

DATACOM



DmOS

DmOS 8.0.2 - Troubleshooting Guide

204.4293.23

LEGAL NOTICE

Although every precaution has been taken in the preparation of this document, DATACOM takes no responsibility for possible errors or omissions, and it will accept no obligation for damages resulting from the use of the information contained in this manual. The specifications provided in this manual are subject to changes without notice, and they will not be recognized as any kind of contract.

© 2017 DATACOM - All rights reserved.

WARRANTY

This product is warranted against material and workmanship defects for the period specified in the sales invoice.

The warranty only includes the repair and replacement of defective components and parts without any resulting burden to the customer. Defects resulting from the following are not covered: improper use of device, faulty electrical power network, nature-related events (lightning discharges, for instance), failure in devices connected to this product, installations with improper grounding or repairs made by personnel not authorized by DATACOM.

This warranty does not cover repairs at the customer's facilities. Equipment must be forwarded for repairs to DATACOM.

CONTACTS

Technical Support

DATAKOM offers a technical support call center to support customers during configuration and use of its equipment, and also to provide a technical assistance for product maintenance and repair.

DATAKOM Technical Support can be reached through the following channels:

e-mail: suporte@datacom.ind.br

phone: +55 51 3933-3122

website: www.datacom.ind.br/en/support

General Information

For any additional information, visit <http://www.datacom.ind.br/en> or contact:

DATAKOM

Rua América, 1000

92990-000 - Eldorado do Sul - RS - Brazil

+55 51 3933-3000

PRODUCT DOCUMENTATION

This manual is part of a set of documents prepared to provide all necessary information about DATACOM products, whether you are a buyer, administrator, manager or operator.

Software Platform - DmOS

- **Command Reference** - Provides all the commands related to the product (only in English)
- **Quick Start Guide** - Provides instructions on how to set functionalities in a quick manner in the equipment
- **Release Notes** - Provides instructions on the new functionalities, identified defects and compatibilities between Software and Hardware
- **Troubleshooting Guide** - Provides instructions on how to analyze, identify and solve problems with the product (only in English)

Hardware Platform

- **Datasheet** - Provides the product technical characteristics
- **Installation Guide** - Provides instructions on the procedures covering product installation

The availability of certain documents may vary depending on the product.

Visit the DATACOM website to locate related documentation for a product or contact Customer Support (see [Contacts](#)).

INTRODUCTION

About this Guide

This guide provides some tips to troubleshoot on DmOS platforms. The document was designed to serve as a source of eventual queries. Therefore, it does not need be read sequentially. So, if an information about how to troubleshoot a specific alarm is required, it will be provided comprehensively, in an own chapter.

It is assumed that the individual or individuals managing any aspect of this product have basic understanding of Ethernet, GPON and Telecommunications networks.

For information about the specific hardware platform supported, refer to the *Installation Guide*.


Intended Audience







This guide is intended for Network Administrators and other qualified service personnel responsible for configuring and maintaining network equipments.

Conventions

In order to improve the agreement, the following conventions are made throughout this guide:

Icons Convention

Icon	Type	Description
	Note	Notes give an explanation about some topic in the foregoing paragraph.

Icon	Type	Description
	Note	WEEE Directive Symbol (Applicable in the European Union and other European countries with separate collection systems). This symbol on the product or its packaging indicates that this product must not be disposed of with other waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your consumer waste equipment for recycling, please contact your local city recycling office or the dealer from whom you originally purchased the product.
	Warning	This symbols means that, case the procedure was not correctly followed, may exist electrical shock risk.
	Warning	Represents laser radiation. It is necessary to avoid eye and skin exposure.
	Warning	Non-ionizing radiation emission.
	Caution	This symbol means that this text is very important and, if the orientations were not correct followed, it may cause damage or hazard.
	Caution	Indicates that equipment, or a part is ESDS (Electrostatic Discharge Sensitive). It should not be handled without grounding wrist strap or equivalent.



A caution type notice calls attention to conditions that, if not avoided, may damage or destroy hardware or software.



A warning type notice calls attention to conditions that, if not avoided, could result in death or serious injury.

Text Convention

This guide uses these text conventions to convey instructions and information:

Convention	Description
Hyperlink	Internet site or an e-mail address. It is also applied to indicate a local link inside the document itself (e.g. a chapter)
<code>Screen</code>	System commands and screen outputs.
<i>Object</i>	Indicates a reference to something. Used to emphasize this referenced object.
Menu > Path	GUI menu paths
[Key]	Keyboard buttons



The text convention shown above differs from *Command Line Interface* syntax convention. See the convention related to commands on [Command Syntax](#).

Table of Contents

Chapter 1: Product Concept	9
Chapter 2: Using the Command-Line Interface	10
Command Syntax	10
Common Parameter Values	11
Using the "No" Form of a Command	11
CLI Output Filtering	11
Command Modes	13
Command Completion and Abbreviation	13
CLI Error Messages	14
CLI Line-Editing Conventions	14
Using CLI Help	16
Accessing the CLI	17
Chapter 3: Alarms Overview	19
Alarms Severity	19
Alarms Status	20
How to check alarms	20
Understanding alarms	20
Chapter 4: Alarms	22
EAPS	22
Loopback Detection	24
Backup Link	25
L2VPN	27
Continuity Check and Fault Management	28
EFM	34
OLT	35
ONU	39
Environment	62
CPU	73

CHAPTER 1: PRODUCT CONCEPT

DmOS offers a Carrier Grade solution to meet the growing needs of Service Providers, which require stringent SLA (Service Level Agreement) for their Ethernet Services.

That product can be managed by using one of the following four methods:

- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)
- NETCONF
- NMS (DmView)

Each of the management methods enables you to configure, manage, and control the software locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private MIB providing control for functions not completely specified in the MIBs.

CHAPTER 2: USING THE COMMAND-LINE INTERFACE

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- [Command Syntax](#)
- [Common Parameter Values](#)
- [Using the "No" Form of a Command](#)
- [CLI Output Filtering](#)
- [Command Modes](#)
- [Command Completion and Abbreviation](#)
- [CLI Error Messages](#)
- [CLI Line-Editing Conventions](#)
- [Using CLI Help](#)
- [Accessing the CLI](#)

COMMAND SYNTAX

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **show ip route** or **clear mac address-table**, do not require parameters. Other commands, such as **aaa authentication**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **aaa authentication** command syntax:

```
aaa authentication user username password password [group admin | config | audit]
```

- **aaa authentication** is the command name.
- **user** and **password** are parameters and represent required options that user must enter after the command keyword.

-
- `username` and `password` are required parameters that user must enter after the **user** and **password** keywords, respectively.
 - `[group {admin | config | audit}]` is an optional parameter that could be (or could not be) inserted after the **password** `password` parameter. Only one of the available values (`admin`, `config` or `audit`) must be typed after the **group** keyword.

The *Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- **Format:** shows the command keywords and the required and optional parameters.
- **Mode:** identifies the command mode you must be in to access the command.
- **Default:** shows the default value, if any, of a configurable setting on the device.

The show commands also contain a description of the information that the command shows.

COMMON PARAMETER VALUES

Parameter values might be names (strings) or numbers. Spaces could be used as part of a name parameter only for `line<N>` parameters, without any kind of delimiter. For example, the expression *System Name with Spaces* will be recognized as a unique value when used as a parameter for the command **snmp-server contact**. Empty strings are not valid user-defined strings.

USING THE "NO" FORM OF A COMMAND

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form to reverse the action of a command or reset a value back to the default. For example, the **no shutdown** configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the **no** form.

CLI OUTPUT FILTERING

Many CLI show commands include considerable content to display to the user. This can make output confusing and cumbersome to parse through to find the information

of desired importance. The CLI Output Filtering feature allows the user, not only when executing CLI show display commands, but specially on these cases, to optionally specify arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI Output Filtering feature are:

- **Pagination Control**
 - Supports enabling/disabling paginated output for all CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue. `-- more --`, next page: Space, continue: g, quit: ^C is displayed at the end of each page.
 - When pagination is enabled, press the return key to advance a single line, press q, Q or Ctrl+C to stop pagination, press g or G to continue up to the end of the output, or press any other key to advance a whole page. These keys are not configurable.
- **Output Filtering**
 - "Grep"-like control for modifying the displayed output to only show the user-desired content.
 - Filter displayed output to only include lines containing a specified string match.
 - Filter displayed output to exclude lines containing a specified string match.
 - Filter displayed output to only include lines including and following a specified string match.
 - String matching should be case insensitive.
 - Pagination, when enabled, also applies to filtered output.

Example: The following shows an example of the extensions made to the CLI commands for the Output Filtering feature.

```
DmOS# show running-config ?
```

```
Possible completions:
```

aaa	Configure authentication, authorization and accounting
alias	Create command alias.
anti-ip-spoofing	Anti ip-spoofing configuration

clock	Set the system clock
dot1q	VLAN Manager Protocol
gpon	GPON configuration
	Output modifiers

```
DmOS# show running-config | ?
```

Possible completions:

append	Append output text to a file
begin	Begin with the line that matches
best-effort	Display data even if data provider is unavailable or continue loading from file in presence of failures
count	Count the number of lines in the output
csv	Show table output in CSV format
de-select	De-select columns
details	Display default values

COMMAND MODES

The CLI groups the commands into modes, according to the command function. Each of the command modes supports specific software commands. The commands in a particular mode will not be available until you switch to that given mode. You can execute Operational commands in the Configure commands mode by using the **do** keyword.

COMMAND COMPLETION AND ABBREVIATION

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the TAB key to complete the word or press SPACE BAR and let that system resolves the command directly from the short version.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

```
DmOS# re
```

Possible completions:

reboot	Reboot the system
reboot-forced	Reboot the system without any checks

```
request          Request system operations
```

```
DmOS(config)# interface gigabit-ethernet 1/1/
```

Possible completions:

```
1 2 3 4 5 6 7 8 9 10 11 12
```



The TAB key will complete the command if there is only one candidate command. Otherwise, a list of all possible commands will be showed.

CLI ERROR MESSAGES

If you enter a command and the system is unable to execute it, an error message appears. Table 1: CLI Error Messages describes the most common CLI error messages.

Table 1: CLI Error Messages

Message Text	Description
<code>syntax error: unknown command</code>	Indicates that the command there is not in the CLI.
<code>syntax error: unknown argument</code>	Indicates that the argument there is not for the command.
<code>syntax error: unknown element</code>	Indicates that the value inserted there is not for the command.

CLI LINE-EDITING CONVENTIONS

Table 2: CLI Editing Conventions describes the key combinations you can use to edit commands or increase the speed of command entry.

Table 2: CLI Editing Conventions

Key Sequence	Description
Ctrl-H or Backspace	Delete previous character.
Ctrl-A	Go to beginning of line.
Ctrl-E	Go to end of line.
Ctrl-F	Go forward one character.
Ctrl-B	Go backward one character.
Ctrl-D	Delete current character.
Ctrl-U or Ctrl-X	Delete to beginning of line.
Ctrl-K	Delete to end of line.
Ctrl-W	Delete previous word.
Ctrl-P	Go to previous line in history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Z	Return to root command prompt.
<Tab>	Command-line completion.
Exit	Go to next lower command prompt.

Table 2: CLI Editing Conventions

Key Sequence	Description
?	List available commands, keywords, or parameters.

USING CLI HELP

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
DmOS# ?
```

```
Possible completions:
```

autowizard	Automatically query for mandatory elements
clear	Clear equipment settings and counters
commit	Confirm a pending commit
compare	Compare running configuration to another configuration or a file
complete-on-space	Enable/disable completion on space
config	Manipulate software configuration information
copy	Copy files to a remote server
display-level	Configure show command display level
exit	Exit the management session

```
DM4610(config)# ?
```

```
Possible completions:
```

aaa	Configure authentication, authorization and accounting
alias	Create command alias.
anti-ip-spoofing	anti ip-spoofing configuration
clear	Clear equipment settings and counters
clock	Set the system clock
copy	Copy a list entry
dot1q	VLAN Manager Protocol
gpon	GPON configuration
hostname	Hostname for this equipment

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
DmOS(config)# router static ?
```

Possible completions:

```
<a.b.c.d/x> or <x:x:x:x::x/x>    IP/IPv6 prefix <network>/<length>  
0.0.0.0/0
```

```
DmOS(config)# interface gigabit-ethernet ?
```

Possible completions:

```
<id:string>  1/1/1  1/1/2  1/1/3  1/1/4  1/1/5  1/1/6  1/1/7  1/1/8  1/1/9  
1/1/10  1/1/11  1/1/12
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
DmOS# show i?
```

Possible completions:

```
interface    Status information about interfaces  
inventory    Physical inventory information  
ip           Display ip information  
ipv6         Display ipv6 information  
|           Output modifiers  
<cr>
```

ACCESSING THE CLI

You can access the CLI by using a direct console connection or by using a SSH connection from a remote management host.

To establish a terminal connection using console interface (VT100), a proper serial cable (provided with the equipment) must be connected between the equipment terminal port and the PC serial port.

Take care to avoid potential difference between RJ45 pin 4 from Switch (signal ground) and DB9 pin 5 from the PC. If it occurs, it may cause damages to the PC and to the equipment's serial interfaces.

To access the terminal, select the serial port of your preference and set the following values on the VT100 emulator (factory default values of equipment):

- Baud Rate: 9600bit/s
- Data: 8 bits
- Flow Control: none
- Stop Bit: 1 bit
- Parity: none

Once the access was successful, a login screen must appear. The login factory defaults are:

- User: admin
- Password:

For the initial connection, you could use also a SSH client, connecting an Ethernet port of your PC to the management port of the switch (10/100Base-T) and accessing the default IP address: 192.168.0.25 (with a 255.255.255.0 subnet mask and without a default gateway), with the same credentials of VT100 terminal. You can set the network configuration information manually, or you can configure the system to accept these settings from a DHCP server on your network. For more information, see Network Interface Commands.

CHAPTER 3: ALARMS OVERVIEW

This chapter gives a overview to understanding about the alarms in DmOS.

ALARMS SEVERITY

Alarms in DmOS can be classified into three levels of severity: Critical, Major and Minor.

- **Critical** (Critical alarms) - Conditions that impact the equipment operation and require immediate correction action. Some examples:
 - One or more hardware components have failed.
 - One or more components have exceeded temperature thresholds.
 - Memory available is lower than 100 MB.
- **Major** (High priority alarms) - Conditions that impact the equipment operation but are not critical. The condition should be investigated to verify the need for immediate action. However, some corrective action is required. Some examples:
 - One or more components have errors and could no be read.
 - Memory available is lower than 300 MB.
 - The overall CPU core usage average is higher than 90%.
- **Minor** (Low priority alarms) - Alarm condition does not prevent the operation of equipment, but the condition must be examined, monitoring and if necessary corrected for not to become more serious. Some examples:
 - The overall CPU core usage average is higher than 70%.
 - FAN speed is above of secure speed threshold.



When a alarm is activated one trap is generated with Critical, Major or Minor severity. On the other hand, when a alarm is disactivated another trap is generated but with **clear** severity, signaling that alarm is not more activated.



Some alarms has more than one severity like CPU and Memory.

ALARMS STATUS

Alarms in DmOS can have two status: Active and Unstable.

- **Active** - Informs that alarm is activated on equipment and some action is necessary to clear.
- **Unstable** - nforms that alarm is activated on equipment but is flapping. This status is detected when at least 5 transactions of alarm have occurred in the last 90 seconds.

HOW TO CHECK ALARMS

CLI (Command Line Interface) can be used to check alarms. The CLI is accessed by using a direct console connection or by using a TELNET or SSH connection from a remote management terminal. Also it is possible to check alarms through DmView. The available command to check alarms in CLI is **show alarm**.

```
DM4610# show alarm
```

Triggered on	Severity	Source	Status	Name	Description
2017-10-17 14:31:30 UTC	CRITICAL	gpon-1/1/1/127	Active	GPON_LOSi	ONU Loss of signal

- **Triggered on** - Time when alarm was triggered.
- **Severity** - Severity of alarm.
- **Source** - Source interface which triggered alarm.
- **Status** - Status of alarm.
- **Name** - Name of alarm. The prefixed "*" is used when the alarm is unstable status.
- **Description** - Description of alarm.

UNDERSTANDING ALARMS

For each alarm presented on the next chapter, the follows items will be showed:

- **Description** - Informs in more details the alarm meaning.
- **Default Severity** - Informs the alarm severity.

- **Impact** - Informs the impacts on equipment due to alarm presence.
- **Possible Cause** - Informs the possible causes for alarm to be activated.
- **Suggestion Action** - Informs some possible actions to help the operator to clear alarm.
- **Trap Name** - Informs the name of trap. The user can to check more details in specific MIB using trap name.

CHAPTER 4: ALARMS

EAPS

EAPS_RING_FAILED

Description

EAPS domain entered on failed state.

Default Severity

Major

Impact

The secondary port of the Master in the EAPS ring will open.
A few loss of protected traffic due to the convergence of EAPS ring.

Possible Cause

There is one or more link failures in EAPS ring.
Wrong configuration of Control VLAN in equipment's of EAPS ring.

Suggested Action

Check control-vlan configurations on equipment's of EAPS ring.
Check the connectivity of links in EAPS ring.

Traps

None

EAPS_FAIL_TIMER_EXPIRED

Description

Fail Timer configured in Master equipment expired because EAPS domain missed consecutive health checks.

Default Severity

Major

Impact

None. But there is some problem in network. The EAPS can go to incomplete state if the Master equipment receive a LINK-DOWN message.

Possible Cause

EAPS misconfiguration in some Transit node of EAPS ring.

A high amount of packets get lifted to the CPU and EAPS hello packets get dropped by congestion in the CPU. Probably due to an accidental loop or abnormal traffic storm.

There is one or more link failures in EAPS ring.

There is a unidirectional link.

There is a storm-control limit configured on links of EAPS ring.

Suggested Action

Check equipment's configuration of EAPS ring.

Check the connectivity of links in EAPS ring.

Traps

None

LOOPBACK DETECTION

LOOPBACK_DETECTED

Description

A network loop was detected by LBD protocol.

Default Severity

Major

Impact

The port on which the loop was detected will not forward any traffic until it stops receiving the control traffic for the amount of time configured in the port's timer:
loopback-detection interface <port> timer <time>

Possible Cause

Wrong physical connection or configuration, usually associated with misconnected optical fibers, defective cabling, or any configuration that would cause a loopback-detection packet to be forwarded back to the port on which it was generated.

Suggested Action

Inspect physical connections and configurations in the network devices.

Traps

loopbackDetectedAlarmTrap

BACKUP LINK

BACKUPLINK_INTERFACE_DEFECT

Description

Main/Backup interface suffered a link failure or is blocked by another protocol.

Default Severity

Major

Impact

Interface cannot transmit/receive packets. It cannot become active in case the other interface has a link failure or becomes blocked.

Possible Cause

There is one or more failures in the reported interface.

Suggested Action

Check interface status using **show interface link**.

Traps

backuplinkInterfaceDefectAlarmTrap

BACKUPLINK_USING_BACKUP_INTERFACE

Description

Main interface suffered a link failure or is blocked by another protocol, resulting in a switchover to the backup interface.

Default Severity

Major

Impact

The main interface is not in use, the backup interface is in use.

Possible Cause

There is/was one or more failures in the main interface.

Suggested Action

Check interface status using **show interface link**.

Traps

backuplinkUsingBackupAlarmTrap

L2VPN

VPWS_RED_MAIN_NEIGHBOR_FAIL

Description

Main neighbor suffered a failure resulting in a switchover to the backup-neighbor.

Default Severity

Major

Impact

The main neighbor pseudo-wire is not in use, the backup-neighbor is in use.

Possible Cause

There is one or more link failures in the main PW.
There is a failure in the access interface of the remote device.
Wrong configuration of local and remote neighbors.

Suggested Action

Check VPWS information to detect failures.

Traps

None

CONTINUITY CHECK AND FAULT MANAGEMENT

CFM_RMEP_CCM

Description

The MEP is not receiving CCMs from at least one of the configured remote MEPs.

Default Severity

Major

Impact

The communication with the remote MEP is lost.

Possible Cause

The CCM transmission is disabled on the remote MEP.
There is a failure on the monitored link.

Suggested Action

Check the configuration of the remote MEPs.
Check the connectivity on the monitored link.

Traps

None

CFM_RMEP_INTF

Description

The port status or interface status received from a configured remote MEP indicates an error condition.

Default Severity

Major

Impact

The interface on which the remote MEP is attached to is unable to forward traffic correctly.

Possible Cause

There is a link failure on the port the remote MEP is attached to.

Suggested Action

Check the connectivity of the links on the equipment the MEP reporting the error is configured.

Traps

None

CFM_XCON_CCM

Description

The MEP is receiving CCMs with wrong MD or MA names, which characterizes a cross-connection error.

Default Severity

major

Impact

Unintended connectivity on the network.

Possible Cause

The MA or MD name on the received CCM does not match the MA or MD configured for the MEP.

Suggested Action

Verify for both local and remote MEPs the configured names of Maintenance Domains and Maintenance Associations.

Traps

None

CFM_RMEP_RDI

Description

A remote MEP is not receiving CCMs from at least one of its remote MEPs.

Default Severity

minor.

Impact

The communication between remote MEP and one of its remote MEPs is lost.

Possible Cause

The CCM transmission is disabled in one of the remote MEPs of a remote MEP.
There is a failure on the monitored link of the remote MEP.

Suggested Action

Check the configuration of the remote MEPs of this remote MEP.
Check the connectivity on the monitored link of the remote MEP.

Traps

None

CFM_ERROR_CCM

Description

The MEP is receiving invalid CCMs.

Default Severity

Major

Impact

Unintended connectivity on the network.

Possible Cause

The MEP ID in the received CCM is not configured in the list of remote MEPs of the receiving MEP.

The MEP ID in the received CCM matches the MEP ID of the receiving MEP.

The CCM interval on the received CCM does not match the one configured for the receiving MEP.

Suggested Action

Verify the configuration of local and remote MEPs.

Traps

None

CFM_ETH_AIS

Description

The MEP is in Alarm Indication Signal condition.

Default Severity

major

Impact

A lower-level MD is unable to forward traffic correctly.

Possible Cause

There is a connectivity failure on a lower-level MD.

Suggested Action

Contact the responsible for the lower-level MD which is generating AIS messages.

Traps

None

EFM

EFM_FAILURE

Description

A failure was detected by EFM protocol in the interface.

Default Severity

Major

Impact

The interface on which the failure was detected will not forward any traffic until its recovery. This behavior is a protection to avoid using an interface under unsafe conditions, such as a unidirectional link.

Possible Cause

EFM failures are detected when the interface stops receiving EFM PDUs from its remote peer, which in turn might have several root causes, such as defective cables/fibers and misconfigurations of network devices. EFM failures are also detected when the remote EFM peer reports a malfunction in its interface, i.e., a failure in the interface of another network device will block a local interface.

Suggested Action

Inspect physical connections and configurations in the network devices that would cause PDUs to be lost.

Traps

efmFailureAlarmTrap

OLT

OLT_ADAPT_FAILURE

Description

There was a non-self-recoverable error in the GPON underlying resource.

Default Severity

Critical

Impact

It is possible that data traffic will keep working but control plane may not work correctly. It is likely that new ONUs will not be able to be provisioned.

Possible Cause

GPON underlying device failure.

There are other possible causes for failure. Check user log.

Suggested Action

Reboot card to restore affected GPON services. Contact DATACOM support team.

Traps

None

GPON_LOS

Description

Loss of signal for PON link.

Default Severity

Critical

Impact

Services of all connected ONUs to the PON link are interrupted.

Possible Cause

The GPON port without SFP.

The fiber that connects this PON was broken.

Attenuation of the very high signal. ONU was disconnected from OLT. All previously activated ONUs are powered off or malfunctioning.

Suggested Action

Check if the fiber between OLT and ONU or splitter is operational.

Check the GPON transceiver of PON port in OLT using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Traps

None

GPON_TX_FAULT

Description

TX Fault for PON Link.

Default Severity

Minor

Impact

PON link traffic. All users of this port go to offline.

Possible Cause

Optical transmitter does not match.

Failure to obtain information from optical transmitter.

Failed to initialize the optical transmitter.

Suggested Action

Check the GPON transceiver of PON port in OLT using **show interface transceivers gpon** command.

Check the fiber between ONU and OLT.

Traps

None

GPON_TF

Description

Transmitter failure. The response signal expected from the card after routing data for one port was not received.

Default Severity

Critical

Impact

PON link traffic. All users of this port go to offline.

Possible Cause

Optical transmitter does not match.
Failure to obtain information from optical transmitter.
Failed to initialize the optical transmitter.

Suggested Action

Check the GPON transceiver of PON port in OLT using **show interface transceivers gpon** command.
Check the fiber between ONU and OLT.

Traps

gPonTFAlarm

ONU

GPON_DOWi

Description

Drift of window of ONU. ONU transmission is received at an unexpected time (the phase shifted).

Default Severity

Critical

Impact

Imperceptible to the customer.

Possible Cause

Condition temporary instability in the fiber. With environmental changes, e.g., temperature or even wind, when used serial cables, the fiber can expand or contract, causing variations in the length, and consequently, the distance between the OLT and the ONU.

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean.

Traps

gPonDOWiAlarm

GPON_LOAi

Description

Loss of acknowledge with ONU. OLT did not receive ONU acknowledgement after issuing DS messages that require US acknowledge from the ONU.

Default Severity

Minor

Impact

User traffic.

Possible Cause

Optical fiber is malfunctioning.

Suggested Action

Check the fiber between ONU and OLT.

Traps

gPonLOAiAlarm

GPON_SFi

Description

Signal fail of ONU. ONU upstream signal exceeds the BER threshold.

Default Severity

Critical

Impact

User traffic.

Possible Cause

Improper fiber connection, damaged fiber connector, dirty fiber or damaged.

High attenuation to the ONU.

Attenuation of the very high signal. The attenuation conditions are the cause of most signal loss problems in the ONU. Alarms related to signal loss in ONT follow an alarm intensity increased as the signal goes deteriorating. To a situation of instability OLT can recalculate the parameters in order to maintain healthy and clean signal the alarm. In adverse fiber conditions or ONU, alarms will appear in the following order:

- SD (Signal Degraded)
- SF (Signal Fail)
- LCDG (Loss of GEM Channel Delineation)
- LOFi (Loss of Frame)
- LOSi (Loss of Signal)

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean.

Traps

gPonSFfiAlarm

GPON_PEEi

Description

Physical equipment error of ONU.

Default Severity

Major

Impact

User traffic. ONU services are stopped.

Possible Cause

ONU is malfunctioning.

Suggested Action

Reinitialize ONU using **onu-reset onu x** command, where **x** is the ONU ID.
Replace ONU.

Traps

gPonPEEiAlarm

GPON_LOSi

Description

Signal loss of ONU.

Default Severity

Critical

Impact

User traffic. Data channel abnormal and cannot transmit data.

Possible Cause

The fiber that connects this ONU was broken.

ONU has a hardware failure, but continues to with power.

Attenuation of the very high signal. The attenuation conditions are the cause of most signal loss problems in the ONU. Alarms related to signal loss in ONT follow an alarm intensity increased as the signal goes deteriorating. To a situation of instability OLT can recalculate the parameters in order to maintain healthy and clean signal the alarm. In adverse fiber conditions or ONU, alarms will appear in the following order:

- SD (Signal Degraded)
- SF (Signal Fail)
- LCDG (Loss of GEM Channel Delineation)
- LOFi (Loss of Frame)
- LOSi (Loss of Signal)

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command. Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU. Check if the link between OLT and ONU or splitter is operational.

Traps

gPonLOSiAlarm

GPON_ONU_EQUIP_FAILURE

Description

The ONU has an internal problem/defect.

Default Severity

Major

Impact

User traffic.

Possible Cause

ONU is malfunctioning.

Suggested Action

Reinitialize ONU using **onu-reset onu x** command, where **x** is the ONU ID.
Replace ONU.

Traps

gPonOnuEquipmentFailureAlarm

GPON_ONU_DOWN

Description

The ONU has an internal problem/defect or ONU was disconnected from the PON link.

Default Severity

Major

Impact

Services of the ONU are interrupted.

Possible Cause

ONU disconnected.

ONU turned off by the user.

Suggested Action

Check if the ONU is operational and connected to OLT using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check the link between ONU and OLT.

Replace ONU.

Traps

None

GPON_DFi

Description

Deactivate failure of ONU. ONU does not react correctly after three Deactivate_ONU-ID or three Disable_Serial_Number messages.

Default Severity

Critical

Impact

User traffic.
ONU still active and allocated band.

Possible Cause

ONU is malfunctioning.

Suggested Action

Check if ONU was physically removed but the configuration on OLT was not removed.

Traps

gPonDFiAlarm

GPON_LOFi

Description

Loss of frame of ONU. OLT received four consecutive invalid delimiters from the ONU.

Default Severity

Critical

Impact

User traffic. Data channel abnormal and cannot transmit data.

Possible Cause

The fiber that connects this ONU was broken.

ONU has a hardware failure, but continues to with power.

Attenuation of the very high signal. The attenuation conditions are the cause of most signal loss problems in the ONU. Alarms related to signal loss in ONT follow an alarm intensity increased as the signal goes deteriorating. To a situation of instability OLT can recalculate the parameters in order to maintain healthy and clean signal the alarm. In adverse fiber conditions or ONU, alarms will appear in the following order:

- SD (Signal Degraded)
- SF (Signal Fail)
- LCDG (Loss of GEM Channel Delineation)
- LOFi (Loss of Frame)
- LOSi (Loss of Signal)

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean.

Replace ONU.

Traps

gPonLOFiAlarm

GPON_LCDGi

Description

Loss of GEM channel delineation. The delimitation of the frame GEM header is incorrect in three consecutive frames.

Default Severity

Major

Impact

User traffic.

Possible Cause

The fiber is defective. It may be improperly connected, aged, bent or damaged, dirty or faulty connector.

Attenuation of the very high signal. The attenuation conditions are the cause of most signal loss problems in the ONU. Alarms related to signal loss in ONT follow an alarm intensity increased as the signal goes deteriorating. To a situation of instability OLT can recalculate the parameters in order to maintain healthy and clean signal the alarm. In adverse fiber conditions or ONU, alarms will appear in the following order:

- SD (Signal Degraded)
- SF (Signal Fail)
- LOFi (Loss of Frame)
- LOSi (Loss of Signal)

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean.

Traps

gPonLCDGiAlarm

GPON_LOAMi

Description

Loss of PLOAM for ONU. Three consecutive PLOAM messages of the ONU are missing after OLT sends PLOAMu request for the ONU.

Default Severity

Minor

Impact

User traffic.

ONU goes to operational state 'down' (Inactive).

Possible Cause

Power failure of the ONU.

This alarm could be showed during ONU activation process. It is cleared after the successful of this activation.

Suggested Action

Check if ONU is in rebooting process.

Check the link between ONU and OLT.

Traps

gPonLOAMiAlarm

GPON_ONU_AUTO_PROV_FAIL

Description

There was an error while adding one or more ONUs by the auto provisioning feature.

Default Severity

Minor

Impact

ONU will not be auto provisioned while error is not corrected.

Possible Cause

PON link reached the maximum number of ONUs.

No more service ports available.

There are other possible causes for failure. Check user log.

Suggested Action

Check logs to find out the error cause and correct it.

Traps

gPonOnuAutoProvAddFailTrap

GPON_ONU_PASSWORD_MISMATCH

Description

ONU password mismatch.

Default Severity

Major

Impact

Services are not configured for the ONU due to authentication failure.

Possible Cause

The authentication password configured is different from ONU authentication password.

Suggested Action

Check password configured for authentication between OLT and ONU.

Traps

gPonOnuPasswordMismatchAlarm

GPON_SUFI

Description

Start-up failure of ONU. ONU ranging failed 2 times while the OLT receives the signal bursts.

Default Severity

Minor

Impact

User traffic.

Possible Cause

Fiber attenuation out of the pattern possibly dirty or damaged fiber connector.

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean and without damaged fiber connector.

Traps

gPonSUFiAlarm

GPON_MISi

Description

Link mismatch of ONU. OLT detected that the PST message sent or received are different.

Default Severity

Major

Impact

User traffic. Data cannot be transmitted and the ONU services are interrupted.

Possible Cause

Optical fiber is malfunctioning.

Suggested Action

Check if the fiber between ONU and OLT is correct.

Traps

gPonMISiAlarm

GPON_DGi

Description

Receive dying gasp of ONU. OLT received message that the ONU has lost AC power or is below a certain threshold.

Default Severity

Critical

Impact

Services of the ONU are interrupted.
ONU go to down state (Inactive).

Possible Cause

Power failure of ONU.
ONU is powered off.

Suggested Action

Check if ONU is powered off or was reseted.

Traps

gPonDGiAlarm

GPON_RDii

Description

Remote defect indication of ONU. The OLT transmission is received with defects at the ONU.

Default Severity

Minor

Impact

User traffic.

Possible Cause

Signal optic is below acceptable limit.

Fiber with maximum length exceeded or exceeded attenuation budget.

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Traps

gPonRDAlarm

GPON_SDi

Description

Signal degraded of ONU. Signal of an ONU deteriorates and the upstream signal reaches the BER threshold.

Default Severity

Major

Impact

User traffic.

Possible Cause

Improper fiber connection, damaged fiber connector, dirty fiber or damaged.
High attenuation to ONU.

Suggested Action

Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.

Check if the TX-Power and RX-Power of link between a specific ONU and OLT are within of recommended values using **show interface gpon 1/1/1 onu 1** command. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

Check if the fiber between ONU and OLT is clean.

Traps

gPonSDiAlarm

GPON_ONU_SELF_TEST_FAILURE

Description

Self Test Failure Indication ONU.

Default Severity

Major

Impact

Functioning of ONU.

Possible Cause

ONU is malfunctioning.

Suggested Action

Reinitialize ONU using **onu-reset onu x** command, where **x** is the ONU ID.
Replace ONU.

Traps

gPonOnuSelfTestFailureAlarm

ENVIRONMENT

TEMP_HIGH

Description

The temperature is higher than the recommended limit.

Default Severity

Critical

Impact

The equipment will operate near the maximum temperature supported by the equipment with possibility of permanent damage.

Possible Cause

Object blocking or obstructing the FAN module operation.
Inadequate environment condition for equipment operation.
FAN module failure.

Suggested Action

Check the environment temperature.
Check if the FAN is broken or unplugged.
Check status of FAN and temperature using **show environment** command.
Check logs of FAN and temperature using **show log component fan temperature** command or only **show log**.
Check if the FAN is clean (without dust).
Check if there is something locking or blocking the FAN.
Contact Support Team of DATACOM.

Traps

tempHighAlarmTrap

PSU_FUSE_FAILURE

Description

The PSU fuse is blown.

Default Severity

Major

Impact

This PSU cannot be used as a backup. If the current main PSU fails or is removed, the device will be powered down.

Possible Cause

The fuse is blown.

Suggested Action

Replace the PSU.

Traps

psuFuseFailureAlarmTrap

FAN_MODULE_NOT_PRESENT

Description

Removable fan module has not been detected.

Default Severity

Major

Impact

The device temperature will increase and the overtemperature protection might be triggered.

Possible Cause

Fan module removal.

Suggested Action

Reconnect the fan module.

Traps

fanModuleNotPresentAlarmTrap

FAN_SPEED_LOW

Description

FAN speed is below of secure speed threshold

Default Severity

Major

Impact

The equipment will operate near the minimum FAN speed supported.

Possible Cause

Inadequate environment condition for equipment operation.
FAN module failure.

Suggested Action

Replace the FAN module.

Traps

fanLowAlarmTrap

FAN_ERROR

Description

FAN status could not be read.

Default Severity

Major

Impact

The equipment operation will try to operate normally.

Possible Cause

Defect in FAN or FAN module.

Suggested Action

Check if the FAN module is installed correctly.
Remove and insert the FAN module again.

Traps

fanErrorAlarmTrap

TEMP_ERROR

Description

Temperature sensor could not be read.

Default Severity

Major

Impact

The equipment operation will try to operate normally but may cause permanent damage if environment temperature remains high or low.

Possible Cause

Inadequate environment condition for equipment operation.
The reading of temperature sensor failed due unknown reason.
The temperature sensor could be on fail.

Suggested Action

Check status of FAN and temperature using **show environment** command.
Check logs of FAN and temperature using **show log component fan temperature** command or only **show log**.
Contact Support Team of DATACOM.

Traps

tempErrorAlarmTrap

TEMP_LOW

Description

The temperature is lower than the recommended limit.

Default Severity

Critical

Impact

The equipment will operate near the minimum temperature supported by the equipment with possibility of permanent damage.

Possible Cause

Inadequate environment condition for equipment operation.

Suggested Action

Check status of temperature using **show environment** command.

Check logs of temperature using **show log component fan temperature** command or only **show log**.

Contact Support Team of DATACOM.

Traps

tempLowAlarmTrap

PSU_POWER_INPUT_FAILURE

Description

The PSU has a power input problem.

Default Severity

Minor

Impact

This PSU cannot be used as a backup. If the current main PSU fails or is removed, the device will be powered down.

Possible Cause

The input cable is disconnected.
The power source is defective.

Suggested Action

Connect the input cable.
Check the power source.
Contact Support Team of DATACOM.

Traps

psuPowerInputFailureAlarmTrap

PSU_UNSUPPORTED

Description

PSU module not supported in this product.

Default Severity

Major

Impact

The use of unsupported PSUs may result in hardware malfunction.

Possible Cause

PSU model not supported.

Suggested Action

Replace the PSU with a supported module.
If the problem persists, contact DATACOM Technical Support.

Traps

psuUnsupportedTrap

FAN_FAIL

Description

One FAN of the FAN module is stopped, jammed or presents failure.

Default Severity

Critical

Impact

The equipment operation will try to operate normally if the others FANS of FAN module will be normal.

Possible interruption in equipment operation with possibility of permanent damage if all FANS go to fail.

Possible Cause

Object locking or blocking FAN operation.

Defect in FAN or FAN module.

Suggested Action

Check if the FAN is broken.

Check status of FAN using **show environment** command.

Check if the FAN is clean (without dust).

Check if there is something locking or blocking the FAN.

Contact Support Team of DATACOM.

Traps

fanFailAlarmTrap

PSU_ERROR

Description

An error occurred when checking the PSU.

Default Severity

Major

Impact

This PSU cannot have its status read. Therefore, there is no way to determine if the PSU can be used as a backup.

Possible Cause

There is a transient failure on the access to the PSU.
The PSU is defective.

Suggested Action

Replace the PSU.
If the problem persists, contact Support Team of DATACOM.

Traps

psuErrorAlarmTrap

CPU

CPU_LOAD_HIGH

Description

1. The CPU usage average is higher than 80% during the last 5 minutes.
2. The CPU usage average is higher than 60% during the last 5 minutes.

Default Severity

1. Critical
2. Major

Impact

Some protocols flapping.
Some packets are dropped in normal requests such as: SNMP and ICMP.
Telnet or SSH sessions may be slow.
Dropped packets or increased latency for packets routed.
Dropped packets of user traffic.

Possible Cause

A large configuration being saved.
Large number of simultaneous requests to CPU.
Frequent or large number of requests to CPU processes.
SNMP polling activities.
ARP broadcast storms.
Ethernet broadcast storms.

Suggested Action

Check Release Notes of software version to eliminate known issues.
Check status of CPU using **show system cpu** command.

Check logs about CPU using **show log component sysmon** command or only **show log**.

Check if the problem is caused by a system process or high network traffic, like a loop.

We recommend that you use the switch console for debugging on these cases.

Contact Support Team of DATACOM.

Traps

cpuLoadHighTrap

CPU_CORE_HIGH

Description

1. The CPU core usage average is higher than 90% during the last 5 minutes.
2. The CPU core usage average is higher than 70% during the last 5 minutes.

Default Severity

1. Major
2. Minor

Impact

Some protocols flapping.

Some packets are dropped in normal requests such as: SNMP and ICMP Telnet or SSH sessions may be slow. Dropped packets or increased latency for packets routed.

Dropped packets of user traffic.

Possible Cause

A large configuration being saved.

Large number of simultaneous requests to CPU.

Frequent or large number of requests to CPU processes.

SNMP polling activities.

ARP broadcast storms.

Ethernet broadcast storms.

Suggested Action

Check Release Notes of software version to eliminate known issues.

Check status of CPU using **show system cpu** command.

Check logs about CPU using **show log component sysmon** command or only **show log**.

Check if the problem is caused by a system process or high network traffic, like a loop.

We recommend that you use the switch console for debugging on these cases.

Contact Support Team of DATACOM.

Traps

cpuCoreHighTrap

MEMORY_AVAILABLE_LOW

Description

1. Memory available is lower than 100 MB during the last 5 minutes.
2. Memory available is lower than 200 MB during the last 5 minutes.

Default Severity

1. Critical
2. Major

Impact

Processes dying unexpectedly.
Protocol status going to down.
Dropped packets of user traffic.
Equipment could be rebooted unexpectedly.

Possible Cause

Big configuration saved in equipment.
Many files saved in equipment.
Memory leak of some process.

Suggested Action

Check Release Notes of software version to eliminate known issues.
Check status of Memory using **show system memory** command.
Check logs of Memory using **show log component sysmon** command or only **show log**.
Check the files stored in equipment using **file list**. Delete some files if necessary.
Check through a monitoring tool if memory is being decreasing constantly or there has been a sudden drop. Contact Support Team of DATACOM.

Traps

memAvailableLowTrap

Command Index

<hr/>		GPONLOAMi.....	53
B		GPONLOFi.....	49
		GPONLOS.....	36
	BACKUPLINKINTERFACEDFECT.....	GPONLOSi.....	44
	BACKUPLINKUSINGBACKUPINTERFACE.....	GPONMISi.....	57
<hr/>		GPONONUAUTOPROVFAIL.....	54
C		GPONONUDOWN.....	47
		GPONONUEQUIPFAILURE.....	46
		GPONONUPASSWORDMISMATCH.....	55
	CFMERRORCCM.....	GPONONUSELFTTESTFAILURE.....	61
	CFMETHAIS.....	GPONPEEi.....	43
	CFMRMEPCCM.....	GPONRDi.....	59
	CFMRMEPINTF.....	GPONSDi.....	60
	CFMRMEPRDI.....	GPONSi.....	41
	CFMXCONCCM.....	GPONSUFi.....	56
	CPUCOREHIGH.....	GPONTF.....	38
	CPULOADHIGH.....	GPONTXFAULT.....	37
<hr/>		<hr/>	
E		L	
	EAPSFALTIMEREXPIRED.....	LOOPBACKDETECTED.....	24
	EAPSRINGFAILED.....		
	EFMFAILURE.....		
<hr/>		<hr/>	
F		M	
	FANERROR.....	MEMORYAVAILABLELOW.....	77
	FANFAIL.....		
	FANMODULENOTPRESENT.....		
	FANSPEEDLOW.....		
<hr/>		<hr/>	
G		O	
	GPONDFi.....	OLTADAPTFAILURE.....	35
	GPONDGi.....		
	GPONDOWi.....		
	GPONLCDGi.....		
	GPONLOAi.....		
<hr/>		<hr/>	
P		P	
	PSUERROR.....	PSUERROR.....	72
	PSUFUSEFAILURE.....	PSUFUSEFAILURE.....	63
	PSUPOWERINPUTFAILURE.....	PSUPOWERINPUTFAILURE.....	69
		PSUUNSUPPORTED.....	70

T

TEMPERROR	67
TEMPHIGH	62
TEMPLOW	68

V

VPWSREDMAINNEIGHBORFAIL	27
-------------------------------	--------------------