**

- c. Optionally set the row's prDescr (description, 0-128 characters)
- d. Set the row's prConfirm to **yes(1)**
- e. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 6 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful by retrieving and checking the row's prStatus:
  - **fail(0)**—The disconnect request was rejected. For example, both the input port and output port lists are specified and are different length, or all specified disconnects were prohibited because their ports were not installed or their connection / disconnection is prohibited by the user's VACM configuration.
  - **pass(1)**—The disconnection command was issued.
5. Optionally check that the disconnected input ports are not in the connection table, see Figure 22 on page 95.
6. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Breaking All Connections

This operation is analogous to the TL1 DLT-CRS-FIBER command listed below; all ports are disconnected. The operation is asynchronous: the SNMP response occurs after connects are initiated, but before the disconnections are complete and the iosConnectionTable (Figure 22 on page 95) is updated.

```
DLT-CRS-FIBER::all:<ctag>::OPMODE=async;
```

To disconnect all (both normal and reference) input and output ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the prIndex (table index) to an unsigned integer value that is not already present in the table. For example, "4" would be valid for the table shown Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **disconnectFull(4)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**
4. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Naming Multiple Connections

This operation is analogous to the TL1 command SET-CRS-NAME listed below; the port list is expanded and for those ports that are involved in a connection the connection is named. If both an input list and output list are defined, then the input list takes precedence.

```
SET-CRS-NAME::<portlist>:<ctag>:::CONNNAME=<connname>;
```

To set the connection name of existing connections for the listed input/output ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the prIndex (table index) to an unsigned integer value that is not already present in the table. For example, "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Either set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets) or set the row's prOutputPorts (output port list, 1-255 characters / 2-193 octets)
  - b. Set the row's prValue (connection name, 0-32 characters)
  - c. Set the row's prCommand to **setConnectionName(5)**
  - d. Optionally set the row's prDescr (description, 0-128 characters)
  - e. Set the row's prConfirm to **yes(1)**
  - f. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the row is not deleted directly after use because the user intends to reissue the operation.

---

4. Optionally verify the provisioning operation was successful by getting and checking the row's prStatus:



- **fail(0)**—The request was rejected. For example, both the input port and output port lists are specified and are different length, or all specified ports are not installed or their connection/disconnection is prohibited by the user's VACM configuration.
  - **pass(1)**—The command was issued.
5. Optionally check connection name for each input port in the connection table (see Figure 22 on page 95).
  6. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Backing Up the System Configuration

Back up the system configuration to a system configuration XML file in the system's download directory (/dnld).

This operation is analogous to the TL1 COPY-CFG command:

```
COPY-CFG:::<ctag>:::[DESCR=<descr>];
```

The back up system configuration command is asynchronous, meaning that the SNMP response occurs after the set values have been validated and the backup initiated, but before the configuration file is created, so the table row's prStatus should be polled until it changes from pending(4) to pass(1) or fail(0). Backup usually completes in less than 1 second.

The system configuration XML file includes identifying information such as: system name, serial number, when the file was created, by whom (user ID/community name) and optional user-entered comments/description. The file also includes read-only information about the system (hardware features, licenses, and embedded software version).

The system configuration may be backed up to an XML file and restored from an XML file via the ClickFlow, SNMP, and TL1 interfaces. HTTPS (ClickFlow), FTP (the COPY-RFILE command in TL1), and SCP/SFTP may be used to copy the system configuration file to/from a Linux server or Windows PC.

To backup the system configuration:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).

2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysBackup(6)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The optional prDescr text is saved in the <userComments> XML file element. The ClickFlow Restore System Configuration window will display the full comment, and the TL1 RTRV-CFG command will display the first 32 characters of the comment.

---

4. Optionally verify the backup operation was successful: Get and check the row's prStatus:
  - **fail(0)** - The command is complete and failed.
  - **pass(1)** - The command is complete and successful.
  - **pending(4)** - The command is not yet complete.
5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

After completing system configuration backup via SNMP, the system configuration XML file (iosconfigbackup.xml) may be copied (exported) from the systems /dnld directory to a Linux/Windows directory via SCP. The following is an example under Windows using the PuTTY distribution pscp command; see the Glimmerglass IOS Installation and Maintenance Guide for more information.

```
pscp -pw <password> admin@<ipaddress>:/dnld/iosconfigbackup.xml .
```

Where:

- <password> is the Maintenance Console's "admin" password
- <ipaddress> is the system's IP address

## Restoring the System Configuration

Restore the system configuration from a system configuration XML (backup) file in the system's download directory (/dnld).

This operation is analogous to the TL1 APPLY-CFG command:

```
APPLY-CFG:::<ctag>;
```

The restore system configuration command is asynchronous, meaning that the SNMP response occurs after the set values have been validated and the restore initiated, but before the restore is completed, so the table row's prStatus should be polled until it changes from pending(4) to pass(1) or fail(0). Restore usually completes in 5 to 10 seconds. If the restored configuration revised the system network parameters (Ethernet IP address, gateway, etc.) the network parameter changes will not take effect until the next system reboot. Similarly if the applied configuration revised the startup parameters (TCP port numbers) the startup parameter changes will not take effect until the next system restart or reboot.

The system configuration XML file includes identifying information such as: system name, serial number, when the file was created, by whom (user-id/community-name) and optional user entered comments/description. The file also includes read-only information about the system (hardware features, licenses and embedded software version); the read-only information is not restored by sysRestore. If the system configuration XML file has format errors, or does not match the system in key areas such as port counts, then the configuration will not be restored. ClickFlow Restore System Configuration will display information re the XML file errors.

The system configuration may be backed up to an XML file and restored from an XML file via the ClickFlow, SNMP and TL1 interfaces. HTTPS (ClickFlow), FTP (the COPY-RFILE command in TL1), and SCP/SFTP may be used to copy the system configuration file to/from a Linux server or Windows PC.

Before initiating system configuration restore via SNMP, the system configuration (backup) XML file (iosconfigbackup.xml) must be copied to the systems /dnld directory. The following is an example under Windows using the PuTTY distribution pscp command; see the Glimmerglass IOS Installation and Maintenance Guide for more information.

```
pscp -pw <password> iosconfigbackup.xml admin@<ipaddress>:/dnld
```

Where:

- <password> is the Maintenance Console's "admin" password
- <ipaddress> is the system's IP address

To restore the system configuration:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysRestore(7)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the restore operation was successful by doing one of the following:
  - Get and check the row's prStatus:
    - **fail(0)** - The command is complete and failed.
    - **pass(1)** - The command is complete and successful.
    - **pending(4)** - The command is not yet complete.
  - Wait for and check the iosSystemAdminTrap trap:
    - **sysRestore(1)**, **taskCompleted(2)**, or **taskFailed(4)**

5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Saving the System Configuration

Save configuration changes to persistent memory (non-volatile memory). Configuration changes not saved will be lost on a power-cycle of the system. By default system configuration changes are saved every 60 seconds, see iosPersistConfiguration on page 48. However, the user may elect to disable automatic configuration saves and explicitly save configuration changes.

This operation is analogous to the TL1 WRT-DB command:

```
WRT-DB:::<ctag>;
```

To save system configuration changes:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).

2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysCheckpoint(8)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 4 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a prior operation."

---

## Upgrading System Software

The system contains two non-volatile Flash RAM partitions (0 and 1), both containing the system software (Linux OS and Intelligent Optical Switch application) and the system configuration data:

- Boot Partition—Contains the current system software release; on a power-cycle or user-initiated reboot the system will boot from the Boot Partition.
- Rollback Partition—Contains the previous software release; if software rollback is initiated the roles of the two partitions are reversed and the system is booted from the former rollback partition.

On a software upgrade the rollback partition is upgraded to the new software, then the roles of the two partitions are reversed, and the system is booted from the former rollback partition.

The system software upgrade process consists of three phases:

Upgrade Phase	Description
1: Upload	Upload the software upgrade file to the system's volatile /dnld directory. The upgrade file size is approximately 17MB. The duration of this upgrade phase is a function of the network speed and the latency between the server/PC containing the upgrade file and the system being upgraded.

Upgrade Phase	Description
2: Upgrade	Verify the upgrade file and then upgrade the non-volatile inactive/rollback partition with the new kernel and application files. System availability is unaffected by this upgrade phase; the system continues to operate under the current release. The duration of this upgrade phase is 3 - 7 minutes as a function of the system model.
3: Reboot	Reboot to activate the upgraded partition. If the upgraded partition is booted successfully, then the roles of the boot and rollback partitions are reversed, otherwise the original boot partition is rebooted. The system is unavailable during this reboot phase. The duration of this final upgrade phase is 2 - 3 minutes.

The three software upgrade phases are supported by each of the user interfaces (ClickFlow, TL1, SNMP, and Maintenance Console) as follows:

Interface	Phase	Description
ClickFlow	Upload	Upgrade System Software window - Upgrade phase 1: Upload ...
	Upgrade	Upgrade System Software window - Upgrade phase 2: Upgrade ...
	Reboot	Upgrade System Software window - Upgrade phase 3: Reboot ...
TL1	Upload	COPY-RFILE:::<ctag>::SRC=<src>,DEST=<dest>;
	Upgrade	APPLY-UPGRADE:::<ctag>;
	Reboot	INIT-SYS:::<ctag>::SOFTREBOOT;
SNMP	Upload	Not supported; upload via SCP/SFTP, ClickFlow (HTTPS), TL1 (FTP), or Maintenance Console (FTP)
	Upgrade	sysProvisionTable.prCommand sysUpgrade
	Reboot	sysProvisionTable.prCommand sysReboot
Maintenance Console	Upload	Main Menu selection "Transfer File to System using FTP"
	Upgrade	Main Menu selection "Upgrade software", optionally includes reboot
	Reboot	Main Menu selection "Reboot"
SCP/SFTP	Upload	Push the upgrade file via SCP/SFTP from a Linux server or Windows PC

The three software upgrade phases do not have to be directly contiguous. For example, a Linux server with TL1 automation scripts could perform the non-disruptive upload and upgrade phases during the normal system high availability hours and then be scheduled to reboot all of the systems at midnight or during a scheduled maintenance period.

---

**NOTE:** Rebooting a system after a system software upgrade phase failure will simply reboot the current release.

---

In addition, the three software upgrade phases do not have to be performed by the same interface. For example, for the upload phase a Linux server script could push the upgrade files to each system via SCP/SFTP, and then complete the remaining phases by TL1 or SNMP.

The SNMP system upgrade command is asynchronous, meaning that the SNMP response occurs after the table values have been validated and the upgrade initiated, but before the upgrade is completed, so the table row's prStatus should be polled until it changes from pending(4) to pass(1) or fail(0).

This operation is analogous to the TL1 APPLY-UPGRADE command:

```
APPLY-UPGRADE:::<ctag>;
```

Before initiating upgrade via SNMP, the system software upgrade file (GGNIOUSUPG.tgz) must be copied to the systems /dnld directory. The following is an example under Windows using the PuTTY distribution pscp command; see the *Glimmerglass IOS Installation and Maintenance Guide* for more information.

```
pscp -pw <password> GGNIOUSUPG.tgz admin@<ipaddress>:/dnld
```

Where:

- <password> is the Maintenance Console's "admin" password
- <ipaddress> is the system's IP address

To initiate system software upgrade:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysUpgrade(9)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**



---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Wait for the upgrade operation to complete and verify it was successful by doing one of the following:
  - Either get and check the row's prStatus:
    - **fail(0)** - The command is complete and failed.
    - **pass(1)** - The command is complete and successful.
    - **pending(4)** - The command is not yet complete.
  - Or wait for and check the iosSystemAdminTrap trap:
    - **sysUpgrade(5)**, **taskCompleted(2)**, or **taskFailed(4)**

5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

6. To activate the upgraded inactive/rollback partition, the system must be rebooted. See "Rebooting/Shutting Down/Restarting System" on page 68.

## Rolling Back System Software

The system contains two non-volatile Flash RAM partitions (0 and 1), both containing the system software (Linux OS and Intelligent Optical Switch application) and the system configuration data. One of the two partitions is marked as the Boot Partition; on a power-cycle or user-initiated reboot the system will boot from the Boot Partition. The other partition is the Rollback Partition. If a software rollback is initiated, the roles of the two partitions are reversed, the system is booted from the former rollback partition, and the system configuration reverts to that at the time of the prior system software upgrade.

System software rollback is supported by the four system interfaces as follows:

Interface	Description
ClickFlow	Rollback System Software window
TL1	APPLY-ROLLBACK:::<ctag>;
SNMP	sysProvisionTable.prCommand sysRollback
Maintenance Console	Main Menu selection "Rollback to other partition"

To initiate system software rollback:



1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysRollback(10)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. The rollback request may be accepted or rejected:
  - The rollback request is accepted:
    - System shutdown and rollback is initiated
    - An iosSystemAdminTrap sysRollback(6) taskInitiated(1) trap is posted
    - An iosSystemAdminTrap sysShutdown(1) taskInitiated(1) is posted
    - An iosSystemAdminTrap sysStartup(2) taskCompleted(2) trap is posted on completion of reboot
  - The rollback request is rejected:
    - The rollback request may be rejected because the most recent upgrade has already been rolled back, or the most recent upgrade was not completed.
    - The row's prStatus is fail(0)
5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Rebooting/Shutting Down/Restarting System

The table below describes the reboot, shutdown, and restart system maintenance operations:

prCommand	Equivalent TL1 Command	Description
sysReboot(11)	INIT-SYS:::<ctag>::SOFTREBOOT;	Reboot the system; the connections are not affected; sysShutdown taskInitiated and sysStartup taskCompleted traps are posted.
sysShutdown(12)	INIT-SYS:::<ctag>::STOPONLY;	Shutdown the system, in preparation for power-off; all connections are broken; a sysShutdown taskInitiated trap is posted.
sysRestart(13)	INIT-SYS:::<ctag>::RESTART;	Restart the switch control application; the connections are not affected; sysShutdown taskInitiated and sysStartup taskCompleted traps are posted

To initiate a system reboot, shutdown, or restart:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

3. In the provisioning table row:
  - a. Set the row's prCommand to one of the following:
    - **sysReboot(11)**
    - **sysShutdown(12)**
    - **sysRestart(13)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row because he/she intends to subsequently reissue the operation.

4. Optionally wait for the sysShutdown(1) trap and then the sysStartup(2) trap (see "IOS System Administration Trap Example—iosSystemAdminTrap" on page 32).

5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Resetting System Configuration to Factory Defaults

This operation breaks all connections, clears the system configuration database, and reboots.

The system's current IP configuration is not defaulted. Therefore, remote network access to the system is not affected by the reset to defaults.

The passwords for all default system accounts are reset to default. These passwords will need to be used when accessing the system via the Maintenance Console, ClickFlow/TL1, or SNMP after the system initializes.

The Runtime parameter options ("System Operation Options—sysOperation " on page 47) will only be defaulted on new systems (Model Numbers GG112-C, GG514-C, GG528-C, or higher). For older systems, these values must be defaulted by the user through ClickFlow, TL1, or SNMP.

To initiate system reset to factory defaults:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows (optional provisioning history).

---

3. In the provisioning table row:
  - a. Set the row's prCommand to **sysResetFactory(14)**
  - b. Optionally set the row's prDescr (description, 0-128 characters)
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row because he/she intends to subsequently reissue the operation.

---

4. Optionally wait for the iosSystemAdminTrap sysResetFactory(3) taskInitiated(1) trap. An iosSystemAdminTrap sysStartup(2) taskCompleted(2) trap will not occur because the snmpTargetAddrTable has been reset to installation defaults.

5. Optionally delete the row entry: Set the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Assigning a Port Group to a list of Ports

Port grouping allows an administrator to explicitly allow or inhibit connections between ports. When the Port Grouping license is enabled (see "System Configuration—sysConfiguration" on page 45), port groups may be configured (see "Port Grouping - iosPortGroupTable" on page 75) and ports may be assigned via the setPortGroup provisioning command (this section) or via the port's port table (iosInputPortTable, iosOutputPortTable, iosVOAPortTable, and iosPMCPortTable).

---

**NOTES:**

- A port may be assigned only to a single port group.
- A port must be assigned to a port group; if a port is not assigned to a user-created port group, then it is automatically assigned to the default port group OpenGroup.
- If the port grouping license is disabled, all ports are assigned to the default port group OpenGroup.

---

This operation is analogous to the TL1 command SET-CFG-FIBER listed below: the input list and output lists are expanded and the port group is assigned to the specified ports. The port tables (iosInputPortTable, iosOutputPortTable, iosVOAPortTable, and iosPMCPortTable) PortGroup entries are updated for the specified port numbers.

```
SET-CFG-FIBER::<inputlist>&<outputlist>:<ctag>::PGROUP=<groupname>];
```

To assign a port group to a list of ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets)
  - b. Set the row's prOutputPorts (output port list, 1-255 characters / 2-193 octets)
  - c. Set the row's prCommand to **setPortGroup(15)**
  - d. Set the row's prValue (port group name, 1-32 characters)
  - e. Optionally set the row's prDescr (description, 0-127 characters)

- f. Set the row's prConfirm to **yes(1)**
- g. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because the user intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful:
  - a. Get and check the row's prStatus:
    - **fail(0)** - The set port group command was rejected, for example the port group name does not exist.
    - **pass(1)** - The set port group command was issued.

5. Optionally delete the row entry:
  - a. Set the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" on page 75.

---

## Assigning a Signal Threshold to a List of Ports

A signal threshold (see "Signal Threshold Table—iosSigThresholdTable " on page 98) may be assigned ports via the port table of which the port is a member (e.g., input, output, VOA, PMC); however one SNMP set is required for each port. The setPortThreshold provisioning command supports assigning a signal threshold to a list of ports.

This operation is analogous to the TL1 command SET-SIGTHRESH-FIBER listed below: the port list is expanded and the signal threshold is assigned to the specified ports.

```
SET-SIGTHRESH-FIBER::<plist>:<ctag>:::SIGTHRESH=<sigthreshname>;
```

To assign a signal threshold to list of ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets)

- b. Set the row's prOutputPorts (output port list, 1-255 characters/2-193 octets)
- c. Set the row's prCommand to **setPortThreshold(16)**
- d. Set the row's prValue (signal threshold name, 1-32 characters)
- e. Optionally set the row's prDescr (description, 0-127 characters)
- f. Set the row's prConfirm to **yes(1)**
- g. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful by checking the row's prStatus:
  - **fail(0)** - The set port signal threshold command was rejected, for example the signal threshold name does not exist.
  - **pass(1)** - The set port signal threshold command was issued.
5. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" below.

---

## Assigning a Waveband to a List of Ports

The Waveband (either 1310 or 1550) may be assigned to input ports via the port table of which the input port is a member (e.g., input, VOA, PMC). However, one SNMP set is required for each port. The setPortWaveband provisioning command supports assigning a signal threshold to a list of input ports.

This operation is analogous to the TL1 command SET-SIGBAND-FIBER listed below: the input port list is expanded and the waveband is assigned to the specified ports. Note that a waveband cannot be assigned to output ports: including output ports will invalidate the operation.

```
SET-SIGBAND-FIBER::<IPLIST>:<ctag>::SIGBAND=<waveband>;
```

To assign a waveband to list of ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets)
  - b. Set the row's prValue to either **1310** or **1550** per the information below:
    - **1310**: Waveband of signal at input is between 1260nm and 1460nm
    - **1550**: Waveband of signal at input is between 1460nm and 1630nm
  - c. Set the row's prCommand to **setPortWaveband(17)**
  - d. Optionally set the row's prDescr (description, 0-127 characters)
  - e. Set the row's prConfirm to **yes(1)**
  - f. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful by checking the row's prStatus:
  - **fail(0)** - The set port waveband command was rejected
  - **pass(1)** - The set port waveband command was issued.
5. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" below.

---

## Assigning an Alarm Severity to a List of Ports

The severity for STMIN, STMAX, and CSFLT alarms may be changed for a port or list of ports. This may be done one SNMP set at a time by changing the value from the port's port table. The setPortSTMIN, setPortSTMAX and setPortCSFLT provisioning commands allow each alarm severity to be set on a list of ports.

This operation is analogous to the TL1 command SET-CFG-FIBER listed below: the port list is expanded and each severity is assigned to the specified ports. Note that the CSFLT severity **ONLY** applies to output ports. Unlike the TL1 command, the provisioning command operates on one alarm type (STMIN, STMAX or CSFLT) at a time by specifying the appropriate provisioning command (setPortSTMIN, setPortSTMAX or setPortCSFLT).

```
SET-CFG-FIBER::<PLIST>:<ctag>:::STMINSEV=<sev>,STMAXSEV=<sev>,CSFLTSEV=<sev>;
```

To assign a severity to a list of ports:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50)



2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the new prIndex (table index) to an unsigned integer value that is not already present in the table, for example "4" would be valid for the table shown in Figure 13 on page 50.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProvisionTable already has 50 rows.

---

3. In the provisioning table row:
  - a. Set the row's prInputPorts (input port list, 1-255 characters / 2-193 octets)

---

**NOTE:** Do not specify prInputPorts if the prCommand (below) to be used is **setPortCSFLT(20)**

---

- b. Set the row's prOutputPorts (output port list, 1-255 characters/2-193 octets)
  - c. Set the row's prCommand for the desired alarm type (one of the below):
    - **setPortSTMIN(18)**
    - **setPortSTMAX(19)**
    - **setPortCSFLT(20)**
  - d. Set the row's prValue to the desired severity (one of the below):
    - **critical**
    - **major**
    - **minor**
    - **notice**
    - **clear**
  - e. Optionally set the row's prDescr (description, 0-127 characters)
  - f. Set the row's prConfirm to **yes(1)**
  - g. Set the row's prRowStatus to **active(1)**

---

**NOTE:** The prDescr is used only to document the table row; it may have value if the user does not delete the row (step 5 below) because he/she intends to subsequently reissue the operation.

---

4. Optionally verify the provisioning operation was successful by checking the row's prStatus:
  - **fail(0)** - the set port alarm severity command was rejected.
  - **pass(1)** - the set port alarm severity command was issued.
5. Optionally delete the row entry by setting the row's prRowStatus to **destroy(6)**.

---

**NOTE:** If the row is not deleted it may be subsequently reused, see "Reissuing a Prior Operation" below.

---



## Reissuing a Prior Operation

In provisioning procedures described above (page 54 through page 75), a table row is created, the appropriate row values entered, the operation is initiated, and the row is optionally deleted. If the row is not deleted, it remains as a history of provisioning operations (up to a total of 50 rows) and the operation can be reissued simply by changing the row status:

1. Browse to and view the iosProvisionTable (Figure 13 on page 50).
2. In the provisioning table row to be reissued/reused:
  - a. Set the row's prRowStatus to **notInService(2)**
  - b. Optionally change one or more of the row's values
  - c. Set the row's prConfirm to **yes(1)**
  - d. Set the row's prRowStatus to **active(1)**

## Port Grouping - iosPortGroupTable

A table with one row for each Port Group (Figure 14 on page 76) per the ClickFlow Port Group window (menu selection **Configure > Port Group**).

Port grouping allows an administrator to explicitly allow or inhibit connections between ports. When the Port Grouping license is enabled (see "System Configuration—sysConfiguration" on page 45), port groups may be configured and ports may be assigned among these port groups. A total of 48 port groups are permitted (including OpenGroup). Each group may allow connections from 8 other user defined port groups. By default, all ports are initially assigned to the system default port group named "OpenGroup".

Port Group Ports	Connection Allowed by Port Grouping
Output ports	To input ports in the same port group
	To input ports in the OpenGroup port group
	To input ports of port groups specified in the port group's Allow list
Input ports	To output ports in the same port group
	To output ports in the OpenGroup port group

- NOTES:**
- A port may only be assigned to a single port group.
  - A port must be assigned to a port group; if a port is not assigned to a user created port group then it is automatically assigned to the default port group OpenGroup.
  - If the port grouping license is disabled, all ports are assigned to the default port group OpenGroup.
  - All ports may be assigned to port groups other OpenGroup, hence the default port group OpenGroup may be "empty".
  - The port group connection rules are not symmetric, so you may optionally allow connections from group A to group B but not vice-versa.
  - Port grouping may be used in conjunction with user port privileges configured by VACM and USM for SNMP users and the Virtual Private Switch feature for ClickFlow and TL1 users.

The port group names and permissions (port group allow list) are established via the iosPortGroupTable (this section). Ports may be assigned to a previously-created port group via the setPortGroup provisioning command (see "Assigning a Port Group to a list of Ports" on page 70) or via the port's port table (iosInputPortTable, iosOutputPortTable, iosVOAPortTable and iosPMCPortTable).

Figure 14 IOS Port Group Table—iosPortGroupTable

The screenshot shows a web interface for the 'iosPortGroupTable'. At the top, there is an 'OID' field with the value '.1.3.6.1.4.1.30742.1.4.1.4.2' and an 'Operations' dropdown set to 'Table View'. Below this is a 'Result Table' tab for '192.168.1.32 - iosPortGroupTable'. The table has a toolbar with 'Rotate', 'Refresh', 'Export', 'Poll', 'SNMP SET', and 'Create Row' buttons. The table itself has 3 columns and 6 rows of data.

	1	2	3
pGroupIndex	red	black	OpenGroup
pGroupName	red	black	OpenGroup
pGroupAllow	OpenGroup	OpenGroup	OpenGroup
pGroupDescr	Unencrypted,Classified	Encrypted	IOS Default Port Group
pGroupRowStatus			

The table below describes the IOS Port Group subtree elements:

Element	Read/Write	Description
pGroupIndex	R/W	Table row index, same as pGroupName
pGroupName	RO	Port group name (1-32 characters)
pGroupAllow	R/W	Port group allow list (0-255 characters) A list of port group names separated by a space character. Input ports in these port groups may be connected to output ports in this port group (defined by pGroupName above).

Element	Read/Write	Description
pGroupDescr	R/W	Port group description (0-32 characters) Optional port group description
pGroupRowStatus	R/W	Table Row Status: <ul style="list-style-type: none"> <li>• <b>active(1)</b> Normal row state</li> <li>• <b>notInService(2)</b> Row created but not yet activated</li> <li>• <b>destroy(6)</b> Delete row (delete server)</li> </ul>

## Adding a Port Group

To add a port group:

1. Browse to and view the iosPortGroupTable (Figure 14 on page 76)
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the table index to the new unique port group name (1-32 characters).

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the ios-PortGroupTable already has 48 rows (port groups).

3. Optionally revise the row's pGroupAllow (Port Group Allow list, a list of one to eight port group names separated by space, 1-255 characters).

**NOTE:** The port group names listed in the allow list must have already been created, hence you may have to define the port groups without changing the allow list and then revise the port groups (see "Revising an Existing Port Group" below) specifying the desired allow list.

4. Optionally set the row's pGroupDescr (Port Group Description, 0-32 characters)
5. Set the row's pGroupRowStatus to **active(1)**.

## Revising an Existing Port Group

To revise a port group:

1. Browse to and view the iosPortGroupTable (Figure 14 on page 76)

2. For the port group row to be revised:
  - a. Set the row's pGroupStatus to **notInService(2)**
  - b. Optionally revise the row's pGroupAllow (Port Group Allow list, a list of port group names separated by space, 1-255 characters).
  - c. Optionally revise the row's pGroupDescr (Port Group Description, 0-32 characters)
  - d. Set the row's pGroupRowStatus to **active(1)**.

## Deleting an Existing Port Group

To delete/remove a port group:

1. Browse to and view the iosPortGroupTable (Figure 14 on page 76)
2. For the port group row to be deleted:
  - a. Set the row's pGroupStatus to **destroy(6)**

---

**NOTE:** The ports that were assigned to the deleted port group will be automatically reassigned to port group OpenGroup.


---

## System Clock - sysClock

A subtree listing the system clock date/time, NTP (Network Time Protocol) service configuration, and synchronization status (Figure 15) per the ClickFlow Date/Time Configuration window (menu selection **System > System Configuration > Date/Time**).

- **clockStatus synchronized(1)** is reported when the NTP service is enabled and the system clock is synchronized with one of the listed servers. Synchronization will normally be reported approximately 5 minutes after an NTP configuration change, presuming that one or more of the NTP servers are reachable. synchronized(1) is also reported when the NTP service is disabled.
- **clockStatus drifting(0)** is reported when the NTP service is enabled and the system clock is not synchronized with any of the listed servers.

Figure 15 IOS System Clock Subtree - sysClock

OID: .1.3.6.1.4.1.30742.1.4.1.5.1	Operations: Get Subtree	
Result Table		
Name/OID	Value	Type
clockDateTime.0	2013-6-22,0:41:25.123,+0:0	OctetString
clockSource.0	ntp (1)	Integer
clockStatus.0	drifting (2)	Integer
clockNtpServerA.0	192.168.1.8	IpAddress
clockNtpServerB.0	0.0.0.0	IpAddress
clockNtpServerC.0	0.0.0.0	IpAddress

The table below describes the IOS System Clock subtree elements:

Element	Read/Write	Description
clockDateTime	R/W	System Date, Time and UTC offset (0): • <b>yyyy-mm-dd,hh:mm:ss.sss,+0:0</b>
clockSource	R/W	Clock Source: • <b>rtc(0)</b> NTP service disabled • <b>ntp(1)</b> NTP service enabled
clockStatus	RO	Clock Synchronization status: • <b>synchronized(1)</b> • <b>drifting(2)</b>
clockNtpServerA	R/W	NTP Server IP Address (0.0.0.0 for no server): • <b>xxx.xxx.xxx.xxx</b>
clockNtpServerB	R/W	NTP Server IP Address (0.0.0.0 for no server): • <b>xxx.xxx.xxx.xxx</b>
clockNtpServerC	R/W	NTP Server IP Address (0.0.0.0 for no server): • <b>xxx.xxx.xxx.xxx</b>

**NOTE:** As defined by the IOS MIB the clockDateTime object is formatted per the SNMPv2-TC DateAndTime textual convention, the MIB browser must convert the text to/from 11 hex octets. If clockSource is ntp(1) then clockDateTime is read-only.

Related SNMP Traps	Description
iosSystemAdminTrap iosSysAdminTask=sysClockRTC(8) iosSysAdminTaskStatus=taskCompleted(2)	Posted when clockSource is set to rtc(0)

Related SNMP Traps	Description
iosSystemAdminTrap iosSysAdminTask=sysClockNTP(9) iosSysAdminTaskStatus=taskInitiated(2)	Posted when clockSource is set to ntp(1)
iosComponentStateTrap iosTrapSeverity=minor(3) iosComponentType=sysClock(19) iosComponentCondition=ccNTPFLT(7)	Posted (alarm) when the clockSource is ntp(1) and either: <ul style="list-style-type: none"> <li>The clockStatus never transitions from drifting(2) to synchronized(1) upon setting the clockSource to ntp(1) or</li> <li>The clockStatus transitions from synchronized(1) to drifting(2).</li> </ul>
iosComponentStateTrap iosTrapSeverity=clear(6) iosComponentType=sysClock(19) iosComponentCondition=ccNTPFLT(7)	Posted (alarm clear) when the clockSource is ntp(1) and the clockStatus transitions from drifting(2) to synchronized(1). This occurs to clear the trap mentioned above.


## System Network - sysNetwork

A subtree listing the system network information (Figure 16) per the ClickFlow Name/IP Configuration window (menu selection **System > System Configuration > Date/Time**) and Startup Options window (menu selection **System > System Configuration > Startup Options**).

Changes to the network section (netHostName though netEther2Mask) will not take effect until after the next system reboot.

Changes to the port section (netTl1FastPort though netSnmpPort) will not take effect until after the next system restart or system reboot.

Figure 16 IOS System Network Subtree - sysNetwork

OID: .1.3.6.1.4.1.30742.1.4.1.5.2		Operations: Get Subtree	
Result Table			
Name/OID	Value	Type	
netHostName.0	BD0466	OctetString	
netGateway.0	192.168.1.254	IpAddress	
netEtherPorts.0	2	Gauge	
netEther1Address.0	192.168.1.32	IpAddress	
netEther1Mask.0	255.255.255.0	IpAddress	
netEther2Address.0	192.168.3.200	IpAddress	
netEther2Mask.0	255.255.255.0	IpAddress	
netTL1FastPort.0	10034	Gauge	
netTL1FastSSLPort.0	10036	Gauge	
netTL1SmartPort.0	10033	Gauge	
netTL1SmartSSLPort.0	10035	Gauge	
netTL1SSLEnable.0	off (0)	Integer	
netWebPort.0	80	Gauge	
netWebSSLPort.0	443	Gauge	
netWebSSLEnable.0	on (1)	Integer	
netSnmpPort.0	161	Gauge	

The table below describes the IOS System Network subtree elements:

Element	Read/Write	Description
netHostName	R/W	System Host Name: <ul style="list-style-type: none"> <li>1-63 characters, alphanumeric and dash ("-") only.</li> </ul> Installation default is derived from the system's serial number
netGateway	R/W	System Gateway IP Address: <ul style="list-style-type: none"> <li><b>xxx.xxx.xxx.xxx</b></li> </ul> Installation default: 192.168.2.201
netEtherPorts	RO	Number of Ethernet Ports: <ul style="list-style-type: none"> <li><b>1 2</b></li> </ul> Systems shipped after December 2006 have two ports
netEther1Address	R/W	System IP Address: <ul style="list-style-type: none"> <li><b>xxx.xxx.xxx.xxx</b></li> </ul> Installation default: 192.168.2.200
netEther1Mask	R/W	System IP Address Subnet Mask: <ul style="list-style-type: none"> <li><b>xxx.xxx.xxx.xxx</b></li> </ul> Installation default: 255.255.255.0
netEther2Address	R/W	Craft Access IP Address (0.0.0.0 if not installed): <ul style="list-style-type: none"> <li><b>xxx.xxx.xxx.xxx</b></li> </ul> Installation default 192.168.3.200

Element	Read/Write	Description
netEther2Mask	R/W	Craft Access IP Address Subnet Mask (0.0.0.0 if not installed): <ul style="list-style-type: none"> <li>• <b>xxx.xxx.xxx.xxx</b></li> </ul> Installation default: 255.255.255.0
netTL1FastPort	R/W	Fast TL1 Port number (unencrypted, for automation): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 10034
netTL1FastSSLPort	R/W	Fast TL1 SSL Port number (encrypted, for automation): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 10036
netTL1SmartPort	R/W	Smart TL1 Port number (unencrypted, for manual access): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 10033
netTL1SmartSSLPort	R/W	Smart TL1 SSL Port number (encrypted, for manual access): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 10035
netTL1SSLEnable	R/W	Enable SSL for TL1 TCP sessions (disable non-SSL ports): <ul style="list-style-type: none"> <li>• <b>off(0)</b> (Installation default)</li> <li>• <b>on(1)</b></li> </ul>
netWebPort	R/W	Web Server HTTP (unencrypted): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 80
netWebSSLPort	R/W	Web Server HTTPS Port (encrypted): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 443
netWebSSLEnable	R/W	Enable Web Server SSL port: <ul style="list-style-type: none"> <li>• <b>off(0)</b></li> <li>• <b>on(1)</b> (Installation default)</li> </ul>
netSnmpPort	R/W	SNMP Port (unencrypted/encrypted): <ul style="list-style-type: none"> <li>• <b>0-65355</b></li> </ul> Installation default: 161

**NOTE:** netEther2Address must not be on the same subnet as netEther1Address.  
The TCP/UDP ports may be disabled by setting the port number to 0.



## System Log (SYSLOG) - sysLog

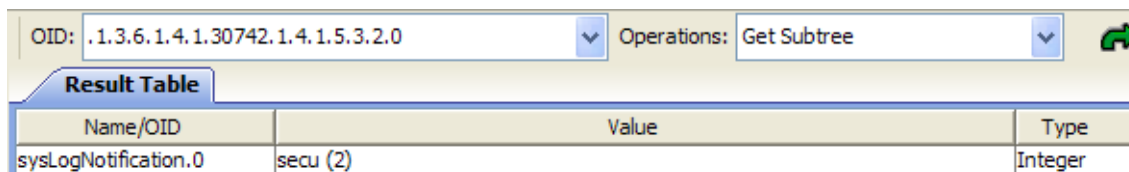
A subtree and table listing the SYSLOG configuration (Figure 17 and Figure 18) per the ClickFlow Syslog Configuration window (menu selection **System > System Configuration > Syslog**).

Configure system logging to a maximum of three external SYSLOG servers. The logging service level may be:

- **off(0)**—Do not log to external SYSLOG servers.
- **auto(1)**—Post messages that are logged to the TL1 AUTO log. These include user actions that change the system configuration, alarm events, and advisory events. The latter excludes actions and events that are related to security, which are posted to the SECU log.
- **secu(2)**—Post messages that are logged to the TL1 SECU log and also messages that are logged to the AUTO log.

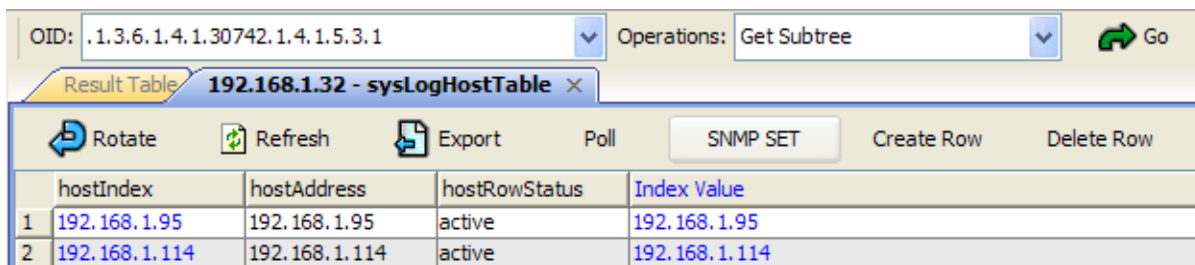
When multiple SYSLOG server IP addresses are specified, the log messages are posted to each of the servers. The latter SYSLOG servers may in turn be configured to forward the messages to other SYSLOG servers.

Figure 17 IOS System Log - sysLog - sysLogNotification



Name/OID	Value	Type
sysLogNotification.0	secu (2)	Integer

Figure 18 IOS System Log - sysLog - sysLogHostTable



hostIndex	hostAddress	hostRowStatus	Index Value
1	192.168.1.95	active	192.168.1.95
2	192.168.1.114	active	192.168.1.114

The table below describes the IOS System Log subtree and table elements:

Element	Read/ Write	Description
sysLogNotification	R/W	Syslog Log/Notification Level: <ul style="list-style-type: none"> <li>• <b>off(0)</b>—Do not log to external SYSLOG servers</li> <li>• <b>auto(1)</b>—Send all except security log messages</li> <li>• <b>secu(2)</b>—Send all log messages</li> </ul>
hostIndex	R/W	Syslog Server IP Address (table index): <ul style="list-style-type: none"> <li>• <b>xxx.xxx.xxx.xxx</b></li> </ul>
hostAddress	RO	Syslog Server IP Address: <ul style="list-style-type: none"> <li>• <b>xxx.xxx.xxx.xxx</b></li> </ul>
hostRowStatus	R/W	Table Row Status: <ul style="list-style-type: none"> <li>• <b>active(1)</b>—Normal row state</li> <li>• <b>notInService(2)</b>—Row created but not yet activated</li> <li>• <b>destroy(6)</b>—Delete row (delete server)</li> </ul>

## Changing the Syslog Notification Level

To change the syslog logging/notification level:

1. Browse to and view the current sysLogNotification level (Figure 17 on page 83).
2. Set the sysLogNotification level:
  - off(0) - Installation default
  - auto(1)
  - secu(2)

## Adding a Syslog Server

To add a syslog server:

1. Browse to and view the sysLogHostTable (Figure 18 on page 83).
2. Create a new table row:
  - a. Select the MIB Browser's Create Row facility
  - b. Select Create and Wait
  - c. Select index Data Type IpAddress (it should have defaulted)

- d. Set the hostIndex (the table index) to the new syslog server IP address. The row will be created and the row's hostAddress entry will automatically default to the hostIndex value.

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the sys-LogHostTable already has 3 rows (syslog servers).

3. Set the row's hostRowStatus to **active(1)**.

## Deleting a Syslog Server


To delete/remove a syslog server:

1. Browse to and view the sysLogHostTable (Figure 18 on page 83).
2. For the server IP address row to be deleted: Set the row's hostRowStatus to **destroy(6)**

## System Alarm—sysAlarm

A subtree listing all hardware and software alarm categories and showing the highest severity alarm in each category. Note that optical alarms are found in the port and connection tables. These values are not reset when alarms are acknowledged via ClickFlow or TL1.

Figure 19 IOS System Alarm Sub-tree—sysAlarm

OID: .1.3.6.1.4.1.30742.1.4.1.5.4		Operations: Get Subtree	
Result Table			
Name/OID	Value	Type	
sysAlarmTemp.0	clear (6)	Integer	
sysAlarmClock.0	clear (6)	Integer	
sysAlarmSecurity.0	clear (6)	Integer	
sysAlarmFan.0	clear (6)	Integer	
sysAlarmHVPS.0	clear (6)	Integer	
sysAlarmDCPower.0	major (2)	Integer	

The table below describes the System Alarm subtree and table elements:

Element	Read/Write	Description
sysAlarmTemp	RO	Engine temperature alarm • <b>critical(1)</b> or <b>clear(6)</b>
sysAlarmClock	RO	NTP loss of synchronization alarm • <b>minor(3)</b> or <b>clear(6)</b>
sysAlarmSecurity	RO	Intrusion alarm • <b>minor(3)</b> or <b>clear(6)</b>
sysAlarmFan	RO	System Fan alarm • <b>major(2)</b> or <b>minor(3)</b> or <b>clear(6)</b> Single fan failure is minor, multiple fan failure is major
sysAlarmHVPS	RO	Internal High Voltage Power Supply failure • <b>critical(1)</b> or <b>clear(6)</b>
sysAlarmDCPower	RO	48V input or 48V fuse alarm • <b>major(2)</b> or <b>clear(6)</b>

## Security Tables—ClickFlow/TL1 Users

There is no correlation between SNMP v3 users (usmUserName) and ClickFlow/TL1 users: adding an SNMP usmUserName does not add a ClickFlow/TL1 user and vice-versa. For a description of ClickFlow/TL1 user management, see the *IOS ClickFlow Graphical User Interface Manual*.

**NOTE:** The IOS SNMP Agent does not support viewing or configuration of ClickFlow/TL1 users and their privileges via SNMP.

### ClickFlow/TL1 User “snmpuser”

IOS Release 7.0 and above include an additional default administrative ClickFlow/TL1 user “snmpuser” that is used as a proxy for SNMP get/set accesses after access is authorized by SNMP USM/VACM. The ClickFlow/TL1 interfaces do not allow a user to log in via the “snmpuser” user name.

ClickFlow and TL1 list “snmpuser” as the connection owner of connections made by the iosProvisionTable (Figure 13 on page 50) and the iosConnectionTable (Figure 22 on page 95). How-

ever, the `iosConnectionTable` `ocOperator` entry and the log entry list the actual SNMP user (`snmpCommunityName` for v2 access or `usmUserName` for v3 access).

## ClickFlow/TL1 Port Privileges—Virtual Private Switch

Since SNMP accesses the switching fabric via the proxy administrative user “snmpuser”, it does not support the ClickFlow/TL1 Virtual Private Switch optional feature which allows configuration of user access privilege (modify/read-write, view/read-only, none) to specified port lists. To make a connection, a user must have the Modify privilege for both ports; to break a connection the user must have Modify privilege for one of the two ports.

## SNMP Port Privileges—VACM

SNMP VACM (View-based Access Control Model) provides a more powerful access control model that may restrict user access (read-write, read-only, none) to individual objects, sub-trees, table columns (a sub-tree) and table rows (an object and mask).

Therefore, port privileges may be implemented by the VACM views of the port tables:

- `iosInputPortTable`, for “normal” input ports (page 87)
- `iosOutputPortTable`, for “normal” output ports (page 91)
- `iosVOAPortTable`, for Switched VOA ports (page 109)
- `iosPMCPortTable`, for Photonic Multicast ports (page 113)

VACM controls access via the OID address, but not the value written to an OID. Hence the IOS SNMP Agent provides an additional access filter in order to control port connection privilege. If a user’s VACM view of a port’s table row index is excluded (none), then the user cannot connect or disconnect that port via the `iosProvisionTable` (Figure 13 on page 50) or the `iosConnectionTable` (Figure 22 on page 95). Disabling access to a port’s table row index does not disable access to the table row, so the row may be viewed or modified in accordance with the row’s VACM view.

## Input Port Table—`iosInputPortTable`

A table with one row for each switch “normal” input port (Figure 20). The Input Port Table may be used to:

- Configure all attributes for an input port: name, port description, port group, port alarm severities, waveband, and signal threshold.
- Retrieve a port 's power and state

**NOTE:**

- “Normal” input ports are switch input ports that are either connected directly to a switch panel input connector or via an input splitter (optional hardware feature).
- “Reference” ports are switch ports connected to non-dedicated internal optional hardware features (PMUs and SVOAs).

Figure 20 IOS Input Port Table—iosInputPortTable

	1	2	3	4	5	
inPortId	10001	10002	10003	10004	10005	10006
inPortNumber	10001	10002	10003	10004	10005	10006
inPortThreshold	1310-In-Net	1550	1310-In-Net	1550	1550	1550
inPortPower	-13.5	-13.2	-13.3	-14.5	-13.1	-13.1
inPortStatus	psNORM	psNORM	psNORM	psNORM	psNORM	psNORM
inPortPeerPort	20003	0	20001	0	20005	0
inPortName	XOP-TX		HAY-TX			
inPortDescr	140.240/29		140.241			
inPortGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup
inPortWaveband	nm1310	nm1550	nm1310	nm1550	nm1550	nm1550
inPortAlarm	clear	clear	clear	clear	clear	clear
inPortSTMIN	major	disable	major	disable	minor	disable
inPortSTMAX	disable	disable	disable	disable	disable	disable

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns, and only the first seven input ports are shown.

The table below describes the Input Port Table elements:

Element	Read/Write	Description
inPortId	IDX	Table Row Index, same as inPortNumber
inPortNumber	RO	Port Number: <ul style="list-style-type: none"> <li>• 10xxx</li> </ul>

Element	Read/Write	Description
inPortThreshold	R/W	Signal Threshold name (1-32 characters), must correspond to a signal threshold listed in the iosSigThresholdTable (see page 98): Installation default: <ul style="list-style-type: none"> <li>• <b>1550</b></li> </ul>
inPortPower	RO	Port power (dBm): <ul style="list-style-type: none"> <li>• <b>[-]xx.x</b> or <b>N/A</b> (if iosInputPowerDetection=no(0))</li> </ul>
inPortStatus	RO	Port status: <ul style="list-style-type: none"> <li>• <b>psDAMAGE(9)</b>—port is marked bad</li> <li>• <b>psSTMAX(3)</b>—port power is above sigThreshPowerMax and below iosMaxSystemPower</li> <li>• <b>psNORM(1)</b>—port power is between sigThreshPowerMin and sigThreshPowerMax</li> <li>• <b>psSTMIN(2)</b>—port power is below sigThreshPowerMin and greater -40 dBm</li> <li>• <b>psPWRMIN(4)</b>—power below -40 dBm</li> <li>• <b>psUDEF(0)</b>—port power unknown - used for systems where iosInputPowerDetection=no(0): in this case, inPortPower will be equal to N/A</li> </ul>
inPortPeerPort	RO	Peer port number: <ul style="list-style-type: none"> <li>• <b>0</b>—Not Connected</li> <li>• <b>20xxx</b>—Connected to output port 20xxx</li> </ul>
inPortName	R/W	Port name (0-32 characters), port names must be unique: Installation default: <ul style="list-style-type: none"> <li>• Null</li> </ul>
inPortDescr	R/W	Port comment/description (0-32 characters): Installation default: <ul style="list-style-type: none"> <li>• Null</li> </ul>
inPortGroup	R/W	Port group name (1-32 characters) Installation Default: <ul style="list-style-type: none"> <li>• <b>OpenGroup</b></li> </ul>
inPortWaveband	R/W	Waveband of signal at input port. <ul style="list-style-type: none"> <li>• <b>nm1310(1)</b>—use when the waveband of the input signal is between 1260nm and 1460nm</li> <li>• <b>nm1550(2)</b>—use when the waveband of the input signal is between 1460nm and 1630nm</li> </ul>
inPortAlarm	RO	Highest severity active alarm on port: <ul style="list-style-type: none"> <li>• No Alarm = <b>clear(6)</b></li> <li>• Alarms = <b>critical(1), major(2), minor(3), notice(4)</b></li> </ul>

Element	Read/Write	Description
inPortSTMIN	R/W	Severity for STMIN alarm on port: <ul style="list-style-type: none"> <li>• Default: <b>disable(5)</b></li> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>
inPortSTMAX	R/W	Severity for STMAX alarm on port: <ul style="list-style-type: none"> <li>• Default: <b>disable(5)</b></li> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>

**NOTE:** The port's sigThreshPowerMax and sigThreshPowerMin values are established by the assigned signal threshold (inPortThreshold). The port state psPWRMAX is transient as the port immediately transitions to psDAMAGE(30). The port damaged condition is latched: it can only be cleared by Glimmerglass Service, and furthermore the damaged port cannot be used in a connection.

## Configuring an Input Port

To configure an input port:

1. Browse to and view the iosInputPortTable (Figure 20 on page 88).
2. For the input port table row to be revised:
  - a. Optionally set the row's inPortThreshold (Signal Threshold Name).
  - b. Optionally set the row's inPortName (Port Name, 0-32 characters). Non-null port names must be unique: no two ports may have the same name.
  - c. Optionally set the row's inPortDescr (Port Comment/Description, 0-32 characters)
  - d. Optionally set the row's inPortGroup (port group name, 1-32 characters) to assign the port to a port group. The port group name must have been defined, see "Port Grouping - iosPortGroupTable" on page 75.
  - e. Optionally set the row's inPortWaveband. This is required if the waveband shown is incorrect. There are two values, **nm1310(1)** or **nm1550(2)**:
    - **nm1310(1)**: Waveband of signal at input is between 1260nm and 1460nm
    - **nm1550(2)**: Waveband of signal at input is between 1460nm and 1630nm
  - f. Optionally set the row's inPortSTMIN (STMIN alarm severity)
  - g. Optionally set the row's inPortSTMAX (STMAX alarm severity)



- NOTES:**
- Changes (SETs) to the port table are effective immediately.
  - Optionally modification of the port group name column may be inhibited via VACM
  - Changes to the inPortThreshold, inPortSTMIN, and inPortSTMAX values may be performed on a list of ports via the iosProvisionTable.

## Output Port Table—iosOutputPortTable

A table with one row for each switch “normal” output port (Figure 21). The Output Port Table may be used to:

- Configure all attributes for an output port: port name, port description, port group, port/connection alarm severities, and signal threshold.
- Retrieve a port ‘s power and state

- NOTE:**
- “Normal” output ports are switch output ports that are connected directly to a switch panel output connector or via an output splitter (optional hardware feature).
  - “Reference” ports are switch ports connected to non-dedicated internal optional hardware features (PMUs and SVOAs).

Figure 21 IOS Output Port Table—iosOutputPortTable

	1	2	3	4	5	6
outPortId	20001	20002	20003	20004	20005	20006
outPortNumber	20001	20002	20003	20004	20005	20006
outPortThreshold	1310-Out-Net	1550	1310-Out-Net	1550	1550	1550
outPortPower	-15.4	-50.9	-15.6	-50.6	-15.4	-51.1
outPortStatus	psNORM	psLGTOFF	psNORM	psLGTOFF	psNORM	psLGTOFF
outPortPeerPort	10003	0	10001	0	10005	0
outPortName	XOP-RX		HAY-RX			
outPortDescr	10GbE		10GbE			
outPortHasDVOA	no	no	no	no	no	no
outPortGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup
outPortWaveband	nm1310	nm1550	nm1310	nm1550	nm1550	nm1550
outPortAlarm	clear	clear	clear	clear	clear	clear
outPortSTMIN	disable	disable	disable	disable	minor	disable
outPortSTMAX	minor	disable	disable	disable	major	disable
outPortCSFLT	critical	critical	critical	critical	critical	critical

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the Output Port Table elements:

Element	Read/Write	Description
outPortId	IDX	Table row index, same as outPortNumber
outPortNumber	RO	Port Number: • <b>20xxx</b>
outPortThreshold	RO	Signal Threshold name (1-32 characters), must correspond to a signal threshold listed in the iosSigThresholdTable (see page 98): Installation default: • <b>1550</b>
outPortPower	RO	Port power (dBm): • <b>[-]xx.x</b>
outPortStatus	RO	Port status: • <b>psDAMAGE(9)</b> —port is marked bad • <b>psSTMAX(3)</b> —port power is above sigThreshPowerMax and below iosMaxSystemPower • <b>psNORM(1)</b> —port power is between sigThreshPowerMin and sigThreshPowerMax • <b>psSTMIN(2)</b> —port power is below sigThreshPowerMin and greater -40 dBm • <b>psPWRMIN(4)</b> —power below -40 dBm for a connected output port (dark connection) • <b>psLGTOFF(6)</b> —port power below -40 dBm for an unconnected output port • <b>psLGTRVRS(8)</b> —port power above -40 dBm for an unconnected output port, or port power is > port power at connected input port (reverse light) • <b>psUDEF(0)</b> —port power unknown - only shown if failure on output power monitor
outPortPeerPort	RO	Peer port number: • <b>0</b> —Not Connected • <b>10xxx</b> —Connected to output port 10xxx
outPortName	R/W	Port name (0-32 characters), port names must be unique: Installation default: • Null or voaUnitAlias (VO- <i>n</i> ) for a DVOA port

Element	Read/Write	Description
outPortDescr	R/W	Port comment/description (0-32 characters): Installation default: • Null
outPortHasDVOA	RO	A VOA is connected between the switch output port and the panel output connector (see iosAttenuator tables on page 106): <b>no(0)</b> or <b>yes(1)</b>
outPortGroup	R/W	Port group name (1-32 characters) Installation Default: • <b>OpenGroup</b>
outPortWaveband	RO	Waveband in use at the output port: • <b>nm1310(1)</b> or <b>nm1550(2)</b> For connected outputs, this value is obtained automatically from the input port in the connection. For unconnected outputs, the value reflects the waveband of the last input port with which the output was connected.
outPortAlarm	RO	Highest severity active alarm on port: • No Alarm = <b>clear(6)</b> • Alarms = <b>critical(1), major(2), minor(3), notice(4)</b>
outPortSTMIN	R/W	Severity for STMIN alarm on port: • Default: <b>disable(5)</b> • Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b>
outPortSTMAX	R/W	Severity for STMAX alarm on port: • Default: <b>disable(5)</b> • Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b>
outPortCSFLT	R/W	Severity for CSFLT alarm on port: • Default: <b>disable(5)</b> • Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b>

**NOTE:** The port's sigThreshPowerMax and sigThreshPowerMin values are established by the signal threshold (outPortThreshold) assigned to the port.

## Configuring an Output Port

To configure an output port:

1. Browse to and view the iosOutputPortTable (Figure 21 on page 91).
2. For the output port table row to be revised:
  - a. Optionally set the row's outPortThreshold (Signal Threshold Name).
  - b. Optionally set the row's outPortName (Port Name, 0-32 characters). Non-null port names must be unique: no two ports may have the same non-null name.
  - c. Optionally set the row's outPortDescr (Port Comment/Description, 0-32 characters)
  - d. Optionally set the row's outPortGroup (port group name, 1-32 characters) to assign the port to a port group. The port group name must have been defined, see "Port Grouping - iosPortGroupTable" on page 75.
  - e. Optionally set the row's outPortSTMIN (STMIN alarm severity).
  - f. Optionally set the row's outPortSTMAX (STMAX alarm severity).
  - g. Optionally set the row's outPortCSFLT (CSFLT alarm severity).

**NOTES:**

- Changes (SETs) to the port table are effective immediately.
- Optionally modification of the port group name column may be inhibited via VACM
- Changes to the outPortThreshold, outPortSTMIN, outPortSTMAX, and outPortCSFLT values may be performed on a list of ports via the iosProvisionTable

## Connection Table—iosConnectionTable

A table with one row for each connection (Figure 22). The Connection Table supports the following connection operations:

Operation	Description	Page
Viewing connections	View current connections, including connection state and port powers	97
Making a connection	Connect an input port that is not involved in an existing connection and optionally assign a connection name	97
Revising a connection	Change the output port for an existing connection and/or change the connection name	97
Breaking a connection	Delete an existing connection	98

Connections are asynchronous: the SNMP response occurs after the set values have been validated and the connection initiated, but before the connection is complete. Multiple connections may be transmitted in a single SNMP UDP packet, however the connections occur one at a time when the connection row's ocRowStatus is set to active(1). For multiple concurrent connections, see "System Provisioning Table—iosProvisionTable" on page 48.

**NOTE:** Unlike the ClickFlow and TL1 user interfaces, the SNMP Agent does not support connect by port names, only connect by port numbers.

Figure 22 IOS Connection Table—*iosConnectionTable*

OID: .1.3.6.1.4.1.30742.1.4.4.1 Operations: Get Next

Result Table 192.168.1.43 - iosConnectionTable

	1	2	3	4	5	6
ocIndex	10003	10007	10008	10011	10012	10057
ocInputNumber	10003	10007	10008	10011	10012	10057
ocOutputNumber	20057	20007	20008	20012	20011	20003
ocInputType	input	input	input	input	input	pmc
ocOutputType	pmc	dvoa	dvoa	output	output	dvoa
ocStatus	csCSSTD	csCSSTD	csCSSTD	csCSSTD	csCSSTD	csCSSTD
ocWaveband	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550
ocPowerLoss	2.2	7.0	5.2	2.5	2.0	2.5
ocInputPower	-12.9	-13.0	-12.8	-13.0	-12.9	-20.9
ocOutputPower	-15.1	-20.0	-18.0	-15.5	-14.9	-23.4
ocName	InPort-to-PMU	VOA@-20dBm	VOA@-18dBm	DuplexConn	DuplexConn	PMU-to-DVOA
ocInputName	InPort3	InPort7	InPort8	InPort11	InPort12	MC-1-1
ocOutputName	MC-1	VO-7	VO-8	OutPort12	OutPort11	VO-3
ocOperator	admin	admin	admin	admin	admin	admin
ocOperatorLock	open	open	open	open	open	open
ocRowStatus	active	active	active	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the Connection Table elements:

Element	Read/Write	Description
ocIndex	IDX	Table row index, same as ocInputNumber
ocInputNumber	RO	Input port number: • <b>10xxx</b>
ocOutputNumber	R/W	Output port number: • <b>20xxx</b>
ocInputType	RO	Input port type: • <b>undef(0)</b> —Transient value while making a connection • <b>input(1)</b> —Normal input port • <b>svoa(4)</b> —Switched VOA output port • <b>pmc(5)</b> —Multicast output port

Element	Read/Write	Description
ocOutputType	RO	Output port type: <ul style="list-style-type: none"> <li>• <b>undef(0)</b>—Transient value while making a connection</li> <li>• <b>output(2)</b>—Normal output port</li> <li>• <b>dvoa(3)</b>—Dedicated VOA output port</li> <li>• <b>svoa(4)</b>—Switched VOA input port</li> <li>• <b>pmc(5)</b>—Multicast input port</li> </ul>
ocStatus	RO	Connection status: <ul style="list-style-type: none"> <li>• <b>csCSSTD(1)</b>—Normal/good connection</li> <li>• <b>csCSFLT(2)</b>—Connection Fault (see note)</li> <li>• <b>csTRANS(3)</b>—Transient value while making a connection</li> </ul>
ocWaveband	RO	Waveband used for the connection (derived from input port): <ul style="list-style-type: none"> <li>• <b>nm1310(1)</b> or <b>nm1550(2)</b></li> </ul>
ocPowerLoss	RO	Input Port Power minus Output Port Power (dB): <ul style="list-style-type: none"> <li>• <b>x.x</b>—For DVOAs this includes the VOA attenuation</li> <li>• <b>N/A</b>—If ocStatus = Connection Fault</li> </ul>
ocInputPower	RO	Input port power (dBm): <ul style="list-style-type: none"> <li>• <b>[-]xx.x</b></li> </ul>
ocOutputPower	RO	Output port power (dBm): <ul style="list-style-type: none"> <li>• <b>[-]xx.x</b></li> </ul>
ocName	R/W	Connection name (0-32 characters): Default: <ul style="list-style-type: none"> <li>• Null</li> </ul>
ocInputName	RO	Input port name (0-32 characters), from the input port
ocOutputName	RO	Output port name (0-32 characters), from the output port
ocOperator	RO	Operator (1-32 characters), ClickFlow/TL1/SNMP user that made/revised the connection
ocOperatorLock	R/W	Connection lock status: <ul style="list-style-type: none"> <li>• <b>open(0)</b>—connection not locked by ocOperator</li> <li>• <b>lock(1)</b>—connection is locked by ocOperator</li> </ul>
ocRowStatus	R/W	Table row status: <ul style="list-style-type: none"> <li>• <b>active(1)</b>—Normal row state</li> <li>• <b>notInService(2)</b>—Row disabled for editing (revise connection)</li> <li>• <b>notReady(3)</b>—One or more required row entries are not set</li> <li>• <b>createAndWait(5)</b>—Create then edit row (make connection)</li> <li>• <b>destroy(6)</b>—Delete row (break connection)</li> </ul>

**NOTE:** A connection fault will trigger when the light at the output port is too low for the connection to be optimized.

## Viewing Connections

To view existing connections, and their state and port power levels:

1. Browse to and view the iosConnectionTable (Figure 22 on page 95).

## Making a New Connection

To connect an input port that is not involved in an existing connection:

1. Browse to and view the iosConnectionTable (Figure 22 on page 95).
2. Select the MIB Browser's Create Row facility, then Create and Wait, and set the ocIndex (table index) to the input port number.

---

**NOTE:** Create and Wait will be rejected if the input port number is invalid or is already in a connection.

---

3. In the new connection table row:
  - a. Set the row's ocOutputNumber to the output port number
  - b. Optionally set the row's ocName (Connection Name, 1-32 characters)
  - c. Set the row's ocRowStatus to **active(1)**

---

**NOTE:** If the output port was involved in an existing connection then that connection will be automatically broken. The row's ocStatus (connection status) is initially notReady this will transition to either csCSSTD or csCSFLT. If csCSFLT is the status and the port's portCSFLT value is not set to notice(4) or disable(5), then an iosConnectionState trap will be generated.

---

## Revising an Existing Connection

To change the output port for an existing connection:

1. Browse to and view the iosConnectionTable (Figure 22 on page 95).
2. For the connection table row to be revised:
  - a. Set the row's ocRowStatus to **notInService(2)**
  - b. Set the row's ocOutputNumber to the output port number
  - c. Optionally set the row's ocName (Connection Name, 1-32 characters)
  - d. Optionally set the row's ocOperatorLock.
  - e. Set the row's ocRowStatus to **active(1)**.

## Breaking an Existing Connection

To break an existing connection:

1. Browse to and view the iosConnectionTable (Figure 22 on page 95).
2. For the connection table row to be deleted, set the row's ocRowStatus to **destroy(6)**.

## Signal Threshold Table—iosSigThresholdTable

A table with one row for each Signal Threshold (Figure 23). The Signal Threshold Table supports the following Signal Threshold operations:

Operation	Description	Page
Viewing signal thresholds	View current signal thresholds	100
Creating a signal threshold	Create a new signal threshold	101
Revising a signal threshold	Revise an existing signal threshold	101
Deleting a signal threshold	Delete an existing signal threshold	102

The signal threshold of a port defines the expected power range and hysteresis gap used for port power threshold crossing monitoring. Configuring a port with the correct signal threshold will optimize the port's performance and power reporting accuracy.

The system has two predefined signal thresholds named 1310 and 1550. These two signal thresholds may not be deleted but their power thresholds and hysteresis may be modified.

Signal thresholds may be assigned directly to ports via the port tables (input, output, PMU, or VOA) or to a list of ports via the setPortThreshold provisioning command ("Assigning a Signal Threshold to a List of Ports" on page 71).



Figure 23 IOS Signal Threshold Table—iosSigThresholdTable

	1	2	3	4
sigThreshIndex	1310	1550	1310-10GbE-In	1310-10GbE-Out
sigThreshName	1310	1550	1310-10GbE-In	1310-10GbE-Out
sigThreshDescr				
sigThreshPowerMin	-20.0	-25.0	-12.0	-15.5
sigThreshPowerMax	5.0	5.0	0.0	-4.0
sigThreshHysteresis	1.0	0.5	0.5	0.5
sigThreshRowStatus	active	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the Signal Threshold Table elements:

Element	Read/Write	Description
sigThreshIndex	IDX	Table row index, same as sigThreshName
sigThreshName	RO	Signal threshold name. Must be unique and non-null. Maximum of 32 characters: Only alphanumeric, hyphen, underscore, and period characters are allowed.
sigThreshDescr	RO	Signal threshold description. Maximum of 32 characters. Semi-colon character is not permitted. <b>NOTE:</b> This field will be implemented in a later release and is read-only at this time.
sigThreshPowerMin	R/W	Signal threshold low/minimum power threshold (dBm): • [-]xx.x Default: -20.0
sigThreshPowerMax	R/W	Signal threshold high/maximum power threshold (dBm): • [-]xx.x Default: 5.0
sigThreshHysteresis	R/W	Signal threshold hysteresis: • x.x Default: 1.0

Element	Read/Write	Description
sigThreshRowStatus	R/W	Table row status: <ul style="list-style-type: none"> <li>• <b>active(1)</b>—Normal row state</li> <li>• <b>notInService(2)</b>—Row disabled for editing (revise signal threshold)</li> <li>• <b>notReady(3)</b>—One or more required row entries are not set</li> <li>• <b>createAndWait(5)</b>—Create then edit row (create signal threshold)</li> <li>• <b>destroy(6)</b>—Delete row (remove signal threshold)</li> </ul>

The sigThreshPowerMax, sigThreshPowerMin, and sigThreshHysteresis values establish the power levels at which psSTMIN and psSTMAX type iosInputSignalTrap and iosOutputSignalTrap traps are generated. These traps are only generated when the xxPortSTMIN or xxPortSTMAX severity is set to a severity of Critical, Major, or Minor in the ports table (where xx indicates the port table: in, out, PMC, or VOA).

iosInputSignalTrap and iosOutputSignalTrap traps are generated, if enabled by the port's port monitoring.

Trap Port Status	Port Power Level Transition	
	From	To
psSTMAX (alarm)	< sigThreshPowerMax - sigThreshHysteresis	> sigThreshPowerMax + sigThreshHysteresis
psSTMAX (clear)	> sigThreshPowerMax + sigThreshHysteresis	< sigThreshPowerMax - sigThreshHysteresis
psSTMIN (alarm)	> sigThreshPowerMin + sigThreshHysteresis	< sigThreshPowerMin - sigThreshHysteresis
psSTMIN (clear)	< sigThreshPowerMin - sigThreshHysteresis	> sigThreshPowerMin + sigThreshHysteresis

## Viewing Signal Thresholds

To view existing signal thresholds:

1. Browse to and view the iosSigThresholdTable (Figure 23 on page 99).

## Creating a New Signal Threshold

To create a new signal threshold:

1. Browse to and view the iosSigThresholdTable (Figure 23 on page 99).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the sigThreshIndex (table index) to a new unique signal threshold name.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosSigThresholdTable already has 200 rows (signal thresholds).

---

3. In the new signal threshold table row:
  - a. Optionally enter a value for the sigThreshDescr.
  - b. Optionally set the row's sigThreshPowerMin value (dBm, default -20.0)
  - c. Optionally set the row's sigThreshPowerMax value (dBm, default 5.0)
  - d. Optionally set the row's sigThreshHysteresis value (dBm, default 1.0)
  - e. Set the row's sigThreshRowStatus to **active(1)**

---

**NOTE:** The signal power values must comply with the following restrictions:

- $\text{iosMinSignalPower} \leq \text{sigThreshPowerMin} \leq \text{sigThreshPowerMax}$
- $\text{sigThreshPowerMin} \leq \text{sigThreshPowerMax} \leq \text{iosMaxSignalPower}$
- $(\text{sigThreshPowerMax} - \text{sigThreshPowerMin}) \leq 25.0$  if  $\text{iosInputPowerDetection}=\text{no}$

See "System Configuration—sysConfiguration" on page 45 for iosInputPowerDetection, iosMinSignalPower and iosMaxSignalPower values.

---

## Revising an Existing Signal Threshold

To revise an existing signal threshold:

1. Browse to and view the iosSigThresholdTable (Figure 23 on page 99).
2. For the signal threshold table row to be revised:
  - a. Set the row's sigThreshRowStatus to **notInService(2)**
  - b. Optionally change the value for the sigThreshDescr.
  - c. Optionally set the row's sigThreshPowerMin value (dBm)
  - d. Optionally set the row's sigThreshPowerMax value (dBm)
  - e. Optionally set the row's sigThreshHysteresis value (dBm)
  - f. Set the row's sigThreshRowStatus to **active(1)**

---

**NOTE:** The Signal Threshold name cannot be revised. The revised power values must comply with the restrictions listed in "Creating a New Signal Threshold" on page 101.

---

## Deleting an Existing Signal Threshold

To delete an existing signal threshold:

1. Browse to and view the iosSigThresholdTable (Figure 23 on page 99).
2. For the signal threshold table row to be deleted, set the row's sigThreshRowStatus to **destroy(6)**.

---

**NOTE:** The system default signal thresholds "1550" and "1310" cannot be deleted.

---

## Protection Rule Table—iosProtectionRuleTable

A table with one row for each Protection Rule (Figure 24). The Protection Rule Table supports the following Protection Rule operations:

Operation	Description	Page
View a Protection Rule	View current Protection Rules and their status	105
Create a Protection Rule	Create a new Protection Rule	105
Delete a Protection Rule	Delete an existing Protection Rule	106

---

**NOTE:** Protection Rules may not be revised. Port Protection Switching is an optional software feature, see iosLicensePortProtection in sysConfiguration (Figure 11 on page 45).

---

The Connection Protection feature allows the user to configure working and protect input ports for either Simplex or Duplex connections. This feature allows the user to externally split a signal and route each leg of the split to a separate input port on the system. If a fiber cut or loss of light occurs on the working path, the system will detect this condition and change the connection(s) to use the protect path. The connection will revert to the working port only if its power has been restored and the power to the protect port is lost. An iosConnectionState trap with status csPROTS is generated when a protection switch occurs. For further information, see the *IOS ClickFlow Graphical User Interface Manual*.

Figure 24 IOS Protection Rule Table—iosProtectionRuleTable

	1	2	3
ruleIndex	1	2	3
ruleProtType	simplex	duplex	duplex
ruleProtStatus	inactive	working	working
ruleProtSymmetric	yes	yes	yes
ruleProtOutputPort	0	20007	20008
ruleWorkingPort	10001	10007	10008
ruleWorkingArmMode	threshold	threshold	threshold
ruleWorkingArmDelay	750	750	750
ruleWorkingTriggerDelay	50	50	50
ruleProtPort	10002	10011	10012
ruleProtArmMode	threshold	threshold	threshold
ruleProtArmDelay	750	750	750
ruleProtTriggerDelay	50	50	50
ruleRowStatus	active	active	active

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the IOS Protection Rule Table elements:

Element	Read/Write	Description
ruleIndex	IDX	SNMP Table Row Index: <ul style="list-style-type: none"> <li><b>1, 2, ...</b>—Unique integer entered when creating the row</li> </ul>
ruleProtType	R/W	Protection Rule Type: <ul style="list-style-type: none"> <li><b>simplex(1)</b>—Protect a simplex connection</li> <li><b>duplex(2)</b>—Protect one side of a duplex connection</li> </ul>
ruleProtStatus	R/W	Protection Rule State: <ul style="list-style-type: none"> <li><b>inactive(0)</b>—Neither input is connected</li> <li><b>activating(1)</b>—Transitional state to working/standby</li> <li><b>working(2)</b>—Output is connected to Working input</li> <li><b>standby(3)</b>—Output is connected to Protect input</li> <li><b>failure(4)</b>—Neither input port has a valid signal</li> </ul>
ruleProtSymmetric	R/W	Protection Rule Symmetric (Protect Port arm mode and delays are the same as the Working Port arm mode and delays): <ul style="list-style-type: none"> <li><b>no(0)</b></li> <li><b>yes(1)</b></li> </ul>

Element	Read/ Write	Description
ruleProtOutputPort	R/W	Protection Rule Output Port Number: <ul style="list-style-type: none"> <li>• <b>0</b>—Not connected</li> <li>• <b>20xxx</b>—Working/Protect port connected to this port</li> </ul>
ruleWorkingPort	R/W	Protection Rule Working Input Port Number: <ul style="list-style-type: none"> <li>• <b>10xxx</b></li> </ul>
ruleWorkingArmMode	R/W	Protection Rule Working Input Arm Mode: <ul style="list-style-type: none"> <li>• <b>threshold(1)</b>—Default (requires input power detection)</li> <li>• <b>timed(2)</b></li> </ul>
ruleWorkingArmDelay	R/W	Protection Rule Working Input Arm Delay (mS): <ul style="list-style-type: none"> <li>• <b>xxx</b></li> </ul> Default: 750
ruleWorkingTriggerDelay	R/W	Protection Rule Working Input Trigger Delay (mS): <ul style="list-style-type: none"> <li>• <b>xxx</b></li> </ul> Default: 50
ruleProtPort	R/W	Protection Rule Protect Input Port Number: <ul style="list-style-type: none"> <li>• <b>10xxx</b></li> </ul>
ruleProtArmMode	R/W	Protection Rule Protect Input Arm Mode: <ul style="list-style-type: none"> <li>• <b>threshold(1)</b>—Default (requires input power detection)</li> <li>• <b>timed(2)</b></li> </ul>
ruleProtArmDelay	R/W	Protection Rule Protect Input Arm Delay (mS): <ul style="list-style-type: none"> <li>• <b>xxx</b></li> </ul> Default: 750
ruleProtTriggerDelay	R/W	Protection Rule Protect Input Trigger Delay (mS): <ul style="list-style-type: none"> <li>• <b>xxx</b></li> </ul> Default: 50
ruleRowStatus	R/W	Table Row Status: <ul style="list-style-type: none"> <li>• <b>active(1)</b>—Normal row state</li> <li>• <b>notInService(2)</b>—Row disabled for editing (creating protection rule)</li> <li>• <b>notReady(3)</b>—One or more required row entries are not set</li> <li>• <b>createAndWait(5)</b>—Create then edit row (create protection rule)</li> <li>• <b>destroy(6)</b>—Delete row (remove protection rule)</li> </ul>

## Viewing Protection Rules

To view existing protection rules:

1. Browse to and view the iosProtectionRuleTable (Figure 24 on page 103).

## Creating a New Protection Rule

To create a new protection rule:

1. Browse to and view the iosProtectionRuleTable (Figure 24 on page 103).
2. Select the MIB Browser's Create Row facility, select Create and Wait, and set the ruleIndex (table index) to an unsigned integer value that is not already present in the table. For example, "4" would be valid for the table shown in Figure 24 on page 103.

---

**NOTE:** Create and Wait will be rejected with "Resource Unavailable" if the iosProtectionRuleTable already has 200 rows (protection rules).

---

3. In the new protection rule table row:
  - a. Optionally change the row's ruleProtType to one of the following:
    - **simplex(1)**—Default
    - **duplex(2)**
  - b. Optionally set the row's ruleProtSymmetric to one of the following:
    - **no(0)**
    - **yes(1)**—Default
  - c. Set the row's ruleWorkingPort (input port number)
  - d. Optionally set the row's ruleWorkingArmMode to one of the following:
    - **threshold(1)**—Default (requires input power detection)
    - **timed(2)**
  - e. If the **timed(2)** was selected then optionally set ruleWorkingArmDelay (mS, default 750)
  - f. Optionally set the row's ruleWorkingTriggerDelay (mS, default 50)
  - g. Set row's ruleProtPort (protection port, input port number)
  - h. If ruleProtSymmetric—**no(0)** was selected above then:
    - Optionally set the row's ruleProtArmMode: **threshold(1)** or **timed(2)**
    - Optionally set the row's ruleProtArmDelay (mS, default 750)
    - Optionally set the row's ruleProtTriggerDelay (mS, default 50)
  - i. Set the row's ruleRowStatus to **active(1)**

## Deleting an Existing Protection Rule

To delete an existing protection rule:

1. Browse to and view the iosProtectionRuleTable (Figure 24 on page 103).
2. For the protection rule table row to be deleted, set the row's ruleRowStatus to **destroy(6)**.

## Attenuator (VOA) Tables

The Variable Optical Attenuation features allow the user to adjust the output power of connections via the IOS user interfaces (ClickFlow, SNMP, and TL1). The integrated VOA feature eliminates the need to separately install either fixed attenuators or standalone VOA devices that require a separate remote software control interface or on-site manual adjustment. The integrated VOAs support 0.1dB resolution with ~10mS response times. Once set, the system monitors the power level and automatically adjusts the VOA setting to maintain operation at the set level.

Glimmerglass offers two implementations for Variable the Optical Attenuation feature:

- **Dedicated VOA:** This feature allows users set/control the output optical power level (dBm) for connections to pre-designated outputs port. The pre-designated output ports are implemented with VOA elements located in-line between the switch and the output power monitor for the port.
- **Switched VOA:** This implementation moves the attenuators from a fixed output port assignment and places the attenuator between an internal output and an internal input port of the switch. This configuration removes the Dedicated VOA constraint of pre-designating which output ports will support attenuation and, therefore, allows attenuation to be performed between any input port and any output port.

The Attenuator (VOA) Tables are tables for viewing/configuring the optional VOAs (Figure 25 on page 107) and their associated ports (Figure 26 on page 109).

VOA Tables	Description	Page
iosVOAUnitTable	A table with one row for each installed Dedicated VOA and Switched VOA: Configure VOA mode and power.	107
iosVOAPortTable	A table with one row for each Dedicated VOA output port, Switched VOA input port, and Switched VOA output port: Configure port name, description/comment, and port group assignment; retrieve port power and state.	109



**NOTE:** DVOAs and SVOAs are hardware optional features, see iosDedicatedVOA and iosSwitchedVOA in sysConfiguration (Figure 11 on page 45).

## VOA Unit Table—VOA Operation Configuration

A table with one row for each installed Dedicated VOA and Switched VOA.

Figure 25 IOS VOA Unit Module Table—iosVOAUnitTable

	voaUnitId	voaUnitType	voaUnitAlias	voaUnitMode	voaUnitPower	voaUnitStatus
1	20001	dVOA	VO-1	off	0.0	ready
2	20002	dVOA	VO-2	off	0.0	ready
3	20003	dVOA	VO-3	power	-23.4	ready
4	20004	dVOA	VO-4	off	0.0	ready
5	20005	dVOA	VO-5	off	0.0	ready
6	20006	dVOA	VO-6	off	0.0	ready
7	20007	dVOA	VO-7	power	-15.8	ready
8	20008	dVOA	VO-8	power	-15.8	ready
9	20049	sVOA	V-1	attenuate	2.0	ready
10	20050	sVOA	V-2	off	0.0	ready
11	20051	sVOA	V-3	off	0.0	ready
12	20052	sVOA	V-4	off	0.0	ready
13	20053	sVOA	V-5	off	0.0	ready
14	20054	sVOA	V-6	off	0.0	ready
15	20055	sVOA	V-7	off	0.0	ready
16	20056	sVOA	V-8	off	0.0	ready

The table below describes the IOS VOA Unit Table elements:

Element	Read/Write	Description
voaUnitId	IDX	Table row index: <ul style="list-style-type: none"> <li><b>20xxx</b>—The VOA output port number</li> </ul>
voaUnitType	RO	VOA type: <ul style="list-style-type: none"> <li><b>dVOA(1)</b>—Dedicated VOA</li> <li><b>sVOA(2)</b>—Switched VOA</li> </ul>

Element	Read/Write	Description
voaUnitAlias	RO	VOA unit alias: <ul style="list-style-type: none"> <li>• <b>VO-<i>n</i></b>—For DVOA, <math>1 &lt; n &lt; 32</math></li> <li>• <b>V-<i>n</i></b>—For SVOA, <math>1 &lt; n &lt; 32</math></li> </ul>
voaUnitMode	R/W	VOA operation mode: <ul style="list-style-type: none"> <li>• <b>off(1)</b>—VOA off (minimum attenuation)</li> <li>• <b>power(2)</b>—Constant output power mode</li> <li>• <b>attenuate(3)</b>—Constant attenuation mode (SVOA only)</li> </ul>
voaUnitPower	R/W	VOA value—Power (dBm) or Attenuation (dB): <ul style="list-style-type: none"> <li>• <b>[<i>-</i>]xx.x</b></li> </ul>
voaUnitStatus	RO	VOA status: <ul style="list-style-type: none"> <li>• <b>ready(1)</b>—Normal VOA operating status</li> <li>• <b>down(2)</b>—VOA failed</li> </ul>

## Configuring a VOA (Power/Attenuation)

To configure a VOA:

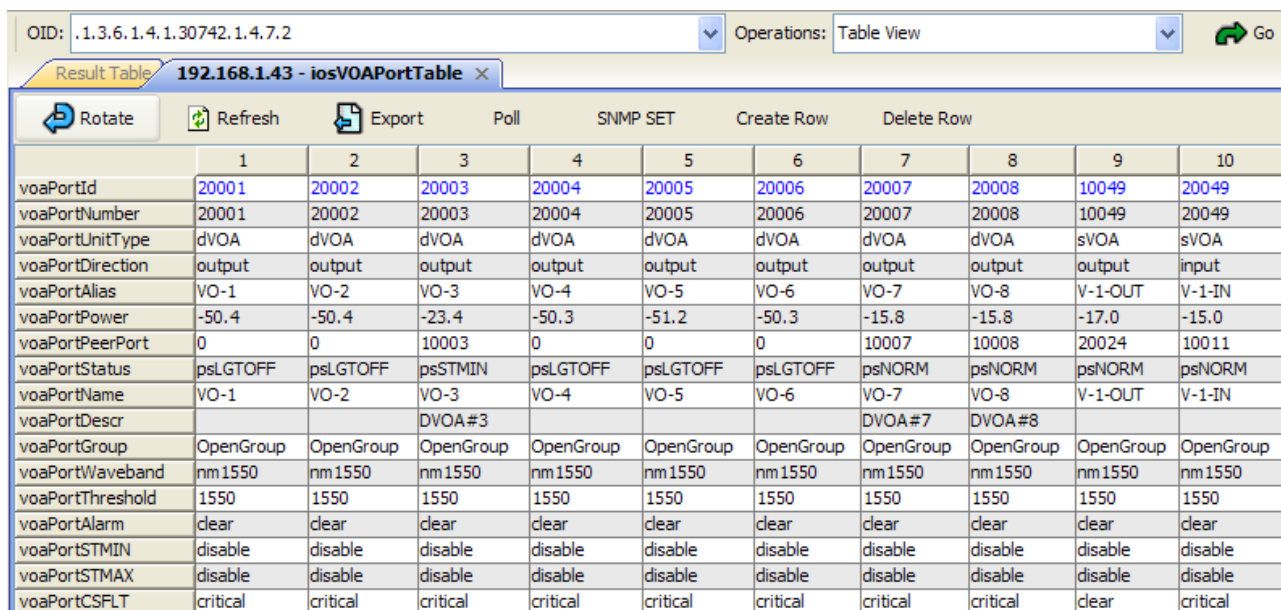
1. Browse to and view the iosVOAUnitTable (Figure 25 on page 107).
2. For the VOA row to be revised:
  - a. Optionally set the row's voaUnitMode:
    - **off(1)**—VOA off (minimum attenuation)
    - **power(2)**—Constant output power mode
    - **attenuate(3)**—Constant attenuation mode (SVOA only)
  - b. Optionally set the row's voaUnitPower
    - **[*-*]xx.x**—Power (dBm) for power mode
    - **xx.x**—Attenuation (dB) for attenuate mode

**NOTE:** Changes (SETs) to the VOA unit table are effective immediately.

## VOA Port Table—VOA Port Configuration

A table with one row for each Dedicated VOA output port, Switched VOA input port, and Switched VOA output port.

Figure 26 IOS VOA Port Table—iosVOAPortTable



	1	2	3	4	5	6	7	8	9	10
voaPortId	20001	20002	20003	20004	20005	20006	20007	20008	10049	20049
voaPortNumber	20001	20002	20003	20004	20005	20006	20007	20008	10049	20049
voaPortUnitType	dVOA	dVOA	dVOA	dVOA	dVOA	dVOA	dVOA	dVOA	sVOA	sVOA
voaPortDirection	output	output	output	output	output	output	output	output	output	input
voaPortAlias	VO-1	VO-2	VO-3	VO-4	VO-5	VO-6	VO-7	VO-8	V-1-OUT	V-1-IN
voaPortPower	-50.4	-50.4	-23.4	-50.3	-51.2	-50.3	-15.8	-15.8	-17.0	-15.0
voaPortPeerPort	0	0	10003	0	0	0	10007	10008	20024	10011
voaPortStatus	psLGTOFF	psLGTOFF	psSTMIN	psLGTOFF	psLGTOFF	psLGTOFF	psNORM	psNORM	psNORM	psNORM
voaPortName	VO-1	VO-2	VO-3	VO-4	VO-5	VO-6	VO-7	VO-8	V-1-OUT	V-1-IN
voaPortDescr			DVOA#3				DVOA#7	DVOA#8		
voaPortGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup
voaPortWaveband	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550
voaPortThreshold	1550	1550	1550	1550	1550	1550	1550	1550	1550	1550
voaPortAlarm	clear	clear	clear	clear	clear	clear	clear	clear	clear	clear
voaPortSTMIN	disable	disable	disable	disable	disable	disable	disable	disable	disable	disable
voaPortSTMAX	disable	disable	disable	disable	disable	disable	disable	disable	disable	disable
voaPortCSFLT	critical	critical	critical	critical	critical	critical	critical	critical	clear	critical

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the IOS VOA Port Table elements:

Element	Read/Write	Description
voaPortId	IDX	Table row index, same as the voaPortNumber
voaPortNumber	RO	VOA port number: <ul style="list-style-type: none"> <li>• <b>10xxx</b>—SVOA output (switch input port)</li> <li>• <b>20xxx</b>—SVOA input (switch output port)</li> <li>• <b>20xxx</b>—DVOA output (switch output port)</li> </ul>
voaPortUnitType	RO	VOA type: <ul style="list-style-type: none"> <li>• <b>dVOA(1)</b>—Dedicated VOA</li> <li>• <b>sVOA(2)</b>—Switched VOA</li> </ul>
voaPortDirection	RO	VOA port direction: <ul style="list-style-type: none"> <li>• <b>input(1)</b>—SVOA input</li> <li>• <b>output(2)</b>—DVOA/SVOA output</li> </ul>

Element	Read/Write	Description
voaPortAlias	RO	VOA port alias: <ul style="list-style-type: none"> <li>• <b>VO-<i>n</i></b>—For DVOA, <math>1 &lt; n &lt; 32</math></li> <li>• <b>V-<i>n</i>-IN</b>—For SVOA input, <math>1 &lt; n &lt; 32</math></li> <li>• <b>V-<i>n</i>-OUT</b>—For SVOA output, <math>1 &lt; n &lt; 32</math></li> </ul>
voaPortPower	RO	VOA port power (dBm): <ul style="list-style-type: none"> <li>• <b>[<i>-</i>]xx.x</b></li> </ul>
voaPortPeerPort	RO	VOA peer port number: <ul style="list-style-type: none"> <li>• <b>0</b>—DVOA/SVOA port not connected</li> <li>• <b>10xxx</b>—DVOA/SVOA input connected to this port</li> <li>• <b>20xxx</b>—DVOA port, SVOA output connected</li> </ul>
voaPortStatus	RO	VOA Port Status: <ul style="list-style-type: none"> <li>• <b>psDAMAGE(9)</b>—port is marked bad</li> <li>• <b>psSTMAX(3)</b>—port power above sigThreshPowerMax and below iosMaxSystemPower</li> <li>• <b>psNORM(1)</b>—port power is between sigThreshPowerMin and sigThreshPowerMax</li> <li>• <b>psSTMIN(2)</b>—port power is below sigThreshPowerMin and greater -40 dBm</li> <li>• <b>psPWRMIN(4)</b>: <ul style="list-style-type: none"> <li>• dVOA output: Connected and power below -40dBm</li> <li>• sVOA output: Connected and power below -40dBm</li> </ul> </li> <li>• <b>psLGTOFF(6)</b>: <ul style="list-style-type: none"> <li>• dVOA output: Not connected, power below -40dBm</li> <li>• sVOA input: Not connected, power below -40dBm</li> </ul> </li> <li>• <b>psLGTRVRS(8)</b>: <ul style="list-style-type: none"> <li>• dVOA output: Not connected and power above -40 dBm (reverse light)</li> <li>• dVOA output: Connected, power higher than connected input (reverse light)</li> <li>• sVOA input: Not connected and power above -40 dBm (reverse light)</li> <li>• sVOA input: Connected, power higher than at sVOA output (reverse light)</li> </ul> </li> <li>• <b>psUDEF(0)</b>—Power monitor failure</li> </ul>
voaPortName	R/W	Port name (0-32 characters), port names must be unique. Installation defaults: <ul style="list-style-type: none"> <li>• DVOA: <b>voaUnitAlias</b></li> <li>• SVOA Input: <b>voaUnitAlias-IN</b></li> <li>• SVOA Output: <b>voaUnitAlias-OUT</b></li> </ul>

Element	Read/Write	Description
voaPortDescr	R/W	Port Comment/Description (0-32 characters). Installation default: <ul style="list-style-type: none"> <li>• Null</li> </ul>
voaPortGroup	R/W	Port group name (1-32 characters) Installation Default: <ul style="list-style-type: none"> <li>• <b>OpenGroup</b></li> </ul>
voaPortWaveband	RO	Waveband in use for port: <ul style="list-style-type: none"> <li>• <b>nm1310(1)</b> or <b>nm1550(2)</b></li> </ul>
voaPortThreshold	R/W	Signal Threshold name (1-32 characters), must correspond to a signal threshold listed in the iosSigThresholdTable (see page 98): Installation default: <ul style="list-style-type: none"> <li>• <b>1550</b></li> </ul>
voaPortAlarm	RO	Current alarm status (most severe). See the description for voaPortStatus on page 110 for possible alarm types. <ul style="list-style-type: none"> <li>• No Alarm = <b>clear(6)</b></li> <li>• Alarms = <b>critical(1), major(2), minor(3), notice(4)</b></li> </ul>
voaPortSTMIN	R/W	Severity for STMIN alarm on port: <ul style="list-style-type: none"> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>
voaPortSTMAX	R/W	Severity for STMAX alarm on port: <ul style="list-style-type: none"> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>
voaPortCSFLT	R/W	Severity setting for DVOA ports and SVOA input ports (voaPortDirection=input). <b>NOTE:</b> This setting has no meaning for SVOA output ports (voaPortDirection=output) as these are actually switch input ports. <ul style="list-style-type: none"> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>

## Configuring a VOA Port (Name/Description)

To configure a VOA port:

1. Browse to and view the iosVOAPortTable (Figure 26 on page 109).
2. For the VOA port table row to be revised:
  - a. Optionally set the row's voaPortName (Port Name, 0-32 characters). Non-null port names must be unique: no two ports may have the same non-null name.
  - b. Optionally set the row's voaPortDescr (Port Comment/Description, 0-32 characters)

- c. Optionally set the row's voaPortGroup (port group name, 1-32 characters) to assign the port to a port group. The port group name must have been defined, see "Port Grouping - iosPortGroupTable" on page 75.
- d. Optionally set the row's voaPortThreshold (signal threshold name, 1-32 characters) to assign the port a new signal threshold. The signal threshold name must have been defined, see "Signal Threshold Table—iosSigThresholdTable " on page 98.
- e. Optionally set the row's voaPortSTMIN (STMIN alarm severity).
- f. Optionally set the row's voaPortSTMAX (STMAX alarm severity).
- g. Optionally set the row's voaPortCSFLT (CSFLT alarm severity).

**NOTES:**

- Changes (SETs) to the port table are effective immediately.
- Optionally modification of the port group name column may be inhibited via VACM

## Multicast (PMU) Tables

The Photonic Multicasting feature allows any incoming signal (port) to be connected to the input of an internal splitter (1xN). The "N" outputs of the splitter may then be connected to any output port. This allows a single incoming signal to be issued to multiple outputs (multicast). The incoming signal content is unchanged by the split, but the output power level on each leg will be lower due to the second pass through the switch, and the loss of the splitter (the number of splits and split ratio; e.g., 1x2 splitter with 50/50 split ratio as opposed to 1x2 splitter with 90/10 ratio).

The Photonic Multicast Unit (PMU) Tables are tables for viewing the optional PMUs (Figure 27) and configuring their associated ports (Figure 28 on page 114).

Multicast Tables	Description	Page
iosPMCUntTable	A read-only table with one row for each installed PMU: Retrieve PMU type and PMU input port number (switch output port number).	112
iosPMCPortTable	A table with one row for each installed PMU input port and output port: Configure port name, description/comment, and port group assignment; retrieve port power and state.	113

**NOTE:** PMUs are a hardware optional feature, see iosPhotonicMulticast in sysConfiguration (Figure 11 on page 45).

### Multicast Unit Table—List of installed PMUs

A read-only table with one row for each installed PMU.

Figure 27 IOS Multicast Unit Table—iosPMCUntTable

	1	2
pmcUnitId	20049	20050
pmcUnitType	pmc1x4	pmc1x2
pmcUnitAlias	MC-1	MC-2
pmcUnitStatus	ready	ready

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the IOS Multicast Unit Table elements:

Element	Read/Write	Description
pmcUnitId	RO	Table row index: <ul style="list-style-type: none"> <li><b>20xxx</b>—PMU input port (switch output port number)</li> </ul>
pmcUnitType	RO	Multicast type: <ul style="list-style-type: none"> <li><b>pmc1xn(n)</b>—1xn splitter (1 input, <i>n</i> outputs)</li> </ul>
pmcUnitAlias	RO	Multicast alias: <ul style="list-style-type: none"> <li><b>MC-<i>n</i></b>—<i>n</i> = 1 for first PMU, 2 for second, etc.</li> </ul>
pmcUnitStatus	RO	PMC status: <ul style="list-style-type: none"> <li><b>ready(1)</b>—Normal PMC operating status</li> <li><b>down(2)</b>—PMC failed (passive PMCs cannot “fail”)</li> </ul>

## Multicast Port Table—PMU Port Configuration

A table with one row for each PMU input port and PMU output port.

Figure 28 IOS Multicast Port Table—iosPMCPortTable

OID: .1.3.6.1.4.1.30742.1.4.8.2 Operations: Table View Go

Result Table 192.168.2.43 - iosPMCPortTable

	1	2	3	4	5	6	7	8
pmcPortId	10049	10050	10051	10052	20049	10053	10054	20050
pmcPortNumber	10049	10050	10051	10052	20049	10053	10054	20050
pmcPortDirection	output	output	output	output	input	output	output	input
pmcPortAlias	MC-1-1	MC-1-2	MC-1-3	MC-1-4	MC-1	MC-2-1	MC-2-2	MC-2
pmcPortPower	-22.3	-22.2	-22.8	-22.5	-15.1	-5.7	-5.6	-2.4
pmcPortPeerPort	20021	0	20023	0	10003	20011	20012	10001
pmcPortStatus	psSTMIN	psSTMIN	psSTMIN	psSTMIN	psNORM	psNORM	psNORM	psNORM
pmcPortName	MC-1-1	MC-1-2	MC-1-3	MC-1-4	MC-1	MC-2-1	MC-2-2	MC-2
pmcPortDescr								
pmcPortGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup	OpenGroup
pmcPortWaveband	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550	nm1550
pmcPortThreshold	1550	1550	1550	1550	1550	1550	1550	1550
pmcPortAlarm	clear	clear	clear	clear	clear	clear	clear	clear
pmcPortSTMIN	disable	disable	disable	disable	disable	disable	disable	disable
pmcPortSTMAX	disable	disable	disable	disable	disable	disable	disable	disable
pmcPortCSFLT	clear	clear	clear	clear	critical	clear	clear	critical

**NOTE:** For presentation clarity, the table display is rotated showing table rows as columns.

The table below describes the IOS Multicast Port Table elements:

Element	Read/Write	Description
pmcPortId	RO	Table row index, per pmcPortNumber
pmcPortNumber	RO	Multicast port number: <ul style="list-style-type: none"> <li>• <b>10xxx</b>—Multicast output (switch input port)</li> <li>• <b>20xxx</b>—Multicast input (switch output port)</li> </ul>
pmcPortDirection	RO	Multicast port direction: <ul style="list-style-type: none"> <li>• <b>input(1)</b>—Multicast input</li> <li>• <b>output(2)</b>—Multicast output</li> </ul>
pmcPortAlias	RO	Multicast port alias: <ul style="list-style-type: none"> <li>• <b>MC-<i>n</i></b>—PMU input, <i>n</i> = 1 for first PMU, 2 for second ...</li> <li>• <b>MC-<i>n-m</i></b>—PMU output, <i>m</i>=1 for first splitter output, 2 ...</li> </ul>
pmcPortPower	RO	Multicast port power (dBm): <ul style="list-style-type: none"> <li>• <b>[<i>-</i>]xx.x</b></li> </ul>
pmcPeerPort	RO	Multicast peer port number: <ul style="list-style-type: none"> <li>• <b>0</b>—Multicast port not connected</li> <li>• <b>10xxx</b>—Multicast input connected to this port</li> <li>• <b>20xxx</b>—Multicast output connected to this port</li> </ul>



Element	Read/Write	Description
pmcPortStatus	RO	<p>Multicast port status:</p> <ul style="list-style-type: none"> <li>• <b>psDAMAGE(9)</b>—port is marked bad</li> <li>• <b>psSTMAX(3)</b>—port power is above sigThreshPowerMax and below iosMaxSystemPower</li> <li>• <b>psNORM(1)</b>—port power is between sigThreshPowerMin and sigThreshPowerMax</li> <li>• <b>psSTMIN(2)</b>—port power is below sigThreshPowerMin and greater -40 dBm</li> <li>• <b>psPWRMIN(4)</b>: <ul style="list-style-type: none"> <li>• multicast output: power below -40 dBm</li> <li>• multicast input: Connected, power below -40dBm</li> </ul> </li> <li>• <b>psLGTOFF(6)</b>—multicast input: Not connected, power below -40dBm</li> <li>• <b>psLGTRVRS(8)</b>—multicast input: Not connected, power above -40dBm, or power is higher than power at multicast output (reverse light)</li> <li>• <b>psUDEF(0)</b>—port power unknown - no input detection in for multicast outputs or failed power monitor.</li> </ul>
pmcPortName	R/W	<p>Port name (0-32 characters), port names must be unique. Installation default:</p> <ul style="list-style-type: none"> <li>• Multicast Input: <b>pmcUnitAlias-1</b></li> <li>• Multicast Output: <b>pmcUnitAlias-n</b></li> </ul>
pmcPortDescr	R/W	<p>Port comment/description (0-32 characters). Installation default:</p> <ul style="list-style-type: none"> <li>• Null</li> </ul>
pmcPortGroup	R/W	<p>Port group name (1-32 characters) Installation Default:</p> <ul style="list-style-type: none"> <li>• <b>OpenGroup</b></li> </ul>
pmcPortWaveband	RO	<p>Waveband in use for port:</p> <ul style="list-style-type: none"> <li>• <b>nm1550</b> or <b>nm1310</b></li> </ul>
pmcPortThreshold	R/W	<p>Signal Threshold name (1-32 characters), must correspond to a signal threshold listed in the iosSigThresholdTable (see page 98): Installation default:</p> <ul style="list-style-type: none"> <li>• <b>1550</b></li> </ul>
pmcPortAlarm	RO	<p>Current alarm status (most severe). See the description for pmcPortStatus on page 115 for possible alarm types.</p> <ul style="list-style-type: none"> <li>• No Alarm = <b>clear(6)</b></li> <li>• Alarms = <b>critical(1), major(2), minor(3), notice(4)</b></li> </ul>
pmcPortSTMIN	R/W	<p>Severity for STMIN alarm on port:</p> <ul style="list-style-type: none"> <li>• Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>

Element	Read/Write	Description
pmcPortSTMAX	R/W	Severity for STMAX alarm on port: <ul style="list-style-type: none"> <li>Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>
pmcPortCSFLT	R/W	Severity setting for input PMU ports (pmcPortDirection=input). <b>NOTE:</b> This setting has no meaning for PMU output ports (pmcPortDirection=output) as these are actually switch input ports. <ul style="list-style-type: none"> <li>Allowed settings: <b>critical(1), major(2), minor(3), notice(4), disable(5)</b></li> </ul>

## Configuring a PMU Port (Name/Description)

To configure a PMU port:

- Browse to and view the iosPMCPortTable (Figure 28 on page 114).
- For the PMC port table row to be revised:
  - Optionally set the row's pmcPortName (Port Name, 0-32 characters). Non-null port names must be unique: no two ports may have the same non-null name.
  - Optionally set the row's pmcPortDescr (Port Comment/Description, 0-32 characters)
  - Optionally set the row's pmcPortGroup (port group name, 1-32 characters) to assign the port to a port group. The port group name must have been defined, see "Port Grouping - iosPortGroupTable" on page 75.
  - Optionally set the row's pmcPortThreshold (signal threshold name, 1-32 characters) to assign the port a new signal threshold. The signal threshold name must have been defined, see "Signal Threshold Table—iosSigThresholdTable" on page 98.
  - Optionally set the row's pmcPortSTMIN (STMIN alarm severity).
  - Optionally set the row's pmcPortSTMAX (STMAX alarm severity).
  - Optionally set the row's pmcPortCSFLT (CSFLT alarm severity).

**NOTES:**

- Changes (SETs) to the port table are effective immediately.
- Optionally modification of the port group name column may be inhibited via VACM