Contents

Figures

Overview

This document explains how to use the Simple Network Management Protocol (SNMP) to manage Xyplex 610 LAN Switch Processors (LSPs). It assumes that you are using an SNMP-based network management software application such as Xyplex ControlPoint™ to manage the 610s. Hereafter, this document refers to your network management application as a Network Operations Center (NOC).

Additionally, this chapter describes the RMON (Remote Monitoring) application and the type of network management applications that enable you to use RMON.

Xyplex SNMP Support

SNMP is an Internet standard protocol, defined by the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157, which specifies how network management information is carried through a network. Xyplex 610s support SNMP by implementing an SNMP agent. The agent stores Management Information Base (MIB) data and makes it available when requested via SNMP Set, Get, and Get_Next requests.

In addition, Xyplex 610s generate SNMP Trap messages. Traps are notices that the 610 sends to an SNMP manager indicating that a specific event has occurred, or that the condition of a unit has changed significantly.

Obtaining/Importing the Supported MIBs

If you are using the Xyplex ControlPoint software, you do not need to import any MIBs. The ControlPoint software package includes all of the required MIBs. If you are not using ControlPoint, you can use SNMP to manage all of the 610's operational parameters if your NOC can compile proprietary MIBs.

The Xyplex proprietary MIBs are available to Premium Support Customers through the Xyplex World Wide Web (WWW) server: http://www.xyplex.com. Select the Customer Support access tab.

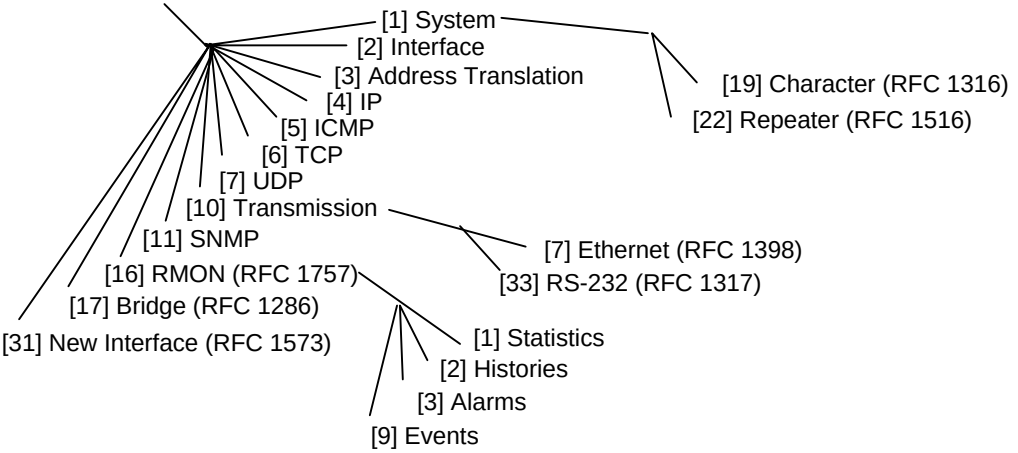
In addition, Xyplex has a MIB kit containing all the standard and Xyplex-proprietary MIBs that Xyplex products support. The kit also includes a text file that lists the MIB groups supported by the 610 SNMP agent, and provides useful information about how the agent handles MIB objects.

To obtain the MIB kit, contact your Xyplex sales representative or distributor or call 1-800-338-5316 (U.S.) or 1-508-952-4700 (international).

The following diagrams show the LSP supported MIBs. Tree nodes give the Abstract Syntax Notation Number One in brackets, followed by the MIB name, and relevant RFC numbers.

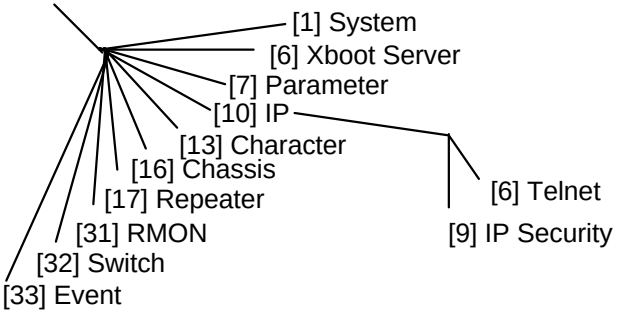
LSP Standard MIB Structure

[1.3.6.1.2] MIB II (RFC1213)



LSP Proprietary MIB Structure

[1.3.6.1.4.1.33] Xyplex MIB



Getting Started

To enable your NOC to communicate with a Xyplex 610, you must assign it an IP address. Use the following command:

```
DEFINE IP  Address  ip-address
```

The address you assign must be valid for the network connected to the 610. In a routed network, depending on the switch location, you also need to assign a subnet mask (optional) and gateway, as follows:

```
DEFINE IP  Address  ip-address  Mask  subnet-mask
```

```
DEFINE IP [PRIMARY]   GATEWAY  ip-address
          [SECONDARY]
```

To make sure that your NOC can exchange information with the 610, Ping the 610 from the NOC.

Examples

```
Xyplex>> define ip address 192.168.26.9 mask 255.255.255.128
Xyplex>> define ip primary gateway   address 192.168.46.3
```

Use the following command to view Help for SNMP commands:

```
Xyplex>> help def snmp
```

Defining a Trap Client

IMPORTANT
A 610 module will not generate SNMP Trap messages until you define a Trap Client.

A Trap Client is a specific NOC to which the 610 sends Trap messages. You can define one or more Trap Clients through the following command:

```
DEFINE SNMP  TRAP CLIENT index  [INTERNET  internet-address ]
                                [ADDRESS  ethernet-address ]
```

An index value is a number from 1 to 4. An internet-address or ethernet-address is the address of the NOC that you want to receive the Trap messages.

Example

```
Xyplex>> define snmp trap client 1 internet 1   72.18.12.3
```

Enabling SNMP Event Logging

You can optionally enable SNMP event logging, as follows:

```
DEFINE EVENT SNMP  LOGGING ENABLED
```

You can view the trap messages the 610 generates with the following command:

```
SHOW/MONITOR EVENT LOG
```

NOTE: The 610 saves Trap messages in its Management Event Log, even when no Trap clients have been defined. Refer to SNMP Traps on page 11 for additional information.

Configuring SNMP Security

A Xyplex 610 accepts SNMP Get, Get_Next, and Set requests from any NOC by default. Optionally, you can restrict SNMP access to the 610 by defining SNMP Clients and Communities. A Client is a specific NOC that you identify with an IP or Ethernet address. A Community refers to one or more NOCs that specify the same Community string in their SNMP messages.

Table 1 shows how Get/Set Client and Community values determine which NOCs can manage a 610:

Table 1. Get/Set Client and Community Settings

Get/Set Client	Get/Set Community	NOCs that Can Issue Get/Set Requests
None	None	Any
None	Defined	NOCs that know the Community value
Defined	None	NOCs defined as Clients
Defined	Defined	NOCs defined as Clients that know the Community value

Defining Get and Set SNMPClients

A Get Client is a specific NOC that is allowed to manage the 610 through Get and Get_Next requests. A Set Client is a NOC that can issue Set requests to the 610. Use the following commands to define up to four of each of these client types:

```
DEFINE SNMP  GET CLIENT  index   [INTERNET  internet-address
                                 [ADDRESS  ethernet-address ]
                                 [NONE]

DEFINE SNMP  SET CLIENT  index   [INTERNET  internet-address ]
                                 [ADDRESS  ethernet-address ]
                                 [NONE]
```

An index value is a number from 1 to 4.

Use the keyword NONE to delete a previously defined Get or Set Client.

NOTE: Be sure to define Get and Set Client entries for your NOC before you define any other Get or Set Clients.

Examples

```
Xyplex>> define snmp set client 1 internet 1   72.18.121.3
Xyplex>> define snmp set client 1 address 00-00-93-a1-23-d2
```

Defining SNMP Communities

Get and Set Communities provide an additional level of SNMP security. If you do not define a Get Clients, the 610 accepts Get and Get_Next requests from any NOC whose Get requests include a Community string matching the 610's Get Community. If you do not define a Get Community, the 610 accepts Get and Get_Next requests from any NOC.

Similarly, if you do not define any Set Clients, the 610 accepts Set requests from any NOC whose messages include a Community string matching the 610's Set Community. If you do not define a Set Community, the 610 accepts Set requests from any NOC.

If you define a Trap Community, the 610 includes the Trap Community string in the Trap messages it generates.

The following commands define Get, Set, and Trap Community strings:

```
DEFINE SNMP  GET COMMUNITY   [“community-string” ]
                             [NONE]

DEFINE SNMP  SET COMMUNITY   [“community-string” ]
                             [NONE]

DEFINE SNMP  TRAP COMMUNITY  “community-string”
```

A community-string can comprise up to 23 characters. Do not include spaces. Use the value NONE to delete a previously defined Get or Set Community.

Examples

```
Xyplex>> define snmp get community none
Xyplex>> define snmp set community “xyplex”
```

SNMP Traps

Traps are notices that the 610 sends to an SNMP manager indicating that a specific event has occurred, or that the condition of a unit has changed significantly.

SNMP Traps are disabled by default. Use the following command to enable SNMP traps:

```
DEFINE SNMP  TRAPS ALL ENABLED
```

To enable or disable individual traps, refer to page 13.

NOTE: Trap messages do not provide an entirely reliable event notification mechanism; they can get dropped, and are not acknowledged or retransmitted once dropped.

Authentication Failures	This trap is generated whenever a login attempt fails during the authentication process on a management port.
Cold Start	The 610 is initializing and the configuration might change. The 610 generates this Trap immediately after loading parameters. (The software is unable to determine where to send the Trap until parameters are loaded.)
Link Status	One of the 610's external ports has come up. or a failure has occurred on one of the ports.
Memory Card Change	A flash memory card has been inserted or removed.

Resource Failures	Insufficient resources prevented the 610 from creating an internal data structure.
RMON Alarm Rising/Falling	An RMON alarm is reporting a rising or falling threshold condition.
Switch Integrity Loss	An external port has lost link integrity.

SNMP generates one trap for each occurrence of its defined event. SNMP sends the Trap message to each recipient in the Trap Client list. If a client is identified through an Ethernet address, the Trap message is sent using SNMP over Ethernet, in accordance with RFC 1089. No Traps are transmitted to IP hosts if the 610 has not been assigned an IP address.

NOTE: You enable or disable RMON trap generation when you configure an RMON alarm. Generation of a trap message is an alarm configuration option. Refer to the ControlPoint Tools User's Guide for additional information on RMON.

Enabling/Disabling Traps

Use the following commands to enable or disable Trap types:

```
DEFINE SNMP  TRAP   [ALL  [ENABLED]]
                         [DISABLED]

                    [AUTHENTICATION FAILURES   [ENABLED]]
                                               [DISABLED]

                    [COLD START   [ENABLED]]
                                  [DISABLED]

                    [COMMUNITY   [ENABLED]]
                                 [DISABLED]

                    [LINKS STATUS   [ENABLED]]
                                    [DISABLED]

                    [MEMORY CARD CHANGE   [ENABLED]]
                                          [DISABLED]

                    [RESOURCE FAILURES    [ENABLED]]
                                          [DISABLED]

                    [SWITCH INTEGRITY LOSS   [ENABLED]]
                                             [DISABLED]
```

Examples

```
Xyplex>> define SNMP trap   cold start  enabled
Xyplex>> define SNMP trap authentication failures enabled
```

The RMON and the proprietary Xyplex XRMON traps are always enabled.

Miscellaneous SNMP Settings

This section explains how to define SNMP Contact and Location strings for a 610.

Contact

An SNMP contact is someone to communicate with when the 610 requires attention. Use this command to define a contact:

```
DEFINE SNMP  CONTACT " contact-string "
```

The "contact-string" can comprise up to 60 characters; it cannot contain spaces.

Example

```
Xyplex>> define SNMP  contact " lexie_bergeron "
```

Location

A Location string specifies where the 610 is located. Use the following command to specify a location:

```
DEFINE SNMP  LOCATION " location-string "
```

The “location-string” can comprise up to 60 characters within quotation marks.

Example

```
Xyplex>> define snmp location “closet_1”
```

Viewing SNMP Settings and Counters

This section describes the commands that you use to view a 610's SNMP settings and status. Use the following commands to generate these displays:

```
SHOW/MONITOR SNMP   {CHARACTERISTICS}
                    [COUNTERS]
```

Use SHOW commands to view current information. Use MONITOR commands to view a continuously updated display. To halt a SHOW display, press the <BREAK> key. Press any key to halt a MONITOR display.

```
Xyplex>> SHOW SNMP CHAR
08-00-87-05-27-A6 (X0527A6)  LP/610S   24 Oct 1995 18:34:46

Contact:
Location:

Get Community:                          Set Community:
Get Client 1: 192.168.23.2              Set Client 1: Kirsten
Get Client 2: 192.168.26.5              Set Client 2: Tim
Get Client 3:                           Set Client 3:
Get Client 4:                           Set Client 4:

Trap Community: public
Trap Client 1:                          Trap Client 3:
Trap Client 2:                          Trap Client 4:

Enabled Traps: All
```

Figure 1. SNMP Characteristics Display

```
Xyplex>> SHOW SNMP COUNTERS
08-00-87-05-27-A6 (X0527A6)           LP/610S       Since Zero:    93120

                                SNMP
Messages Received:             2988   Messages Sent:                  2988
Get Requests Received:            4   Get Requests Sent:                 0
Get Next Requests Received:    2984   Get Next Requests Sent:            0
Get Responses Received:           0   Get Responses Sent:             2988
Set Requests Received:            0   Set Requests Sent:                 0
                                      Traps Sent:

Requested Objects:             3376   Set Objects:                       0
                              SNMP   ERRORS
Version:                          0   Too Big:                           0
Community Name:                   0   No Such Name:                      0
Community Use:                    0   Bad Value:                         0
ASN Parse:                        0   Read Only:                         0
Other:                            0
```

Figure 2. SNMP Counters Display

Field	Description (since the last zero command)
SNMP ERRORS	
Version	Packets the 610 has received that included an incorrect SNMP version number (not currently supported).
Community Name	Packets the 610 received that included an invalid Community name.
Community Use	Packets the 610 received that included a valid Community name, but for the wrong type of request.
ASN Parse	Packets the 610 received that contained a message that could not be processed (parsed).
Other	Miscellaneous errors the 610 has detected.
Too Big	Response packets that the 610 could not finish because the response message was too big for an Ethernet frame.
No Such Name	Requests the 610 received for objects that are not included in the supported MIBs, or set requests by read-only objects..
Bad Value	Values the 610 received in Set requests that were out of range for the corresponding object. For example, if you define a Forwarding Age Timer value that is out of the 360 to 1800 seconds range, you receive a Bad Value error.
Read Only	Set Requests the 610 received for objects that are read-only

RMON (Remote Monitoring)

The 610 software includes an RMON agent. Standard RMON is a network monitoring application that is defined by IETF RFC 1757, which specifies a standard method of providing information about network activity. RMON is enabled by default on the 610.

You access and manage RMON through SNMP. Therefore, you must have an RMON client network management application. Xyplex offers these options:

- Xyplex ControlPoint
- AXON™ Networks LANServant™ Manager

ControlPoint RMON support enables you to perform distributed network management and monitoring.

RMON enables you to configure switching ports, on a per-port basis, to report when traffic or error thresholds are reached and when specific events occur.

The 610 supports the following standard RMON MIB groups:

RMON Statistics – Defines statistics that are collected for a given interface, which is an Ethernet port.

RMON History – Collects a historical view of user-selected variables. The Xyplex RMON History extensions allow you to collect history on any MIB variable, in addition to the standard RMON Statistics. You can designate separate buffers that gather samples at different time sequences; for example, every 30 seconds for one hour, or every hour for two days.

RMON Alarm – Defines device thresholds and triggers events when the thresholds are crossed.

RMON Event – Defines the action taken when an associated alarm is detected; for example, you can instruct the 610 to log the event and send a trap to the network manager.

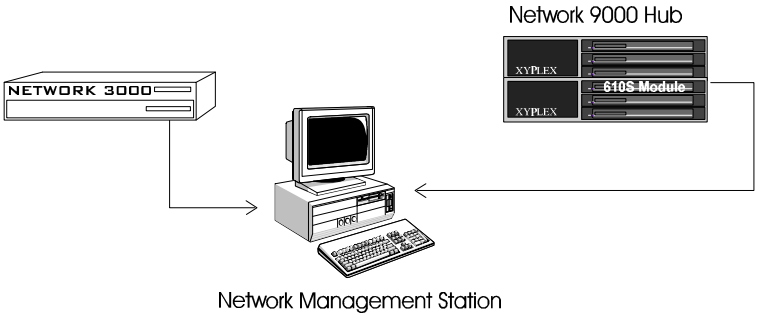


Figure 3. RMON Distributed Monitoring

You can configure the 610 to:

- Generate an SNMP trap message when an alarm condition occurs.
- Record alarms in its Event Log.
- Collect historical data automatically to help establish baseline behavior for a device.

Sample RMON History Configuration

ControlPoint Releases 4.1 and later support the RMON History Group through the Get/Set Parameters (Status and Configuration) application. In addition to the RMON History Configuration view shown in Figure 4, you can also generate:

RMON History Study Data View– Shows all data samples for a specified history study.

RMON History Summary View– Shows a summary of all configured history studies.

RMON History Table View– Shows the RMON standard control and data tables.

Refer to the ControlPoint Tools User's Guide for an explanation on how to configure RMON History, Alarms, Events, and Log Summaries.

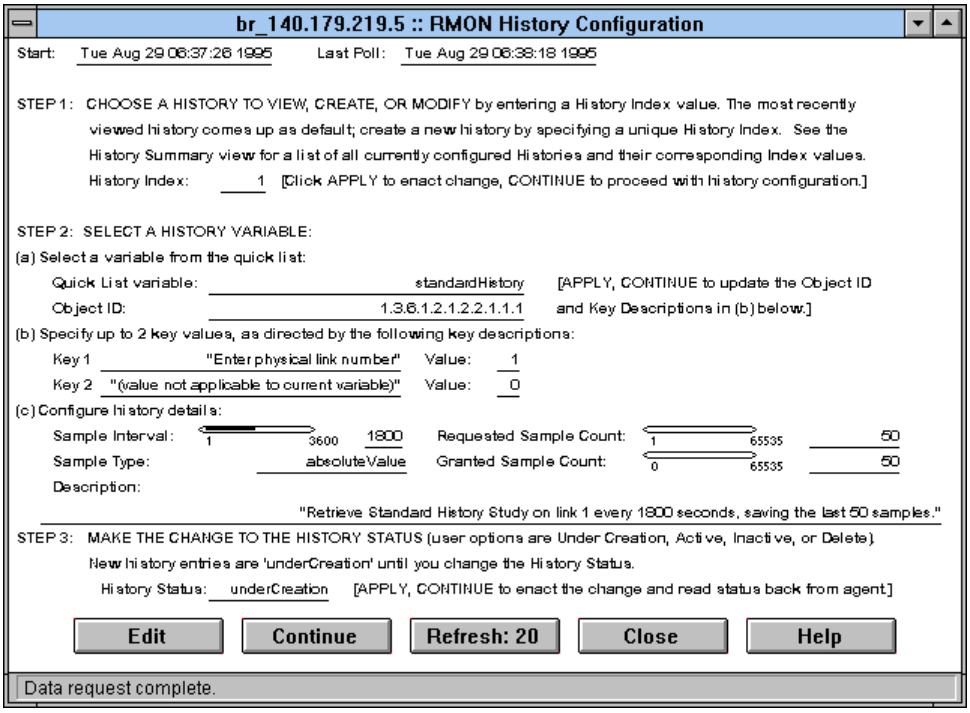


Figure 4. ControlPoint RMON History Configuration View

Sample RMON Alarm Configuration

ControlPoint Releases 4.1 and later include RMON Alarm Configuration. Figure 5 shows a sample of the ControlPoint RMON Alarm Configuration view. Refer to the ControlPoint Tools User's Guide for details on how to use RMON Alarm Configuration.

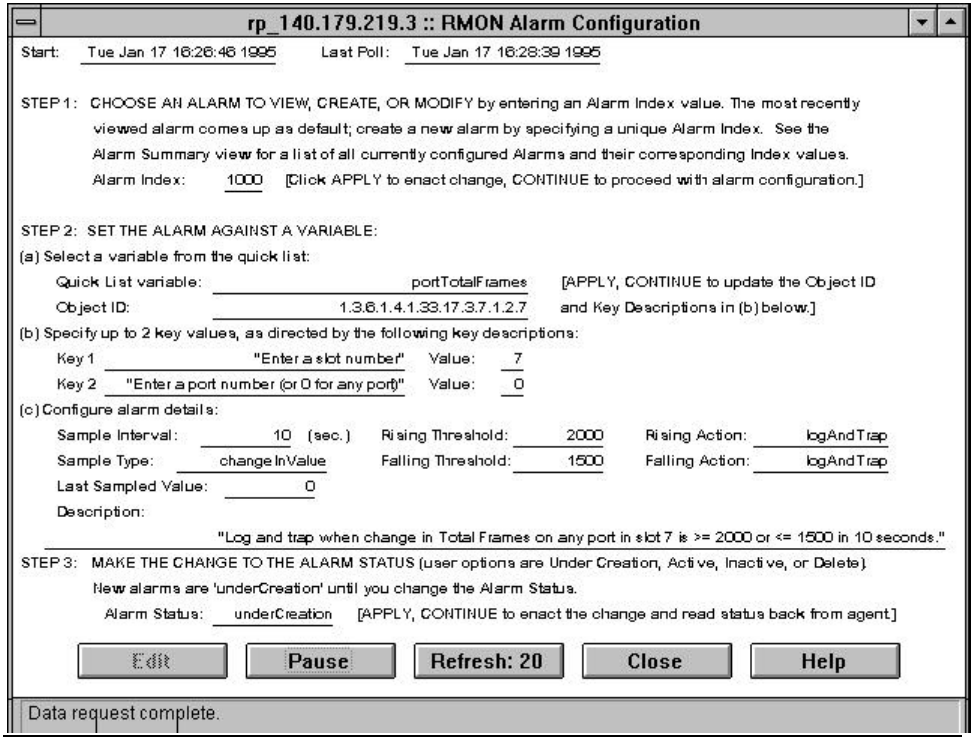


Figure 5. ControlPoint RMON Alarm Configuration View

Viewing RMON Events

When the 610 generates SNMP traps in response to RMON alarms, it also logs the alarms in its Event Log. To view the log (Figure 6 shows a sample display), enter the command:

```
SHOW EVENT LOG
```

```
Xyplex>> sh event log
08-00-87-05-70-13 (X057013)                LP/610S

Timestamp                Event Log
10 Nov 1995 20:38:09 (L) FSM: Cpu Unicast Frame addr = 800, 8705, 7013 dst port
10 Nov 1995 20:38:49 (L) FSM: Cpu Unicast Frame addr = 800, 8705, 7013 dst port
10 Nov 1995 20:38:49 (L) FSM: Cpu Unicast Frame addr = 800, 8705, 7013 dst port
10 Nov 1995 20:41:56 (L) VLMP: Frame type 0 received.
10 Nov 1995 20:43:34 (L) FSM: Cpu Unicast Frame addr = 0, c025, 3e0e dst port
10 Nov 1995 20:43:35 (L) FSM: Cpu Unicast Frame addr = 0, c054, c4d dst port
10 Nov 1995 20:43:38 (L) FSM: Cpu Frame addr = 800, 8705, 6ef5 Flooded to port
10 Nov 1995 20:43:39 (L) FSM: Cpu Frame addr = 800, 8702, 6be3 Flooded to port
10 Nov 1995 20:43:40 (L) FSM: Cpu Multicast Frame addr = 900, 8790, ffff, Mask
```

Figure 6. Show Event Log Display

Refer to the chapter “RMON (Remote Monitoring)” in the ControlPoint Tools User’s Guide for additional information.

Network Management Applications

You perform RMON configuration and monitoring through one of the following applications:

- ControlPoint, Release 4.1 or later
- Third-party RMON client software, such as the AXON Networks LANServant Manager
- SNMP MIB Browser application

These applications provide a graphical user interface to RMON functions.

The following sections describe the options available for interoperability with a standard RMON client. Refer to the documentation supplied with your network management application for specific instructions.

ControlPoint

ControlPoint Release 4.1 provides tools that simplify the generation of RMON history and statistics tables, as well as configuring and monitoring RMON alarms and events. ControlPoint also supports Xyplex extensions to RMON History, enabling you to collect historical data on any variable.

AXON Networks LANServant Manager

The AXON Networks LANServant Manager enables you to configure and monitor a distributed network environment from a single console. AXON Networks LANServant Manager supports the nine standard RMON MIB groups, including:

- Statistics
- History
- Alarm
- Event
- Host
- HostTopN
- Matrix
- Filter
- Packet Capture

MIB Browser

If you are using a third-party RMON client, you can use a MIB browser to configure RMON MIB groups.

Most network management platforms provide a MIB browser application or tool. The specific procedure that you use depends on the MIB browser application.

NOTE: You must have the Xyplex RMON MIB to manage Xyplex devices through a third-party MIB browser. The Xyplex RMON MIB is available to Premium Support Customers through the Xyplex World Wide Web (WWW) server: http://www.xyplex.com. Select the Customer Support access tab.

Index

Index