MXK-F Monitoring Guide

For software version 3.3
Aug, 2020
Document Part Number: 830-04155-06

Enabling the
Hyper-Connected World

DZS AMERICAS
Global Headquarters &
Regional Headquarters
Plano, TX, USA
info@dzsi.com
www.dzsi.com/contact-us/

DZS-KEYMILE EMEA
Regional Headquarters
Hanover,
Germany
info.emea@dzsi.com
www.keymile.com/en/web/keymile/contact_sales

DZS KOREA-APAC
Regional Headquarters
Seongnam-si, Geyonggi-do,
South Korea
info@dzsi.com
www.dzsi.com/contact-us/

TABLE OF CONTENTS

About This Guide

This document provides information about one or more specific DZS products as identified on the document Cover page and in the chapters that follow. This Preface explains some of the conventions that are used in this document and explains how to contact DZS Quality and Service for support. Carefully read and follow the instructions included in this document.

Style and notation conventions

The following style and notation conventions are used in this document.

Alerting Messages

Special Alerting Messages, like the ones below, are used to alert users to information that is instructional, warns of potential damage to system equipment or data, and warns of potential injury or death. Carefully read and follow the instructions included in this document.

Note: A note provides important supplemental or amplified information.

Caution: A caution alerts users to conditions or actions that could damage equipment or data.

Tip: A tip provides additional information that enables users to more readily complete their tasks.

WARNING! A warning alerts users to conditions or actions that could lead to injury or death.

WARNING! A warning with this icon alerts users to conditions or actions that could lead to injury caused by a laser.

Typographical conventions

The following typographical styles are used in this guide to represent specific types of information.

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
`Fixed`	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
`Fixed Bold`	Used in code examples for text typed by users.
Italic	Used for book titles, chapter titles, file path names, notes in body text requiring special attention, section titles, emphasized terms, and variables.
PLAIN UPPER CASE	Used for user configured/selected variables.

Related documentation

Refer to the following documents for additional information:

MXK-F Hardware and Installation Guide — contains information about the MXK-F chassis including environmental and power requirements, procedures on how to prepare, install, and maintain the MXK-F chassis, install and remove slot cards, and to add them to the system to make them available for configuration.

MXK-F Management Guide — explains how to access the MXK-F, manage user accounts, navigate the MXK-F file system, manage cards and ports, configure clocking options and the security available for the MXK-F.

MXK-F Configuration Guide — explains how to configure the MXK-F for passing data, providing rate limiting, fault tolerance, redundancy and link aggregation, and mass provisioning devices connected to the MXK-F.

SLMS GPON Troubleshooting Guide — explains how to troubleshoot faults/ alarms that can occur in a GPON system and provides some background information about GPON technology.

Refer to the release notes for software installation information and for changes in features and functionality of the product (if any).

Acronyms & Definitions

The following acronyms and definitions are related to DZS products and may appear throughout this manual:

Table 1: Acronyms and Definitions

Acronym	Description
ARP	Address resolution protocol
MIB	Management Information Base
OLT	Optical Line Terminal. An electronic device/equipment at the beginning (core/network side) of the optical access network that connects to ONT/ONUs.
ONT	Optical Network Terminal (a type of ONU). An electronic device at the end (subscriber side) of the access optical network located on the subscriber side.
ONU	Optical Network Unit. An electronic device at the end of the access optical network located on the subscriber side.
SFP	Small Form factor Pluggable module
SLMS	Single Line Multi-Service
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
ZMS	DZS Management System

Contacting DZS Quality & Service

All new DZS equipment purchases include one year of HW Warranty and 90 days of Bronze-level Technical Support.

If your product is not within 90 days of the purchase date or you do not have a valid support contract, please contact your local sales representative to get a quote on a support contract.

Customers with a valid support contract or are eligible for 90 days technical support associated with a new product purchase can request technical support by opening a case at:

https://dzsi.com/support/#TAC

Customers with a valid support contract have access to technical product documentation, software downloads, knowledge base and consultation on the covered DZS product at the same support portal.

For repair services within the HW Warranty period or under an Extended Warranty support contract, a Return Material Authorization (RMA) must be obtained before sending the equipment for repair. RMA requests can be submitted at:

https://dzsi.com/support/#RMA

Technical support

The Technical Assistance Center (TAC) is available with experienced support engineers who can handle questions, assist with service requests, and help troubleshoot systems.

Hours of operation	Monday - Friday, 8 a.m. to 6 p.m, Eastern Time (excluding U.S. holidays)
Telephone (North America)	877-946-6320, prompt #3, #1
Telephone (International)	510-777-7133, prompt #3, #1
E-mail	support@dzsi.com
Web - available 24 x 7 to submit and track field issues/ problem reports	https://dzsi.com/support/#TAC Click **DZS Problem Reporting System**

If you purchased the product from an authorized dealer, distributor, Value Added Reseller (VAR), or third party, contact that supplier for technical assistance and warranty support.

Hardware repair

If the product malfunctions, all repairs must be authorized by DZS with a Return Merchandise Authorization (RMA) and performed by the manufacturer or a DZS-authorized agent. It is the responsibility of users

requiring service to report the need for repair to DZS Quality & Service as follows:

- Complete the RMA Request form (https://dzsi.com/support/#RMA) or contact DZS Quality & Service via phone or email:

  Hours of operation: Monday - Friday, 8 a.m. to 6 p.m, Eastern Time (excluding U.S. holidays)

  E-mail: support@dzsi.com (preferred)

  Phone:877-946-6320 or 510-777-7133, prompt #3, #2

- Provide the part numbers and serial numbers of the products to be repaired.
- All product lines ship with a minimum one year standard warranty (may vary by contract). DZS warrants all repairs for 90 days or the remainder of the standard warranty (whichever is greater).
- DZS will verify the warranty and provide the customer with a repair quote for anything that is not under warranty. DZS requires a purchase order or credit card for out of warranty fees.

CHAPTER 1 MONITORING OVERVIEW

This document explains how to monitor DZS's MXK-F multi-card chassis products which include the MXK-F1419, F1421 and F219. The MXK-F1419 and F1421 are referred to as MXK-F14xx. All three are referred to as MXK-F (MXK-F1419, F1421 and F219).

1-1 MXK-F OVERVIEW

The MXK-F14xx and MXK-F219 chassis support high-density 1G and 10G Active Ethernet, ITU-T G.984 GPON, ITU-T G.987 XG-PON1 and ITU-T G.989 NG-PON2 Line Cards. Each Line Card slot can support up to 200 Gbps of bandwidth that will enable even higher bandwidth services in the future.

The MXK-F, in conjunction with zNIDs, provides a complete end-to-end access solution for GPON and Active Ethernet fiber deployments that support triple-play services to subscribers.The MXK-F management architecture sets new standards for system availability, reliability and manageability and is based on the same SLMS code base as other DZS products ensuring seamless integration with other DZS solutions and management systems.

Note: The terms "ONU" and "ONT" have been used interchangeably throughout this document unless noted otherwise. The CLI command term "onu" is unique and cannot be substituted with "ont".

1-2 MONITORING AND TROUBLESHOOTING OVERVIEW

This monitoring guide contains various CLI commands used to display monitoring information provided for different components of the MXK-F including the chassis, cards, ports, SFPs, and ONUs.

This guide provides the following information:

- *Chapter 2, Basic Component & Port Status Monitoring,* on page 15

  This chapter covers the monitoring commands.

- *Chapter 3, Logs for the MXK-F,* on page 45

  This chapter describes how to use logs and generate system messages.

- *Chapter 4, Traps and Alarms on the MXK-F,* on page 59

This chapter describes the alarms and how to configure them.

- *Chapter 5, Statistics on the MXK-F,* on page 115

  This chapter describes runtime statistics.

CHAPTER 2 BASIC COMPONENT & PORT STATUS MONITORING

This chapter provides an overview of the basic component status monitoring.

2- 1 MONITOR THE CHASSIS AND FAN TRAY

This section describes how to monitor the MXK-F14xx and the MXK-F219:

2- 1.1 Monitor the MXK-F14xx Chassis and Fan Tray

The MXK-F supports monitoring the chassis/fan tray through the CLI.

The fan trays for the MXK-F support enhanced monitoring capabilities:

- individual fan rotation
- ambient air temperature
- three-point exhaust air temperature
- battery and return voltage measurement

To view the chassis environmental status, use the **shelfctrl monitor** command:

```
zSH> shelfctrl monitor
Shelf                          Status
-------------------------------------------------------------------------------
Uptime                         3 hours, 55 minutes
Shelf start time               1437502799
```

```
Upper Fan Tray:
   FPGA version                0.2
   Firmware version            0.0
Lower Fan Tray:
   FPGA version                0.2
   Firmware version            0.0
Management Card Glue version   0.15
Chassis Temperatures           Celsius(C)             Fahrenheit(F)
-------------------------------------------------------------------------
Ambient                        56                     132
Outlet                         62                     143
Temperature reading            normal
Fan Power Supplies & Alarm     Status
-------------------------------------------------------------------------
Upper Fan Tray:
   Fan Power 1                 normal
   Fan Power 2                 normal
   Fan alarm                   ok
Lower Fan Tray:
   Fan Power 1                 normal
   Fan Power 2                 normal
   Fan alarm                   ok
Power Supplies                 Volts(V)               Status
-------------------------------------------------------------------------
Battery A                      -52.84V                normal
Battery B                      -52.82V                normal
Battery A return               -0.49V
Battery B return               -0.48V
Device                         Status
-------------------------------------------------------------------------
System                         Critical alarm set
Card m1                        Critical alarm set
Card m2                        Critical alarm set
Card a                         Critical alarm set
Card b                         Critical alarm set

Alarm I/O Board
-------------------------------------------------------------------------
CPLD version                   0.0
Present:                       Yes
Alarm input:                       Ai1  Ai2  Ai3  Ai4  Ai5  Ai6  Ai7  Ai8
Status (Energized/de-energized):   d    d    d    d    d    d    d    d
NormalOpen/NormalClosed/NotSpec:   NS   NS   NS   NS   NS   NS   NS   NS
Alarm Active:                      No   No   No   No   No   No   No   No
```

System and **Card <#>** will show **Critical alarm set** when an alarm has been triggered. Other parameters provide full descriptions such as **warning fans A, B, C, F are stopped** or **warning all fans are stopped** for the Fan alarm.

The Battery A and Battery B voltages are measured relative to battery return (+). The Battery return voltage measurement is relative to ground (i.e., the chassis).

2- 1.2 Monitor the MXK-F219 Chassis and Fan Tray

The MXK-F219 fan tray supports a subset of the monitoring features.

- individual fan rotation
- ambient air temperature
- three-point exhaust air temperature
- battery and return voltage measurement

Note: The MXK-F219 fan tray is controlled by the m1/m2 management cards. To prevent overheating if neither (m1/m2) card is installed the line cards power down through hardware.

To view the chassis environmental status, use the **shelfctrl monitor** command:

```
zSH> shelfctrl monitor
Shelf                          Status
-------------------------------------------------------------------------
Uptime                         3 days, 2 hours, 5 minutes
FPGA version                   0.3
Firmware version               0.0
Management Card Glue version   1.15

Chassis Temperatures           Celsius(C)             Fahrenheit(F)
-------------------------------------------------------------------------
Ambient                        28                     82
Outlet                         30                     86
Temperature reading            normal

Fan Power Supplies & Alarm     Status
-------------------------------------------------------------------------
Fan Power 1                    normal
Fan Power 2                    normal
Fan alarm                      ok

Power Supplies                 Volts(V)               Status
-------------------------------------------------------------------------
Battery A                      -53.57V                normal
Battery B                      -53.55V                normal
Battery A return               -0.16V
Battery B return               -0.18V

Device                         Status
-------------------------------------------------------------------------
System                         Critical alarm set
Card m1                        Critical alarm set
Card m2                        Critical alarm set

Alarm I/O Board
-------------------------------------------------------------------------
CPLD version                   0.3
Present:                       Yes
Alarm input:                       Ai1  Ai2  Ai3  Ai4  Ai5  Ai6  Ai7  Ai8
Status (Energized/de-energized):   d    d    d    d    d    d    d    d
NormalOpen/NormalClosed/NotSpec:   NS   NS   NS   NS   NS   NS   NS   NS
Alarm Active:                      No   No   No   No   No   No   No   No
```

2- 2 MONITOR MXK-F CARDS

This section describes how to monitor MXK-F cards:

2- 2.1 Viewing Cards Overview

You can view information by entering the **slots** *slot_number* command to view card information including

- ROM Version
- Software Version
- Card-Profile ID

The **slots** command displays the cards currently provisioned in the MXK-F chassis and their state which can include: running, loading, not provisioned, booting, and configuring.

```
zSH> slots
MXK 1421

Management Cards
 m1:*MXK-MC-TOP, 14U MGMT W/ TOP (RUNNING)
 m2: MXK-MC-TOP, 14U MGMT W/ TOP (RUNNING)

Fabric Cards
  a:*MXK-FC-AETG8, 14U FABRIC W/ 8x10G AE (RUNNING+TRAFFIC)
  b: MXK-FC-AETG8, 14U FABRIC W/ 8x10G AE (RUNNING+TRAFFIC)

Line Cards
  3: MXK-LC-GP16, LINE CARD W/ 16 GPON (RUNNING)
  4: MXK-LC-GP16, LINE CARD W/ 16 GPON (RUNNING)
  9: MXK-LC-AEG32, LINE CARD W/ 32x1G AE ANGL (RUNNING)
```

2- 2.2 View Management Cards for the MXK-F14xx

The asterisk next to the card type indicates the card is in a redundant configuration. Enter the **slots m1** or **slots m2** command to view management card information.

```
zSH> slots m1
MXK 1421
Type            :*MXK-MC-TOP, 14U MGMT W/ TOP
Card Version    : 800-03404-02-A
EEPROM Version  : 1
```

```
Serial #        : 7986440
CLEI Code       : No CLEI
Card-Profile ID : 1/m1/20001
Shelf           : 1
Slot            : m1
ROM Version     : MXK 3.1.1.141
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED JUL 22 23:30:38 2015
Heartbeat resp  : 8976
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 19
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 hours, 29 minutes

zSH> slots m2
MXK 1421
Type            : MXK-MC-TOP, 14U MGMT W/ TOP
Card Version    : 800-03404-02-A
EEPROM Version  : 1
Serial #        : 7985260
CLEI Code       : No CLEI
Card-Profile ID : 1/m2/20001
Shelf           : 1
Slot            : m2
ROM Version     : MXK 3.1.1.141
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED JUL 22 23:30:38 2015
Heartbeat resp  : 9022
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 7
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 hours, 30 minutes
```

2- 2.3 View Fabric Cards for the MXK-F14xx

Enter the **slots a** or the **slots b** command to view fabric card information.

```
zSH> slots a
MXK 1421
Type            :*MXK-FC-AETG8, 14U FABRIC W/ 8x10G AE
Card Version    : 800-03383-01-A
EEPROM Version  : 1
Serial #        : 8089780
CLEI Code       : No CLEI
Card-Profile ID : 1/a/20104
Shelf           : 1
Slot            : a
ROM Version     : MXK 3.1.1.141
```

```
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED JUL 22 23:30:38 2015
Heartbeat resp  : 9577
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 3
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 hours, 39 minutes

zSH> slots b
MXK 1421
Type            : MXK-FC-AETG8, 14U FABRIC W/ 8x10G AE
Card Version    : 800-03383-01-A
EEPROM Version  : 1
Serial #        : 8088740
CLEI Code       : No CLEI
Card-Profile ID : 1/b/20104
Shelf           : 1
Slot            : b
ROM Version     : MXK 3.1.1.141
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED JUL 22 23:30:38 2015
Heartbeat resp  : 9709
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 4
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 hours, 41 minutes
```

2- 2.4 View Line Cards for the MXK-F14xx

Enter the **slots** *slot_number* command to view line card information. In this case GPON.

```
zSH> slots 3
MXK 1421
Type            : MXK-LC-GP16, LINE CARD W/ 16 GPON
Card Version    : 800-03401-02-A
EEPROM Version  : 1
Serial #        : 8088071
CLEI Code       : No CLEI
Card-Profile ID : 1/3/20201
Shelf           : 1
Slot            : 3
ROM Version     : MXK 3.1.1.121
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
```

```
Heartbeat last  : WED JUL 22 23:30:38 2015
Heartbeat resp  : 9921
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 12
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 hours, 45 minutes
```

Enter the **slots** *slot_number* command to view line card information. In this case Ethernet.

```
zSH> slots 9
MXK 1421
Type            : MXK-LC-AEG32, LINE CARD W/ 32x1G AE ANGL
Card Version    : 800-03440-01-A
EEPROM Version  : 1
Serial #        : 10886240
CLEI Code       : No CLEI
Card-Profile ID : 1/9/20222
Shelf           : 1
Slot            : 9
ROM Version     : MXK 3.1.1.211
Software Version: MXK 3.1.1.219
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED JUL 22 23:33:32 2015
Heartbeat resp  : 28110
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 26
Fault reset     : enabled
Power fault mon : supported
Uptime          : 12 minutes
```

2- 2.5 View Management Cards for the MXK-F219

The asterisk next to the type of card indicates that this card is in a redundant configuration. Enter the **slots m1** or **slots m2** command to view management card information.

```
zSH> slots
MXK 219
Management Cards
 m1:*MXK-MC-AETG2-TOP, 2U MGMT W/ 2x10G AE, W/ TOP (RUNNING)
 m2: MXK-MC-AETG2-TOP, 2U MGMT W/ 2x10G AE, W/ TOP (RUNNING)
Line Cards
  1:*MXK-LC-GP16, LINE CARD W/ 16 GPON (RUNNING)
  2: MXK-LC-GP16, LINE CARD W/ 16 GPON (RUNNING)

zSH> slots m1
MXK 219
Type            :*MXK-MC-AETG2-TOP, 2U MGMT W/ 2x10G AE, W/ TOP
Card Version    : 800-03432-01-A
EEPROM Version  : 1
Serial #        : 13481460
```

```
CLEI Code       : No CLEI
Card-Profile ID : 1/m1/20002
Shelf           : 1
Slot            : m1
ROM Version     : MXK 3.1.1.248
Software Version: MXK 3.1.2.129
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : FRI NOV 04 15:09:48 2016
Heartbeat resp  : 233933
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 12
Fault reset     : enabled
Power fault mon : supported
Uptime          : 2 days, 16 hours, 58 minutes
Start time      : 1478038256
```

2- 2.6 View Line Cards for the MXK-F219

Enter the **slots** *slot_number* command to view line card information. In this case GPON.

```
zSH> slots 1
MXK 219
Type            : MXK-LC-GP16, LINE CARD W/ 16 GPON
Card Version    : 800-03401-04-AA
EEPROM Version  : 1
Serial #        : 10082790
CLEI Code       : No CLEI
Card-Profile ID : 1/1/20201
Shelf           : 1
Slot            : 1
ROM Version     : MXK 3.1.2.101
Software Version: MXK 3.1.2.120
State           : RUNNING
Mode            : FUNCTIONAL
Heartbeat check : enabled
Heartbeat last  : WED SEP 21 23:04:00 2016
Heartbeat resp  : 13172
Heartbeat late  : 0
Hbeat seq error : 0
Hbeat longest   : 17
Fault reset     : enabled
Power fault mon : supported
Uptime          : 1 hour, 49 minutes
Traffic Ready   : yes
Database Ready  : yes
Bridge Count    : 2
```

2- 3 MONITOR MXK-F14XX PORTS

This section describes port monitoring:

- port status and port show Command, page 23

- port testing Command, page 24

2- 3.1 port status and port show Command

Use the **port status** command to view the operational status, speed, and duplex mode of an Ethernet port.

Note: The **port status** command is only valid for Ethernet ports.

```
zSH> port status 1-a-1-0/eth
Operational status  : Up
Rate in Mbps        : 10000
Duplex              : Full
```

Use the **port show** command to view the administrative status of a port or interface.

```
zSH> port show 1-a-1-0/eth
Interface 1-a-1-0/eth
        Physical location:     1/a/1/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        DDM data:
                Temperature:        30c
                Voltage:           3.29v
                Tx bias current:     27mA
                Transmit power:    -2.3dBm
                Receive power:     0.2dBm
```

Use the **port show** command to view the status of an GPON OLT.

```
zSH> port show 1-3-1-0/gponolt
Interface 1-3-1-0/gponolt
        Physical location:     1/3/1/0/gponolt
        Administrative status: up
```

Use the **port show** command to view the status of a GPON ONU.

```
zSH> port show 1-1-1-1/gpononu
Interface 1-1-1-1/gpononu
        Administrative status: up
```

Use **port show** command to view the status of a line card Ethernet port.

```
zSH> port show 1-9-1-0/eth
Interface 1-9-1-0/eth
        Physical location:     1/9/1/0/eth

        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
```

```
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        DDM data:
                Temperature:         0c
                Voltage:           0.00v
                Tx bias current:       0mA
                Transmit power:    0.0dBm
                Receive power:     0.0dBm
```

Use the **port show** command to view the status of a port with a configured bridge.

```
zSH> port show ethernet1-800/bridge
Interface ethernet1-800/bridge
        Administrative status: up
```

2- 3.2 port testing Command

Use the **port testing** command to set the administrative state to testing on an Ethernet port.

```
zSH> port testing 1-a-2-0/eth
1-a-2-0/eth set to admin state TESTING
```

Verify the state.

```
zSH> port show 1-a-2-0/eth
Interface 1-a-2-0/eth
        Physical location:     1/a/2/0/eth
        Administrative status: testing
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        DDM data:
                Temperature:        29c
                Voltage:           3.29v
                Tx bias current:     28mA
                Transmit power:    -2.4dBm
                Receive power:     -4.0dBm
```

Use the **port testing** command to set the administrative state to testing on an GPON ONU port.

```
zSH> port testing 1-1-1-1/gpononu
1-1-1-1/gpononu set to admin state TESTING
```

Verify the state.

```
zSH> port show 1-1-1-1/gpononu
Interface 1-1-1-1/gpononu
        Administrative status: testing
```

2- 4 MONITOR MXK-F219 PORTS

This section describes port monitoring:

2- 4.1 port status and port show Command

Use the **port status** command to view the operational status, speed, and duplex mode of an Ethernet port.

Note: The **port status** command is only valid for Ethernet ports.

```
zSH> port status 1-1-101-0/eth
Operational status  : Up
Rate in Mbps        : 10000
Duplex              : Full
```

Use the **port show** command to view the administrative status of a port or interface.

```
zSH> port show 1-1-101-0/eth
Interface 1-1-101-0/eth
        Physical location:     1/1/101/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Egress rate: 0 Kbps burst size: 0 Kbits
        DDM not supported

zSH> port show 1-m1-1-0/eth
Interface 1-m1-1-0/eth
        Physical location:     1/m1/1/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Egress rate: 0 Kbps burst size: 0 Kbits
        No DDM data available from ethernet port
```

Use the **port show** command to view the status of an GPON OLT.

```
zSH> port show 1-1-1-0/gponolt
Interface 1-1-1-0/gponolt
        Physical location:     1/1/1/0/gponolt
        Administrative status: up
```

Use the **port show** command to view the status of a GPON ONU.

```
zSH> port show 1-1-1-1/gpononu
Interface 1-1-1-1/gpononu
```

```
        Administrative status: up
```

Use the **port show** command to view the status of a port with a configured bridge.

```
zSH> port show ethernet1-800/bridge
Interface ethernet1-800/bridge
        Administrative status: up
```

2- 4.2 port testing Command

Use the **port testing** command to set the administrative state to testing on an Ethernet port.

```
zSH> port testing 1-1-102-0/eth
1-1-102-0/eth set to admin state TESTING
```

Verify the state.

```
zSH> port show 1-1-102-0/eth
Interface 1-1-102-0/eth
        Physical location:     1/1/102/0/eth

        Administrative status: testing
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Egress rate: 0 Kbps burst size: 0 Kbits
        DDM not supported
```

Use the **port testing** command to set the administrative state to testing on an GPON ONU port.

```
zSH> port testing 1-1-1-1/gpononu
1-1-1-1/gpononu set to admin state TESTING
```

Verify the state.

```
zSH> port show 1-1-1-1/gpononu
Interface 1-1-1-1/gpononu
        Administrative status: testing
```

2- 5 MONITOR SFPS AND QSFPS

2- 5.1 View SFP Information

To view the presence of SFPs on the MXK-F, enter the **sfp show all** command:

```
zSH> sfp show all
SFP Data for interface 1-a-1-0/eth
vendorName                                Ligent Photonics
vendorOui                                 00-01-47
vendorPartNumber                          LTF8502-BH
vendorRevisionLevel                       1
serialNumber                              LIGL7641000350
manufacturingDateCode                     140126
complianceCode                            unknown value (0x0000)
connectorType                             lc (7)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         unknownOrUnspecified (6)
channelLinkLength                         unknown value (0x0000)
channelTransmitterTechnology              unknown value (0x0000)
channelTransmitterMedia                   unknown value (0x0000)
channelSpeed                              unknown value (0x0000)
nineTo125mmFiberLinkLengthKm              0
nineTo125mmFiberLinkLength100m            0
fiftyTo125mmFiberLinkLength10m            8
sixtyTwoDot5To125mmFiberLinkLength10m      3
nominalBitRate                            103
upperBitRateMarginPercentage              20
lowerBitRateMarginPercentage              20
copperLinkLength                          0


SFP Data for interface 1-a-2-0/eth
vendorName                                Titan Photonics
vendorOui                                 00-01-47
vendorPartNumber                          MXK-10GE-SFP+-SR
vendorRevisionLevel                       A
serialNumber                              TITD140909009
manufacturingDateCode                     140909
complianceCode                            unknown value (0x0000)
connectorType                             lc (7)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         unknownOrUnspecified (6)
channelLinkLength                         intermediate-distance (0x0020)
channelTransmitterTechnology              shortwavelaser-without-ofc (0x2040)
channelTransmitterMedia                   multimode-50m | multimode-62dot5m (0x000c)
channelSpeed                              unknown value (0x0080)
nineTo125mmFiberLinkLengthKm              0
nineTo125mmFiberLinkLength100m            0
fiftyTo125mmFiberLinkLength10m            8
sixtyTwoDot5To125mmFiberLinkLength10m      3
nominalBitRate                            103
upperBitRateMarginPercentage              0
lowerBitRateMarginPercentage              0
copperLinkLength                          0

SFP Data for interface 1-a-3-0/eth
```

```
** No SFP present **

SFP Data for interface 1-a-4-0/eth
vendorName                                FINISAR CORP.
vendorOui                                 00-90-65
vendorPartNumber                          FCLF-8521-3
vendorRevisionLevel                       A
serialNumber                              PDK1YWE
manufacturingDateCode                     080506
complianceCode                            base1000T (0x0008)
connectorType                             unknownOrUnspecified (0)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         eightb10b (1)
channelLinkLength                         unknown value (0x0000)
channelTransmitterTechnology              unknown value (0x0000)
channelTransmitterMedia                   unknown value (0x0000)
channelSpeed                              unknown value (0x0000)
nineTo125mmFiberLinkLengthKm              0
nineTo125mmFiberLinkLength100m            0
fiftyTo125mmFiberLinkLength10m            0
sixtyTwoDot5To125mmFiberLinkLength10m     0
nominalBitRate                            12
upperBitRateMarginPercentage              0
lowerBitRateMarginPercentage              0
copperLinkLength                          100

SFP Data for interface 1-a-5-0/eth
vendorName                                FINISAR CORP.
vendorOui                                 00-90-65
vendorPartNumber                          FCLF-8521-3
vendorRevisionLevel                       A
serialNumber                              PD53726
manufacturingDateCode                     080131
complianceCode                            base1000T (0x0008)
connectorType                             unknownOrUnspecified (0)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         eightb10b (1)
channelLinkLength                         unknown value (0x0000)
channelTransmitterTechnology              unknown value (0x0000)
channelTransmitterMedia                   unknown value (0x0000)
channelSpeed                              unknown value (0x0000)
nineTo125mmFiberLinkLengthKm              0
nineTo125mmFiberLinkLength100m            0
fiftyTo125mmFiberLinkLength10m            0
sixtyTwoDot5To125mmFiberLinkLength10m     0
nominalBitRate                            12
upperBitRateMarginPercentage              0
lowerBitRateMarginPercentage              0
copperLinkLength                          100

SFP Data for interface 1-a-6-0/eth
** No SFP present **

SFP Data for interface 1-a-7-0/eth
** No SFP present **

SFP Data for interface 1-a-8-0/eth
```

```
** No SFP present **

SFP Data for interface 1-b-1-0/eth
vendorName                                Ligent Photonics
vendorOui                                 00-01-47
vendorPartNumber                          LTF8502-BH
vendorRevisionLevel                       1
serialNumber                              LIGL7641000359
manufacturingDateCode                     140126
complianceCode                            unknown value (0x0000)
connectorType                             lc (7)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         unknownOrUnspecified (6)
channelLinkLength                         unknown value (0x0000)
channelTransmitterTechnology              unknown value (0x0000)
channelTransmitterMedia                   unknown value (0x0000)
channelSpeed                              unknown value (0x0000)
nineTo125mmFiberLinkLengthKm              0
nineTo125mmFiberLinkLength100m            0
fiftyTo125mmFiberLinkLength10m            8
sixtyTwoDot5To125mmFiberLinkLength10m     3
nominalBitRate                            103
upperBitRateMarginPercentage              20
lowerBitRateMarginPercentage              20
copperLinkLength                          0

SFP Data for interface 1-3-1-0/gponolt
vendorName                                Ligent
vendorOui                                 00-01-47
vendorPartNumber                          LTE3680M-BH
vendorRevisionLevel                       1.0
serialNumber                              LIGJ0348000622
manufacturingDateCode                     140804
complianceCode                            unknown value (0x0000)
connectorType                             sc (1)
transceiverType                           sfp (3)
extendedIdentifier                        4
encodingAlgorithm                         nrz (3)
channelLinkLength                         unknown value (0x0000)
channelTransmitterTechnology              unknown value (0x0000)
channelTransmitterMedia                   unknown value (0x0000)
channelSpeed                              unknown value (0x0000)
nineTo125mmFiberLinkLengthKm              20
nineTo125mmFiberLinkLength100m            200
fiftyTo125mmFiberLinkLength10m            0
sixtyTwoDot5To125mmFiberLinkLength10m     0
nominalBitRate                            25
upperBitRateMarginPercentage              20
lowerBitRateMarginPercentage              20
copperLinkLength                          0

SFP Data for interface 1-3-2-0/gponolt
** No SFP present **

SFP Data for interface 1-3-3-0/gponolt
** No SFP present **

SFP Data for interface 1-3-4-0/gponolt
```

```
** No SFP present **

SFP Data for interface 1-3-5-0/gponolt
** No SFP present **

SFP Data for interface 1-3-6-0/gponolt
** No SFP present **

SFP Data for interface 1-3-7-0/gponolt
** No SFP present **

SFP Data for interface 1-3-8-0/gponolt
** No SFP present **

SFP Data for interface 1-3-9-0/gponolt
** No SFP present **

SFP Data for interface 1-3-10-0/gponolt
** No SFP present **

SFP Data for interface 1-3-11-0/gponolt
** No SFP present **

SFP Data for interface 1-3-12-0/gponolt
** No SFP present **

SFP Data for interface 1-3-13-0/gponolt
** No SFP present **

SFP Data for interface 1-3-14-0/gponolt
** No SFP present **

SFP Data for interface 1-3-15-0/gponolt
** No SFP present **

SFP Data for interface 1-3-16-0/gponolt
** No SFP present **

SFP Data for interface 1-4-1-0/gponolt
vendorName                              Ligent
vendorOui                               00-01-47
vendorPartNumber                        LTE3680M-BH
vendorRevisionLevel                     1.0
serialNumber                            LIGJ0348000314
manufacturingDateCode                   140804
complianceCode                          unknown value (0x0000)
connectorType                           sc (1)
transceiverType                         sfp (3)
extendedIdentifier                      4
encodingAlgorithm                       nrz (3)
channelLinkLength                       unknown value (0x0000)
channelTransmitterTechnology            unknown value (0x0000)
channelTransmitterMedia                 unknown value (0x0000)
channelSpeed                            unknown value (0x0000)
nineTo125mmFiberLinkLengthKm            20
nineTo125mmFiberLinkLength100m          200
fiftyTo125mmFiberLinkLength10m          0
sixtyTwoDot5To125mmFiberLinkLength10m    0
nominalBitRate                          25
```

```
upperBitRateMarginPercentage            20
lowerBitRateMarginPercentage            20
copperLinkLength                        0

SFP Data for interface 1-4-2-0/gponolt
** No SFP present **

SFP Data for interface 1-4-3-0/gponolt
** No SFP present **

SFP Data for interface 1-4-4-0/gponolt
** No SFP present **

SFP Data for interface 1-4-5-0/gponolt
** No SFP present **

SFP Data for interface 1-4-6-0/gponolt
** No SFP present **

SFP Data for interface 1-4-7-0/gponolt
** No SFP present **

SFP Data for interface 1-4-8-0/gponolt
** No SFP present **

SFP Data for interface 1-4-9-0/gponolt
** No SFP present **

SFP Data for interface 1-4-10-0/gponolt
** No SFP present **

SFP Data for interface 1-4-11-0/gponolt
** No SFP present **

SFP Data for interface 1-4-12-0/gponolt
** No SFP present **

SFP Data for interface 1-4-13-0/gponolt
** No SFP present **

SFP Data for interface 1-4-14-0/gponolt
** No SFP present **

SFP Data for interface 1-4-15-0/gponolt
** No SFP present **

SFP Data for interface 1-4-16-0/gponolt
```

2- 5.2 View QSFP Information

To view the presence of QSFPs on the MXK-F, enter the **qsfp show all** command:

```
zSH> qsfp show all
QSFP Data for interface 1-a-1-0/eth
vendorName                              WTD
```

```
vendorOui                               00-1c-ad
vendorPartNumber                        RTXM320-400
vendorRevisionLevel                     A
serialNumber                            RD155103000010
manufacturingDateCode                   151217
complianceCode1040GbEthernet            40GbEthernet-lr4 (0x40000000)
complianceCodeSonet                     unknown value (0x0000)
complianceCodeSas                       unknown value (0x0000)
connectorType                           lc (7)
transceiverType                         qsfp-plus (13)
extendedIdentifier                      192
encodingSupport                         sixtyfourB-per-66B (5)
deviceTechnology                        64
fiberLinkLength1Km                      10
extendedFiberLinkLength                 0
mm62Dot5umFiberLinkLength1m             0
mm50umFiberLinkLength1m                 0
bitRate                                 103
bitRateExtended                         0
enhancedOptions                         0

QSFP Data for interface 1-a-2-0/eth
vendorName                              WTD
vendorOui                               00-1c-ad
vendorPartNumber                        RTXM320-551
vendorRevisionLevel                     10
serialNumber                            RD143710100001
manufacturingDateCode                   140904
complianceCode1040GbEthernet            40GbEthernet-sr4 (0x20000000)
complianceCodeSonet                     unknown value (0x0000)
complianceCodeSas                       unknown value (0x0000)
connectorType                           mpo (12)
transceiverType                         qsfp-plus (13)
extendedIdentifier                      0
encodingSupport                         sixtyfourB-per-66B (5)
deviceTechnology                        0
fiberLinkLength1Km                      0
extendedFiberLinkLength                 50
mm62Dot5umFiberLinkLength1m             0
mm50umFiberLinkLength1m                 0
bitRate                                 105
bitRateExtended                         0
enhancedOptions                         0

QSFP Data for interface 1-b-1-0/eth
vendorName                              Ligent Photonics
vendorOui                               00-00-00
vendorPartNumber                        LTA8511-PC
vendorRevisionLevel                     1
serialNumber                            E335B000137
manufacturingDateCode                   151110
complianceCode1040GbEthernet            40GbEthernet-sr4 (0x20000000)
complianceCodeSonet                     unknown value (0x0000)
complianceCodeSas                       unknown value (0x0000)
connectorType                           mpo (12)
transceiverType                         qsfp-plus (13)
extendedIdentifier                      0
encodingSupport                         nrz (3)
deviceTechnology                        0
```

```
fiberLinkLength1Km                  0
extendedFiberLinkLength             50
mm62Dot5umFiberLinkLength1m         0
mm50umFiberLinkLength1m             0
bitRate                             103
bitRateExtended                     0
enhancedOptions                     0
```

2- 5.3 Active Ethernet and Uplink Port - SFP Monitoring

The MXK-F uplink and Active Ethernet card ports use Ethernet SFPs. Some Ethernet SFPs support Digital Diagnostic Monitoring (DDM) that provides the temperature, supply voltage, transmit bias current, transmit power, and receive power of the SFP.

The **port show** *interface/type* command is used to display DDM data on Ethernet ports that have DDM-capable SFPs. Table 2. describes the DDM displayed data fields.

Table 2: port show Command Output Fields for DDM data on Ethernet Ports

Field	Description
Temperature	Internally measured Transceiver Temperature in degrees celsius.
Voltage	Internally measured Transceiver Supply Voltage in hundredths of volts.
Tx Bias Current	Measured Tx Bias current in milliamperes.
Transmit Power	Measured Tx Output power in tenths of dB.
Receive Power	Measured Rx power in tenths of dB.

2- 5.3.1 Read DDM Info on Ethernet SFPs

The examples that follow are for the MXK-F14xx Fabric/uplink ports.

The same procedures can be used for MXK-F219 (m1/m2) uplink ports and for Active Ethernet Line Card ports by using the appropriate interface names (e.g. replace the F14xx interface = 1-a-1-0/eth with the F219 interface name = 1-1-101-0 or the Active Ethernet Line Card name = 1-7-4-0/eth).

Read the DDM info of an Ethernet SFP on an MXK-F14xx fabric card.

```
zSH> port show 1-a-1-0/eth
Interface 1-a-1-0/eth
        Physical location:     1/a/1/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        DDM data:
```

```
                Temperature:        29c
                Voltage:           3.29v
                Tx bias current:      5mA
                Transmit power:    -2.1dBm
                Receive power:     -4.0dBm
```

Ethernet port on fabric card with QSFP that supports DDM data.

```
zSH> port show 1-a-1-0/eth
Interface 1-a-1-0/eth
        Physical location:     1/a/1/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Egress rate: 0 Kbps burst size: 0 Kbits
        DDM data:
                Temperature:         0c
                Voltage:           0.00v
                Tx bias current:      0mA
                Transmit power:    -40.0dBm
                Receive power:     -4.0dBm
```

Ethernet port on fabric card without SFP.

```
zSH> port show 1-a-3-0/eth
Interface 1-a-3-0/eth
        Physical location:     1/a/3/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        SFP not present
```

Ethernet port on fabric card with SFP that does not support DDM data.

```
zSH> port show 1-a-5-0/eth
Interface 1-a-5-0/eth
        Physical location:     1/a/5/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        DDM not supported
```

Ethernet management port that does not use an SFP.

```
zSH> port show 1-m1-1-0/eth
Interface 1-m1-1-0/eth
        Physical location:     1/m1/1/0/eth
        Administrative status: up
        Port type specific information:
                Frame size: 0 bytes
                Ingress rate: 0 Kbps burst size: 0 Kbits
                Engress rate: 0 Kbps burst size: 0 Kbits
        No DDM data available from ethernet port
```

2- 5.4 GPON Port - SFP Monitoring

DDM and Received Signal Strength Indication (RSSI) are types of info that are provided by some GPON SFPs. DDM provides basic info like SFP temperature (the MXK-F GPON DDM info is slightly different from the AE/ uplink DDM info; compare Table 2 with Table 3). GPON RSSI provides more detailed information about the OLT/ONT connections.

Procedure: *Read DDM Info on a GPON SFP*

The **gponolt show port** command reads the SFP DDM info for GPON ports.

Table 3: gponolt show port Command Output Fields for DDM data from GPON Line Card SFPs

Field	Description
Temperature	Internally measured Transceiver Temperature of the OLT in Celsius.
Voltage	Internally measured Transceiver Supply Voltage of the OLT in Volts.
Tx Bias Current	Measured Tx Bias current per OLT in Milli Amperes.
Tx Power	Measured Tx Output Power of the OLT in dBm. The OLT SFP measures its own TX Power output level. The level should be in the range +5 dBm to +1.5 dBm (for B+ optical level SFPs). If the output level is not in this range, one or more ONTs may have downstream data errors or may be lost. If the output is higher than +5 dBm, the optical transceiver of one or more ONTs may die prematurely (cause a shorter end of life time period)
End of Life Status	When the End Of Life (EOL) Alarm bit is set an alarm will be raised. SFP automatically maintains a laser output optical power by adjusting the laser current. Alarm is raised when the SFP reaches the end of life which is about 150% of original current. Alarm will be cleared when the SFP is connected. The alarm severity level is Major. Values: **ok** No alarm conditions are raised **warning** Warning is set when EOL is at about 130% original current. **alarm** Alarm conditions are raised **SFP not present** SFP is not detected

Read the DDM parameters on a GPON OLT card with the **gponolt show port** [*slot* [/*olt*]] command.

```
zSH> gponolt show port
SLOT/OLT Temperature  Voltage Tx Bias Current Tx Power End Of Life Status
======== =========== ======= ============== ======== ================
 1/1        43c        3.3v         13mA      3.7dBm    Ok
 1/2        48c        3.3v         13mA      3.7dBm    Ok
 1/3        48c        3.3v         14mA      3.8dBm    Ok
 1/4        43c        3.3v         12mA      3.7dBm    Ok
 1/5        47c        3.3v         13mA      3.8dBm    Ok
 1/6        48c        3.3v         13mA      3.7dBm    Ok
 1/7        43c        3.3v         14mA      3.7dBm    Ok
 1/8        47c        3.3v         15mA      3.8dBm    Ok
```

```
 1/9        46c        3.3v          14mA       3.9dBm    Ok
 1/10       43c        3.3v          15mA       3.7dBm    Ok
 1/11       42c        3.3v          14mA       3.7dBm    Ok
 1/12       39c        3.3v          14mA       3.8dBm    Ok
 1/13       42c        3.3v          13mA       3.9dBm    Ok
 1/14       42c        3.3v          12mA       3.6dBm    Ok
 1/15       37c        3.3v          12mA       3.9dBm    Ok
 1/16       39c        3.3v          12mA       3.8dBm    Ok

SLOT/OLT Temperature  Voltage Tx Bias Current Tx Power End Of Life Status
======== =========== ======= ============== ======== ================
 2/1        50c        3.3v          15mA       3.7dBm    Ok
 2/2        46c        3.3v          14mA       3.5dBm    Ok
 2/3        52c        3.3v          15mA       3.7dBm    Ok
 2/4        50c        3.3v          15mA       3.7dBm    Ok
 2/5        43c        3.3v          18mA       3.7dBm    Ok
 2/6        45c        3.3v          15mA       3.9dBm    Ok
 2/7        48c        3.3v          15mA       3.8dBm    Ok
 2/8        43c        3.3v          16mA       3.7dBm    Ok
 2/9        48c        3.3v          14mA       3.8dBm    Ok
 2/10       44c        3.3v          16mA       3.9dBm    Ok
 2/11       44c        3.3v          14mA       3.9dBm    Ok
 2/12       45c        3.3v          14mA       3.8dBm    Ok
 2/13       45c        3.3v          14mA       4.2dBm    Ok
 2/14       44c        3.3v          14mA       3.8dBm    Ok
 2/15       38c        3.3v          11mA       3.8dBm    Ok
 2/16       37c        3.3v           9mA       3.7dBm    Ok
.....
```

Procedure:

Read RSSI Info on a GPON SFP

The GPON technology allows more than one ONT on a single GPON OLT port, which leads to the need for more information than is provided by DDM. RSSI provides info to determine which ONT connections are working properly and which are not. ONT and OLT RX power levels aid in diagnosing the cause of ONT/OLT faults.

RSSI also provides the distance to each ONT, which can be useful to diagnose problems, but is primarily needed for the (hidden) GPON inter-workings that enable multiple ONTs to more efficiently use a single GPON optical fiber without colliding (without one ONT transmitting on top of other ONTs' data).

The user can view the upstream optical power level received at the OLT, and the downstream optical power level received at the ONT.

The downstream optical power received at an ONT should be -28 or above for SFP-B+ (i.e. RSSI ONT Rx Power = ONT Receive Power). Otherwise the ONT connection may fail, be intermittent or have data errors.

By default, if the upstream optical power of an ONT received at the OLT is outside the range of -10 dBm to -30 dBm, the MXK will trigger a local alarm, and send a trap to ZMS (i.e. RSSI OLT Rx Power = OLT Receive Power; RX signal too high or too low). Although the OLT may continue to forward ONT data when the OLT RX Power is out of range, this fault should be corrected. A signal that is too high or low may cause intermittent or constant downstream

data errors or loss of an ONT. A signal that is too high can cause an OLT optical transceiver to die prematurely (e.g. -7 dBm; shorter end of life).

If an OLT RX Power level is reported for an ONT, the ONT is still functioning (but perhaps with data errors). Properly functioning ONTs do not transmit to the OLT unless they properly receive a downstream signal from the OLT.

The following example shows that the ONT and OLT RX power for the four ONTs on GPON card slot 3, port 1 are within the normal ranges.

```
    zSH> gpononu power show 3/1
Processing list of 32
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
                      OLT             ONT
     Interface        Receive Power   Receive Power
==================   ============   ============
1-3-1-1                 -14.1 dBm      -13.9 dBm
1-3-1-2                 -13.2 dBm      -14.5 dBm
1-3-1-3                 -13.9 dBm      -14.6 dBm
1-3-1-4                 -14.2 dBm      -14.7 dBm
Total ONUs = 4
```

If there is no SFP inserted in the OLT, or the OLT/ ONU admin status is set to down, then the ONT's Receive Power fields display "NA".

If the Receive Power field displays the value "error", it means the measurement failed. Users can run the **gpononu power show** command again.

The OLT RX Power and ONT RX Power info can also be read using other commands. See *ONT Inventory Reports on page 37* and *GPON ONT Status on page 40*

2- 6 ONT INVENTORY AND STATUS

2- 6.1 ONT Inventory Reports

The **onu inventory** command generates a list of all Active Ethernet and GPON ONTs connected to an MXK-F. There are some small differences between the lists generated for Active Ethernet as compared to GPON ONTs.

A per-system list of Active Ethernet and GPON ONTs can be generated using the onu inventory command without a slot/port ID. The information provided for the GPON and Active Ethernet ONTs is similar, but with some differences that are primarily due to the differences between Ethernet and GPON SFPs.

The Active Ethernet and GPON ONTs can easily be distinguished from each other in these lists by their sub-port IDs. Active Ethernet ONT subport IDs are always “0” (e.g. “0” in the interface = 1-7-4-0) while GPON ONT subport IDs are always “non-zero” numbers (e.g. “4” in the interface = 1-3-1-4).

```
zSH> onu inventory
Processing list of 994
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
              Serial   Vendor Model  ONT            SW             ONT      OLT       Distance
ID  Interface Number   ID     ID     Version        Version        Rx Pwr   Rx Pwr    (KM)
=== ========= ======== ====== ====== ======== ======== ======= ======= ========
1   1-3-1-1   032AFD56 ZNTS   2426   S2.5.037       S2.5.037       -13.9 dBm -14.1 dBm    0.0000
2   1-3-1-2   A4907360 ZNTS   2520   00144-00011-27 R3.4.2.270sbn -14.5 dBm -13.4 dBm    0.0000
3   1-3-1-3   93425012 ZNTS   5114   00124-00044-01 R3.4.2.272c   -14.6 dBm -14.3 dBm    0.0000
4   1-3-1-4   032AECB8 ZNTS   2427   S3.1.209       S3.1.209       -14.7 dBm -14.2 dBm    0.0000
Total ONUs = 4
...

Slot 7
                    Serial    Vendor  Model     Act S/W     Stby S/W    Operational
     Interface      Number      ID      ID      Version     Version       Status
================== ========= ======= ===== ============ =========   ==========
1-7-1-0             00485890   ZNTS    2608T   S3.1.266       S3.0.711     Up
1-7-2-0             00486310   ZNTS    2608T   S3.1.266       S3.0.711     Up
1-7-3-0             15862810   ZNTS    2608T   S3.1.266       S3.0.711     Up
1-7-4-0             00485650   ZNTS    2608T   S3.1.266       S3.0.711     Up
1-7-15-0 +             -         -       -          -            -       Down
1-7-17-0 +             -         -       -          -            -       Down
1-7-19-0 +             -         -       -          -            -       Down
1-7-21-0 +             -         -       -          -            -       Up
Total CPEs = 8
    * against interface name indicates CPE is not configured
    + against interface name indicates CPE is misconfigured



Slot 9
                    Serial    Vendor  Model     Act S/W     Stby S/W    Operational
     Interface      Number      ID      ID      Version     Version       Status
================== ========= ======= ===== ============ =========   ==========
1-9-1-0             306484238  ZNTS    2804D   S3.1.266       S3.1.268     Up
1-9-2-0             306484212  ZNTS    2804D   S3.1.266       S3.1.268     Up
1-9-3-0             306484194  ZNTS    2804D   S3.1.266       S3.1.268     Up
1-9-4-0             306484164  ZNTS    2804D   S3.1.266       S3.1.268     Up
Total CPEs = 4
    + against interface name indicates CPE is misconfigured
          * against interface name indicates CPE is not configured
```

2- 6.1.1 Additional GPON ONT Inventory Reports

GPON ONTs can also be listed per GPON card, per GPON OLT port, or per an individual ONT.

The following generates a report for all ONTs on the GPON card in slot 3:

```
zSH> onu inventory 3
Processing list of 994
```

```
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
               Serial   Vendor Model  ONT            SW             ONT      OLT       Distance
ID  Interface  Number   ID     ID     Version        Version        Rx Pwr   Rx Pwr    (KM)
=== ========== ======== ====== ====== ========       ========       ======== ========  ========
1   1-3-1-1    032AFD56 ZNTS   2426   S2.5.037       S2.5.037       -13.9 dBm -14.1 dBm    0.0000
2   1-3-1-2    A4907360 ZNTS   2520   00144-00011-27 R3.4.2.270sbn -14.5 dBm -13.4 dBm    0.0000
3   1-3-1-3    93425012 ZNTS   5114   00124-00044-01 R3.4.2.272c   -14.6 dBm -14.3 dBm    0.0000
4   1-3-1-4    032AECB8 ZNTS   2427   S3.1.209       S3.1.209       -14.7 dBm -14.2 dBm    0.0000
Total ONUs = 4
...
```

The following generates a report for all ONTs on GPON OLT port 3/1:

```
zSH> onu inventory 3/1
Processing list of 32
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
               Serial   Vendor Model  ONT            SW             ONT      OLT       Distance
ID  Interface  Number   ID     ID     Version        Version        Rx Pwr   Rx Pwr    (KM)
=== ========== ======== ====== ====== ========       ========       ======== ========  ========
1   1-3-1-1    032AFD56 ZNTS   2426   S2.5.037       S2.5.037       -13.9 dBm -14.1 dBm    0.0000
2   1-3-1-2    A4907360 ZNTS   2520   00144-00011-27 R3.4.2.270sbn -14.5 dBm -13.3 dBm    0.0000
3   1-3-1-3    93425012 ZNTS   5114   00124-00044-01 R3.4.2.272c   -14.6 dBm -14.3 dBm    0.0000
4   1-3-1-4    032AECB8 ZNTS   2427   S3.1.209       S3.1.209       -14.7 dBm -14.2 dBm    0.0000
Total ONUs = 4
...
```

The following example generates a report for GPON ONT 3/1/1:

```
zSH> onu inventory 3/1/1
               Serial   Vendor Model  ONT            SW             ONT      OLT       Distance
ID  Interface  Number   ID     ID     Version        Version        Rx Pwr   Rx Pwr    (KM)
=== ========== ======== ====== ====== ========       ========       ======== ========  ========
1   1-3-1-1    032AFD56 ZNTS   2426   S2.5.037       S2.5.037       -13.9 dBm -14.6 dBm    0.0000
```

2- 6.1.2 Additional Active Ethernet ONT Inventory Reports

Active Ethernet ONTs can also be listed per Active Ethernet card or per Active Ethernet card port. Each Active Ethernet card port can only support one ONT, so a “per Active Ethernet ONT” request is not useful.

The following lists the ONTs on the Active Ethernet card in slot 7:

```
zSH> onu inventory 7
Processing list of 32
This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
Slot 7
                    Serial    Vendor  Model     Act S/W     Stby S/W    Operational
     Interface      Number      ID      ID       Version     Version       Status
================== ========= ======= ======= ============ ========== ===========
1-7-1-0            00485890   ZNTS    2608T  S3.1.266       S3.0.711     Up
1-7-2-0            00486310   ZNTS    2608T  S3.1.266       S3.0.711     Up
1-7-3-0            15862810   ZNTS    2608T  S3.1.266       S3.0.711     Up
1-7-4-0            00485650   ZNTS    2608T  S3.1.266       S3.0.711     Up
1-7-15-0 +            -         -       -         -            -        Down
1-7-17-0 +            -         -       -         -            -        Down
```

```
1-7-19-0 +              -        -      -         -           -       Down
1-7-21-0 +              -        -      -         -           -       Up
Total CPEs = 8
    * against interface name indicates CPE is not configured
    + against interface name indicates CPE is misconfigured
```

When a slot and port ID of an Active Ethernet card are included with the **onu inventory** command, the ONT on that port is listed (per Active Ethernet port).

The following lists the ONT on port 4 of the Active Ethernet card in slot 7:

```
zSH> onu inventory 7/4
                     Serial    Vendor  Model     Act S/W     Stby S/W    Operational
     Interface       Number      ID      ID      Version     Version       Status
================== ========= ======= ======= ============ ========= ==========
1-7-4-0             00485650   ZNTS    2608T  S3.1.266        S3.0.711     Up
```

2- 6.2 GPON ONT and ONT Port Status Monitoring

2- 6.2.1 GPON ONT Status

There are GPON ONT status commands that have no equivalent Active Ethernet ONT commands. The additional info provided by these commands are part of the GPON standards to provide information for maintaining and diagnosing GPON networks.

View status and alarms generated on an ONT with the **gpononu status** command.

Table 4 provides the output fields description for this command.

Table 4: gpononu status Command Output Field Explanations

Field	Description
ID	The ONU ID. In the range of 1 to 64.
Onu	The ONU interface name. By default in the format of shelf ID-Slot ID-OLT ID-ONU ID
OperStatus	The operational status of the ONU. Values: **Up** **Down**

Table 4: gpononu status Command Output Field Explanations (Continued)

Field	Description
ConfigState	The OMCI configuration states on the ONU. It is detected by the OLT side with respect to the ONU. Values: **None** This will probably only show during a bootup. Not yet queued for configuration. **Queue** Waiting to be configured. **Configuring** Being configured. **Active** configuration was successful. **Inactive** The ONU is down. **Non-OMCI** not provisioned for OMCI or SNMP. **RgComError** (for RG-enabled ONTs) SNMP cannot communicate with the ONT. **RgServiceSetupErr** (for RG-enabled ONTs) One or more SNMP commands failed. **OmciError** an error occurred during the OMCI configuration. **OmciErr+RgComErr** both an OMCI error and SNMP communications failure. **OmciErr+RgServErr** both an OMCI error and failure of one or more SNMP commands.
GponOnuStatus	The standard GPON MAC alarms of the ONU detected on the OLT. Values: **Active** ONU is active, no alarm **Inactive** ONU is inactive, cannot get alarm **LOS** Lost of Signal **LOF** Lost of Frame **DOW** Drift of Window **DG** Dying Gasp **SF** Signal Fail **SD** Signal Degrade **LCDG** Lost of GEM Channel Delinquency **RD** Remote Defect **RXPWRDSA** Received Power of Range, and ONU is disabled **TF** Transmitter Failure **SUF** Start Up Failure **LOA** Lost of Ack **MEM** Message error **PEE** Physical equipment error **OAML** Lost of OAM

Table 4: gpononu status Command Output Field Explanations (Continued)

Field	Description
DownloadState	ONT software image download states. Values: — this ONU is not configured with OMCI **None** **Queued** **NoUpgrade** **Downloading** **Complete** **Error** **Aborted**
OLT Rx Power	Upstream optical power level received at the OLT.
ONT Rx Power	Downstream optical power level received at the ONU.
Distance (KM)	Calculated distance of an ONU from the OLT.

This example shows the output of a gpononu status command. This command displays considerable output and can take up to several minutes. The syntax for this command can be gpononu status or onu status.

Note: The “gpononu” argument can be replaced in many of the cli commands with the abbreviated “onu” (as in **onu status**).

```
zSH> onu status
Processing list of 3908 GPON ONTs and 0 ActiveE CPEs

This command may take several minutes to complete.
Do you want to continue?  (yes or no) [no] yes
Slot 1  olt 1
                                    Download      OLT       ONT     Distance Gpon              AutoConfig
ID    Onu    OperStatus ConfigState State      Rx Power  Rx Power   (KM)     OnuStatus           State
== ======= ========== =========== ========= ========  ========  ======== ================= ======
 1  1-1-1-1     Up     Active     NoUpgrade -25.2dBm -19.5dBm  0.0391  Active             Init
 2  1-1-1-2     Up     Active     NoUpgrade -25.6dBm -19.8dBm  0.0382  Active             Init
 3  1-1-1-3     Up     Active     NoUpgrade -25.2dBm -19.1dBm  0.0385  Active             Init
 4  1-1-1-4    Down    Inactive   None        error    error    error   Inactive+LOS+LOF   Init
                                                                       +SUF+OAML
 5  1-1-1-5     Up     Active     NoUpgrade -24.2dBm -20.0dBm  0.0394  Active             Init
 6  1-1-1-6     Up     Active     NoUpgrade -27.9dBm -20.9dBm  0.0391  Active             Init
 7  1-1-1-7     Up     Active     NoUpgrade -25.8dBm -19.8dBm  0.0394  Active             Init
 8  1-1-1-8     Up     Active     NoUpgrade -24.9dBm -19.2dBm  0.0388  Active             Init
 9  1-1-1-9     Up     Active     NoUpgrade -23.8dBm -19.8dBm  0.0386  Active             Init
10  1-1-1-10    Up     Active     NoUpgrade -24.4dBm -19.3dBm  0.0386  Active             Init
11  1-1-1-11    Up     Active     NoUpgrade -24.0dBm -18.7dBm  0.0381  Active             Init
12  1-1-1-12    Up     Active     NoUpgrade -24.2dBm -18.6dBm  0.0382  Active             Init
13  1-1-1-13    Up     Active     NoUpgrade -24.3dBm -18.8dBm  0.0386  Active             Init
14  1-1-1-14    Up     Active     NoUpgrade -24.3dBm -19.9dBm  0.0379  Active             Init

Slot 2  olt 1
```

```
                                    Download      OLT       ONT     Distance Gpon              AutoConfig
ID     Onu    OperStatus ConfigState State      Rx Power  Rx Power   (KM)     OnuStatus           State
=== ======= ========== =========== ========= ========= ========= ======= ================== ======
 1  1-1-1-1      Up     Active     NoUpgrade -25.0 dBm -19.5 dBm  0.0391 Active             Init
 2  1-1-1-2      Up     Active     NoUpgrade -25.6 dBm -19.9 dBm  0.0382 Active             Init
 3  1-1-1-3      Up     Active     NoUpgrade -25.2 dBm -19.1 dBm  0.0385 Active             Init
 4  1-1-1-4     Down    Inactive   None         error     error      error Inactive+LOS+LOF  Init
                                                                         +SUF+OAML
 5  1-1-1-5      Up     Active     NoUpgrade -24.3 dBm -20.0 dBm  0.0394 Active             Init
 6  1-1-1-6      Up     Active     NoUpgrade -27.9 dBm -21.0 dBm  0.0391 Active             Init
 7  1-1-1-7      Up     Active     NoUpgrade -25.8 dBm -19.8 dBm  0.0394 Active             Init
 8  1-1-1-8      Up     Active     NoUpgrade -25.0 dBm -19.2 dBm  0.0388 Active             Init
 9  1-1-1-9      Up     Active     NoUpgrade -23.7 dBm -19.8 dBm  0.0386 Active             Init
10  1-1-1-10     Up     Active     NoUpgrade -24.5 dBm -19.3 dBm  0.0386 Active             Init
11  1-1-1-11     Up     Active     NoUpgrade -24.0 dBm -18.7 dBm  0.0381 Active             Init
12  1-1-1-12     Up     Active     NoUpgrade -24.2 dBm -18.6 dBm  0.0382 Active             Init
13  1-1-1-13     Up     Active     NoUpgrade -24.2 dBm -18.8 dBm  0.0386 Active             Init
14  1-1-1-14     Up     Active     NoUpgrade -24.4 dBm -19.9 dBm  0.0379 Active             Init
```

This example shows an operational ONT that completes OMCI provisioning.

```
zSH> onu status 1/7/5
                                    Download      OLT       ONT     Distance Gpon              AutoConfig
ID     Onu    OperStatus ConfigState State      Rx Power  Rx Power   (KM)     OnuStatus           State
=== ======= ========== =========== ========= ========= ========= ======= ================== ======
 5  1-1-7-5 Up          Active     NoUpgrade -13.3dBm -14.2dBm  0.0260  Active            Init
```

This example shows an operational ONT that gave a “dying gasp” message before going down. The OnuStatus message is stored for diagnostics.

```
zSH> onu status 1/7/5
                                    Download      OLT       ONT     Distance Gpon              AutoConfig
ID     Onu    OperStatus ConfigState State      Rx Power  Rx Power   (KM)     OnuStatus           State
=== ======= ========== =========== ========= ========= ========= ======= ================== ======
 5  1-1-7-5 Down        Inactive      None      error     error      error  Inactive+LOS+LOF   Init
                                                                          +DG+OAML
```

2- 6.2.2 GPON ONT Subscriber Facing Port - Status

When the port argument is used with the **gpononu status** command, the command displays the status of ports on the ONT using OMCI.

gpononu status [<<*slot*>[/*olt*[/*onu*>>]> | <*ifname*>] [*port* <*all* |<*portType*> <*portNumber*>] >]

The administrative state and operational state of the subscriber facing port on ONU is also displayed.

The *portType* is based on what is supported by the ONU model. The possible port types could be *eth* (Ethernet port), *pots* (POTS port), *rf* (RF port), and *ces* (T1/E1 port).

This example shows the status of an Ethernet port on ONU:

```
zSH> gpononu status 3/1/1 port eth 1
3/1/1 ONU Port Status
       Ethernet Port Status - Port  1
```

```
Configured Auto-Detection       auto
Administrative State            up
Operational State               active
Connection Type                 100BaseT full duplex
```

CHAPTER 3 LOGS FOR THE MXK-F

This chapter provides an overview of logging on the MXK-F.

3- 1 LOGGING ON THE SERIAL PORT

Procedure: *Enabling and Disabling logging*

By default, log messages are enabled on the serial craft port. Use the **log serial** command and the **log session** command to enable/disable logging:

The **log serial** command enables/disables logging messages for the session on the serial craft port. This command can be used in both Telnet connections and serial port connections to turn on and off the serial craft port logs.

This command setting persists across system reboots and serial logging is *on* by default.

To enable/disable logging for the serial craft port enter:

```
zSH> log serial off
Serial port logging disabled.

zSH> log serial on
Serial port logging enabled.
```

The **log session** command enables/disables logging messages for that session only when connected to the device through a Telnet session. If the user logs out, the logging setting returns to the default.

This command setting does not persist across system reboots and is *off* by default.

To enable/disable logging for the current Telnet session only enter:

```
zSH> log session on
Logging enabled.

zSH> log session off
Logging disabled.
```

3- 2 MONITOR THE SYSTEM WITH LOG FILES

This section provides the following information on how logs work on the MXK-F

3- 2.1 Overview

Logging enables administrators to monitor system events by generating system messages. It sends these messages to:

- A temporary management session (either on the serial craft port or over a Telnet session)
- Log modules to create permanent log files
- A syslog server (optional)

The type of information sent in these messages can be configured using the **log** command. By default, the system sends the same type of information to all log message destinations. If you want to send different types of messages to the syslog daemon, use the **syslog** command.

3- 2.2 Default Log Store Level

The default log store level is now set to emergency so by default the **log display** command displays only emergency level messages. Use the **log cache** command to display all messages that have been logged to console.

Use the **cd log** and **dir** commands to view the log file history. The log files in this directory record console activity on the MXK-F for the running image, and preserve a copy of the last two reboots. The files *consolelog1.txt* and *consolelog2.txt* hold 10000 lines of console output each. Once the file reaches

10000 lines, the filename is changed to *.old* and a new *.txt* file is used. After a reboot, the *.txt* files are also saved as .old files. Use the **consolelog display <filename>** command to view the contents for a consolelog file. These files are used for troubleshooting and system activity monitoring.

3- 2.3 User Login Notification

Notifications of user login are sent to the console log.

```
APR 09 11:06:01: notice : 1/m1/12  : shelfctrl: Slot m1, max temp 66C(150F) is back to normal operational
condition
APR 09 11:06:01: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Minor   Slot m1, max temp 66C(150F) is normal
APR 09 11:53:59: critical: 1/m1/1027: rebootserver:
* * * * Slot Reboot : type = 2, shelf = 1, slot = 9
APR 09 11:54:01: critical: 1/m1/1027: rebootserver:
* * * * Slot Reboot : type = 2, shelf = 1, slot = 11
APR 09 11:54:04: critical: 1/m1/1027: rebootserver:
* * * * Slot Reboot : type = 2, shelf = 1, slot = 13
APR 09 11:54:08: critical: 1/m1/1027: rebootserver:
* * * * Slot Reboot : type = 2, shelf = 1, slot = 15
```

3- 2.4 Enable/disable Logging

By default, log messages are enabled on the serial craft port. Use the **log session** command and the **log serial** command to enable/disable logging:

The **log session** command enables/disables logging messages for that session only. If the user logs out, the logging setting returns to the default. To enable logging for the only the current session:

```
zSH> log session on
Logging enabled.
```

To disable logging for the session:

```
zSH> log session off
Logging disabled.
```

The **log serial** command enables/disables logging messages for all sessions on the serial craft port. This setting persists across system reboots. To enable/disable logging for the serial craft port:

```
zSH> log serial on
Serial port logging enabled.
```

To disable logging for the serial port:

```
zSH> log serial off
Serial port logging disabled.
```

3- 2.5 Log Message Format

Log messages contain the following information

Table 5: Default Log Message Fields

Option	Description
Date	Date stamp of log message. Enabled by default.
Time	Time stamp of log message. Enabled by default.
Ticks	Current tick count. When the **tick** option is used, the date and time fields are not displayed.
Level	Logging level of the message. Enabled by default.
Address	The shelf and slot and application identifier causing the alarm.
Logtest	Log handle.
Taskname	Name of task that generated the log message. This is generally useful only for DZS development engineers. Enabled by default.
Function	Function that generated the log message.
Line	Line in code that generated the log message. This is generally useful only for DZS support staff.
Port	Port related to the log message.
Category	Category of the log message.
System	System related to the log message.
All	Controls all log message options.
Default	Controls the default log message options.
Message text	A description of the error that caused the alarm.

To change the information displayed in the log messages, use the **log option** command. First, display the available options:

```
zSH> log option
Usage: log option  < time          | 1 >  < on | off >
                   < date          | 2 >  < on | off >
                   < level         | 3 >  < on | off >
                   < taskname      | 4 >  < on | off >
                   < taskid        | 5 >  < on | off >
                   < file          | 6 >  < on | off >
                   < function      | 7 >  < on | off >
                   < line          | 8 >  < on | off >
                   < port          | 9 >  < on | off >
                   < category      | 10 > < on | off >
                   < system        | 11 > < on | off >
                   < ticks         | 12 > < on | off >
                   < stack         | 13 > < on | off >
                   < globalticks   | 14 > < on | off >
                   < all           | 14 > < on | off >
```

```
                < default       | 15 > < on | off >
options 'time' & 'date' supercede option 'ticks'
time: date: level: address: log: port: category: system:  (0x707)
```

Then, turn the option **on** or **off**. For example, the following command will turn the task ID on or off in log messages:

```
zSH> log option taskid on
time: date: level: address: log: taskid: port: category: system:  (0x717)

zSH> log option taskid off
time: date: level: address: log: port: category: system:  (0x707)
```

The following commands will turn on or off the tick count display in log messages:

```
zSH> log option ticks on
time: date: level: address: log: port: category: system: ticks:  (0xf07)

zSH> log option ticks off
time: date: level: address: log: port: category: system:  (0x707)
```

The following command will turn all options on in log messages:

```
zSH> log option all on
time: date: level: address: log: taskname: taskid: file: function: line: port: category: system: ticks:
stack: globalticks:  (0x3fff)
```

3- 2.6 Modify Logging Levels

To modify logging, use the **log** command. To modify syslog messages, use the **syslog** command.

Caution: Changing the log level may generate enough output to disrupt service.

To display the current levels for all logging modules, use the **log show** command:

```
zSH> log show
MODULE                                          LEVEL         STATUS
alarm_mgr                                       error         enabled
alarmconfigmibhdlr                              error         enabled
assert                                          error         enabled
attproxy                                        error         enabled
atttree                                         error         enabled
autocfg                                         error         enabled
bds                                             error         enabled
bds_client                                      error         enabled
bridgemib                                       error         enabled
bulkstats                                       error         enabled
bulkstatshdlr                                   error         enabled
cam                                             error         enabled
card                                            error         enabled
```

```
card_resource                                    error       enabled
carddeletehdlr                                   info        enabled
cardred                                          error       enabled
cardsvchdlr                                      error       enabled
cli                                              error       enabled
clkmgr                                           warning     enabled
cpecfg                                           error       enabled
cpemgr                                           error       enabled
...
```

Logging levels determine the number of messages that are displayed on the console. The higher the log level, the more messages are displayed. The MXK-F supports the following log levels:

- 1: emergency
- 2: alert
- 3: critical
- 4: error
- 5: warning
- 6: notice
- 7: information
- 8: debug

To change the log level, use the **log** *module* **level** command. For example, the following command changes the card module logging level to emergency:

Caution: Changing the log level may generate enough output to disrupt service.

```
zSH> log level card emergency
Module: card at level: emergency
```

To enable or disable log levels for a module, use the log enable or log disable commands. For example:

```
zSH> log disable card
Module: card is now disabled
```

3- 2.7 Non-persistent Log Messages

The **log cache** command displays the non-persistent log cache messages:

```
zSH> log cache
[1]: FEB 06 22:30:07: notice : 1/m1/12   : shelfctrl: Resetting card 4.
[2]: FEB 06 22:30:07: notice : 1/m1/12   : shelfctrl: Resetting card m2.
[3]: FEB 06 22:30:07: notice : 1/m1/12   : shelfctrl: Resetting card a.
[4]: FEB 06 22:30:07: notice : 1/m1/12   : shelfctrl: Resetting card b.
[5]: FEB 06 22:30:08: alert  : 1/m1/1025: alarm_mgr: 01:m1:01 Minor ETHERNET Up - Ethernet line up
```

```
[6]: FEB 06 22:30:10: alert  : 1/m1/12  : shelfctrl: Card in slot m2 in the fault state. cause=0x8
POST=0x0.
[7]: FEB 06 22:30:10: notice : 1/m1/12  : shelfctrl: Resetting card m2.
[8]: FEB 06 22:30:10: notice : 1/m1/12  : shelfctrl: Upper and lower fan trays detected.
[9]: FEB 06 22:30:10: alert  : 1/m1/1025: alarm_mgr: 01:m2:00 Major   Card running
```

The **log cache max length** command sets the maximum number of log messages to store. The maximum log cache size is 2147483647, depending in the amount of memory available.

log cache max length

To change the current configured log cache size:

```
zSH> log cache max 200
Maximum number of log messages that can be saved: 200
```

The **log cache grep pattern** command searches through the log cache for the specified regular expression.

log cache grep pattern

The following example searches through the log cache for the string "Critical":

```
zSH> log cache grep Major
Searching for: "Major"
[1]: JAN 01 00:02:00: alert  : 1/m1/1025: alarm_mgr: 01:m2:00 Major   Card running
[2]: JAN 01 04:11:53: alert  : 1/m1/1025: alarm_mgr: 01:m2:00 Major   Card running
```

The **log cache clear** command clears the log cache.

log cache clear

The **log cache size** command sets the maximum amount of memory for the log cache. Without options, displays the current log size.

```
zSH> log cache size
Number of log messages in the cache: 20
Total bytes used by the cache: 2052
```

The **log cache help** command displays the help information for the **log cache** command:

```
zSH> log cache help
Usage: log cache < max   > < length  >
                 < grep  > < pattern >
                 < clear >
                 < size  >
                 < help  >
With no arguments the 'log cache' command prints out all the
log messages currently in the cache.
The 'max' command is used to view/set the maximum number of
log messages that can be cached at one time.  If the cache is
full then the oldest log is discarded and the new log is
inserted.  If no value is given then the current setting is
displayed
The 'size' command is used to display the amount of memory
```

```
currently being used by the log cache.
The 'clear' command is used to erase the log cache.
The 'grep' command is used for searching the log cache for a
specific pattern.  Extended regular expressions are supported.
```

3- 2.8 Persistent Log Messages

Use the **log cache** command to view the persistent logs which only stores emergency level logs. For example:

```
zSH> log display
JAN 01 04:27:02: emergency: 1/m1/12  : shelfctrl: Critical alarm set!
JAN 01 04:27:02: emergency: 1/m1/12  : shelfctrl: Critical alarm set!
```

3- 2.9 Example Log Messages

This section provides examples of how to interpret log messages.

The following message appears when a card in the MXK chassis comes up or goes down.

The most important parts of the message are the date and time the event occurred, the shelf/slot of the event, and the message text. The remainder of the information is only useful for DZS development engineers.

For example:

```
[5]: JAN 01 04:27:02: emergency: 1/m1/12  : shelfctrl: Critical alarm set!

[97]: JAN 02 02:17:29: alert  : 1/a/1025: alarm_mgr: 01: a:01 Critical ETHERNET Down - Ethernet uplink
down
```

3- 2.10 Log Filter Command

The **log filter** command is available as part of the log command functionality. This command enables users to show, set and delete log filters. Log filters limit the scope of log messages to a specific entity for troubleshooting and diagnostics. When a log filter is set, the filter is assigned an index number and only messages relate the specified entity are displayed. Filters can be set for a specific ifindex, slot/port or subscriber.

log filter

Restrict the display of log messages to only the log messages for a specified entity.

Syntax: **log filter show | set (ifindex|port *slotport*|vcl *ifindex vpi vci*|subscriber *endpoint*)| delete**

```
zSH> log filter set ifindex 12
New filter saved.

zSH> log filter set port 5 24
```

```
New filter saved.

zSH> log filter set subscriber 22
New filter saved.

zSH> log filter show
Index   Type            Filter Parameters
------  ------------    -----------------------------
 1      Port            slot=1, port=1
 2      Port            slot=1, port=4
 3      IfIndex         IfIndex=12
 4      Port            slot=5, port=24
 6      IfIndex         IfIndex=100
 7      IfIndex         IfIndex=104
 8      IfIndex         IfIndex=109
 9      IfIndex         IfIndex=103
10      IfIndex         IfIndex=107

zSH> log filter delete 10
Log filter 10 deleted
```

3- 2.11 Send Messages to a Syslog Server

Table 6 describes the parameters in the **syslog-destination** profile you can modify to send messages to a syslog server.

Table 6: syslog-destination Profile Parameters

Parameter	Description
address	The IP address of the machine hosting the syslog server. Default: **0.0.0.0**
port	The UDP port to which the syslog messages will be sent. Default: **514**

Table 6: syslog-destination Profile Parameters (Continued)

Parameter	Description
facility	The syslog facility to which the syslog messages will be sent. Values: **local0** **local1** **local2** **local3** **local4** **local5** **local6** **local7** **no-map** Default: **local0**
severity	The severity level used to filter messages being set to the syslog server. Values: **emergency** **alert** **critical** **error** **warning** **notice** **info** **debug** Default: **debug**

```
zSH> new syslog-destination  1
Please provide the following: [q]uit.
address: -->  {0.0.0.0}: 192.200.42.5 IP address of the syslog server
port: ----->  {514}: leave at default
facility: ->  {local0}:
severity: ->  {debug}:
.................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3- 2.12 Specify Different Log Formats for System and Syslog Messages

Table 7 describes the **log-module** profile that supports the configuration of persistent log messages, syslog messages, and persistent storage levels by module. Modify this profile when you need to send different messages to admin sessions, the persistent logs, and the syslog server.

Table 7: log-module Profile Parameters

Parameter	Description
name	The name of the module whose logging is controlled by this profile. Default: **logtest**
display	Controls the display of messages on the system. Messages logged at this level and above will be displayed. Values: **emergency** **alert** **critical** **error** **warning** **notice** **info** **debug** Default: **error**

Table 7: log-module Profile Parameters (Continued)

Parameter	Description
syslog	Controls the format of messages sent to the syslog server described in the **syslog-destination** profile. This field is similar to the display field, except for the **trackdisplay** value. Values: **emergency** **alert** **critical** **error** **warning** **notice** **info** **debug** **trackdisplay** Messages logged at, and above, the level set in the **display** parameter will also be recorded in the syslog server. Default: **trackdisplay**
store	Controls the persistent storage of messages. This field is similar to the display field, except for the **trackdisplay** value. Values: **emergency** **alert** **critical** **error** **warning** **notice** **info** **debug** **trackdisplay** Messages logged at, and above, the level set in the **display** parameter will also be recorded in the syslog server. Default: **trackdisplay**

```
zSH> new log-module 1
Please provide the following: [q]uit.
name: ----> {logtest}: test1
display: -> {error}: warning
syslog: --> {trackdisplay}:
store: ---> {trackdisplay}:
.....................
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

In this case, the **log-module 1** will display to the screen, all messages at and above *warning*. The variable *trackdisplay* means that the same messages as defined in display are also sent to the syslog and storage. If different level of

messages are needed for the different destinations, the variables for **display**, **syslog**, and **store** can be set at different levels.

CHAPTER 4 TRAPS AND ALARMS ON THE MXK-F

This chapter describes MXK-F traps and alarms:

4-1 SYSTEM 0 DEFAULT TRAPS AND ALARMS

A default **system 0** profile exists with the following configuration:

- Authentication traps are not enabled
- ZMS communication is not configured
- Alarm notification and output are enabled for all severity levels

```
zSH> get system 0
system  0
syscontact: ----------->  {}
sysname: -------------->  {}
syslocation: ---------->  {}
enableauthtraps: ------>  {disabled}
setserialno: ---------->  {0}
zmsexists: ------------>  {false}
zmsconnectionstatus: -->  {inactive}
zmsipaddress: --------->  {0.0.0.0}
configsyncexists: ----->  {false}
configsyncoverflow: --->  {false}
configsyncpriority: --->  {high}
configsyncaction: ----->  {noaction}
configsyncfilename: --->  {172.16.160.49_4_1392921484267}
configsyncstatus: ----->  {synccomplete}
configsyncuser: ------->  {zmsftp}
configsyncpasswd: ----->  ** private **
numshelves: ----------->  {1}
shelvesarray: ---------->  {}
numcards: ------------->  {3}
ipaddress: ------------>  {172.16.160.49}
alternateipaddress: --->  {0.0.0.0}
countryregion: -------->  {us}
primaryclocksource: --->  {0/0/0/0/0}
ringsource: ----------->  {internalringsourcelabel}
```

```
revertiveclocksource: ->  {true}
voicebandwidthcheck: -->  {false}
alarm-levels-enabled: ->  {critical+major+minor+warning}
userauthmode: --------->  {local}
radiusauthindex: ------>  {0}
secure: --------------->  {disabled}
webinterface: --------->  {enabled}
options: -------------->  {disdefpktrules}
reservedVlanIdStart: -->  {0}
reservedVlanIdCount: -->  {0}
snmpVersion: ---------->  {snmpv2}
persistentLogging: ---->  {disabled}
outletTemperatureHighThreshold: ->  {65}
outletTemperatureLowThreshold: -->  {-12}
```

4-2 ALARM MANAGER

Note: For GPON ONU alarms, refer to the MXK-F Configuration Guide. The **alarm show** command does not display GPON ONU alarms.

The MXK-F central alarm manager includes the ability to view the active alarms on the system (using the **alarm show** command) and the ability to store active alarms on the device. ZMS can use the alarms stored on the device to recreate the state of the alarms if it becomes disconnected.

The alarm command uses the following syntax:

alarm show [**summary**]

For example, the following command displays the number of current active alarms, the total number of alarms, the number of cleared alarms, as well as each active alarm and its severity:

```
zSH> alarm show
************    Central Alarm Manager    ************
        ActiveAlarmCurrentCount         :9
        AlarmTotalCount                 :21
        ClearAlarmTotalCount            :12
        OverflowAlarmTableCount         :0

ResourceId              AlarmType                               AlarmSeverity
----------              ---------                               -------------
1-3-1-0/gponolt         linkDown                                   critical
1-4-1-0/gponolt         linkDown                                   critical
1-b-3-0/eth             linkDown                                   critical
1-b-4-0/eth             linkDown                                   critical
1-b-6-0/eth             linkDown                                   critical
1-b-7-0/eth             linkDown                                   critical
1-b-8-0/eth             linkDown                                   critical
```

The **summary** option displays the number of current active alarms, the total number of alarms, the number of system cleared alarms:

```
zSH> alarm show summary
```

```
************    Central Alarm Manager    ************
        ActiveAlarmCurrentCount         :9
        AlarmTotalCount                 :21
        ClearAlarmTotalCount            :12
        OverflowAlarmTableCount         :0
```

The **alarm clear** command clears a transient alarm the system was unable to clear.

Caution: Alarms cleared with the **alarm clear** command will not be redisplayed if condition reoccurs. The alarm will redisplay only if the condition reoccurs, goes away, and then reoccurs.

```
zSH> alarm clear
 Num  ResourceId              AlarmType                    AlarmSeverity
----------------          ---------                   -------------
   1  1-3-1-0/gponolt          linkDown                        critical
   2  1-4-1-0/gponolt          linkDown                        critical
   3  1-b-3-0/eth              linkDown                        critical
   4  1-b-4-0/eth              linkDown                        critical
   5  1-b-6-0/eth              linkDown                        critical
   6  1-b-7-0/eth              linkDown                        critical
   7  1-b-8-0/eth              linkDown                        critical

Caution: use this option with discretion.
   Alarm will not be redisplayed if condition reoccurs. Alarm will redisplay only
   if condition reoccurs, goes away, and then reoccurs.

Enter alarm number from list, or 'q' to quit:
```

The **alarm clear** command only clears alarms one at a time by the alarm number displayed in the *Num* column.

4- 3 ALARM SUPPRESSION

The alarm suppression feature allows alarm/LED notification and output to be disabled based on alarm severity level for existing and future alarms. When an alarm level is disabled, all existing alarms of that type are cleared from the system. Future alarms of that type do not set LEDs or alarm relays and are not displayed in alarm output.

Alarm suppression is also supported in ZMS.

Table 8 lists the alarm suppression options and the resulting behaviors. By default, alarms for all severity levels are enabled.

Table 8: Alarm Suppression Options

Alarm Levels Enabled Setting	Alarm Behavior
critical+major+minor+warning	Enables all alarm levels. The default setting.
critical+major+minor	Disables all warning alarms.

Table 8: Alarm Suppression Options (Continued)

Alarm Levels Enabled Setting	Alarm Behavior
critical+major	Disables all minor, and warning alarms.
critical+major+warning	Disables all minor alarms.
critical+minor+warning	Disables all major alarms.
critical+minor	Disables all major and warning alarms.
critical+warning	Disables all major and warning alarms.
critical	Disables all major, minor, and warning alarms.
major	Disables all critical, minor, and warning alarms.
major+minor+warning	Disables all critical alarms.
major+minor	Disables all critical and warning alarms.
major+warning	Disables all critical and minor alarms.
minor	Disables all critical, major, and warning alarms.
minor+warning	Disables all critical and major alarms.
(no levels)	Disables all alarm levels.

This example disables alarm/LED notification and output for all current and future alarms with the severity levels minor and warning.

```
zSH> update system 0
system  0
Please provide the following: [q]uit.
syscontact: ----------->  {}:
sysname: ------------->  {}:
syslocation: ---------->  {}:
enableauthtraps: ------>  {disabled}:
setserialno: ---------->  {0}:
zmsexists: ------------>  {false}:
zmsconnectionstatus: -->  {inactive}:
zmsipaddress: --------->  {0.0.0.0}:
configsyncexists: ----->  {false}:
configsyncoverflow: --->  {false}:
configsyncpriority: --->  {high}:
configsyncaction: ----->  {noaction}:
configsyncfilename: --->  {}:
configsyncstatus: ----->  {syncinitializing}:
configsyncuser: ------->  {}:
configsyncpasswd: ----->  ** private **
numshelves: ----------->  {1}:
shelvesarray: ---------->  {}:
numcards: ------------->  {3}:
ipaddress: ------------>  {0.0.0.0}:
alternateipaddress: --->  {0.0.0.0}:
countryregion: -------->  {us}:
primaryclocksource: --->  {0/0/0/0/0}:
ringsource: ----------->  {internalringsourcelabel}:
revertiveclocksource: ->  {true}:
```

```
voicebandwidthcheck: -->  {false}:
alarm-levels-enabled: ->  {critical+major+minor+warning}: critical+major
userauthmode: --------->  {local}:
radiusauthindex: ------>  {0}:
secure: --------------->  {disabled}:
webinterface: --------->  {enabled}:
options: -------------->  {NONE(0)}:
reservedVlanIdStart: -->  {0}:
reservedVlanIdCount: -->  {0}:
snmpVersion: ---------->  {snmpv2}:
persistentLogging: ---->  {disabled}
outletTemperatureHighThreshold: ->  {65}
outletTemperatureLowThreshold: -->  {-12}
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

4-4 CONFIGURABLE HIGH AND LOW CHASSIS TEMPERATURE ALARMS

High and low temperature threshold parameters were added to the **system** profile:

```
zSH> show system
...
outletTemperatureHighThreshold:->   {35 - 65}
outletTemperatureLowThreshold:-->   {-40 - 0}
```

Parameter defaults are:

```
zSH> get system 0
...
outletTemperatureHighThreshold: ->  {65}
outletTemperatureLowThreshold: -->  {-12}
```

A minor alarm is raised when the outlet temperature is at the **outletTemperatureHighThreshold**. Major alarm is raised when the outlet temperature is **outletTemperatureHighThreshold**+*5*. Critical alarm is raised when the outlet temperature is **outletTemperatureHighThreshold**+*10*. For example, if the **outletTemperatureHighThreshold** is configured as 35, alarms will be in the order of 35, 40, 45 for Minor, Major, and Critical. If the **outletTemperatureHighThreshold** is configured as 65, alarms will be in the order of 65, 70, 75 for Minor, Major, and Critical.

When the **outletTemperatureLowThreshold** is set and the outlet sensor reaches the configured temperature, a Minor alarm is raised.

Procedure: *Configuring high and low chassis temperature alarms*

1 Configure the **outletTemperatureHighThreshold** and the **outletTemperatureLowThreshold** parameter in the **system 0** profile.

```
zSH> update system 0
system  0
```

```
Please provide the following: [q]uit.
syscontact: ---------------------->  {}:
sysname: ------------------------->  {}:
syslocation: --------------------->  {}:
enableauthtraps: ----------------->  {disabled}:
setserialno: --------------------->  {0}:
zmsexists: ----------------------->  {true}:
zmsconnectionstatus: ------------->  {inactive}:
zmsipaddress: -------------------->  {10.51.1.241}:
configsyncexists: ---------------->  {false}:
configsyncoverflow: -------------->  {false}:
configsyncpriority: -------------->  {high}:
configsyncaction: ---------------->  {noaction}:
configsyncfilename: -------------->  {10.51.1.118_4_1405380127627}:
configsyncstatus: ---------------->  {synccomplete}:
configsyncuser: ------------------>  {zmsftp}:
configsyncpasswd: ---------------->  {** private **}:  ** read-only **
numshelves: ---------------------->  {1}:
shelvesarray: -------------------->  {}:
numcards: ------------------------>  {3}:
ipaddress: ------------------------>  {10.51.1.118}:
alternateipaddress: -------------->  {0.0.0.0}:
countryregion: -------------------->  {us}:
primaryclocksource: -------------->  {0/0/0/0/0}:
ringsource: ---------------------->  {internalringsourcelabel}:
revertiveclocksource: ------------>  {true}:
voicebandwidthcheck: ------------->  {false}:
alarm-levels-enabled: ------------>  {critical+major+minor+warning}:
userauthmode: -------------------->  {local}:
radiusauthindex: ----------------->  {0}:
secure: -------------------------->  {disabled}:
webinterface: -------------------->  {enabled}:
options: ------------------------->  {NONE(0)}:
reservedVlanIdStart: ------------->  {0}:
reservedVlanIdCount: ------------->  {0}:
snmpVersion: --------------------->  {snmpv2}:
persistentLogging: --------------->  {disabled}:
outletTemperatureHighThreshold: ->  {65}: 55
outletTemperatureLowThreshold: -->  {-12}: 0
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

2 Verify the changes.

```
zSH> get system 0
system  0
syscontact: ---------------------->  {}
sysname: ------------------------->  {}
syslocation: --------------------->  {}
enableauthtraps: ----------------->  {disabled}
setserialno: --------------------->  {0}
zmsexists: ----------------------->  {true}
zmsconnectionstatus: ------------->  {inactive}
zmsipaddress: -------------------->  {10.51.1.241}
configsyncexists: ---------------->  {false}
configsyncoverflow: -------------->  {false}
configsyncpriority: -------------->  {high}
configsyncaction: ---------------->  {noaction}
```

```
configsyncfilename: ------------->  {10.51.1.118_4_1405380127627}
configsyncstatus: --------------->  {synccomplete}
configsyncuser: ----------------->  {zmsftp}
configsyncpasswd: --------------->  ** private **
numshelves: --------------------->  {1}
shelvesarray: ------------------->  {}
numcards: ----------------------->  {3}
ipaddress: ---------------------->  {10.51.1.118}
alternateipaddress: ------------->  {0.0.0.0}
countryregion: ------------------>  {us}
primaryclocksource: ------------->  {0/0/0/0/0}
ringsource: --------------------->  {internalringsourcelabel}
revertiveclocksource: ----------->  {true}
voicebandwidthcheck: ------------>  {false}
alarm-levels-enabled: ----------->  {critical+major+minor+warning}
userauthmode: ------------------->  {local}
radiusauthindex: ---------------->  {0}
secure: ------------------------->  {disabled}
webinterface: ------------------->  {enabled}
options: ------------------------>  {NONE(0)}
reservedVlanIdStart: ------------>  {0}
reservedVlanIdCount: ------------>  {0}
snmpVersion: -------------------->  {snmpv2}
persistentLogging: -------------->  {disabled}
outletTemperatureHighThreshold: ->  {55}
outletTemperatureLowThreshold: -->  {0}
```

3 View the alarms sent in the console window when thresholds are met or exceeded or use the **alarm show** command.

Alarm output will display in the console with **log ses on**.

```
zSH> log ses on
Logging is already enabled for this session.

JUN 18 09:59:58: alert  : 1/m1/12  : shelfctrl: Chassis Outlet temperature 55 degrees C (131 F)
zSH> JUN 18 09:59:58: alert  : 1/m1/12  : shelfctrl: Warning: Chassis temperature is above 55 degrees C
(131 F) threshold
JUN 18 10:05:02: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Minor   Updating Chassis Temperature alarm
severity
JUN 18 09:59:58: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Minor   Chassis Temperature above 55 degrees C
(131 F) threshold

JUN 18 10:05:02: alert  : 1/m1/12  : shelfctrl: Chassis Outlet temperature 60 degrees C (140 F)
JUN 18 10:05:02: alert  : 1/m1/12  : shelfctrl: Warning: Chassis temperature is above 60 degrees C (140
F) threshold.
JUN 18 10:05:02: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Major   Updating Chassis Temperature alarm
severity
JUN 18 10:05:02: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Major   Chassis temperature above 60 degrees C
(140 F) threshold

JUN 18 10:10:08: alert  : 1/m1/12  : shelfctrl: Chassis Outlet temperature 65 degrees C (149 F)
JUN 18 10:10:08: alert  : 1/m1/12  : shelfctrl: Warning: Chassis temperature is above 65 degrees C (149
F) threshold.
JUN 18 10:10:08: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Critical Updating Chassis Temperature alarm
severity
JUN 18 10:10:08: alert  : 1/m1/1025: alarm_mgr: 01:m1:00 Critical   Chassis temperature above 65 degrees
C (149 F) threshold
```

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :21
       AlarmTotalCount                 :100
       ClearAlarmTotalCount            :79
       OverflowAlarmTableCount         :0
ResourceId               AlarmType                              AlarmSeverity
----------               ---------                              -------------
...
system                   temp_over_limit                           minor
...
```

View the alarm when the outlet temperature exceeds the configured temperature high threshold by +5.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :21
       AlarmTotalCount                 :101
       ClearAlarmTotalCount            :80
       OverflowAlarmTableCount         :0
ResourceId               AlarmType                              AlarmSeverity
----------               ---------                              -------------
...
system                   temp_over_limit                           major
...
```

View the alarm when the outlet temperature exceeds the configured temperature high threshold by +10.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :21
       AlarmTotalCount                 :102
       ClearAlarmTotalCount            :81
       OverflowAlarmTableCount         :0
ResourceId               AlarmType                              AlarmSeverity
----------               ---------                              -------------
...
system                   temp_over_limit                           critical
...
```

View the alarm when the outlet temperature reaches the configured temperature low threshold.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :21
       AlarmTotalCount                 :112
       ClearAlarmTotalCount            :91
       OverflowAlarmTableCount         :0
ResourceId               AlarmType                              AlarmSeverity
----------               ---------                              -------------
...
system                   temp_under_limit                          minor
...
```

The temperature of the chassis can also be viewed with the **shelfctrl monitor** command.

```
zSH> shelfctrl monitor
Shelf                          Status
-------------------------------------------------------------------------
Uptime                         6 hours, 10 minutes
Upper Fan Tray:
   FPGA version                0.1
   Firmware version            0.0
Lower Fan Tray:
   FPGA version                0.1
   Firmware version            0.0
Management Card Glue version   0.15

Chassis Temperatures           Celsius(C)             Fahrenheit(F)
-------------------------------------------------------------------------
Ambient                        74                     165
Outlet                         93                     199
Temperature reading            failure - Over 75 C / 167 F

Fan Power Supplies & Alarm     Status
-------------------------------------------------------------------------
Upper Fan Tray:
   Fan Power 1                 normal
   Fan Power 2                 normal
   Fan alarm                   ok
Lower Fan Tray:
   Fan Power 1                 normal
   Fan Power 2                 normal
   Fan alarm                   ok

Power Supplies                 Volts(V)               Status
-------------------------------------------------------------------------
Battery A                      -0.44V                 failure
Battery B                      -51.74V                normal
Battery A return               ----
Battery B return               -0.51V

Device                         Status
-------------------------------------------------------------------------
System                         Critical alarm set
Card m1                        Critical alarm set
Card m2                        Critical alarm set
Card a                         Critical alarm set
Card b                         Critical alarm set

Alarm I/O Board
-------------------------------------------------------------------------
CPLD version                   0.0
Present:                       Yes
Alarm input:                       Ai1  Ai2  Ai3  Ai4  Ai5  Ai6  Ai7  Ai8
Status (Energized/de-energized):   d    d    d    d    d    d    d    d
NormalOpen/NormalClosed/NotSpec:   NS   NS   NS   NS   NS   NS   NS   NS
Alarm Active:                      No   No   No   No   No   No   No   No
```

4- 5 SETTABLE ALARMS ON ETHERNET PORTS

The alarm severity for Ethernet ports can be set to the following levels: *critical*, *major*, *minor*, or *warning*.

Procedure: *Viewing Alarms on Ethernet Ports*

1 View the current alarm setting on an single Ethernet port.

```
zSH> port show alarm 1-m1-1-0/eth
-------------------------------------------------------------------
       Interface              Alarm severity         Status trap
-------------------------------------------------------------------
       1-m1-1-0/eth           CRITICAL                   ENABLED
-------------------------------------------------------------------
```

2 View the current alarms on multiple Ethernet fabric card ports with wildcard.

```
zSH> port show alarm 1-a-*-*/eth
-------------------------------------------------------------------
       Interface              Alarm severity         Status trap
-------------------------------------------------------------------
       1-a-1-0/eth
       1-a-8-0/eth            CRITICAL                   ENABLED
       1-a-7-0/eth            CRITICAL                   ENABLED
       1-a-6-0/eth            CRITICAL                   ENABLED
       1-a-5-0/eth            CRITICAL                   ENABLED
       1-a-4-0/eth            CRITICAL                   ENABLED
       1-a-3-0/eth            CRITICAL                   ENABLED
       1-a-2-0/eth            CRITICAL                   ENABLED
-------------------------------------------------------------------
```

Procedure: *Changing the alarm severity level for one Ethernet port*

Use the **port config alarm** *interfaceName/type* **severity** <*severity level*> command to set the severity level on an Ethernet port.

Configure a different alarm setting on an Ethernet port.

```
zSH> port config alarm 1-9-1-0/eth severity major
Alarm severity level set for 1-9-1-0/eth is major
```

Procedure: *Changing the alarm severity level for multiple Ethernet ports*

Use the **port config alarm** *interfaceName/type* **severity** <*severity level*> command to set the severity level on multiple Ethernet ports.

Change the alarm setting of all Ethernet ports on the line card.

```
zSH> port config alarm 1-9-*-*/eth severity critical
Alarm severity level set for 1/9/32/0/eth is critical
Alarm severity level set for 1/9/31/0/eth is critical
Alarm severity level set for 1/9/30/0/eth is critical
Alarm severity level set for 1/9/29/0/eth is critical
Alarm severity level set for 1/9/28/0/eth is critical
Alarm severity level set for 1/9/27/0/eth is critical
```

```
Alarm severity level set for 1/9/26/0/eth is critical
Alarm severity level set for 1/9/25/0/eth is critical
Alarm severity level set for 1/9/24/0/eth is critical
Alarm severity level set for 1/9/23/0/eth is critical
Alarm severity level set for 1/9/22/0/eth is critical
Alarm severity level set for 1/9/21/0/eth is critical
Alarm severity level set for 1/9/20/0/eth is critical
Alarm severity level set for 1/9/19/0/eth is critical
Alarm severity level set for 1/9/18/0/eth is critical
Alarm severity level set for 1/9/17/0/eth is critical
Alarm severity level set for 1/9/16/0/eth is critical
Alarm severity level set for 1/9/15/0/eth is critical
Alarm severity level set for 1/9/14/0/eth is critical
Alarm severity level set for 1/9/13/0/eth is critical
Alarm severity level set for 1/9/12/0/eth is critical
Alarm severity level set for 1/9/11/0/eth is critical
Alarm severity level set for 1/9/10/0/eth is critical
Alarm severity level set for 1/9/9/0/eth is critical
Alarm severity level set for 1/9/8/0/eth is critical
Alarm severity level set for 1/9/7/0/eth is critical
Alarm severity level set for 1/9/6/0/eth is critical
Alarm severity level set for 1/9/5/0/eth is critical
Alarm severity level set for 1/9/4/0/eth is critical
Alarm severity level set for 1/9/3/0/eth is critical
Alarm severity level set for 1/9/2/0/eth is critical
Alarm severity level set for 1/9/1/0/eth is critical
```

4- 6 GPON, XGPON1 AND NG-PON2 ALARMS AND TRAPS

The GPON, XGPON1 and NG-PON2 alarms and traps are the same, and identified as “GPON” alarms and traps unless otherwise noted. This sections describes the following topics:

4- 6.1 GPON Alarms

4- 6.1.1 Retrieve Alarm Information From an ONU

View alarms that are internal to the ONU and ONU LAN facing port with the **gpononu alarms** command.

```
zSH> gpononu alarms 1/7/1
1/7/1 ONU Active Alarms
  MINOR     PptpEthUni 0x0504 LanLo
```

4- 6.1.2 Monitor GPON Alarms

Users can monitor GPON alarms in different levels:

- If users want to view the standard GPON MAC alarms that generated on the ONU and detected on the OLT, use the **gpononu status** command. For example: LOS (Lost Of Signal) alarm or DG (Dying Gasp) alarm of an ONU.
- If users want to view the internal alarms that generated on the ONU UNI ports (also called LAN facing ports or subscriber facing ports) and detected on the ONU, use the **gpononu alarms** command. For example: LanLos alarm of an Ethernet UNI port.
- If users want to view the ONU and OLT alarms that generated on the MXK system, use the **alarm show** command. For example: GPON BIP threshold crossing monitor alarms, GPON high and low receive power threshold alarms, or rogue ONU detection and rogue ONU alarms.

  The GPON alarms reported with the **alarm show** command are described in the following section.

4- 6.1.3 GPON BIP Threshold Crossing Monitor Alarms

Users can monitor BIP threshold crossing alarms, set the threshold for BIP errors on GPON, and also configure whether or not to auto-disable the ONU if the threshold has been exceeded. BIP is a counter representing bit errors on the PON link to a specific ONU. This is configured on a per-OLT basis, but is monitored per ONU. To configure the GPON BIP threshold on all ONUs under an OLT, use the **update gpon-olt-config** command.

ONU raises a “bip threshold exceeded” alarm if bip-error-monitoring-mode in the gpon-olt-config profile is set to either monitorOnly or blockOnError and the alarm condition exists. When the alarm is set, the MXK will periodically restart the BIP error measurement. If the condition that cause the alarm is improved, a deactivated ONU is reactivated, and the alarm is cleared. The default interval for the periodic measurement is 5 minutes.

```
zSH> update gpon-olt-config 1-1-1-0/gponolt
 gpon-olt-config  1-1-1-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: ----->  {200}:
max-onu-response-time: ------->  {50}:
preassigned-eqd: ------------->  {0}:
los-alpha: ------------------->  {4}:
```

```
lof-alpha: ------------------->  {4}:
loam-alpha: ------------------>  {3}:
scrambler: ------------------->  {enabled}:
fec-mode: -------------------->  {disabled}:
auto-learn: ------------------>  {enabled}:
power-level: ----------------->  {0}:
guard-bit-count: ------------->  {32}:
dba-mode: -------------------->  {predictive}:
gem-block-size: -------------->  {16}:
us-ber-interval: ------------->  {5000}:
ds-ber-interval: ------------->  {5000}:
ber-sf-threshold: ------------>  {3}:
ber-sd-threshold: ------------>  {5}:
fec-request: ----------------->  {disabled}:
key-exchange: ---------------->  {disabled}:
min-rt-propagation-delay: ---->  {0}:
min-onu-response-time: ------->  {10}:
eqd-measure-cycles: ---------->  {5}:
drift-ctrl-interval: --------->  {1000}:
drift-ctrl-limit: ------------>  {3}:
alloc-cycle-length: ---------->  {2}:
min-us-alloc: ---------------->  {16}:
ack-timeout: ----------------->  {2000}:
pls-max-alloc-size: ---------->  {120}:
dba-cycle: ------------------->  {2}:
sr-dba-reporting-block-size: ->  {48}:
protection-switchover-timer: ->  {500}:
preamble-override: ----------->  {disabled}:
preamble-type-0: ------------->  {0x00}:
preamble-type-1: ------------->  {0x00}:
preamble-type-3-pre-range: --->  {0x0b}:
preamble-type-3-post-range: -->  {0x08}:
preamble-type-3-pattern: ----->  {0xaa}:
bip-error-monitoring-mode: --->  {monitorOnly}:
errors-per-sample-threshold: ->  {100}:
errored-samples-threshold: --->  {10}:
bip-max-sample-gap: ---------->  {10}:
rogue-onu-detection: ----------> {disabled}:
rogue-onu-detect-frequency: ----> {10}:
rogue-onu-rx-power-threshold: --> {-30}:
.....................
Save changes? [s]ave, [c]hange or [q]uit:q
```

Table 9: BIP Error Threshold Attributes in gpon-olt-config Profile

Attribute	Description
bip-error-monitoring-mode	Disable or enable the BIP error monitoring. Values: **disabled** The BIP error monitoring feature is disabled. **monitorOnly** Monitor BIP errors. When the ONU crosses the BIP error threshold, trigger a local alarm and send a trap to ZMS. **blockOnError** Monitor BIP errors. When the ONU crosses the BIP error threshold, trigger a local alarm, send a trap to ZMS, disable ONU ranging and set ONU line status to DSA (i.e. disabled). Default: **monitorOnly**
errors-per-sample-threshold	If the number of BIP errors per sample exceeds this threshold, it is counted as an errored sample. Default: **100**
errored-samples-threshold	If the number of errored samples exceed this sample threshold, report and disable the onu if in blockOnError mode, otherwise simply report the threshold as being exceeded. Default: **10**
bip-max-sample-gap	If two adjacent errored samples were taken farther apart than this threshold, do not count the earlier sample as an errored sample. This value is in the unit of seconds. Default: **10**

Procedure: *Configuring GPON BIP Error Threshold Crossing Monitor Alarms*

1 View the ONU status.

```
zSH> onu status 1/1/2
                          Omci       Gpon    Download    OLT      ONT      Distance
ID   Onu   OperStatus ConfigState OnuStatus State     Rx Power  Rx Power  (KM)
== ======= ========== =========== ======== ========= ========= ========= =======
2  1-1-1-2     Up     Active      Active    NoUpgrade -23.8 dBm -23.0 dBm   18
```

2 Configure the BIP error monitoring mode and thresholds as desired. This example changes the monitoring mode to **blockonerror**, and changes the BIP error threshold values.

```
zSH> update gpon-olt-config 1-1-1-0/gponolt
 gpon-olt-config  1-1-1-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: ----->  {200}:
max-onu-response-time: ------->  {50}:
preassigned-eqd: ------------->  {0}:
los-alpha: ------------------->  {4}:
lof-alpha: ------------------->  {4}:
loam-alpha: ------------------>  {3}:
scrambler: ------------------->  {enabled}:
fec-mode: -------------------->  {disabled}:
auto-learn: ------------------>  {enabled}:
power-level: ----------------->  {0}:
guard-bit-count: ------------->  {32}:
```

```
dba-mode: ---------------------> {predictive}:
gem-block-size: --------------> {16}:
us-ber-interval: -------------> {5000}:
ds-ber-interval: -------------> {5000}:
ber-sf-threshold: ------------> {3}:
ber-sd-threshold: ------------> {5}:
fec-request: -----------------> {disabled}:
key-exchange: ----------------> {disabled}:
min-rt-propagation-delay: ----> {0}:
min-onu-response-time: -------> {10}:
eqd-measure-cycles: ----------> {5}:
drift-ctrl-interval: ---------> {1000}:
drift-ctrl-limit: ------------> {3}:
alloc-cycle-length: ----------> {2}:
min-us-alloc: ----------------> {16}:
ack-timeout: -----------------> {2000}:
pls-max-alloc-size: ----------> {120}:
dba-cycle: -------------------> {2}:
sr-dba-reporting-block-size: -> {48}:
protection-switchover-timer: -> {500}:
preamble-override: -----------> {disabled}:
preamble-type-0: -------------> {0x00}:
preamble-type-1: -------------> {0x00}:
preamble-type-3-pre-range: ---> {0x0b}:
preamble-type-3-post-range: --> {0x08}:
preamble-type-3-pattern: -----> {0xaa}:
bip-error-monitoring-mode: ---> {monitorOnly}:blockonerror
errors-per-sample-threshold: -> {100}: 99
errored-samples-threshold: ---> {10}:9
bip-max-sample-gap: ----------> {10}:9
rogue-onu-detection: -----------> {disabled}:
rogue-onu-detect-frequency: ----> {10}:
rogue-onu-rx-power-threshold: --> {-30}:
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

3 View the ONU status. This example assumes the BIP error on this ONU exceeded the threshold values. With the **blockonerror** mode, the ONU will raise an alarm and be auto-disabled. The **GponOnuStatus** in this example shows a brief description about this ONU is inactive and EXCBIPDSA (i.e. exceeded BIP threshold, and ONU is disabled.).

```
zSH> onu status 1/1/2
                          Omci       Gpon              Download  OLT    ONT  Dist.
ID   Onu    OperStatus ConfigState OnuStatus          State    Rx Pwr Rx Pwr(KM)
== ====== ======== ========= ================ ======= ===== ==== ====
2  1-1-1-2   Down     Inactive    Inactive+EXCBIPDSA  None    error  error  0.0
```

GponOnuStatus acronym definitions:

“Active” - ONU is Active

“Inactive” - ONU is Inactive

“LOS” - Loss of Signal

“LOF” - Loss of Frame

“SD” - Drift Of Window

“SF” - Signal Fail

“SD” - Signal Degrade

“LCDG” - Loss of GEM channel delineation

“RD” - Remote defect

“TF” - Transmitter Failure

“SUF” - Start-up Failure

“LOA” - Loss of Acknowledge

“DG” - Receive Dying-gasp

“OAML” - PLOAM Cell Loss

“MEM” - Message Error Message

“PEE” - Physical Equipment Error

“EXCBIPDSA” - Disable Onu, excessive BIP errors

“EXCBIP” - Excessive BIP errors. ONU is not disabled

“RXPWRDSA” - Upstream Rx Power out of range. ONU is disabled.

“RXPWRNOTDSA” - Upstream Rx Power out of range. ONU is not disabled.

4 View the raised alarms on this ONU at the system level.

```
zSH> alarm show
************    Central Alarm Manager    ************
        ActiveAlarmCurrentCount         :8
        AlarmTotalCount                 :15
        ClearAlarmTotalCount            :7
        OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-1-0/gponolt         linkDown                                  critical
1-1-2-0/gponolt         linkDown                                  critical
1-1-3-0/gponolt         linkDown                                  critical
1-1-4-0/gponolt         linkDown                                  critical
1-1-1-2/gpononu          linkDown                                          minor
1-1-1-2/gpononu          inactive,bip threshold exceeded,dsa               minor
```

Note: If more than one error condition is present (example: Excessive BIP errors and Optical Rx Power too high), the local alarm text may be too long to fit within the display output. In this case, AlarmType shows “issue 'onu status' command 0x300002” in order to prompt user to enter the **onu status** command for more details. The “0x300002” value is the actual alarm status word and will vary.

```
zSH> alarm show
************    Central Alarm Manager    ************
```

```
        ActiveAlarmCurrentCount         :8
        AlarmTotalCount                 :32
        ClearAlarmTotalCount            :24
        OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-1-1-2/gpononu         issue 'onu status' command 0x300002       minor
```

4- 6.1.4 GPON High and Low Receive Power Threshold Alarms

By default, the MXK will trigger a local alarm, and send a trap to ZMS when the GPON high/low receive power thresholds are crossed for the ONU received power on the upstream. The default value of the High threshold is -10 dbm. The default value of the Low threshold is -30 dbm. Users can change the default threshold values, and choose the upstream received power monitoring mode as desired.

ONU raises a “rx power out of range” alarm if us-rx-power-monitoring-mode in **gpon-olt-onu-config** profile is set to either monitorOnly or blockOnError and the alarm condition exists. When the alarm is set, the MXK will periodically restart the power level measurement. If the condition that cause the alarm is improved, a deactivated ONU is reactivated, and the alarm is cleared. The default interval for the periodic measurement is 5 minutes.

The GPON high/low receive power threshold values and monitoring modes are configured on a per-ONU basis with the **update gpon-olt-onu-config** command.

```
zSH> update gpon-olt-onu-config 1-1-1-2/gpononu
gpon-olt-onu-config  1-1-1-2/gpononu
Please provide the following: [q]uit.
serial-no-vendor-id: ------------------>  {ZNTS}:  ** read-only **
serial-no-vendor-specific: ------------>  {2216690777}:  ** read-only **
password: ----------------------------->  {}:
auto-learn: --------------------------->  {enabled}:
power-level: -------------------------->  {0}:
us-ber-interval: ---------------------->  {5000}:
ds-ber-interval: ---------------------->  {5000}:
onu-added: ---------------------------->  {true}:
omci-file-name: ----------------------->  {}:
ONU-Managed-Entity-Profile-name: ------>  {znid-gpon-2510-omci-4port-me}:
ONU-Generic-Assignments-Profile-name: ->  {znid-gpon-2510-omci-4port-gen}:
physical-traps: ----------------------->  {disabled}:
ont-traps: ---------------------------->  {disabled}:
line-status-traps: -------------------->  {disabled}:
auto-upgrade: ------------------------->  {enabled}:
serial-no-vendor-specific-fsan: ------->  {84200459}:  ** read-only **
use-reg-id: --------------------------->  {disabled}:
us-rx-power-monitoring-mode: ---------->  {monitorOnly}:
us-rx-power-high-threshold: ----------->  {-10}:
us-rx-power-low-threshold: ------------>  {-30}:
dba-status-reporting: ----------------->  {disabled}
.................
Save changes? [s]ave, [c]hange or [q]uit:q
```

Table 10: Received Power Threshold Attributes in gpon-olt-onu-config Profile

Attribute	Description
us-rx-power-monitoring-mode	Disable or enable the received power threshold alarm. Values: **disabled** This feature is disabled. **monitorOnly** Monitor ONU Receive Power Level. When ONU Receive Power Level crosses either the High or Low thresholds, trigger a local alarm, and send trap to ZMS. **blockOnError** Monitor ONU Receive Power Level. When ONU Receive Power Level crosses either the High or Low thresholds, trigger a local alarm, send trap to ZMS, disable ONT ranging and set ONT line status to DSA. Default: **monitorOnly**
us-rx-power-high-threshold	Upstream Receive Power High Threshold value, in the unit of dbm. Default: **-10**
us-rx-power-low-threshold	Upstream Receive Power Low Threshold value, in the unit of dbm. Default: **-30**

Procedure: *Configuring GPON High and Low Received Power Threshold Alarms*

1 View the ONU status. In this example, the upstream ONU received power under the OLT Rx Power column is -13.7 dBm, which is within the default value range of the GPON high and low received power threshold (-10 to -30).

```
zSH> onu status 1/1/2
                                                Download     OLT      ONT       Distance      Gpon
AutoConfig
ID          Onu          OperStatus     ConfigState       State    Rx Power  Rx Power      (KM)
OnuStatus         State
=== ================ ========= =============== ========= ======== ======== ==========
=============== ==========
  2          1-1-1-2 Up          Active       NoUpgrade   -13.7 dBm -15.4 dBm     0.0240 Active
Init
```

2 Configure the upstream ONU received power monitoring mode and thresholds as desired.

This example changes the low-threshold to -20 from the default value -30, and changes the monitoring mode to **blockonerror.** If the current OLT RX power has crossed the low threshold, a received power threshold alarm will be triggered, and the ONU will be disabled.

```
zSH> update gpon-olt-onu-config 1-1-1-2/gpononu
gpon-olt-onu-config  1-1-1-2/gpononu
Please provide the following: [q]uit.
serial-no-vendor-id: ------------------>  {ZNTS}:  ** read-only **
serial-no-vendor-specific: ------------>  {2216690777}:  ** read-only **
password: ----------------------------->  {}:
auto-learn: --------------------------->  {enabled}:
power-level: -------------------------->  {0}:
us-ber-interval: ---------------------->  {5000}:
```

```
ds-ber-interval: ---------------------->  {5000}:
onu-added: ---------------------------->  {true}:
omci-file-name: ----------------------->  {}:
ONU-Managed-Entity-Profile-name: ------>  {znid-gpon-2510-omci-4port-me}:
ONU-Generic-Assignments-Profile-name: ->  {znid-gpon-2510-omci-4port-gen}:
physical-traps: ----------------------->  {disabled}:
ont-traps: ---------------------------->  {disabled}:
line-status-traps: -------------------->  {disabled}:
auto-upgrade: ------------------------->  {enabled}:
serial-no-vendor-specific-fsan: ------->  {84200459}:  ** read-only **
use-reg-id: --------------------------->  {disabled}:
us-rx-power-monitoring-mode: ---------->  {monitorOnly}:blockonerror
us-rx-power-high-threshold: ----------->  {-10}:
us-rx-power-low-threshold: ------------>  {-30}:-20
dba-status-reporting: ----------------->  {disabled}
.....................
Save changes? [s]ave, [c]hange or [q]uit:s
```

3 View the ONU status.

This example shows GponOnuStatus is inactive and RXPWRDSA (i.e. received power out of range, and ONU is disabled.) Refer to the **alarm show** command for the explanation of the cryptic acronyms.

```
zSH> onu status 1/1/2
                          Omci       Gpon             Download    OLT       ONT       Distance
ID    Onu    OperStatus ConfigState OnuStatus          State     Rx Power Rx Power   (KM)
== ======== ========== =========== ================ ======== ======== ======== =======
2  1-1-1-2     Down     Inactive  Inactive+RXPWRDSA   None       error    error     0.0
```

4 View the alarms on this ONU at the system level.

Two alarms are raised, link down and Rx power threshold alarms.

```
zSH> alarm show
************    Central Alarm Manager    ************
        ActiveAlarmCurrentCount         :8
        AlarmTotalCount                 :32
        ClearAlarmTotalCount            :24
        OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-1-0/gponolt         linkDown                                  critical
1-1-2-0/gponolt         linkDown                                  critical
1-1-3-0/gponolt         linkDown                                  critical
1-1-4-0/gponolt         linkDown                                  critical
1-1-1-2/gpononu         linkDown                                           minor
1-1-1-2/gpononu         inactive,rx power out of range,dsa         minor
```

4- 6.1.5 Rogue ONU Detection and Rogue ONU Alarms

A rogue ONU is an ONU that transmits outside of its allocated bandwidth map. It can cause disruption to multiple subscribers or to all subscribers on a PON. DZS provides versatile ways to detect a rogue ONU that is present on

the PON and/or shut it down. That saves the other subscribers from experiencing any service issues.

To detect and/or shutdown a rogue ONU, use the following detection modes per OLT basis:

1. Periodical background process detection mode

   Periodical background process detection mode can detect certain cases of rogue ONUs, but will not disable rogue ONUs. If a rogue ONU has been detected on the OLT, an OLT-level alarm "**gpon_olt_rogue_onu_detected**" is raised.

   Refer to *Periodical Background Process Detection Mode* on page 80 for the details.

2. Rogue RSSI detection mode

   Rogue RSSI detection mode can detect and disable rogue ONUs by using the RSSI measurement on ONUs. If a rogue ONU has been detected on an OLT, an OLT-level alarm "**gpon_olt-rssi_rogue_onu_detected**" is raised. And then this rogue ONU will be identified, isolated, and disabled. An ONU-level alarm "**inactive, rogue ONU**" will be raised too.

   Refer to *Rogue RSSI Detection Mode* on page 83 for the details.

3. Auto rogue RSSI detection mode

   Auto rogue RSSI detection mode normally functions as disabled, it will be switched to the rogue RSSI detection mode only under certain circumstances.

   Refer to *Auto Rogue RSSI Detection Mode* on page 87 for the details.

   All three kinds of rogue ONU alarms have severity levels as minor.

Note: As a rule users only want to use either **disabled** or **autorssi** mode under normal conditions, although users might want to set either **roguerssi** or **backgroundprocess** if users suspect a rogue ONU for some reasons that is not detected or not isolated by **autorssi** mode.

Users can configure the ONU detection modes in the gpon-olt-config profile. This profile contains three rogue ONU detection related attributes:

```
zSH> show gpon-olt-config
max-rt-propagation-delay:----->   {0 - 0}
max-onu-response-time:-------->   {0 - 0}
preassigned-eqd:-------------->   {0 - 0}
los-alpha:-------------------->   {0 - 0}
lof-alpha:-------------------->   {0 - 0}
loam-alpha:------------------->   {0 - 0}
scrambler:-------------------->   enabled  disabled
fec-mode:--------------------->   enabled  disabled
auto-learn:------------------->   enabled  disabled
power-level:------------------>   {0 - 0}
guard-bit-count:-------------->   {0 - 0}
dba-mode:--------------------->   predictive  piggyback  wholereport
```

```
gem-block-size:--------------->   {0 - 0}
us-ber-interval:-------------->   {0 - 0}
ds-ber-interval:-------------->   {0 - 0}
ber-sf-threshold:------------->   {3 - 8}
ber-sd-threshold:------------->   {4 - 9}
fec-request:------------------>   enabled  disabled
key-exchange:----------------->   enabled  disabled
min-rt-propagation-delay:----->   {0 - 0}
min-onu-response-time:-------->   {0 - 0}
eqd-measure-cycles:----------->   {0 - 0}
drift-ctrl-interval:---------->   {0 - 0}
drift-ctrl-limit:------------->   {0 - 0}
alloc-cycle-length:----------->   {1 - 10}
min-us-alloc:----------------->   {0 - 0}
ack-timeout:------------------>   {0 - 0}
pls-max-alloc-size:----------->   {0 - 0}
dba-cycle:-------------------->   {2 - 10}
sr-dba-reporting-block-size:-->   {0 - 0}
protection-switchover-timer:-->   {0 - 0}
preamble-override:------------>   enabled  disabled
preamble-type-0:-------------->   {8}
preamble-type-1:-------------->   {8}
preamble-type-3-pre-range:---->   {8}
preamble-type-3-post-range:--->   {8}
preamble-type-3-pattern:------>   {8}
bip-error-monitoring-mode:---->   disabled  monitoronly  blockonerror
errors-per-sample-threshold:-->   {0 - 0}
errored-samples-threshold:---->   {0 - 0}
bip-max-sample-gap:----------->   {0 - 0}
rogue-onu-detection:---------->   disabled  roguerssi  backgroundprocess autorssi
rogue-onu-detect-frequency:--->   {1 - 60}
rogue-onu-rx-power-threshold:->   {0 - 0}
```

Table 11: rogue ONU Detection Attributes in gpon-olt-config Profile

Attribute	Description
rogue-onu-detection	Disable or enable the rogue ONU detection modes. Values: **disabled** Disable all the rogue ONU detection mode. **roguerssi** Enable rogue RSSI detection. When a rogue ONU RSSI measurement crosses the rogue-onu-rx-power-threshold, an attempt is made to isolate the rogue ONU. If successful, disable the rogue ONU. Trigger a local alarm and send a trap to ZMS. **backgroundprocess** Enable background process detection. When a rogue transmission is detected, trigger a local alarm and send a trap to ZMS. **autorssi** Enable auto RSSI detection. In this mode, it normally stays as disabled, it will switch to the rogue RSSI detection mode 1) if more than half the active ONUs go down within a brief interval, 2) or if BIP errors exceed threshold on any ONU. Note that the second case is a detect only measurement, no attempt to disable the rogue ONU will be automatically performed. Default: **disabled**
rogue-onu-detect-frequency	How often to run a detection after enabling the detection. Default: **10 seconds**

Table 11: rogue ONU Detection Attributes in gpon-olt-config Profile

Attribute	Description
rogue-onu-rx-power-threshold	Upstream Receive Power High Threshold value for detecting rogue ONU, in the unit of dbm. RSSI upstream received power is measured on an unused ONU, which should measure zero, if the measurement exceeds the threshold, an alarm is reported and isolation is attempted. This is ignored in background process mode. Default: **-30**

4- 6.1.5: 1 Periodical Background Process Detection Mode

Certain rogue behaviors can only be detected by running the periodical background process detection mode on an OLT. This mode can only be used to detect the condition, rather than disable it.

The periodical background process opens a special allocation window and monitors for potential rogue transmission. The special window is opened with an unused Alloc_ID, for which no response is expected unless there is a rogue ONU. The window is opened so that it may detect a transmission either within the PON distance or further.

When a rogue ONU transmission is detected in the special window, "**gpon_olt_rogue_onu_detected**" alarm is raised on the OLT port. It shows there is a rogue ONU has been detected on this OLT. The alarm severity level is minor.

Procedure: *Running the Periodical Background Process Detection and Viewing OLT-level Rogue ONU Alarms*

1 Set the rogue ONU detection mode to the periodical background process.

This example uses the default settings 10 seconds in the rogue-onu-detect-frequency field. After enabling the periodical background process, the process will run every 10 seconds.

```
zSH> update gpon-olt-config 1-1-1-0/gponolt
gpon-olt-config  1-1-1-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: -----> {200}:
max-onu-response-time: --------> {50}:
preassigned-eqd: --------------> {0}:
los-alpha: --------------------> {4}:
lof-alpha: --------------------> {4}:
loam-alpha: -------------------> {3}:
scrambler: --------------------> {enabled}:
fec-mode: ---------------------> {disabled}:
auto-learn: -------------------> {enabled}:
power-level: ------------------> {0}:
guard-bit-count: --------------> {32}:
dba-mode: ---------------------> {predictive}:
gem-block-size: ---------------> {16}:
us-ber-interval: --------------> {5000}:
ds-ber-interval: --------------> {5000}:
```

```
ber-sf-threshold: ------------->  {3}:
ber-sd-threshold: ------------->  {5}:
fec-request: ------------------>  {disabled}:
key-exchange: ----------------->  {disabled}:
min-rt-propagation-delay: ----->  {0}:
min-onu-response-time: -------->  {10}:
eqd-measure-cycles: ----------->  {5}:
drift-ctrl-interval: ---------->  {1000}:
drift-ctrl-limit: ------------->  {3}:
alloc-cycle-length: ----------->  {2}:
min-us-alloc: ----------------->  {16}:
ack-timeout: ------------------>  {2000}:
pls-max-alloc-size: ----------->  {120}:
dba-cycle: -------------------->  {2}:
sr-dba-reporting-block-size: -->  {48}:
protection-switchover-timer: -->  {500}:
preamble-override: ------------>  {disabled}:
preamble-type-0: -------------->  {0x00}:
preamble-type-1: -------------->  {0x00}:
preamble-type-3-pre-range: ---->  {0x0b}:
preamble-type-3-post-range: --->  {0x08}:
preamble-type-3-pattern: ------>  {0xaa}:
bip-error-monitoring-mode: ---->  {monitoronly}:
errors-per-sample-threshold: -->  {100}:
errored-samples-threshold: ---->  {10}:
bip-max-sample-gap: ----------->  {10}:
rogue-onu-detection: ---------->  {disabled}:backgroundprocess
rogue-onu-detect-frequency: --->  {10}:
rogue-onu-rx-power-threshold: ->  {-30}:
.....................

Save changes? [s]ave, [c]hange or [q]uit:s
```

2 If there are any rogue ONUs under this OLT port have been detected by running the periodical background process, the rogue ONU alarm will be raised on the OLT port.

Use the **alarm show** command to check the rogue ONU alarms:

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :8
       AlarmTotalCount                 :15
       ClearAlarmTotalCount            :7
       OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-1-0/gponolt         gpon_olt_rogue_onu_detected                     minor
...
```

Procedure: *Clearing OLT-level Rogue ONU Alarms*

To clear the OLT level rogue ONU alarm “gpon_olt_rogue_onu_detected”, ONTs must be manually disabled one by one until the condition is no longer detected, at which time the alarm will go away.

If the rogue ONU detection mode is switched back to normal states, the alarm will clear, but condition still stay.

Procedure: *Switching the Rogue ONU Detection Mode Back to Normal States from the Periodical Background Process Mode*

After finished the periodical background process, follow the rule to set the rogue ONU detection mode back to the normal states. Normal states could be disabled or auto RSSI mode.

```
zSH> update gpon-olt-config 1-1-1-0/gponolt
gpon-olt-config  1-1-1-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: -----> {200}:
max-onu-response-time: --------> {50}:
preassigned-eqd: --------------> {0}:
los-alpha: --------------------> {4}:
lof-alpha: --------------------> {4}:
loam-alpha: -------------------> {3}:
scrambler: --------------------> {enabled}:
fec-mode: ---------------------> {disabled}:
auto-learn: -------------------> {enabled}:
power-level: ------------------> {0}:
guard-bit-count: --------------> {32}:
dba-mode: ---------------------> {predictive}:
gem-block-size: ---------------> {16}:
us-ber-interval: --------------> {5000}:
ds-ber-interval: --------------> {5000}:
ber-sf-threshold: -------------> {3}:
ber-sd-threshold: -------------> {5}:
fec-request: ------------------> {disabled}:
key-exchange: -----------------> {disabled}:
min-rt-propagation-delay: -----> {0}:
min-onu-response-time: --------> {10}:
eqd-measure-cycles: -----------> {5}:
drift-ctrl-interval: ----------> {1000}:
drift-ctrl-limit: -------------> {3}:
alloc-cycle-length: -----------> {2}:
min-us-alloc: -----------------> {16}:
ack-timeout: ------------------> {2000}:
pls-max-alloc-size: -----------> {120}:
dba-cycle: --------------------> {2}:
sr-dba-reporting-block-size: --> {48}:
protection-switchover-timer: --> {500}:
preamble-override: ------------> {disabled}:
preamble-type-0: --------------> {0x00}:
preamble-type-1: --------------> {0x00}:
preamble-type-3-pre-range: ----> {0x0b}:
preamble-type-3-post-range: ---> {0x08}:
preamble-type-3-pattern: ------> {0xaa}:
bip-error-monitoring-mode: ----> {monitoronly}:
errors-per-sample-threshold: --> {100}:
errored-samples-threshold: ----> {10}:
bip-max-sample-gap: -----------> {10}:
rogue-onu-detection: ----------> {backgroundprocess}:disabled or autorssi
rogue-onu-detect-frequency: ---> {10}:
rogue-onu-rx-power-threshold: -> {-30}:
.....................
```

```
Save changes? [s]ave, [c]hange or [q]uit:s
```

4- 6.1.5: 2 Rogue RSSI Detection Mode

Caution: The rogue RSSI measurement is a semi-invasive mode. During the activation of the RSSI measurement on an OLT port it is not allowed to provision Alloc_IDs or to activate ONUs under that OLT port.

The rogue RSSI detection not only can detect the rogue ONU, and also can disable it. Note that after the rogue ONU had been disabled, this disabled ONU must be cleared and physically removed.

If the periodical background process detection cannot find the rogue ONU, users can run the rogue RSSI detection.

If users want to provision Alloc_IDs (by creating bridges/interfaces on ONU Gemports), and activate ONUs (by assigning serial numbers to ONUs ports), users must change the rogue-onu-detection mode from rogue RSSI to auto RSSI mode or disabled, after clearing any disabled ONUs.

A rogue RSSI detection performs the following two parts:

1. **1st part**: Detect rogue ONUs and get OLT-level alarms

   The rogue RSSI detection uses the rogue RSSI measurement to identify a rogue ONU by measuring transmission power on an unused ONU.

   The RSSI measurement is a stand-alone utility for testing rogue transmission when no upstream burst is expected. The intention is to identify when a rogue ONU injects a constant energy on the link, and does not respond to OLT allocations.

   If the rogue ONU RSSI measurement is higher than the rogue-onu-rx-power-threshold defined in the **gpon-olt-config** profile, an OLT-level alarm **"gpon_olt_rssi_rogue_onu_detected**" and trap will be sent. This rogue ONU alarm shows there is a rogue ONU has been detected with the RSSI measurement on the OLT.

2. **2nd part**: Isolate and shutdown rogue ONUs, and get ONU-level alarms

   Once the rogue RSSI detection is determined that a rogue ONU does exist on an OLT, it will start the process to determine which one is the rogue ONU and disable it. The process disables ONTs one at a time, each time it will perform a rogue RSSI measurement, until get a good reading, at which time it declare the last ONU disabled as rogue, and enable all the other "good" ONUs. An ONU error will be raised on the isolated ONU, and this ONU shows as disabled in the showline.

   When this rogue ONU is disabled, an ONU-level alarm "**inactive, rogue onu**" and trap will be sent.

Note that the **2nd part** may fail, in which case the OLT-level alarm continues to be displayed. Reasons for failing to isolate rogue ONUs could be:

- Certain models of ONT do not disable transmission

- If a rogue ONU is connected with OLT on the fiber but not activated (by associating an ONU port ID with its serial number with the **onu set** command), it will not be isolated
- If the ONT is too “bad” to respond to a disable request.

Procedure: *Running the RSSI Rogue ONT Detection and Viewing OLT-Level and ONU-Level RSSI Rogue Alarms*

1 To enable the RSSI rogue ONT detection mode, change the rogue-onu-detection field of the gpon-olt-config profile to **roguerssi**.

This example uses the default values set in the rogue-onu-detect-frequency field and rogue-onu-rx-power-threshold field. That means the RSSI rogue ONT detection will run every 10 seconds, and if the RSSI measurement exceeds -30 dbm, an alarm is reported and isolation is attempted.

```
zSH> update gpon-olt-config 1-1-4-0/gponolt
gpon-olt-config  1-1-4-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: -----> {200}:
max-onu-response-time: --------> {50}:
preassigned-eqd: --------------> {0}:
los-alpha: --------------------> {4}:
lof-alpha: --------------------> {4}:
loam-alpha: -------------------> {3}:
scrambler: --------------------> {enabled}:
fec-mode: ---------------------> {disabled}:
auto-learn: -------------------> {enabled}:
power-level: ------------------> {0}:
guard-bit-count: --------------> {32}:
dba-mode: ---------------------> {predictive}:
gem-block-size: ---------------> {16}:
us-ber-interval: --------------> {5000}:
ds-ber-interval: --------------> {5000}:
ber-sf-threshold: -------------> {3}:
ber-sd-threshold: -------------> {5}:
fec-request: ------------------> {disabled}:
key-exchange: -----------------> {disabled}:
min-rt-propagation-delay: -----> {0}:
min-onu-response-time: --------> {10}:
eqd-measure-cycles: -----------> {5}:
drift-ctrl-interval: ----------> {1000}:
drift-ctrl-limit: -------------> {3}:
alloc-cycle-length: -----------> {2}:
min-us-alloc: -----------------> {16}:
ack-timeout: ------------------> {2000}:
pls-max-alloc-size: -----------> {120}:
dba-cycle: --------------------> {2}:
sr-dba-reporting-block-size: --> {48}:
protection-switchover-timer: --> {500}:
preamble-override: ------------> {disabled}:
preamble-type-0: --------------> {0x00}:
preamble-type-1: --------------> {0x00}:
preamble-type-3-pre-range: ----> {0x0b}:
preamble-type-3-post-range: ---> {0x08}:
```

```
preamble-type-3-pattern: ------>  {0xaa}:
bip-error-monitoring-mode: ---->  {monitoronly}:
errors-per-sample-threshold: -->  {100}:
errored-samples-threshold: ---->  {10}:
bip-max-sample-gap: ----------->  {10}:
rogue-onu-detection: ---------->  {disabled}:roguerssi
rogue-onu-detect-frequency: --->  {10}:
rogue-onu-rx-power-threshold: ->  {-30}:
.....................

Save changes? [s]ave, [c]hange or [q]uit:s
```

2 If a rogue ONU is detected, users will see a rogue ONU alarm on the OLT port.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :8
       AlarmTotalCount                 :15
       ClearAlarmTotalCount            :7
       OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-4-0/gponolt         gpon_olt_rssi_rogue_onu_detected                 minor
...
```

3 If a rogue ONU is isolated and disabled, users will see a rogue ONU alarm on the ONU port. This alarm will clear the OLT-level alarm listed in the previous step, unless there are more rogue ONUs under this OLT port, or failed to isolate and shutdown the detected rogue ONUs.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :8
       AlarmTotalCount                 :15
       ClearAlarmTotalCount            :7
       OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-4-1/gpononu         inactive,rogue onu                               minor
...
```

Procedure:

Clearing OLT-Level and ONU-Level RSSI Rogue Alarms

To clear the ONU level RSSI rogue alarm “inactive, rogue onu”, the ONT must be physically removed from the network before using the **gpononu clear** command.

To clear the OLT-level RSSI rogue alarms, “gpon_olt_rssi_rogue_onu_detected”, use the same method shown in Clearing OLT-level Rogue ONU Alarms, page 81.

Note that alarms can be cleared by changing detect mode or threshold, but this will not clear the condition.

Procedure: *Switching the Rogue ONT Detection Back to Normal States from the Rogue RSSI Mode*

After users detected a rogue ONU on an OLT by running the rogue RSSI detection mode, the OLT port is in a restricted mode keeps users from activating any ONUs connected to it. To go back to the normal states, perform the following steps:

1. Physically unplug the rogue ONU.
2. Clear the rogue ONU. This step will clear the onu-level “inactive, rogue onu” alarm too.

```
zSH> gpononu clear 1/4/1
```

3. Set the rogue ONU detection mode back to the normal states (disabled or auto RSSI mode).

```
zSH> update gpon-olt-config 1-1-4-0/gponolt
gpon-olt-config  1-1-4-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: -----> {200}:
max-onu-response-time: --------> {50}:
preassigned-eqd: --------------> {0}:
los-alpha: --------------------> {4}:
lof-alpha: --------------------> {4}:
loam-alpha: -------------------> {3}:
scrambler: --------------------> {enabled}:
fec-mode: ---------------------> {disabled}:
auto-learn: -------------------> {enabled}:
power-level: ------------------> {0}:
guard-bit-count: --------------> {32}:
dba-mode: ---------------------> {predictive}:
gem-block-size: ---------------> {16}:
us-ber-interval: --------------> {5000}:
ds-ber-interval: --------------> {5000}:
ber-sf-threshold: -------------> {3}:
ber-sd-threshold: -------------> {5}:
fec-request: ------------------> {disabled}:
key-exchange: -----------------> {disabled}:
min-rt-propagation-delay: -----> {0}:
min-onu-response-time: --------> {10}:
eqd-measure-cycles: -----------> {5}:
drift-ctrl-interval: ----------> {1000}:
drift-ctrl-limit: -------------> {3}:
alloc-cycle-length: -----------> {2}:
min-us-alloc: -----------------> {16}:
ack-timeout: ------------------> {2000}:
pls-max-alloc-size: -----------> {120}:
dba-cycle: --------------------> {2}:
sr-dba-reporting-block-size: --> {48}:
protection-switchover-timer: --> {500}:
preamble-override: ------------> {disabled}:
preamble-type-0: --------------> {0x00}:
preamble-type-1: --------------> {0x00}:
preamble-type-3-pre-range: ----> {0x0b}:
preamble-type-3-post-range: ---> {0x08}:
preamble-type-3-pattern: ------> {0xaa}:
```

```
bip-error-monitoring-mode: ----> {monitoronly}:
errors-per-sample-threshold: --> {100}:
errored-samples-threshold: ----> {10}:
bip-max-sample-gap: -----------> {10}:
rogue-onu-detection: ----------> {roguerssi}:disabled or autorssi
rogue-onu-detect-frequency: ---> {10}:
rogue-onu-rx-power-threshold: -> {-30}:
.....................

Save changes? [s]ave, [c]hange or [q]uit:s
```

4- 6.1.5: 3 Auto Rogue RSSI Detection Mode

The auto rogue ONU RSSI detection mode normally functions as disabled, it will be switched to the rogue RSSI detection mode only if one of the following two cases happened:

1. Case 1: If more than half the active ONUs on the OLT go down within a brief interval (currently 1 minute), then the disabled mode will be switched to the rogue RSSI detection mode for one measurement cycle.

   In case 1, there are three possible outcomes:

   No.1 The process did not detect presence of a rogue ONU. Then the detection mode will be switched back to the disabled mode, with a "no rogue ONU was detected" message shown on the console.

   No.2 A rogue ONU was detected and isolated. In this case, the rogue RSSI mode is retained, so that the ONU stays disabled until it is cleared, or until the rogue detection mode is changed.

   An ONU-level alarm "**inactive, rogue onu**" and trap will be sent.

   No.3 Presence of rogue ONU is detected, but unable to isolate the ONU. In this case, the detection mode will be switched back to disabled.

   An OLT-level alarm **"gpon_olt_rssi_rogue_onu_detected**" and trap will be sent.

2. Case 2: If BIP errors exceed threshold on any ONU, the disabled mode will be switched to rogue RSSI detection mode. But in this case, it is a "detect only" measurement. No attempt at isolation will be automatically performed, only **No.1** and **No.3** of the above outcomes are possible.

Procedure: *Running the Auto RSSI Rogue ONT Detection and Viewing RSSI Rogue ONU Alarm on an ONU*

1 To enable the auto RSSI rogue ONT detection mode, change the rogue-onu-detection field of the gpon-olt-config profile to **autorssi**.

```
zSH> update gpon-olt-config 1-1-4-0/gponolt
gpon-olt-config  1-1-4-0/gponolt
Please provide the following: [q]uit.
max-rt-propagation-delay: -----> {200}:
max-onu-response-time: --------> {50}:
preassigned-eqd: --------------> {0}:
los-alpha: --------------------> {4}:
```

```
lof-alpha: ---------------------> {4}:
loam-alpha: --------------------> {3}:
scrambler: ---------------------> {enabled}:
fec-mode: ----------------------> {disabled}:
auto-learn: --------------------> {enabled}:
power-level: -------------------> {0}:
guard-bit-count: ---------------> {32}:
dba-mode: ----------------------> {predictive}:
gem-block-size: ----------------> {16}:
us-ber-interval: ---------------> {5000}:
ds-ber-interval: ---------------> {5000}:
ber-sf-threshold: --------------> {3}:
ber-sd-threshold: --------------> {5}:
fec-request: -------------------> {disabled}:
key-exchange: ------------------> {disabled}:
min-rt-propagation-delay: -----> {0}:
min-onu-response-time: --------> {10}:
eqd-measure-cycles: ------------> {5}:
drift-ctrl-interval: -----------> {1000}:
drift-ctrl-limit: --------------> {3}:
alloc-cycle-length: ------------> {2}:
min-us-alloc: ------------------> {16}:
ack-timeout: -------------------> {2000}:
pls-max-alloc-size: ------------> {120}:
dba-cycle: ---------------------> {2}:
sr-dba-reporting-block-size: --> {48}:
protection-switchover-timer: --> {500}:
preamble-override: -------------> {disabled}:
preamble-type-0: ---------------> {0x00}:
preamble-type-1: ---------------> {0x00}:
preamble-type-3-pre-range: ----> {0x0b}:
preamble-type-3-post-range: ---> {0x08}:
preamble-type-3-pattern: ------> {0xaa}:
bip-error-monitoring-mode: ----> {monitoronly}:
errors-per-sample-threshold: --> {100}:
errored-samples-threshold: ----> {10}:
bip-max-sample-gap: ------------> {10}:
rogue-onu-detection: ----------> {disabled}:autorssi
rogue-onu-rx-power-threshold: -> {-30}:
.....................

Save changes? [s]ave, [c]hange or [q]uit:s
```

2 If a rogue ONU is detected, users will see a rogue ONU alarm on the OLT port.

```
zSH> alarm show
************    Central Alarm Manager    ************
        ActiveAlarmCurrentCount         :8
        AlarmTotalCount                 :15
        ClearAlarmTotalCount            :7
        OverflowAlarmTableCount         :0
ResourceId              AlarmType                                AlarmSeverity
----------              ---------                                -------------
1-a-3-0/eth             linkDown                                    critical
1-1-4-0/gponolt         gpon_olt_rssi_rogue_onu_detected              minor
...
```

3 If a rogue ONU is isolated and disabled, users will see a rogue ONU alarm on the ONU port. This alarm will clear the OLT-level alarm listed in the previous step, unless there are more rogue ONUs under this OLT port, or failed to isolate and shutdown the detected rogue ONUs.

```
zSH> alarm show
************    Central Alarm Manager    ************
       ActiveAlarmCurrentCount         :8
       AlarmTotalCount                 :15
       ClearAlarmTotalCount            :7
       OverflowAlarmTableCount         :0
ResourceId              AlarmType                              AlarmSeverity
----------              ---------                              -------------
1-a-3-0/eth             linkDown                                  critical
1-1-4-1/gpononu         inactive,rogue onu                             minor
...
```

4- 6.1.6 ONU Dying Gasp Alarms

When an ONU is power down, and the line-status-traps field in the gpon-olt-onu-config profile has been set to enabled or auto, then the lineStatusChange trap will be sent and the Dying Gasp Alarm will be raised.

Dying gasp alarm provides ONU information to the service provider when this ONU is about to power down. The dying gasp event is followed by an ONU down event.

If there is a link down alarm prior to receiving the dying gasp alarm, link down alarm will be cleared and dying gasp alarm will be created.

Procedure: *Viewing ONU Dying Gasp Alarm on an ONU*

1 To enable the ONU dying gasp alarm, change the line-status-traps field of the gpon-olt-onu-config profile to **auto or enabled**.

This example sets enabled for line-status-traps field:

```
zSH> update gpon-olt-onu-config line-status-traps=enabled 1-7-1-1/gpononu
gpon-olt-onu-config  1-7-1-1/gpononu
Record updated.
```

2 Create trap-destination profile to define a trap recipient the MXK-F will send traps to.

```
zSH> new trap-destination 1
trap-destination  1
Please provide the following: [q]uit.
trapdestination: -------> {0.0.0.0}: 172.16.80.39      the IP address of the SNMP trap server
communityname: ---------> {}:
resendseqno: -----------> {0}:
ackedseqno: ------------> {0}:
traplevel: -------------> {low}:
traptype: --------------> {0}:
trapadminstatus: -------> {enabled}:
gatewaytrapserveraddr: -> {none}:
...................
Save new record? [s]ave, [c]hange or [q]uit: s
```

```
New record saved.
```

3 Power down this ONU.

4 User will see Dying Gasp in the alarm or trap description:

a Send lineStatusChange trap with trap value as inactive | dyinggasp.

You can check the trap values in the trap recipient console in MIB browser.

b Raise alarm string as Dying Gasp received.

```
OCT 23 11:46:13: alert  : 1/7/1025: alarm_mgr: _laMgrLogMsg(): l=295 : tLineAlarm: 01: 7:01:01 Minor ONU
Down
Line 1/7/1/1/gpononu CAUSE: Dying Gasp received
```

c Get the onuStatus as Inactive+DG:

```
zSH> onu status 7/1/1
                                    Download    OLT   ONT    Distance Gpon                      AutoConfig
ID     Onu    OperStatus ConfigState State     Rx Pwr Rx Pwr  (KM)     OnuStatus                 State
=== ======= ========= ========= ======== ===== ====== ======= ======================== ======
 1  1-7-1-1 Down      Inactive   None    error  error   error  Inactive+DG            Init
```

4- 6.1.7 ONU Manual Reboot Alarms

When an ONU is rebooted manually from ZMS or MXK, and the line-status-traps in the gpon-olt-onu-config profile has been set to enabled or auto, then the lineStatusChange trap will be sent and the ONU manual reboot alarm will be raised.R

Procedure: *Viewing ONU Manual Rebooted Alarm on an ONU*

1 To enable the ONU manual rebooted alarm, change the line-status-traps field of the gpon-olt-onu-config profile to **auto or enabled**.

This example sets enabled for line-status-traps field:

```
zSH> update gpon-olt-onu-config line-status-traps=enabled 1-7-1-1/gpononu
gpon-olt-onu-config  1-7-1-1/gpononu
Record updated.
```

2 Create trap-destination profile to define a trap recipient the MXK-F will send traps to.

```
zSH> new trap-destination 1
trap-destination  1
Please provide the following: [q]uit.
trapdestination: -------> {0.0.0.0}: 172.16.80.39      the IP address of the SNMP trap server
communityname: ---------> {}:
resendseqno: -----------> {0}:
ackedseqno: ------------> {0}:
traplevel: -------------> {low}:
traptype: --------------> {0}:
trapadminstatus: -------> {enabled}:
gatewaytrapserveraddr: -> {none}:
.....................
```

```
Save new record? [s]ave, [c]hange or [q]uit: s
New record saved.
```

3 Reboot this ONU:

```
zSH> onu reboot 7/1/1
```

4 User will see ONU reboot in the alarm or trap description:

a Send lineStatusChange trap with trap value as inactive | onu rebooted. You can check the trap values in the trap recipient console in MIB browser.

b Raise alarm string as onu rebooted.

```
OCT 23 09:52:32: alert  : 1/7/1025: alarm_mgr: _laMgrLogMsg(): l=295 : tLineAlarm: 01: 7:01:01 Minor ONU
Down
Line 1/7/1/1/gpononu CAUSE: ONU rebooted
```

c Get the onuStatus as Inactive+onuRebooted:

```
zSH> onu status 7/1/1
                                    Download    OLT   ONT    Distance Gpon                      AutoConfig
ID     Onu    OperStatus ConfigState State     Rx Pwr Rx Pwr  (KM)     OnuStatus                 State
=== ======= ========== =========== ======== ===== ====== ======= ======================== ======
 1  1-7-1-1  Down     Inactive   None    error  error  error   Inactive+onuRebooted    Init
```

4- 6.2 GPON Traps

- View or Change Trap Reporting Status on an ONU, page 91
- Change Alarm Severity for LineStatusTraps, page 92

4- 6.2.1 View or Change Trap Reporting Status on an ONU

The conditions that cause asynchronous reporting traps can be controlled from the OLT through SNMP. The purpose of these controls is to reduce trap traffic between the MXK and ZMS to allow more information about critical or failing ONUs.

These three trap types are reported on an ONU:

- phy (PhysicalTraps): Includes the power status, battery status, and physical intrusion conditions as reported from the ONU through OMCI.

  The options for the PhysicalTraps are:

  – enable: The PhysicalTraps are sent.

  – disable: The PhysicalTraps are not sent. Default value.

- ont (OntTraps): The status of LAN facing ports on the ONU (e.g. ethernet port LanLos).

  The options for the OntTraps are:

  – enable: The OntTraps are sent.

  - disable: The OntTraps are not sent. Default value.

- line (LineStatusTraps): It is originated on the MXK, and reports the ONU line going up or down.

  The options for the LineStatusTraps are:

  - enable: The linkUp, linkDown, and lineStatusChange traps are sent.
  - disable: The lineStatusTraps are not sent. Default value.
  - auto: In this setting, the linkUp or linkDown traps are not sent, only the lineStatusChange trap is sent if the line is going down with dying gasp (presumably powered down), if there is a manual ONU reboot; or if the line is coming up.
  - linkonly: Sends traps to set and clear ONU linkDown alarm only. Dying Gasp alarm is suppressed in this mode.

View the current reporting status of traps on ONU(s) with the **gpononu traps show** [*slot*[/*olt*[/*onu*]]command.

```
zSH> gpononu traps show 1/4/2
Slot 1 olt 4
ONU       Name         PhysicalTraps   OntTraps    LineStatusTraps
=== ================ ============   ========   ==============
  2          1-1-4-2     enabled      disabled         auto
```

Change the current reporting status of traps on ONU 1/4/2 with the **gpononu traps enable|disable|auto|linkonly** *slot/olt/onu* **phy|ont|line** command.

Note that only LineStatusTraps (i.e. line) has auto and linkonly options.

```
zSH> gpononu traps disable 1/4/2 phy
zSH> gpononu traps linkonly 1/4/2 line
```

Verify the settings in the show command:

```
zSH> gpononu traps show 1/4/2
Slot 1 olt 4
ONU       Name         PhysicalTraps   OntTraps    LineStatusTraps
=== ================ ============   ========   ==============
  2          1-1-4-2     disabled      disabled         linkonly
```

4- 6.2.2 Change Alarm Severity for LineStatusTraps

Users can change the alarm severity for an ONT when the LineStatusTraps are sent. The LineStatusTraps includes linkUp, linkDown, and lineStatusChange traps.

To change the alarm severity of LineStatusTraps, use the “link-status-alarm-severity” field in the **gpon-olt-onu-confg** profile. By default, the alarm severity is minor, it could be changed to major or critical.

The following example sets **LineStatusTraps** to *auto*, and sets the alarm severity level of **LineStatusTraps** to *major*:

```
zSH> update gpon-olt-onu-config 1-1-1-1
gpon-olt-onu-config  1-1-1-1/gpononu
```

```
Please provide the following: [q]uit.
serial-no-vendor-id: ------------------>  {ZNTS}:  ** read-only **
serial-no-vendor-specific: ------------>  {51974624}:  ** read-only **
password: ----------------------------->  {}:
auto-learn: --------------------------->  {enabled}:
power-level: -------------------------->  {0}:
us-ber-interval: ---------------------->  {5000}:
ds-ber-interval: ---------------------->  {5000}:
onu-added: ---------------------------->  {true}:
omci-file-name: ----------------------->  {}:
ONU-Managed-Entity-Profile-name: ------>  {zhone-2425}:
ONU-Generic-Assignments-Profile-name: ->  {}:
physical-traps: ----------------------->  {disabled}:
ont-traps: ---------------------------->  {disabled}:
line-status-traps: -------------------->  {disabled}: auto
auto-upgrade: ------------------------->  {enabled}:
serial-no-vendor-specific-fsan: ------->  {031911E0}:  ** read-only **
use-reg-id: --------------------------->  {disabled}:
us-rx-power-monitoring-mode: ---------->  {monitoronly}:
us-rx-power-high-threshold: ----------->  {-10}:
us-rx-power-low-threshold: ------------>  {-30}:
dba-status-reporting: ----------------->  {disabled}:
auto-config-state: -------------------->  {init}:  ** read-only **
link-status-alarm-severity: ----------->  {minor}: major
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
```

4- 7 BRIDGE RELATED

4- 7.1 Bridge Loop Prevention

This section covers:

4- 7.1.1 Bridge Loop Prevention Overview

This section covers:

Bridge loop prevention can be configured on either asymmetrical or TLS bridges to resolve certain incorrect MAC address behaviors.

4- 7.1.1: 1 Bridge Loop Prevention on Asymmetrical Bridges

Bridge loop prevention can be configured on the bridge path of the bridge interface when a MAC address on asymmetrical bridges is seen as coming in on both the uplink and the downlink.

When bridge loop behavior occurs and *block blockAsym* is configured on the uplink bridge interface with VLAN ID the system blocks the downlink after detecting this incorrect MAC address behavior.

After the blocked bridge receives an offending MAC address, the system sends a MAJOR alarm that indicates a bridge was blocked to prevent a loop. This alarm displays the bridge interface and the offending MAC address.

In this case, the blocked bridge interface must be unblocked with the **bridge unblock** *interface/type* command.

When bridge loop behavior occurs and *block blockAsymAuto* is configured on the uplink bridge interface with VLAN ID, the system initiates a series of three cyclic monitoring checks to see if the bridge loop condition is resolved. If the bridge loop condition is resolved, the bridge interface is automatically unblocked and a bridge loop clear alarm is sent.

If the condition is not resolved, the MAJOR alarm is cleared and a CRITICAL alarm is sent. In this case, the blocked bridge interface must be unblocked with the **bridge unblock** *interface/type* command.

4- 7.1.1: 2 Bridge Loop Prevention on TLS Bridges

Bridge loop prevention can be configured on the bridge path of a TLS bridge when a MAC address is seen as coming in on one TLS bridge and then as coming in on another TLS bridge.

When configuring the TLS network facing bridge, the bridge type *tls-gw must* be used. That way, when this behavior occurs, the network facing TLS bridge remains up and passing traffic. The subscriber facing bridge will be the one to be blocked.

When this behavior occurs and *block blockall* is configured on the VLAN ID of the TLS bridges, the system blocks the subscriber facing TLS bridge and then sends a MAJOR alarm describing that a second TLS bridge that saw the MAC address. The subscriber facing bridge is then blocked to prevent a loop.

When this occurs, the blocked bridge interface must be unblocked with the **bridge unblock** *interface/type* command.

When bridge loop behavior occurs and *block blockAsymAuto* is configured on the TLS bridge interface with VLAN ID, the system initiates a series of three cyclic monitoring checks to see if the bridge loop condition is resolved. If the bridge loop condition is resolved, the bridge interface is automatically unblocked and a bridge loop clear alarm is sent.

If the condition is not resolved, the MAJOR alarm is cleared and a CRITICAL alarm is sent. In this case, the blocked bridge interface must be unblocked with the **bridge unblock** *interface/type* command.

4- 7.1.2 Configure Bridge Loop Prevention

Procedure: *Configuring bridge loop prevention on asymmetric bridges with blockAsym*

1 Create the asymmetrical bridging configuration.

Create an uplink bridge.

```
zSH> bridge add 1-a-4-0/eth uplink vlan 100
Adding bridge on 1-a-4-0/eth
Created bridge-interface-record ethernet4-100/bridge
Bridge-path added successfully
```

2 Modify the bridge path to enable asymmetrical bridge blocking using **bridge-path modify** *interface/type vlan default block blockasym*.

```
zSH> bridge-path modify ethernet4-100/bridge vlan 100 default block blockAsym
Bridge-path ethernet4-100/bridge/3/100/0/0/0/0/0/0/0 has been modified
```

Note: Enter exactly the same command syntax to enable blocking on an existing bridge path. The existing bridge path will be overwritten, and blocking will be enabled.

View the bridge path.

```
zSH> bridge-path show
VLAN/SLAN   Bridge                          Address
-------------------------------------------------------------------------------
       100 ethernet4-100/bridge             Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
                                            IGMP DSCP: 0, Flap Mode: Default, Block: Asym
```

3 Create a downlink bridge.

```
zSH> bridge add 1-6-1-501/gponport gtp 1 downlink-data vlan 100 tagged
Adding bridge on 1-6-1-501/gponport
Created bridge-interface-record 1-6-1-501-gponport-100/bridge
```

View the bridges.

```
zSH> bridge show
        Orig
Type    VLAN/SLAN  VLAN/SLAN   Physical         Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------
dwn-dat           Tagged 100   1/6/1/1/gpononu  1-6-1-501-gponport-100/bridge  DWN
upl               Tagged 100   1/a/4/0/eth      ethernet4-100/bridge           DWN S VLAN 100 default
2 Bridge Interfaces displayed
```

Procedure: *Configuring Bridge Loop Prevention on Asymmetric Bridges with blockAsymAuto*

1 Create the asymmetrical bridging configuration.

Create an uplink bridge.

```
zSH> bridge add 1-a-2-0/eth uplink vlan 200 tagged
Adding bridge on 1-a-2-0/eth
Created bridge-interface-record ethernet2-200/bridge
```

```
Bridge-path added successfully
```

2 Modify the bridge path to enable asymmetrical bridge auto unblocking using **bridge-path modify** *interface/type vlan default block blockAsymAuto*.

```
zSH> bridge-path modify ethernet2-200/bridge vlan 200 default block blockAsymAuto
Bridge-path ethernet2-200/bridge/3/200/0/0/0/0/0/0/0 has been modified
```

View the bridge bath:

```
zSH> bridge-path show
VLAN/SLAN  Bridge                 Address
-------------------------------------------------------------------------------------------------------
       200 ethernet2-200/bridge   Default, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
                                  IGMP DSCP: 0, Flap Mode: Default, Block: Asym/Auto
```

3 Create a downlink bridge on the same VLAN ID.

```
zSH> bridge add 1-1-6-0/eth downlink-data vlan 200 tagged
Adding bridge on 1-1-6-0/eth
Created bridge-interface-record 1-1-6-0-eth-200/bridge
```

4 View the bridges:

```
zSH> bridge show
        Orig
Type    VLAN/SLAN  VLAN/SLAN  Physical        Bridge                        St  Table Data
-------------------------------------------------------------------------------------------------------
dwn-dat           Tagged 200  1/1/6/0/eth     1-1-6-0-eth-200/bridge        DWN
upl               Tagged 200  1/a/2/0/eth     ethernet2-200/bridge          UP  S VLAN 200 default
2 Bridge Interfaces displayed
```

Procedure: *Configuring Bridge Loop Prevention on TLS Bridges with blockAll*

1 Create the network facing TLS bridge with the bridge type *tls-gw*.

```
zSH> bridge add 1-a-4-0/eth tls-gw vlan 999
Adding bridge on 1-a-4-0/eth
Created bridge-interface-record ethernet4/bridge
Bridge-path added successfully
```

2 Modify the bridge path on the VLAN ID to enable TLS bridge blocking using **bridge-path modify** *interface/type vlan <vlanid> block blockasym*.

```
zSH> bridge-path modify vlan 999 block blockAll
Bridge-path /14/999/0/0/0/0/0/0/0 has been modified
```

3 View the bridge-path.

```
zSH> bridge-path show
VLAN/SLAN  Bridge                 Address
-------------------------------------------------------------------------------------------------------
       999 N/A                    VLAN, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
                                  IGMP DSCP: 0, Flap Mode: Fast, Block: All
```

4 Create the subscriber facing TLS bridges.

```
zSH> bridge add 1-6-12-0/eth tls vlan 999
Adding bridge on 1-6-12-0/eth
Created bridge-interface-record 1-6-12-0-eth/bridge

zSH> bridge add 1-6-13-0/eth tls vlan 999
Adding bridge on 1-6-13-0/eth
Created bridge-interface-record 1-6-13-0-eth/bridge
```

Procedure: *Configuring Bridge Loop Prevention on TLS Bridges with blockAllAuto*

1 Create the network facing TLS bridge with the *tls-gw* bridge type.

The network facing TLS bridge must be configured with the tls-gw bridge type.

```
zSH> bridge add 1-a-3-0/eth tls-gw vlan 700
Adding bridge on 1-a-3-0/eth
Created bridge-interface-record ethernet3/bridge
Bridge-path added successfully
```

2 Modify the bridge path on the VLAN ID to enable TLS bridge blocking using **bridge-path modify** *interface/type vlan <vlanid> block blockasym*.

```
zSH> bridge-path modify vlan 700 block blockAllAuto
Bridge-path /14/700/0/0/0/0/0/0/0 has been modified
```

3 View the bridge-path.

```
zSH> bridge-path show
VLAN/SLAN  Bridge                Address
-------------------------------------------------------------------------------------------------
       700 N/A                   VLAN, Age: 3600, MCAST Age: 250, IGMP Query Interval: 0,
                                 IGMP DSCP: 0, Flap Mode: Fast, Block: All/Auto
```

4 Create the subscriber facing TLS bridges.

```
zSH> bridge add 1-6-1-0/eth tls vlan 700
Adding bridge on 1-6-1-0/eth
Created bridge-interface-record 1-6-1-0-eth/bridge

zSH> bridge add 1-6-2-0/eth tls vlan 700
Adding bridge on 1-6-2-0/eth
Created bridge-interface-record 1-6-2-0-eth/bridge
```

4- 7.1.3 View Bridge Loop Detection Alarms

Procedure: *Viewing Loop Detected Alarms*

1 On the console, the following alarm appears when a loop is detected.

```
zSH> JUN 22 02:12:40: alert : 1/a/1093: bridge: BridgeTrapSend(): l=1223: tBridgeMain: Bridge Loop
detected on 1-10-1-501-gponport-100:(0/100/00:15:C5:3A:A3:B8) .
```

2 Enter **alarm show** to display the loop detection alarm at the system level.

```
zSH> alarm show
```

```
************ Central Alarm Manager ************
        ActiveAlarmCurrentCount :13
        AlarmTotalCount :16
        ClearAlarmTotalCount :3
        OverflowAlarmTableCount :0
ResourceId AlarmType AlarmSeverity
---------- --------- -------------
1-a-2-0/eth linkDown critical
1-a-3-0/eth linkDown critical
1-a-6-0/eth linkDown critical
1-a-7-0/eth linkDown critical
1-a-8-0/eth linkDown critical
1-a-9-0/eth linkDown critical
1-a-10-0/eth linkDown critical
1-a-11-0/eth linkDown critical
1-10-2-0/gponolt linkDown critical
1-10-3-0/gponolt linkDown critical
1-10-4-0/gponolt linkDown critical
system not_in_redundant_mode major
1-10-1-501-gponport-100 bridgeLoopDetect 0/100/00:15:C5:3A:A3:B8 major
```

4- 7.1.4 View Bridge Loop Prevention on a Bridge Interface

All bridges that are blocked by bridge loop protection, RSTP, or EAPS are displayed with the **bridge show blk** command.

Note: The **bridge show blk** command displays bridges that are normally blocked in EAPS or RSTP configurations.

Bridges configured with the *block blockassym* variable for bridge loop prevention will display the MAC address as well as the bridge interface name. Bridges blocked as a normal part of RSTP or EAPS configurations do not display MAC addresses and should remain blocked. Do not unblock the RSTP and EAPS interfaces.

Procedure:

Finding Bridges That Were Blocked By Bridge Loop Protection

Enter the **bridge show blk** command to view blocked bridges.

This example confirms that there are no existing blocked bridges.

```
zSH> bridge show blk
No Bridge Interfaces found.
```

This example confirms that a blocked bridge exists.

A bridge loop alarm appears in the console window.

```
zSH> AUG 05 19:38:38: alert  : 1/b/1062: bridge: BridgeTrapSend():
l=1233: tBridgeMain: Bridge Loop detected on
1-9-4-0-eth-100:(0/100/00:00:00:00:00:04) .
AUG 05 19:38:42: alert  : 1/a/1093: bridge: BridgeTrapSend(): l=1233:
tBridgeMain: Bridge Loop detected on
1-9-4-0-eth-100:(0/100/00:00:00:00:00:04) .
```

The **bridge show blk** command displays a blocked bridge.

```
zSH> bridge show blk
       Orig
Type    VLAN/SLAN  VLAN/SLAN  Physical        Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------
dwn               Tagged 100  1/9/4/0/eth     1-9-4-0-eth-100/bridge          BLK  A 00:00:00:00:00:04
1 Bridge Interfaces displayed
```

4- 7.1.5 Unblock a Bridge Interface

The syntax for unblocking a blocked bridge interface is:

```
bridge unblock <interface>/<type> |
       [slot <slotNum]
       [vlan <vlanId>]
       [slan <slanId>]
       [vlan-count <value>]
       [mvr [<mvrVlan>]]
       [secure]
       [uplink | downlink | intralink | tls | rlink | pppoa | wire |
        mvr | user | downlink-video | downlink-data | downlink-pppoe |
        downlink-p2p | downlink-voice | downlink-upmcast | ipob-tls |
        ipob-uplink | ipob-downlink]
       [verbose]
Unblocks bridge interfaces which have been blocked due to bridge storm
detection (BSD) and due to bridge loop detection.
Where:
    <interface>/<type>
           The interface can be a bridge, GPON OLT, Ethernet Port, etc.
           Wildcard formats are supported.  The interface must come immediately
           after "bridge unblock".
    slot <slotNum>
            Process all bridge interfaces for ports in the specified slot.
           <slotNum> may be a single number, a bracketed list containing
           comma-separated numbers or a dash-separated number range or a
           combination of both.
    vlan <vlanId>
            Process all bridge interfaces for the specified VLAN.
           <vlanId> may be a single number, a bracketed list containing
           comma-separated numbers or a dash-separated number range or a
           combination of both.
    vlan-count <count>
           Process bridges that have VLAN ID values in the range
           <vlan> to <vlan+count>
    slan <slanId>
            Process all bridge interfaces for the specified SLAN.
           <slanId> may be a single number, a bracketed list containing
           comma-separated numbers or a dash-separated number range or a
           combination of both.
    secure
            Process secure bridges.
    mvr [<mvrVlan>]
            Process all bridge interfaces associated with the given MVR
            vlan.  <mvrVlan> may be a single number, a bracketed list containing
           comma-separated numbers or a dash-separated number range or a
           combination of both.  If no MVR vlan or 0 is entered, all MVR related
            bridges are processed.
    uplink | downlink | intralink | tls | rlink | pppoa | wire |
    mvr | user | downlink-video | downlink-data | downlink-pppoe |
```

```
downlink-p2p | downlink-voice | downlink-upmcast | ipob-tls |
ipob-uplink | ipob-downlink]
        Process bridges of the specified bridge-type.   Multiple bridge
        types can be specified.
verbose
        display "unblock" operation status
```

Procedure: *Unblocking the Bridge Interface*

For example, to unblock a bridge that is blocked because of loop prevention using the bridge interface enter.

```
zSH> bridge unblock 1-10-1-501-gponport/bridge
```

The following type of information is displayed in the console window.

```
zSH> JUN 22 02:14:15: alert : 1/a/1027: bridge: BridgeTrapSend(): l=1233: tCliInit0: Bridge Loop Alarm
for 1-10-1-501-gponport-100 cleared.
```

To unblock a bridge using the slot number and VLAN ID enter:

```
zSH> bridge unblock slot 5 vlan 100
```

To unblock a bridge using the VLAN ID enter:

```
zSH> bridge unblock vlan 100
```

4- 7.2 Bridge storm protection

This section describes the packet rule for bridge storm protection:

4- 7.2.1 Bridge storm protection overview

The **bridgestormdetect** filter provides a way to analyze packets by capturing discarded packets when a certain threshold is reached and is configured only on the ingress of a bridge interface.

This packet rule will capture the first N packets after the target packets-per-second threshold is reached. Since all discarded packets are not captured, and there may be multiple interfaces with a bridge storm, some

packets on the first interface with a bridge storm are captured, then some packets on the next interface with a bridge storm are captured, and so on.

The **rule add bridgestormdetect** command syntax is:

```
rule add bridgestormdetect <group/member> <discard | discardandalarm |discardandalarmandblock>
<packets-per-second>[<consecutive-seconds>]
```

If the **rule add bridgestormdetect** command is configured with *discard*, only the *packets-per-seconds* is set.

If the **rule add bridgestormdetect** command is configured with *discardandalarm* or *discardandalarmandblock,* both the *packets-per-seconds* and the *consecutive-seconds* fields must be set.

If the card reboots, the captured packets are lost.

4- 7.2.2 Default packet rule filters (bridgestormdetect)

Currently, default packet rules are created only for the **bridgestormdetect** filter.

The default **bridgestormdetect** rule is configured for *discard+alarm+block* with defined auto-enable intervals.

4- 7.2.2: 1 Rules for default packet rule bridgestormdetect

The rules for the default **bridgestormdetect** packet rule filters are:

- A default packet rule filter for **bridgestormdetect** is automatically defined and applied to *downlink*, *tls*, and *wire* bridge interfaces when a **bridgestormdetect** packet rule is not currently applied.
- If an eligible bridge type is configured with packet rules other than **bridgestormdetect**, the default **bridgestormdetect** rule is applied.
- The default packet rules are configured in group *0*.
- The group/member *0/1* **bridgestormdetect** rule is automatically applied to *downlink* bridge interfaces and rule *0/2* is automatically applied to *tls* and *wire* bridge interfaces.
- The default **bridgestormdetect** rule is not applied to other bridge types.

The default rules are always displayed with the **rule show** command:

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 30 cs 30
                                                              auto-enable-interval (def) 300 600 1200
         Default tls/wire (0/2)             bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval (def) 300 600 1200
2 record(s) found
```

The **rule showuser default** command displays bridges with the default packet rule **bridgestormdetect**.

```
zSH> rule showuser default
             Group/Member                          Type        IfIndex  IfAddr
-------------------------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect     1359  1-4-1-303-gponport-100/bridge
(ingress)
              Default dwn (0/1)             bridgestormdetect     1362  1-4-1-501-gponport/bridge
(ingress)
2 record(s) found
```

4- 7.2.2: 2 Disable the bridgestromdetect packet rules

The default **bridgestormdetect** rules can be disabled by entering the *disdefpktrules* keyword to the **options** parameter in **system 0**. Both default packet rules are disabled.

The default rules *0/1* and *0/2* cannot be deleted with the **rule delete** command.

```
zSH> rule delete 0/1
Not allowed to delete from default group index 0
```

Procedure: *Disabling the default bridgestormdetect packet rules*

Update the **system 0** file.

```
zSH> update system 0
system  0
Please provide the following: [q]uit.
syscontact: ----------->  {}:
sysname: -------------->  {}:
syslocation: ---------->  {}:
enableauthtraps: ------>  {disabled}:
setserialno: ---------->  {0}:
zmsexists: ------------>  {false}:
zmsconnectionstatus: -->  {inactive}:
zmsipaddress: --------->  {0.0.0.0}:
configsyncexists: ----->  {false}:
configsyncoverflow: --->  {false}:
configsyncpriority: --->  {high}:
configsyncaction: ----->  {noaction}:
configsyncfilename: --->  {}:
configsyncstatus: ----->  {syncinitializing}:
configsyncuser: ------->  {}:
configsyncpasswd: ----->  {** private **}:  ** read-only **
numshelves: ----------->  {1}:
shelvesarray: --------->  {}:
numcards: ------------->  {3}:
ipaddress: ------------>  {0.0.0.0}:
alternateipaddress: --->  {0.0.0.0}:
countryregion: -------->  {us}:
primaryclocksource: --->  {0/0/0/0/0}:
ringsource: ----------->  {internalringsourcelabel}:
revertiveclocksource: ->  {true}:
voicebandwidthcheck: -->  {false}:
alarm-levels-enabled: ->  {critical+major+minor+warning}:
userauthmode: --------->  {local}:
radiusauthindex: ------>  {0}:
secure: --------------->  {disabled}:
webinterface: --------->  {enabled}:
```

```
options: -------------->  {NONE(0)}: disdefpktrules <--------------------
reservedVlanIdStart: -->  {0}:
reservedVlanIdCount: -->  {0}:
snmpVersion: ---------->  {snmpv2}
persistentLogging: ---->  {disabled}
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

Procedure: *Re-enabling the default bridgestormdetect packet rule*

Update **system 0** by entering the *none 0* keyword to the **options** parameter.

```
zSH> update system 0
system  0
Please provide the following: [q]uit.
syscontact: ------------>  {}:
sysname: --------------->  {}:
syslocation: ----------->  {}:
enableauthtraps: ------>  {disabled}:
setserialno: ----------->  {0}:
zmsexists: ------------->  {false}:
zmsconnectionstatus: -->  {inactive}:
zmsipaddress: ---------->  {0.0.0.0}:
configsyncexists: ----->  {false}:
configsyncoverflow: --->  {false}:
configsyncpriority: --->  {high}:
configsyncaction: ----->  {noaction}:
configsyncfilename: --->  {}:
configsyncstatus: ----->  {syncinitializing}:
configsyncuser: -------->  {}:
configsyncpasswd: ----->  {** private **}:  ** read-only **
numshelves: ------------>  {1}:
shelvesarray: ---------->  {}:
numcards: -------------->  {3}:
ipaddress: ------------->  {0.0.0.0}:
alternateipaddress: --->  {0.0.0.0}:
countryregion: --------->  {us}:
primaryclocksource: --->  {0/0/0/0/0}:
ringsource: ------------>  {internalringsourcelabel}:
revertiveclocksource: ->  {true}:
voicebandwidthcheck: -->  {false}:
alarm-levels-enabled: ->  {critical+major+minor+warning}:
userauthmode: ---------->  {local}:
radiusauthindex: ------>  {0}:
secure: ---------------->  {disabled}:
webinterface: ---------->  {enabled}:
options: -------------->  {disdefpktrules}: none 0 <--------------------
reservedVlanIdStart: -->  {0}:
reservedVlanIdCount: -->  {0}:
snmpVersion: ---------->  {snmpv2}
persistentLogging: ---->  {disabled}
.....................
Save changes? [s]ave, [c]hange or [q]uit: s
Record updated.
```

4- 7.2.3 Case 1: bridgestormdetect packet rule for discard

Procedure: *Configuring a bridge discard*

Configuring the *bridgestormdetect* packet rule for *discard*, means that when the packets exceed the packets-per-second threshold, the overall traffic on the bridge will be limited.

1 Enter the **rule add** command to create the *bridgestormdetect* packet rule for *discard* and set the packets-per-seconds threshold.

```
zSH> rule add bridgestormdetect 1/1 discard pps 20
Created packet-rule-record 1/1 (bridgestormdetect)
```

Verify the rule.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 30 cs 30
                                                              auto-enable-interval (def) 300 600 1200
         Default tls/wire (0/2)             bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval (def) 300 600 1200
                           1/1              bridgestormdetect discard pps 20
3 record(s) found
```

2 Apply the rule to a bridge interface.

```
zSH> bridge add 1-6-1-0/eth downlink vlan 100 tagged ipktrule 1
Adding bridge on 1-6-1-0/eth
Created bridge-interface-record 1-6-1-0-eth-100/bridge
```

Verify the bridge.

```
zSH> bridge show
        Orig
Type    VLAN/SLAN  VLAN/SLAN  Physical         Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------
dwn               Tagged 100  1/6/1/0/eth      1-6-1-0-eth-100/bridge          UP  D 00:01:47:31:dc:1a
1 Bridge Interfaces displayed
```

Verify the rule *1/1* is applied to the bridge.

```
zSH> rule showuser
             Group/Member                          Type        IfIndex  IfAddr
-------------------------------------------------------------------------------------------
                           1/1             bridgestormdetect     1354  1-6-1-0-eth-100/bridge (ingress)
1 record(s) found
```

4- 7.2.4 Case 2: bridgestormdetect packet rule for discard + alarm

Procedure: *Configuring a rule for discard + alarm*

Configuring the *bridgestormdetect* packet rule for *discard* + *alarm*, means that when the packets exceeds the packets-per-second threshold over a

configured number of seconds, the overall traffic on the bridge will be limited and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm is sent.

1 Enter the **rule add** command to create the *bridgestormdetect* packet rule for *discard* + *alarm*.

```
zSH> rule add bridgestormdetect 2/1 discardandalarm pps 20 cs 10
Created packet-rule-record 2/1 (bridgestormdetect)
```

Verify the rule.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 30 cs 30
                                                              auto-enable-interval (def) 300 600 1200
          Default tls/wire (0/2)            bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval (def) 300 600 1200
                            1/1             bridgestormdetect discard pps 20
                            2/1             bridgestormdetect discard+alarm pps 20 cs 10
4 record(s) found
```

2 Apply the rule to a bridge interface.

```
zSH> bridge add 1-6-2-0/eth downlink vlan 400 tagged ipktrule 2
Adding bridge on 1-6-2-0/eth
Created bridge-interface-record 1-6-2-0-eth-400/bridge
```

Verify the bridge.

```
zSH> bridge show
        Orig
Type    VLAN/SLAN  VLAN/SLAN  Physical         Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------
dwn               Tagged 100  1/6/1/0/eth      1-6-1-0-eth-100/bridge          UP  D 00:01:47:31:dc:1a
dwn               Tagged 400  1/6/2/0/eth      1-6-2-0-eth-400/bridge          UP
2 Bridge Interfaces displayed
```

Verify the rule *2/1* is applied to the bridge.

```
zSH> rule showuser
             Group/Member                          Type        IfIndex  IfAddr
-------------------------------------------------------------------------------------------
                            1/1             bridgestormdetect     1354  1-6-1-0-eth-100/bridge (ingress)
                            2/1             bridgestormdetect     1356  1-6-2-0-eth-400/bridge (ingress)
2 record(s) found
```

4- 7.2.5 Case 3: bridgestormdetect packet rule for discard + alarm + block

Configuring the *bridgestormdetect* packet rule for *discard* + *alarm* + *block*, means that when the packets exceeds the packets-per-second threshold over a configured number of seconds, the overall traffic on the bridge will be completely blocked and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm is sent.

The *bridgestormdetect* packet rule for *discard + alarm + block* automatically creates an **auto-enable-interval** parameter configured for *300* seconds, *600* seconds, and *1200* seconds. The first value indicates that the bridge will automatically unblock after 300 seconds (five minutes). The second value indicates that when the next bridge storm occurs, the bridge will unblock after 600 seconds (ten minutes), and after the third bridge storm detection, the bridge will unblock after 1200 seconds (20 minutes). After the third time, if the storm continues, the bridge remains blocked and must be unblocked through the CLI. See Unblock a bridge, page 112.

Procedure: *Configuring a rule for discard + alarm + block*

1 Enter the **rule add** command to create the *bridgestormdetect* packet rule for *discard + alarm + block*.

```
zSH> rule add bridgestormdetect 3/1 discardandalarmandblock pps 20 cs 10
Created packet-rule-record 3/1 (bridgestormdetect)
```

Verify the rule.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 30 cs 30
                                                              auto-enable-interval (def) 300 600 1200
          Default tls/wire (0/2)            bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval (def) 300 600 1200
                           1/1              bridgestormdetect discard pps 20
                           2/1              bridgestormdetect discard+alarm pps 20 cs 10
                           3/1              bridgestormdetect discard+alarm+block pps 20 cs 10
                                                              auto-enable-interval (def) 300 600 1200
5 record(s) found
```

2 Apply the rule to a bridge interface.

```
zSH> bridge add 1-6-3-0/eth downlink vlan 500 tagged ipktrule 3
Adding bridge on 1-6-3-0/eth
Created bridge-interface-record 1-6-3-0-eth-500/bridge
```

Verify the bridge.

```
zSH> bridge show
        Orig
Type    VLAN/SLAN  VLAN/SLAN  Physical         Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------
dwn               Tagged 100  1/6/1/0/eth      1-6-1-0-eth-100/bridge          UP  D 00:01:47:31:dc:1a
dwn               Tagged 400  1/6/2/0/eth      1-6-2-0-eth-400/bridge          DWN
dwn               Tagged 500  1/6/3/0/eth      1-6-3-0-eth-500/bridge          DWN
3 Bridge Interfaces displayed
```

Verify the rule *3/1* is applied to the bridge.

```
zSH> rule showuser
             Group/Member                          Type        IfIndex  IfAddr
-------------------------------------------------------------------------------------------
                           1/1             bridgestormdetect     1354  1-6-1-0-eth-100/bridge (ingress)
                           2/1             bridgestormdetect     1356  1-6-2-0-eth-400/bridge (ingress)
```

```
                        3/1             bridgestormdetect     1357  1-6-3-0-eth-500/bridge (ingress)
3 record(s) found
```

4- 7.2.6 Modify the default bridgestormdetect rules

The default parameters in the **bridgestormdetect** rule can be modified by the user.

The syntax for the **rule modify bridgestormdetect** is:

```
rule modify bridgestormdetect <group/member>
    [<discard | discardandalarm | discardandalarmandblock >]
    [pps <packets-per-second>] [cs <consecutive-seconds>]
    [auto-enable-interval <param0> [<param1> [<param2>]]]
```

The **rule modify** command allows you to disable or change the *auto-enable-interval* values as well as the threshold *pps* and *cs*.

4- 7.2.6: 1 Modify default bridgestormdetect pps and cs values

The **bridgestormdetect** *discardandalarmandblock* packet rule blocks the bridge interface when packets exceed a level configured by the *pps* over time set by the *cs* value.

The default values for *pps* and *cs* in default *0/1* and *0/2* differ due to higher normal traffic on *tls* and *wire* bridges.

The range for consecutive alarm seconds values is 5 to 30 seconds.

Procedure: *Modifying default pps and cs values*

1. Enter the **rule modify bridgestormdetect** command to change the default values.

```
zSH> rule modify bridgestormdetect 0/1 discardandalarmandblock pps 25 cs 25
Modified packet-rule-record 0/1 (bridgestormdetect)
```

2. Verify the changes.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------------------
              Default dwn (0/1)              bridgestormdetect discard+alarm+block pps 25 cs 25

                                  auto-enable-interval (def) 300 600 1200
         Default tls/wire (0/2)              bridgestormdetect discard+alarm+block pps 100 cs 30
                                                               auto-enable-interval (def) 300 600 1200
2 record(s) found
```

4- 7.2.6: 2 Default bridgestormdetect auto-enable-interval values

The default *auto-disable-interval* parameter sets the time in seconds when the bridge is unblocked and allowed to pass traffic at *300*, *600*, and *1200* seconds.

When a bridge interface is blocked the first time, it is unblocked after 300 seconds. The second time, if the storm continues, the interface is unblocked

after 600 seconds. The third time, if the storm continues, the bridge interface is unblocked at 1200 seconds. After the third time, if the storm continues, the bridge remains blocked and must be unblocked through the CLI. See Unblock a bridge, page 112.

The *auto-enable-interval* times in seconds can be modified or disabled.

Procedure: *Modifying the auto-enable-interval values*

1 Enter the **rule modify bridgestormdetect** command to change the default values for *auto-enable-interval*.

```
zSH> rule modify bridgestormdetect 0/1 discardandalarmandblock pps 25 cs 25
auto-enable-interval 60 300 600
Modified packet-rule-record 0/1 (bridgestormdetect)
```

2 Verify the changes.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 25 cs 25
                                                              auto-enable-interval 60 300 600
          Default tls/wire (0/2)            bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval (def) 300 600 1200
2 record(s) found
```

Procedure: *Disabling the default auto-enable-interval*

Entering the value *0* to the first field of the **auto-enable-interval** parameter disables the re-enable traffic feature of **bridgestormdetect**.

1 Enter the **rule modify bridgestormdetect** command to disable the r *auto-enable-interval*.

```
zSH> rule modify bridgestormdetect 0/2 discardandalarmandblock pps 100 cs 30
auto-enable-interval 0
Modified packet-rule-record 0/2 (bridgestormdetect)
```

The bridge interface will be blocked and must be unblocked through CLI. See *Unblock a bridge* on page 112

2 Verify the change.

```
zSH> rule show
             Group/Member                          Type Value(s)
-------------------------------------------------------------------------------------------
              Default dwn (0/1)             bridgestormdetect discard+alarm+block pps 25 cs 25
                                                              auto-enable-interval 60 300 600
          Default tls/wire (0/2)            bridgestormdetect discard+alarm+block pps 100 cs 30
                                                              auto-enable-interval 0
2 record(s) found
```

4- 7.2.7 View detected packets statistics

Procedure: *Viewing detected packets statistics*

The **bridge stats** *interface/type* command sorts and displays the detected packets into unicast, multicast, or broadcast and displays the number of alarms sent.

```
zSH> bridge stats 1/9/1/4/gpononu
Interface                          Received Packets        Transmitted Packets          Storm Detect
Packets         Byte Counters
Name                             UCast  MCast  BCast   UCast  MCast  Bcast  Error   UCast  MCast  Bcast
Alarm   Received  Transmitted
1-9-1-304-gponport-1001/bridge     0      0      0       0      0      0      0       0      0      0
0       0         0
1-9-1-904-gponport-998/bridge      0      0      49      227    529    3883   0       0      0      0
0       360       169k
```

4- 7.2.8 View the packets

Use the **bridge capture show** command to view which interfaces had a bridge storm and how many packets were captured.

The Packet column shows the number of packets captured, and the Count column displays the number of packets allowed to be captured.

Each interface having a bridge storm will capture fewer packets. The first interface that has a bridge storm can capture eight packets, the next interface that has a bridge storm can capture six packets, and so on.

Procedure: *Viewing the packets*

You must connect to the line card before using the **bridge capture show** command.

1 Connect to the line card by entering **connect** and the slot number of the line card.

```
zSH> connect 9
Connecting to shelf: 1, slot: 3 ......
Connection established.
```

2 Enter the **bridge capture show** command to view which interfaces had a bridge storm and how many packets were captured.

```
1/9-qzSH> bridge capture show
Interface Name                  Packet Count
-----------------------------------------------------------
1-9-1-304-gponport-1001              8/    8
<Queue Empty>                        0/    6
<Queue Empty>                        0/    4
<Queue Empty>                        0/    2
```

3 Enter the **bridge capture dump** *interface/type* command to view the captured packets.

```
1/9-zSH> bridge capture dump 1-9-1-304-gponport-1001 # 1-9-1-304-gponport-1001, IfIndex = 1111 # tick =
0x00000034822d3bf4
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 58 c0 09 32 58 c0 ".>........X..2X."
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x00000034822d52cf
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 9e 78 03 e6 9e 78 ".>.........x...x"
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x00000034822d6800
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 74 79 70 65 20 3d ".>........type ="
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x00000034822d9677
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 64 64 72 36 20 3d
".>........ddr6 ="
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x00000034822e9b03
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 63 61 64 64 72 33 ".>........caddr3"
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x00000034822f55b7
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 ".........."."#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K............"
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
```

```
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'.............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 00 00 00 00 00 00 ".>.............."
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x000000348bb7e71e
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 "...........".#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K..........."
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'.............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 00 00 00 00 00 00 ".>.............."
# 1-9-1-304-gponport-1001, IfIndex = 1111
# tick = 0x000000348bb89f5d
   00000000: 33 33 00 01 00 02 00 00 00 00 00 01 81 00 03 e9 "33.............."
   00000010: 86 dd 60 00 00 00 00 40 11 01 fe 80 00 00 00 00 "..`....@........"
   00000020: 00 00 02 15 c5 ff fe 57 b6 3e ff 02 00 00 00 00 ".......W.>......"
   00000030: 00 00 00 00 00 00 00 01 00 02 02 22 02 23 00 40 "...........".#.@"
   00000040: 14 5d 01 d1 4b 90 00 01 00 0e 00 01 00 01 1c ed ".]..K..........."
   00000050: e7 34 00 15 c5 57 b6 3e 00 06 00 08 00 17 00 18 ".4...W.>........"
   00000060: 00 27 00 1f 00 08 00 02 ff ff 00 03 00 0c c5 57 ".'.............W"
   00000070: b6 3e 00 00 0e 10 00 00 15 18 15 d0 0a 5d 15 d0 ".>...........].."
```

Note: For customers who want to view output in a packet capture tool such as wireshark, copy the output into a notepad file, then run the *text2pcap* application. The output should then be in a viewable state.

4 Enter the **bridge capture clear -all** command to clear all the interfaces with bridge storms, then verify the output with the **bridge capture show** command.

You can also enter the bridge capture clear *interface/type* command to clear individual bridge interfaces.

```
1/9-zSH> bridge capture clear -all

1/9-zSH> bridge capture show
Interface Name                   Packet Count
-------------------------------------------------------------
<Queue Empty>                         0/    8
<Queue Empty>                         0/    6
<Queue Empty>                         0/    4
<Queue Empty>                         0/    2
```

5 Close the connection to the line card by entering the **exit** command.

```
zSH> exit
Connection closed.
```

4- 7.2.9 Unblock a bridge

Procedure: *Unblocking a bridge*

Use the **bridge unblock** *interface/type* command to unblock a blocked bridge interface configured with the **bridgestormdetect** packet rule *discard* + *alarm* + *block*.

Enter the **bridge unblock** command.

```
zSH> bridge unblock 1-6-1-0-eth-100/bridge
```

4- 8 MONITORING MXK-F MANAGEMENT CARDS

The MXK-F14xx and MXK-F219 chassis each provide two slots, *m1* and *m2*, for redundant management cards that provide the controller and database functions for the chassis.

4- 8.1 Redundancy Status Information

To display summary redundancy status, enter the **showredundancy** command:

```
zSH> showredundancy
Redundancy status for card 01:m1 - Safe, all services have redundant peers
01:m1 is active storage
01:m2 is standby storage
```

To display detailed redundancy status, enter the **showredundancy -d** command.

```
zSH> showredundancy -d
Redundancy status for card 01:m1 -
Taskname            Active Addr     Standby Addr   Stdby Ready?
========            ===========     ============   ============
InfoServer          01:m1:02        01:m2:02       Yes
RdsServer           01:m1:03        01:m2:03       Yes
tNumSrv             01:m1:1043      01:m2:1032     Yes
tShelfRR            01:m1:1044      01:m2:1033     Yes
tMAXTask            01:m1:1045      01:m2:1034     Yes
zCardRed            01:m1:26        01:m2:26       Yes
trapSrv             01:m1:25        01:m2:25       Yes
tFTD                01:m1:67        01:m2:67       Yes
TadSrvTask          01:m1:1047      01:m2:1036     Yes
ifcfgtask           01:m1:78        01:m2:78       Yes
L-RR-1/m1           01:m1:79        01:m2:79       Yes
_RedSpawnSvrTask    01:m1:1051      01:m2:1040     Yes
LogServer           01:m1:08        01:m2:08       Yes
gponOltMibHdlr      01:m1:1078      01:m2:1055     Yes
DhcpServerTask      01:m1:90        01:m2:90       Yes
RlyAlmHdlr          01:m1:1084      01:m2:1042     Yes
tIPSIM              01:m1:75        01:m2:75       Yes
tEtherOamRp         01:m1:83        01:m2:83       Yes
```

```
bridgeMibHdlr       01:m1:1087      01:m2:1062      Yes
tDS1RP              01:m1:1086      01:m2:1061      Yes

Safe, all services have redundant peers
01:m1 is active storage
01:m2 is standby storage
```

CHAPTER 5 STATISTICS ON THE MXK-F

This chapter provides statistics commands for the MXK-F:

5-1 VIEW RUNTIME STATISTICS ON THE MXK-F

The **card stats** command displays runtime statistics for the MXK-F14xx device.

```
zSH> card stats
     ------- cpu % utilization ----- ------ memory (KB)------ Card Mem   uptime
slot idle usage high serv frmwrk low % Used  Tot   Peak  Avail Status ddd:hh:mm:ss s/w version
==== ==== ===== ==== ==== ===== == ===== ===== ===== ===== ====== ========== ========
 m1*  97    3     0    1     0    1  21.25 966358 209937 761003 1-OK   0:21:07:01 MXK 3.1.1.215
```

The **card stats all** command displays information for all the cards.

```
zSH> card stats all
     ------- cpu % utilization ----- ------ memory (KB)------ Card Mem   uptime
slot idle usage high serv frmwrk low %Used  Tot    Peak  Avail Status ddd:hh:mm:ss s/w version
==== ==== ===== ==== ==== ===== == ===== ===== ===== ===== ====== ========== ========
  1   92    8     3    4     0     5  22.58 939295 212078 727226 1 - OK  0:20:56:58 MXK 3.1.1.215
  2   91    9     3    4     0     5  22.54 939295 211819 727577 1 - OK  0:20:56:29 MXK 3.1.1.215
  3   92    8     3    4     0     5  22.49 939296 211257 728049 1 - OK  0:20:56:21 MXK 3.1.1.215
  4   92    8     3    4     0     5  22.52 939295 211505 727800 1 - OK  0:20:56:30 MXK 3.1.1.215
  5   92    8     3    4     0     5  22.63 939294 212588 726716 1 - OK  0:20:47:42 MXK 3.1.1.215
  6   92    8     3    4     0     5  22.66 939293 212854 726448 1 - OK  0:20:47:07 MXK 3.1.1.215
  7   92    8     3    4     0     5  22.67 939293 212936 726367 1 - OK  0:20:47:18 MXK 3.1.1.215
  8   92    8     3    4     0     5  22.67 939294 213069 726318 1 - OK  0:20:47:34 MXK 3.1.1.215
  9   92    8     3    4     0     6  22.64 939292 212670 726631 1 - OK  0:20:35:27 MXK 3.1.1.215
 10   92    8     3    4     0     6  22.66 939294 212878 726425 1 - OK  0:20:35:26 MXK 3.1.1.215
 11   92    8     3    4     0     6  22.68 939293 212999 726303 1 - OK  0:20:35:40 MXK 3.1.1.215
 12   92    8     3    4     0     6  22.68 939291 213023 726278 1 - OK  0:20:34:56 MXK 3.1.1.215
 13   92    8     3    4     0     5  22.70 939292 217150 726053 1 - OK  0:20:07:41 MXK 3.1.1.215
 14   92    8     3    4     0     6  22.70 939292 216083 726068 1 - OK  0:20:07:19 MXK 3.1.1.215
 m1*  97    3     0    1     0     1  21.25 966358 209937 761003 1 - OK  0:21:07:08 MXK 3.1.1.215
 m2   98    2     0    0     0     1  12.97 966359 125372 841037 1 - OK  0:21:04:34 MXK 3.1.1.215
  a   88   12     2    8     0     0  18.77 944282 177269 767022 1 - OK 0:21:05:00 MXK 3.1.1.215
  b   89   11     2    7     0     0  18.77 944282 177250 767052 1 - OK 0:21:04:36 MXK 3.1.1.215
```

The **card stats** command displays runtime statistics for the MXK-F219 device.

```
zSH> card stats
     ------- cpu % utilization ----- ------ memory (KB)------ Card Mem   uptime
slot idle usage high serv frmwrk low %Used  Tot    Peak  Avail Status ddd:hh:mm:ss s/w version
==== ==== ===== ==== ==== ====== === ===== ====== ====== ===== ====== ========== =========
 m1*  97    3     0    1     0     1   5.24 203905 106923 193213 1 - OK 0:14:47:11 MXK 3.1.2.110
```

The **card stats all** command displays information for all the cards.

```
zSH> card stats all
     ------- cpu % utilization ----- ------ memory (KB)------ Card Mem   uptime
slot idle usage high serv frmwrk low %Used  Tot    Peak  Avail Status ddd:hh:mm:ss s/w version
==== ==== ===== ==== ==== ====== === ===== ====== ====== ===== ====== ========== =========
  1    92    8    2     5     0     2  21.96 948744 209313 740394 1 - OK 0:14:42:55 MXK 3.1.2.110
  2    91    9    3     5     0     2  22.30 948745 211654 737148 1 - OK 0:14:40:21 MXK 3.1.2.110
 m1*   97    3    0    1     0     1   5.24 203905 106925 193213 1 - OK 0:14:47:19 MXK 3.1.2.110
 m2    98    2    0    0     0     1  4.65 203905  94827 194432 1 - OK 0:14:44:23 MXK 3.1.2.110
```

Table 12: card stats Command Fields

Section	Field
CPU% utilization	**slot** Textual description of the unit/card or access device type.
	idle Percentage of time the CPU has spent executing tasks with priority of 200 or less. Tasks with priority of 200 or less (the higher the number, the lower the priority) are considered idle tasks.
	usage Percentage of time the CPU has spent executing tasks with priority of 199 or higher
	high High priority tasks are primarily related to packet processing and critical system monitoring. Percentage of time the CPU has spent executing tasks with priority of 001 to 099. High priority tasks are primarily related to packet processing and critical system monitoring.
	services Services are primarily line monitoring tasks for line state and alarms. Percentage of time the CPU has spent executing tasks with priority of 100 to 179. Services tasks are primarily line monitoring tasks for line state and alarms.

Table 12: card stats Command Fields (Continued)

Section	Field
	framework Framework tasks are primarily database and network management system related activities such as config synch and backup. Percentage of time the CPU has spent executing tasks with priority of 180 to 199. Framework tasks are primarily database and network management system related activities such as config synch and backup.
	low Percentage of time the CPU has spent executing tasks with priority of 200 to 250
memory (KB)	**Used** Percentage of time the CPU has spent executing tasks with priority of 199 or higher.
	Total The amount of physical memory contained by the device/card.
	Peak The maximum physical memory that has been allocated at any time by the device/card.
	Avail The amount of physical memory that is unallocated and not in use by the device/card.
Card Memory Status	Memory status of the card sent with memory trap. A trap is sent when each condition occurs. 1 - ramMemOK less then 90% of ram is used 2 - ramMemLow more then 90% of ram is used 3 - flashMemOK enough flash for maximum database 4- flashMemLow not enough flash for maximum database 5 - flashMemOut no more flash memory, data no longer persistent
uptime ddd:hh:mm:ss	Uptime is calculated as sysUpTime - ifLastChange (assuming the device/card is running).
s/w version	Software version.

5- 2 VIEW BRIDGE STATISTICS

This section describes:

5- 2.1 Bridge Interface Statistics Overview

There are two commands for viewing statistics on bridge interfaces. The first command, **bridge stats**, displays all of the packet counters that have passed through the interface.The second command, **bridge rates**, displays all of the packets that pass through the bridge interface in rate-per-second.

The **bridge stats** command can display statistics for all bridge interfaces that display statistics, for a specified bridge interface, or for bridges on a specified VLAN ID.

The default counters for the **bridge stats** command are packet counters. Counters in bytes are also displayed in the Byte Counters columns.

5- 2.2 Bridge Statistics Commands

- *View Bridge Interface Statistics* on page 118
- *Use the bridge stats reset, clear, list, and rules Commands for Statistics* on page 119

5- 2.2.1 View Bridge Interface Statistics

- *Viewing Bridge Statistics* on page 118
- *Viewing Bridge Statistics By VLAN ID* on page 119

Procedure: *Viewing Bridge Statistics*

Enter the **bridge stats** *interfaceName/bridge* command to view statistics on a bridge interface.

In this case, the bridge interface is *GPON*.

```
zSH> bridge stats 1-3-1-704-gponport-3003/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
1-3-1-704-gponport-3003/bridge  3     0     0   1577    0     0    0     0     0     0    0   668 119k
```

Enter the **bridge rates** *interfaceName/bridge* command to view statistics in rate-per-second.

```
zSH> bridge rates 1-3-1-704-gponport-3003/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
1-3-1-704-gponport-3003/bridge  1     0     0     1     0     0    0     0     0     0    0      1  39
```

Enter the **bridge stats** *interfaceName/bridge* command to view statistics on a bridge interface.

In this case, the bridge interface is Active Ethernet.

```
zSH> bridge stats 1-9-21-0-eth/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
```

```
1-9-21-0-eth/bridge         1   4923  302  988k  803  383   0    0     0    0   0     0 159M
```

Enter the **bridge rates** *interfaceName/bridge* command to view statistics in rate-per-second.

```
zSH> bridge rates 1-9-21-0-eth/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
1-9-21-0-eth/bridge         1    1     1    11    1    1    0    0    0     0   0     0 1651
```

Procedure: *Viewing Bridge Statistics By VLAN ID*

Enter the **bridge stats** *vlanid* command to view bridge statistics by VLAN ID.

```
zSH> bridge stats vlan 3003
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
ethernet2-3003/bridge      1680   0    0     3    0    0    0    0    0     0   0  121k 656
1-3-1-704-gponport-3003/bridge    3   0     0   1680    0     0    0     0     0     0    0    668 127k
1-9-1-0-eth-3003/bridge           0   0     0      0    0     0     0    0     0     0    0     0   0
```

5- 2.2.2 Use the bridge stats reset, clear, list, and rules Commands for Statistics

Procedure: *Using the Bridge Statistics Reset Command*

Use the **bridge statistics reset** *interfaceName/bridge* command to display and clear statistics and rates on bridge interfaces.

1. Enter the **bridge stats reset** *interfaceName/bridge* command to display and reset statistical counters to 0, and resume counting.

   Bridge interface with statistics-on-demand enabled.

```
zSH> bridge stats reset ethernet1-840/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
ethernet1-840/bridge          971M   0    244  2600M   0    2695  0     0     0     0    0  8004G 193G
```

2. Enter the **bridge stats** *interfaceName/bridge* command immediately following the **bridge stats reset** *interfaceName/bridge* command to display counters reset.

```
zSH> bridge stats reset ethernet1-840/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
ethernet1-840/bridge          430k   0     0   2066k   0     0    0     0     0     0    0  6529M 1537M
```

3. Enter the **bridge stats** *interfaceName/bridge* command after an interval to display the reset packet counter information.

```
zSH> bridge stats ethernet1-840/bridge
Interface                    ----Rcvd Pkts---- -------Xmt Pkts------  --Storm Detect Pkts-   Byte Count
Name                         UCast MCast BCast UCast MCast Bcast Err  UCast MCast Bcast Alm  Rcvd Xmt
ethernet1-840/bridge          645M   0    244  224M    0    2695  0     0     0     0    0   751G 182G
```

Procedure: *Entering the bridge stats clear Command*

Enter the **bridge stats clear** *interfaceName/bridge* command to clear statistics and rates without displaying them.

```
zSH> bridge stats clear ethernet5-3605/bridge
Bridge statistics cleared
```

5- 2.3 Bridge Statistics Display

Table 13 defines the columns the **bridge stats** and **bridge stats rules** commands display.

Table 13: bridge stats Display Columns

Column	Description
enabled	The on-demand stats collection for this bridge interface will be enabled and packets will be counted.
enabled, bytes	The on-demand stats collection for this bridge interface will be enabled and bytes will be counted.
ucastRx	Unicast packets received.
mcastRx	Multicast packets received.
bcastRx	Broadcast packets received.
ucastTx	Unicast packets sent.
mcastTx	Multicast packets sent.
errorTx	Error packets sent.
RulesSupported	The number of supported ingress statistics available for a line card.
RulesRemaining	The number of remaining ingress statistics available for a line card.
UcastPktBlocked	The number of unicast packets dropped due to bridge packet storm detection threshold exceeded.
McastPktBlocked	Number of multicast packets dropped due to bridge packet storm detection threshold exceeded.
BcastPktBlocked	Number of broadcast packets dropped due to bridge packet storm detection threshold exceeded.
AlarmCnt	This counter reflects the number of times this interface has transitioned to the alarm state due to the bridge packet storm detection threshold being exceeded for a pre-defined number of seconds.
bytesRcvd	This is a count of the number of bytes received. On-demand stats must be enabled for byte counters otherwise this counter is zero.
bytesSent	This is a count of the number of bytes transmitted. On-demand stats must be enabled for byte counters otherwise this counter is zero.

5- 3 ETHERNET PORT STATISTICS

Use **port stats** command to display or clear various statistical information.

port stats <*ifName/Type*> <*intf|rmon|eth|all|clear*>

The **port stats** *interface/type intf* command displays mib2 interface statistics.

See Table 14 on page 124 for parameter definitions.

```
zSH> port stats 1-1-19-0/eth intf
Interface Name                                  1-1-19-0
Operational Status                              Up
Received Bytes                                  660624000
Received Packets                                436317
Received Multicast Packets                      3830
Received Broadcast Packets                      269
Transmitted Bytes                               673299000
Transmitted Unicast Packets                     448250
Transmitted Multicast Packets                   307
Transmitted Broadcast Packets                   309
Received Discards                               1110
Received Errors                                 0
Received Unknown Protocols                      0
Transmitted Discards                            0
Transmitted Errors                              0
Speed Bits per Second                           *** n/a ***
Speed Megabits per Second                       100
```

The **port stats** *interface/type rmon* command displays Ethernet remote monitoring statistics.

```
zSH> port stats 1-1-19-0/eth rmon
Total Dropped Events                            0
Total Dropped Frames                            0
Total Bytes                                     2115147000
Total Packets                                   1410098
Transmitted Packets                             709274
Received Packets                                700824
Transmitted Multicast Bytes                     0
Received Multicast Bytes                        5745000
Received Multicast Dropped Bytes                0
Transmitted Average Throughput                  72672000
Received Average Throughput                     72672000
Transmitted Bandwidth Occupancy                 72
Received Bandwidth Occupancy                    72
Total Broadcast Packets                         578
Total Multicast Packets                         4137
CRC Align Errors                                0
Undersize Packets                               0
Oversize Packets                                0
Transmitted Oversize Packets                    0
Received Oversize Packets                       0
Fragments                                       0
Jabbers                                         0
Collisions                                      0
Transmitted No Errors                           709274
Received No Errors                              700824
IPMC Bridged Packets                            3830
```

```
IPMC Routed Packets                          0
Transmitted IPMC Dropped Packets             0
Received IPMC Dropped Packets                0
Total Packets 0 to 64 Bytes                  0
Total Packets 65 to 127 Bytes                0
Total Packets 128 to 255 Bytes               0
Total Packets 256 to 511 Bytes               0
Total Packets 512 to 1023 Bytes              0
Total Packets 1024 to 1518 Bytes             1410098
Total Packets 1519 to 2047 Bytes             0
Total Packets 2048 to 4095 Bytes             0
Total Packets 4095 to 9216 Bytes             0
Received Packets 0 to 64 Bytes               0
Received Packets 65 to 127 Bytes             0
Received Packets 128 to 255 Bytes            0
Received Packets 256 to 511 Bytes            0
Received Packets 512 to 1023 Bytes           0
Received Packets 1024 to 1518 Bytes          700824
Received Packets 1519 to 2047 Bytes          0
Received Packets 2048 to 4095 Bytes          0
Received Packets 4095 to 9216 Bytes          0
Transmitted Packets 0 to 64 Bytes            0
Transmitted Packets 65 to 127 Bytes          0
Transmitted Packets 128 to 255 Bytes         0
Transmitted Packets 256 to 511 Bytes         0
Transmitted Packets 512 to 1023 Bytes        0
Transmitted Packets 1024 to 1518 Bytes       709274
Transmitted Packets 1519 to 2047 Bytes       0
Transmitted Packets 2048 to 4095 Bytes       0
Transmitted Packets 4095 to 9216 Bytes       0
```

The **port stats** *interface/type eth* command displays the Ethernet dot3 statistics.

```
zSH> port stats 1-1-19-0/eth eth
Alignment Errors                             0
FCS Errors                                   0
Single Collision Frames                      0
Multiple Collision Frames                    0
SQE Test Errors                              0
Deferred Transmissions                       0
Late Collisions                              0
Excessive Collisions                         0
Internal Mac Transmit Errors                 0
Carrier Sense Errors                         0
FrameTooLongs                                0
InternalMacReceiveErrors                     0
SymbolErrors                                 0
DuplexStatus                                 Full
```

The **port stats** *interface/type all* commands displays all of the Ethernet statistics.

```
zSH> port stats 1-1-19-0/eth all
******  eth  ******
Alignment Errors                             0
FCS Errors                                   0
Single Collision Frames                      0
```

Multiple Collision Frames	0
SQE Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
Internal Mac Transmit Errors	0
Carrier Sense Errors	0
FrameTooLongs	0
InternalMacReceiveErrors	0
SymbolErrors	0
DuplexStatus	Full
****** rmon ******	
Total Dropped Events	0
Total Dropped Frames	0
Total Bytes	3405022500
Total Packets	2270015
Transmitted Packets	1139233
Received Packets	1130782
Transmitted Multicast Bytes	0
Received Multicast Bytes	5745000
Received Multicast Dropped Bytes	0
Transmitted Average Throughput	71659832
Received Average Throughput	71659664
Transmitted Bandwidth Occupancy	71
Received Bandwidth Occupancy	71
Total Broadcast Packets	578
Total Multicast Packets	4137
CRC Align Errors	0
Undersize Packets	0
Oversize Packets	0
Transmitted Oversize Packets	0
Received Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Transmitted No Errors	1139233
Received No Errors	1130782
IPMC Bridged Packets	3830
IPMC Routed Packets	0
Transmitted IPMC Dropped Packets	0
Received IPMC Dropped Packets	0
Total Packets 0 to 64 Bytes	0
Total Packets 65 to 127 Bytes	0
Total Packets 128 to 255 Bytes	0
Total Packets 256 to 511 Bytes	0
Total Packets 512 to 1023 Bytes	0
Total Packets 1024 to 1518 Bytes	2270015
Total Packets 1519 to 2047 Bytes	0
Total Packets 2048 to 4095 Bytes	0
Total Packets 4095 to 9216 Bytes	0
Received Packets 0 to 64 Bytes	0
Received Packets 65 to 127 Bytes	0
Received Packets 128 to 255 Bytes	0
Received Packets 256 to 511 Bytes	0
Received Packets 512 to 1023 Bytes	0
Received Packets 1024 to 1518 Bytes	1130782
Received Packets 1519 to 2047 Bytes	0
Received Packets 2048 to 4095 Bytes	0
Received Packets 4095 to 9216 Bytes	0

```
Transmitted Packets 0 to 64 Bytes                    0
Transmitted Packets 65 to 127 Bytes                  0
Transmitted Packets 128 to 255 Bytes                 0
Transmitted Packets 256 to 511 Bytes                 0
Transmitted Packets 512 to 1023 Bytes                0
Transmitted Packets 1024 to 1518 Bytes               1139233
Transmitted Packets 1519 to 2047 Bytes               0
Transmitted Packets 2048 to 4095 Bytes               0
Transmitted Packets 4095 to 9216 Bytes               0
******  intf  ******
Interface Name                                       1-1-19-0
Operational Status                                   Up
Received Bytes                                       1696173000
Received Packets                                     1126682
Received Multicast Packets                           3830
Received Broadcast Packets                           269
Transmitted Bytes                                    1708849500
Transmitted Unicast Packets                          1138617
Transmitted Multicast Packets                        307
Transmitted Broadcast Packets                        309
Received Discards                                    1110
Received Errors                                      0
Received Unknown Protocols                           0
Transmitted Discards                                 0
Transmitted Errors                                   0
Speed Bits per Second                                *** n/a ***
Speed Megabits per Second                            100
```

The **port stats clear** *interface/type* command clears all port stats counters.

```
zSH> port stats clear 1-1-19-0/eth
INTF Stats cleared
```

Table 14 defines the parameters for all of the Ethernet statistics.

Table 14: MXK-F Enhanced Ethernet port statistics

Parameter	Description
eth	
Alignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignment Error status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. This counter does not increment for 8-bit wide group encoding schemes. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Note: Coding errors detected by the physical layer for speeds above 10 Mb/s will cause the frame to fail the FCS check. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Single Collision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Multiple Collision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 1998 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mb/s, or on interfaces operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Late Collisions	The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Internal Mac Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
InternalMacReceive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime
SymbolErrors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
DuplexStatus	The current mode of operation of the MAC entity. 'unknown' indicates that the current duplex mode could not be determined. Management control of the duplex mode is accomplished through the MAU MIB. When an interface does not support autonegotiation, or when autonegotiation is not enabled, the duplex mode is controlled using ifMauDefaultType. When autonegotiation is supported and enabled, duplex mode is controlled using ifMauAutoNegAdvertisedBits. In either case, the currently operating duplex mode is reflected both in this object and in ifMauType. Note that this object provides redundant information with ifMauType. Normally, redundant objects are discouraged. However, in this instance, it allows a management application to determine the duplex status of an interface without having to know every possible value of ifMauType. This was felt to be sufficiently valuable to justify the redundancy. Values: **unknown** **halfDuplex** **fullDuplex**
rmon	**Remote Network Monitoring**
Total Dropped Events	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
Total Dropped Frames	The total number of frames that were received by the probe and therefore not accounted for in the zhoneEtherStatsDropEvents, but that the probe chose not to count for this entry for whatever reason. Most often, this event occurs when the probe is out of some resources and decides to shed load from this collection. This count does not include packets that were not counted because they had MAC-layer errors. Note that, unlike the dropEvents counter, this number is the exact number of frames dropped.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Total Bytes	The total number of octets of data (including those in bad packets) transmitted and received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of 10-Megabit ethernet utilization. If greater precision is desired, the zhoneEtherStatsPkts and zhoneEtherStatsOctets objects should be sampled before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate the Utilization as follows: Pkts * (9.6 + 6.4) + (Octets *.8) Utilization = ---------- Interval * 10,000 The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.
Total Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) transmitted and received.
Transmitted Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) transmitted.
Received Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Transmitted Multicast Bytes	Transmitted multicast bytes.
Received Multicast Bytes	Received multicast bytes.
Received Multicast Dropped Bytes	Dropped multicast bytes.
Transmitted Average Throughput	Average transmit throughput in bits per second since last query. For accuracy purposes, it is recommended that this object be queried in intervals of five (5) seconds or greater.
Received Average Throughput	Average receive throughput in bits per second since last query. For accuracy purposes, it is recommended that this object be queried in intervals of five (5) seconds or greater.
Transmitted Bandwidth Occupancy	Percentage of bandwidth currently being utilized for transmitting traffic. This rate is calculated based on the delta between prior and current query of this object. For accuracy purposes, it is recommended that this object be queried in intervals of five (5) seconds or greater.
Received Bandwidth Occupancy	Percentage of bandwidth currently being utilized for receiving traffic. This rate is calculated based on the delta between prior and current query of this object. For accuracy purposes, it is recommended that this object be queried in intervals of five (5) seconds or greater.
Total Broadcast Packets	The total number of good packets transmitted and received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Total Multicast Packets	The total number of good packets transmitted and received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets transmitted and received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Transmitted Oversize Packets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Received Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for zhoneEtherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. Note also that an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
Transmitted No Errors	The total number of TX packets transmitted without error.
Received No Errors	The total number of RX packets received without error.
IPMC Bridged Packets	Broadcom IPMC Bridged Packet count.
IPMC Routed Packets	Broadcom IPMC Routed Packet count.
Transmitted IPMC Dropped Packets	Broadcom IPMC Tx Dropped Packet count.
Received IPMC Dropped Packets	Broadcom IPMC Rx Dropped Packet count.
Total Packets 0 to 64 Bytes	The total number of packets (including bad packets) transmitted and received that were 64 octets in length (excluding framing bits but including FCS octets).
Total Packets 65 to 127 Bytes	The total number of packets (including bad packets) transmitted and received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 128 to 255 Bytes	The total number of packets (including bad packets) transmitted and received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 256 to 511 Bytes	The total number of packets (including bad packets) transmitted and received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 512 to 1023 Bytes	The total number of packets (including bad packets) transmitted and received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Total Packets 1024 to 1518 Bytes	The total number of packets (including bad packets) transmitted and received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 1519 to 2047 Bytes	The total number of packets (including bad packets) transmitted and received that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 2048 to 4095 Bytes	The total number of packets (including bad packets) transmitted and received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets 4095 to 9216 Bytes	The total number of packets (including bad packets) transmitted and received that were between 4095 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 0 to 64 Bytes	The total number of packets (including bad packets) received that were between 0 and 64 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 65 to 127 Bytes	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 128 to 255 Bytes	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 256 to 511 Bytes	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 512 to 1023 Bytes	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 1024 to 1518 Bytes	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 1519 to 2047 Bytes	The total number of packets (including bad packets) received that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 2048 to 4095 Bytes	The total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Received Packets 4095 to 9216 Bytes	The total number of packets (including bad packets) received that were between 4095 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 0 to 64 Bytes	The total number of packets (including bad packets) transmitted that were between 0 and 64 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 65 to 127 Bytes	The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 128 to 255 Bytes	The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Transmitted Packets 256 to 511 Bytes	The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 512 to 1023 Bytes	The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 1024 to 1518 Bytes	The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 1519 to 2047 Bytes	The total number of packets (including bad packets) transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 2048 to 4095 Bytes	The total number of packets (including bad packets) transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Transmitted Packets 4095 to 9216 Bytes	The total number of packets (including bad packets) transmitted that were between 4095 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).

intf	**Interface statistics**

Interface Name	The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `le0' or a simple port number, such as `1', depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. Note that for an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Operational Status	The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components. Values: **up** **down** **testing** **unknown** **dormant** **notPResent** **lowerLayerDown**
Received Bytes	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value ofifCounterDiscontinuityTime.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Transmitted Bytes	The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Received Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Received Errors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Received Unknown Protocols	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Table 14: MXK-F Enhanced Ethernet port statistics (Continued)

Parameter	Description
Transmitted Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Transmitted Errors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Speed Bits per Second	An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero.
Speed Megabits per Second	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is somewhere in the range of `n-500,000' to `n+499,999'. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero.

5- 4 GPON OMCI (ONT) AND PON STATISTICS

This section includes:

5- 4.1 OMCI (ONT) Statistics

The MXK obtains ONU statistics from the ONU using the ITU standardized OMCI protocol. The MXK sends standards based OMCI commands to retrieve statistics information. The statistics are maintained on the ONU in 15-minute intervals. There are 2 intervals of statistics that is stored in the ONU, current and previous. When an ONU is activated, the ONU starts storing statistics. These statistics are stored under the current category of statistics. After a 15 minute time period, the statistics value are reset. The statistics tracked during the past 15 minute period are stored as the previous interval. A new set of the current interval statistics is tracked. After every 15-minute period the current interval is saved as previous and a new current category is created with zeroed out values.

Display OMCI statistics for selected ONU(s) with the **gpononu statistics** command.

Syntax:

gpononu statistics [previous] [***slot***[***/olt***[***/onu***]|***ifName***]

previous

The system retrieves the statistics collected during the previous 15 minutes interval. Without **previous**, the system retrieves the statistics collected in current 15 minutes interval.

slot[*/olt*[*/onu*]|*ifName*

The ONU(s) users want to collect statistics on.

Example:

```
zSH> gpononu statistics previous 4/1/1
4/1/1 ONU Statistics (previous)
       Ethernet Performance Monitoring History Data - Port 1
                  32 Interval Time
                   0 Threshold Data Pointer
                   0 FCS Errors
                   0 Excessive Collision Counter
                   0 Late Collision Counter
                   0 Frame Too Long
                   0 Buffer Overflows on Receive
                   0 Buffer Overflows on Transmit
                   0 Single Collision Frame Counter
                   0 Multiple Collisions Frame Counter
                   0 SQE Counter
                   0 Deferred Transmission Counter
                   0 Internal MAC Transmit Error Counter
                   0 Carrier Sense Error Counter
                   0 Alignment Error Counter
                   0 Internal MAC Receive Error Counter
       Ethernet Performance Monitoring History Data - Port 2
                  32 Interval Time
                   0 Threshold Data Pointer
                   0 FCS Errors
                   0 Excessive Collision Counter
                   0 Late Collision Counter
                   0 Frame Too Long
                   0 Buffer Overflows on Receive
                   0 Buffer Overflows on Transmit
                   0 Single Collision Frame Counter
                   0 Multiple Collisions Frame Counter
                   0 SQE Counter
                   0 Deferred Transmission Counter
                   0 Internal MAC Transmit Error Counter
                   0 Carrier Sense Error Counter
                   0 Alignment Error Counter
                   0 Internal MAC Receive Error Counter
       Ethernet Performance Monitoring History Data - Port 3
                  32 Interval Time
                   0 Threshold Data Pointer
                   0 FCS Errors
```

```
              0 Excessive Collision Counter
              0 Late Collision Counter
              0 Frame Too Long
              0 Buffer Overflows on Receive
              0 Buffer Overflows on Transmit
              0 Single Collision Frame Counter
              0 Multiple Collisions Frame Counter
              0 SQE Counter
              0 Deferred Transmission Counter
              0 Internal MAC Transmit Error Counter
              0 Carrier Sense Error Counter
              0 Alignment Error Counter
              0 Internal MAC Receive Error Counter
Ethernet Performance Monitoring History Data - Port 4
             32 Interval Time
              0 Threshold Data Pointer
              0 FCS Errors
              0 Excessive Collision Counter
              0 Late Collision Counter
              0 Frame Too Long
              0 Buffer Overflows on Receive
              0 Buffer Overflows on Transmit
              0 Single Collision Frame Counter
              0 Multiple Collisions Frame Counter
              0 SQE Counter
              0 Deferred Transmission Counter
              0 Internal MAC Transmit Error Counter
              0 Carrier Sense Error Counter
              0 Alignment Error Counter
              0 Internal MAC Receive Error Counter
Ethernet Performance Monitoring History Data 2 - Port 1
             32 Interval Time
              0 Threshold Data Pointer
              0 PPPoE Filtered Frame Counter
Ethernet Performance Monitoring History Data 2 - Port 2
             32 Interval Time
              0 Threshold Data Pointer
              0 PPPoE Filtered Frame Counter
Ethernet Performance Monitoring History Data 2 - Port 3
             32 Interval Time
              0 Threshold Data Pointer
              0 PPPoE Filtered Frame Counter
Ethernet Performance Monitoring History Data 2 - Port 4
             32 Interval Time
              0 Threshold Data Pointer
              0 PPPoE Filtered Frame Counter
GEM Port Protocol Monitoring History Data - Port 501
        no data available
GEM Port Protocol Monitoring History Data - Port 701
        no data available
GEM Port Protocol Monitoring History Data - Port 901
        no data available
GEM Port Protocol Monitoring History Data - Port 1101
        no data available
GEM Port Protocol Monitoring History Data - Port 1301
        no data available
GEM Port Protocol Monitoring History Data - IPTV Port 4095
        no data available
Ethernet Performance Monitoring History Data 3 - Port 1
```

```
           32 Interval Time
            0 Threshold Data 1/2 id
            0 Drop Events
            0 Octets
            0 Packets
            0 Broadcast Packets
            0 Multicast Packets
            0 Undersize Packets
            0 Fragments
            0 Jabbers
            0 Packets 64 Octets
            0 Packets 65 to 127 Octets
            0 Packets 128 to 255 Octets
            0 Packets 256 to 511 Octets
            0 Packets 512 to 1023 Octets
            0 Packets 1024 to 1518 Octets
Ethernet Performance Monitoring History Data 3 - Port 2
           32 Interval Time
            0 Threshold Data 1/2 id
            0 Drop Events
            0 Octets
            0 Packets
            0 Broadcast Packets
            0 Multicast Packets
            0 Undersize Packets
            0 Fragments
            0 Jabbers
            0 Packets 64 Octets
            0 Packets 65 to 127 Octets
            0 Packets 128 to 255 Octets
            0 Packets 256 to 511 Octets
            0 Packets 512 to 1023 Octets
            0 Packets 1024 to 1518 Octets
Ethernet Performance Monitoring History Data 3 - Port 3
           32 Interval Time
            0 Threshold Data 1/2 id
            0 Drop Events
            0 Octets
            0 Packets
            0 Broadcast Packets
            0 Multicast Packets
            0 Undersize Packets
            0 Fragments
            0 Jabbers
            0 Packets 64 Octets
            0 Packets 65 to 127 Octets
            0 Packets 128 to 255 Octets
            0 Packets 256 to 511 Octets
            0 Packets 512 to 1023 Octets
            0 Packets 1024 to 1518 Octets
Ethernet Performance Monitoring History Data 3 - Port 4
           32 Interval Time
            0 Threshold Data 1/2 id
            0 Drop Events
            0 Octets
            0 Packets
            0 Broadcast Packets
            0 Multicast Packets
            0 Undersize Packets
```

```
0 Fragments
0 Jabbers
0 Packets 64 Octets
0 Packets 65 to 127 Octets
0 Packets 128 to 255 Octets
0 Packets 256 to 511 Octets
0 Packets 512 to 1023 Octets
0 Packets 1024 to 1518 Octets
```

Table 15 defines the OMCI statistics displayed in the **gpononu statistics** command.

Table 15: OMCI Statistics Attributes

Attribute	Description
Interval end time	This attribute identifies the most recently finished 15-minute interval.
Threshold data pointer	This attribute points to an instance of the threshold data 1 and 2 managed entities that contains Performance Monitoring threshold values.
FCS errors	This attribute counts frames received on a particular interface that were an integral number of octets in length but failed the frame check sequence (FCS) check. The count is incremented when the MAC service returns the frameCheckError status to the link layer control (LLC) or other MAC user. Received frames for which multiple error conditions are obtained are counted according to the error status presented to the LLC.
Excessive collision counter	This attribute counts frames whose transmission failed due to excessive collisions.
Late collision counter	This attribute counts the number of times that a collision was detected later than 512 bit times into the transmission of a packet.
Frames too long	This attribute counts received frames that exceeded the maximum permitted frame size. The count is incremented when the MAC service returns the frameTooLong status to the LLC.
Buffer overflows on receive	This attribute counts the number of times that the receive buffer overflowed.
Buffer overflows on transmit	This attribute counts the number of times that the transmit buffer overflowed.
Single collision frame counter	This attribute counts successfully transmitted frames whose transmission was delayed by exactly one collision.
Multiple collisions frame counter	This attribute counts successfully transmitted frames whose transmission was delayed by more than one collision.
SQE counter	This attribute counts the number of times that the SQE test error message was generated by the PLS sublayer.
Deferred transmission counter	This attribute counts frames whose first transmission attempt was delayed because the medium was busy. The count does not include frames involved in collisions.

Table 15: OMCI Statistics Attributes

Attribute	Description
Internal MAC transmit error counter	This attribute counts frames whose transmission failed due to an internal MAC sublayer transmit error.

5- 4.2 PON Statistics

This section includes the following topics:

- View OLT Statistics, page 141
- View ONU Statistics, page 148

PON statistics are the OLT or ONU statistics collected and reported by the MXK-F OLT.

The Downstream stats are the stats that were sent from the MXK to the ONU, and the upstream stats was sent from the ONU to the MXK.

5- 4.2.1 View OLT Statistics

The MXK-F OLT can report these stats types for an OLT interface: GPON physical layer stats for OLT (i.e. gpon), Ethernet layer stats (i.e. rmon), and interface layer stats (i.e. intf). The GPON physical layer stats are only available on OLT interfaces.

The MXK-F OLT can report these stats types for an ONU interface: ONU physical layer stats for ONU (i.e. onu) and interface layer stats (i.e. intf). The ONU physical layer stats are only available on ONU interfaces.

Collects and display OLT and ONU statistics with the **port statistics** command when specifying an OLT or ONU interface in the *interface name/type*.

Syntax:

port stats *interface name*/*type stats options*

interface name

interface name, in the format of *shelfID-SlotID-OLTID-ONUID*

Type

interface type. e.g. *gponolt*, *gpononu*, eth, linegroup, etc.

To display stats for the OLT or ONU interface, users must use either *gponolt* or *gpononu* as the *type*.

StatsType

statistics type. The possible stats types are:

- **intf**

refers to mib2 interface statistics. intf is the default value, if there is no stats type specified, system shows intf stats. It is valid for all interface type.

- **rmon**

  refers to ethernet remote monitoring statistics. It is valid for ethernet or gponolt interfaces.

- **eth**

  refers to ethernet dot3 statistics.

- **olt**

  refers to GPON OLT traffic management statistics. It is valid for **gponolt** interfaces only.

- **onu**

  refers to GPON ONU error statistics as reported by the MXK OLT. It is valid for **gpononu** interfaces only.

- **all**

  refers to all statistics relevant to the interface type.

Procedure: *Viewing OLT Statistics*

1 When specifying **all** as the stats type, the rmon, OLT and interface stats are displayed for this OLT interface.

```
zSH> port stats 1-3-1-0/gponolt all
******  rmon  ******

Total Dropped Events                          0
Total Dropped Frames                          0
Total Bytes                                   866284
Total Packets                                 10426
Transmitted Packets                           7942
Received Packets                              2484
Transmitted Multicast Bytes                   0
Received Multicast Bytes                      0
Received Multicast Dropped Bytes              0
Transmitted Average Throughput                456
Received Average Throughput                   160
Transmitted Bandwidth Occupancy               0
Received Bandwidth Occupancy                  0
Total Broadcast Packets                       38
Total Multicast Packets                       5494
CRC Align Errors                              0
Undersize Packets                             0
Oversize Packets                              0
Transmitted Oversize Packets                  0
Received Oversize Packets                     0
Fragments                                     0
Jabbers                                       0
Collisions                                    0
Transmitted No Errors                         7942
Received No Errors                            2484
```

```
IPMC Bridged Packets                          0
IPMC Routed Packets                           0
Transmitted IPMC Dropped Packets              0
Received IPMC Dropped Packets                 0
Total Packets 0 to 64 Bytes                   0
Total Packets 65 to 127 Bytes                 10403
Total Packets 128 to 255 Bytes                0
Total Packets 256 to 511 Bytes                23
Total Packets 512 to 1023 Bytes               0
Total Packets 1024 to 1518 Bytes              0
Total Packets 1519 to 2047 Bytes              0
Total Packets 2048 to 4095 Bytes              0
Total Packets 4095 to 9216 Bytes              0
Received Packets 0 to 64 Bytes                0
Received Packets 65 to 127 Bytes              2473
Received Packets 128 to 255 Bytes             0
Received Packets 256 to 511 Bytes             11
Received Packets 512 to 1023 Bytes            0
Received Packets 1024 to 1518 Bytes           0
Received Packets 1519 to 2047 Bytes           0
Received Packets 2048 to 4095 Bytes           0
Received Packets 4095 to 9216 Bytes           0
Transmitted Packets 0 to 64 Bytes             0
Transmitted Packets 65 to 127 Bytes           7930
Transmitted Packets 128 to 255 Bytes          0
Transmitted Packets 256 to 511 Bytes          12
Transmitted Packets 512 to 1023 Bytes         0
Transmitted Packets 1024 to 1518 Bytes        0
Transmitted Packets 1519 to 2047 Bytes        0
Transmitted Packets 2048 to 4095 Bytes        0
Transmitted Packets 4095 to 9216 Bytes        0

******  olt  ******

Upstream Valid Gem Frames                     2484
Upstream Discarded Frames                     0
Upstream Gem Frames                           2484
Upstream Omci Frames                          2446
Upstream Ploam Frames                         11009722
Upstream Idle Ploam Frames                    11005260
Downstream Valid Gem Frames                   7943
Downstream Discarded Frames                   3
Downstream Gem Frames                         7946
Downstream Omci Frames                        2410
Downstream Ploam Frames                       7836
Downstream Idle Ploam Frames                  0
Downstream Pon Valid Ethernet Packtes         5530
Downstream Pon Cpu Packets                    2409
Downstream Transmitted Bytes                  517230
Upstream Pon Valid Packets                    38
Upstream Pon Valid Not Idle Ploams            4462
Upstream Pon Error Ploams                     0
Upstream Pon Invalid Packets                  0
Upstream Dropped Packets                      0
Upstream Dropped Ploams Fifo Full             0
Downstream TM Valid Packets                   7943
Downstream TM Crc Packets                     0
Downstream TM Dropped Cpu Packets             0
Downstream TM MAC Lookup Miss                 0
```

```
Downstream TM Packets Forwarded From Hm To Pon            5530
Downstream TM Packets Dropped Gem Pid Not Enabled         3
Downstream TM Q0 Valid Packets                            5533
Downstream TM Q0 Dropped Packets                          0
Downstream TM Q1 Valid Packets                            0
Downstream TM Q1 Dropped Packets                          0
Downstream TM Q2 Valid Packets                            0
Downstream TM Q2 Dropped Packets                          0
Downstream TM Q3 Valid Packets                            0
Downstream TM Q3 Dropped Packets                          0
Downstream TM Q4 Valid Packets                            0
Downstream TM Q4 Dropped Packets                          0
Downstream TM Q5 Valid Packets                            0
Downstream TM Q5 Dropped Packets                          0
Downstream TM Q6 Valid Packets                            0
Downstream TM Q6 Dropped Packets                          0
Downstream TM Q7 Valid Packets                            0
Downstream TM Q7 Dropped Packets                          0
Upstream TM Dropped Cpu Packets                           0
Upstream TM Dropped Packets Crc Error                     0
Upstream TM Dropped Packets Security                      0
Upstream TM Learn Failures                                0
Upstream TM Q0 Valid Packets                              38
Upstream TM Q0 Dropped Packets                            0
Upstream TM Q1 Valid Packets                              0
Upstream TM Q1 Dropped Packets                            0
Upstream TM Q2 Valid Packets                              0
Upstream TM Q2 Dropped Packets                            0
Upstream TM Q3 Valid Packets                              0
Upstream TM Q3 Dropped Packets                            0
Upstream TM Q4 Valid Packets                              0
Upstream TM Q4 Dropped Packets                            0
Upstream TM Q5 Valid Packets                              0
Upstream TM Q5 Dropped Packets                            0
Upstream TM Q6 Valid Packets                              0
Upstream TM Q6 Dropped Packets                            0
Upstream TM Q7 Valid Packets                              0
Upstream TM Q7 Dropped Packets                            0


******  intf  ******

Interface Name                                            1-3-1-0
Operational Status                                        Up
Received Bytes                                            225530
Received Packets                                          2467
Received Multicast Packets                                0
Received Broadcast Packets                                17
Transmitted Bytes                                         640830
Transmitted Unicast Packets                               2427
Transmitted Multicast Packets                             5495
Transmitted Broadcast Packets                             21
Received Discards                                         2472
Received Errors                                           0
Received Unknown Protocols                                0
Transmitted Discards                                      5504
Transmitted Errors                                        0
Speed Bits per Second                                     *** n/a ***
Speed Megabits per Second                                 2400
```

2 When specifying **olt** as the stats type, only the GPON OLT physical layer statistics are displayed for this OLT interface.

```
zSH> port stats 1-3-1-0/gponolt olt
Upstream Valid Gem Frames                          8591
Upstream Discarded Frames                          0
Upstream Gem Frames                                8591
Upstream Omci Frames                               4645
Upstream Ploam Frames                              34031574
Upstream Idle Ploam Frames                         34017856
Downstream Valid Gem Frames                        14400
Downstream Discarded Frames                        3
Downstream Gem Frames                              14403
Downstream Omci Frames                             4588
Downstream Ploam Frames                            12045
Downstream Idle Ploam Frames                       0
Downstream Pon Valid Ethernet Packtes              9809
Downstream Pon Cpu Packets                         4585
Downstream Transmitted Bytes                       920581
Upstream Pon Valid Packets                         3946
Upstream Pon Valid Not Idle Ploams                 13718
Upstream Pon Error Ploams                          0
Upstream Pon Invalid Packets                       0
Upstream Dropped Packets                           0
Upstream Dropped Ploams Fifo Full                  0
Downstream TM Valid Packets                        14400
Downstream TM Crc Packets                          0
Downstream TM Dropped Cpu Packets                  0
Downstream TM MAC Lookup Miss                      0
Downstream TM Packets Forwarded From Hm To Pon     9809
Downstream TM Packets Dropped Gem Pid Not Enabled  3
Downstream TM Q0 Valid Packets                     9812
Downstream TM Q0 Dropped Packets                   0
Downstream TM Q1 Valid Packets                     0
Downstream TM Q1 Dropped Packets                   0
Downstream TM Q2 Valid Packets                     0
Downstream TM Q2 Dropped Packets                   0
Downstream TM Q3 Valid Packets                     0
Downstream TM Q3 Dropped Packets                   0
Downstream TM Q4 Valid Packets                     0
Downstream TM Q4 Dropped Packets                   0
Downstream TM Q5 Valid Packets                     0
Downstream TM Q5 Dropped Packets                   0
Downstream TM Q6 Valid Packets                     0
Downstream TM Q6 Dropped Packets                   0
Downstream TM Q7 Valid Packets                     0
Downstream TM Q7 Dropped Packets                   0
Upstream TM Dropped Cpu Packets                    0
Upstream TM Dropped Packets Crc Error              0
Upstream TM Dropped Packets Security               0
Upstream TM Learn Failures                         0
Upstream TM Q0 Valid Packets                       3946
Upstream TM Q0 Dropped Packets                     0
Upstream TM Q1 Valid Packets                       0
Upstream TM Q1 Dropped Packets                     0
Upstream TM Q2 Valid Packets                       0
```

```
Upstream TM Q2 Dropped Packets                    0
Upstream TM Q3 Valid Packets                      0
Upstream TM Q3 Dropped Packets                    0
Upstream TM Q4 Valid Packets                      0
Upstream TM Q4 Dropped Packets                    0
Upstream TM Q5 Valid Packets                      0
Upstream TM Q5 Dropped Packets                    0
Upstream TM Q6 Valid Packets                      0
Upstream TM Q6 Dropped Packets                    0
Upstream TM Q7 Valid Packets                      0
Upstream TM Q7 Dropped Packets                    0
```

Table 16 defines the GPON OLT physical layer statistics displayed in the **port stats** *ifName*/**gponolt** command.

Note that the Downstream stats are the stats that were sent from MXK to ONU, and the upstream stats was sent from ONU to MXK.

Table 16: GPON OLT Physical Layer Statistics Attributes

Attribute	Description
Upstream Valid Gem Frames	The number of valid GEM frames sent in upstream direction.
Upstream Discarded Frames	Total number of discarded GEM frames sent in upstream direction.
Upstream Gem Frames	The number of GEM frames sent in the upstream direction.
Upstream Omci Framers	The number of OMCI frames sent in the upstream direction.
Upstream Ploam Frames	Total number of Physical Layer Operations, Administration and Maintenance (PLOAM) frames sent in the upstream direction. This includes: • Total number of PLOAM messages, including idle PLOAMs. • Total number of valid PLOAM messages (not including idle PLOAMs) • Total number of PLOAM messages dropped due to Cyclic Redundancy Check (CRC) errors.
Upstream Idle Ploam Frames	Total number of idle PLOAM frames sent in upstream direction.
Downstream Valid Gem Frames	Total number of valid GEM frames sent in downstream direction.
Downstream Discarded Frames	The number of downstream packets discarded due to CRC errors, MAC lookup miss, congestion, etc.
Downstream Gem Frames	Total number of GEM frames sent in downstream direction.
Downstream Omci Frames	Total number of OMCI frames sent in downstream direction.

Table 16: GPON OLT Physical Layer Statistics Attributes (Continued)

Attribute	Description
Downstream Ploam Frames	Total number of PLOAM frames sent in downstream direction.
Downstream Idle Ploam Frames	Total number of idle PLOAM frames sent in downstream direction.
Downstream PON Valid Ethernet Packets	Total number of valid Ethernet packets sent in downstream direction.
Downstream PON CPU Packets	The number of downstream packets generated by the CPU (MIPS).
Downstream Transmitted Bytes	Total number of bytes transmitted sent in downstream direction.
Upstream PON Valid Packets	Total number of valid PON packets sent in upstream direction.
Upstream PON Valid Not Idle Ploams	Total number of valid non-idle PLOAM messages sent in upstream direction.
Upstream PON Error Ploams	Total number of PON error PLOAM messages sent in upstream direction.
Upstream PON Invalid Packets	The number of upstream errored packets.
Upstream Dropped Packets Inactive Ports	Total number of upstream packets that were dropped because the GEM port ID was not configured.
Upstream Dropped Ploams Fifo Full	Total number of upstream PLOAMs that were dropped because the FIFO buffer was full.
Downstream TM Valid Packets	Total number of valid packets that were sent in downstream direction.
Downstream TM Crc Packets	The number of dropped downstream packets due to CRC errors.
Downstream TM Dropped Cpu Packets	The number of dropped downstream packets originated by the CPU (MIPS).
Downstream TM MAC Lookup Miss	The number of downstream MAC lookup miss events.
Downstream TM Packets Forwarded From Hm To PON	The number of downstream packets forwarded from the header modification stage to the PON.

Table 16: GPON OLT Physical Layer Statistics Attributes (Continued)

Attribute	Description
Downstream TM Packets Dropped Gem Pid Not Enabled	The number of downstream packets dropped because the GEM port ID was not configured correctly.
Downstream TM QN Valid Packets (N=0 to 7)	The number of downstream packets forwarded by egress priority queue [0 to 7] to the PON. Queue 0 is the highest priority; queue 7 is the lowest priority. Packets in the lowest priority queues are dropped first. When the PON link is not active, this counter will not increment.
Downstream TM QN Dropped Packets (N=0 to 7)	The number of downstream packets dropped by egress priority queue [0 to 7] due to congestion. Queue 0 is the highest priority; queue 7 is the lowest priority. Packets in the lowest priority queues are dropped first. When the PON link is not active, this counter will not increment.
Upstream TM Dropped Cpu Packets	The number of upstream packets dropped by the CPU(MIPS), not sent to SGMI interface.
Upstream TM Dropped Packets Crc Error	The number of upstream packets that were dropped because of CRC errors.
Upstream TM Dropped Packets Security	Total number of upstream packets that were dropped because they didn't pass the security rules.
Upstream TM Learn Failures	MAC address learning failures from traffic sent in upstream direction that were due to a full FIFO buffer.
Upstream TM QN Valid Packets (N=0 to 7)	Number of upstream packets forwarded by egress priority queue [0 to 7] to the MXK. Queue 0 is the highest priority; queue 7 is the lowest priority. Packets in the lowest priority queues are dropped first. When the PON link is not active, this counter will not increment.
Upstream TM QN Dropped Packets (N=0 to 7)	Number of upstream packets dropped by egress priority queue [0 to 7] due to congestion. Queue 0 is the highest priority; queue 7 is the lowest priority. Packets in the lowest priority queues are dropped first. When the PON link is not active, this counter will not increment.

5- 4.2.2 View ONU Statistics

Procedure: *Viewing ONU Statistics*

1 When specifying **onu** as the stats type, the ONU physical layer statistics are displayed for this ONU interface.

```
zSH> port stats 1-3-1-1/gpononu onu
Upstream BIP8 Errors                                0
Upstream FEC Corrected Bytes                        0
Upstream FEC Corrected Code-words                   0
Upstream FEC Uncorrectable Code-words               0
```

```
Upstream Received Code-words                    0
Upstream Unreceived Bursts                      0
Downstream Remote BIP8 Errors                   0
Upstream Remote BIP8 Errors                     0
Drift Of Window Indications                     0
Message Error Message                           0
```

2 When specifying **all** as the stats type, only ONU stats type is displayed for the ONU interface.

```
zSH> port stats 1-3-1-1/gpononu all
Upstream BIP8 Errors                            0
Upstream FEC Corrected Bytes                    0
Upstream FEC Corrected Code-words               0
Upstream FEC Uncorrectable Code-words           0
Upstream Received Code-words                    0
Upstream Unreceived Bursts                      0
Downstream Remote BIP8 Errors                   0
Upstream Remote BIP8 Errors                     0
Drift Of Window Indications                     0
Message Error Message                           0
```

Table 17 defines the GPON ONU physical layer statistics displayed in the **port stats** *interface/gpononu* command.

Table 17: GPON ONU Physical Layer Statistics Attributes

Attribute	Description
Upstream BIP8 Errors	Total number of upstream Bit-Interleaved Parity with eight bit (BIP8) errors per ONU-ID.
Upstream FEC Corrected Bytes	Total number of upstream FEC corrected bytes per ONU-ID.
Upstream FEC Corrected Code-words	Total number of upstream FEC corrected code words per ONU-ID.
Upstream FEC Uncorrectable Code-words	Total number of upstream FEC uncorrected code words per ONU-ID.
Upstream Received Code-words	Total number of upstream code words transmitted per ONU-ID.
Upstream Unreceived Bursts	Total number of upstream un-received bursts per ONU-ID.
Downstream Remote BIP8 Errors	Total number of downstream remote BIP8 errors per ONU-ID.

Table 17: GPON ONU Physical Layer Statistics Attributes

Attribute	Description
Upstream Remote BIP8 Errors	Total number of upstream remote BIP8 errors per ONU-ID.
Drift Of Window Indications	The number of times the average drift for the ONU exceeds the drift threshold.
Message Error Message	The number of error messages sent from the ONU.

INDEX

R

S

T

Z