

DATACOM



DmOS

DATACOM OPERATING SYSTEM

Version 9.4.0

TROUBLESHOOTING AND MAINTENANCE GUIDE

204.4293.29 - December 19, 2023

Contacts

Technical Support

Datacom has available a support portal - DmSupport, to help the customers in use and config of our equipment.

Access to the DmSupport can be made through link: <https://supportcenter.datacom.com.br>

In this site the following are available: firmwares, technical datasheets, config guide, MIBs and manuals for download. In addition, it allows opening of calls for assistance with our technical team.

Telephone Number: **+55 51 3933-3122**

We would like to highlight that our assistance through telephone support is available from Monday through Friday from 08:00 AM through 05:30 PM.

Important: For support assistance 24x7, please request a quotation to our sales department.

General Information

For any other additional information, please visit the <https://www.datacom.com.br/en> or call:

DATAKOM

Rua América, 1000

92990-000 - Eldorado do Sul - RS - Brazil

+55 51 3933-3000

Product Documentation

This document is part of a set of documents prepared to provide all necessary information about DATACOM products.

Software Platform

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

Hardware Platform

- **Datasheet** - Provides the Hardware and Software technical characteristics of product
- **Installation Guide** - Provides instructions on the procedures covering product installation

The availability of some documents can vary depending on the type of product.

Access <https://supportcenter.datacom.com.br> to locate the related documents or contact the Technical Support for additional information.



Introduction to the document

About this Document

The present document is a set of instructions that provide a quick and objective explanation on the use of the functionalities available in the product.

This document was developed to be used as an eventual source for solution of technical issues, and for this reason its sequential reading is not mandatory.

It is presumed that the individual or individuals that manage any aspect of the product should have the basic knowledge of Ethernet, network protocols and communication networks in general.

Audience







This guide is directed to network administrators, technicians or teams qualified to install, set, plan and maintain this product.

Conventions

To facilitate understanding of the present manual, the following conventions were adopted:

Icons

Icon	Type	Description
	Note	The notes explain in a better manner a detail included in the text.

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 warning icon requests special attention to the conditions that, if not avoided, may cause physical damages to the equipment.



A caution icon requests special attention to the conditions that, if not avoided, may result in risk of death of serious injury.

Text Convention

This report 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).
Terminal	System commands and screen outputs.
Object	Indicates a reference to something. Used to emphasize this referenced object.
Menu > Path	GUI (Graphic User Interface) menu paths.
[Key]	Keyboard buttons.



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

Table of Contents

Contacts	2
Product Documentation	3
Introduction to the document	4
1 Alarms	9
1.1 Alarms Severity	9
1.2 Alarms Status	10
1.3 How to Check Alarms	10
1.4 Understanding Alarms	10
2 MIB	11
2.1 Exporting the SNMP MIBs	11
2.2 Querying an SNMP object	11
3 Management	12
3.1 CPU	12
3.1.1 Troubleshooting	12
3.1.2 Alarms	12
3.2 Environment	14
3.2.1 Troubleshooting	14
3.2.2 Alarms	14
3.3 Memory	20
3.3.1 Troubleshooting	20
3.3.2 Alarms	21
4 OAM	22
4.1 CFM	22
4.1.1 Troubleshooting	22
4.1.2 Alarms	22
4.2 EFM	25
4.2.1 Troubleshooting	25
4.2.2 Alarms	25
5 Interface	27
5.1 Backup-Link	27
5.1.1 Troubleshooting	27
5.1.2 Alarms	27
6 GPON	29

6.1 OLT	29
6.1.1 Troubleshooting	29
6.1.2 Alarms	29
6.2 ONU	31
6.2.1 Troubleshooting	31
6.2.2 Alarms	32
7 Switching	45
7.1 EAPS	45
7.1.1 Troubleshooting	45
7.1.2 Alarms	45
7.2 Loopback Detection	46
7.2.1 Troubleshooting	46
7.2.2 Alarms	46
8 MPLS	48
8.1 L2VPN	48
8.1.1 Troubleshooting	48
8.1.2 Alarms	48
Legal Note	49
Warranty	49

1 Alarms

This chapter gives to understanding about the alarms in DmOS.

- [Alarms Severity](#)
- [Alarms Status](#)
- [How to Check Alarms](#)
- [Understanding Alarms](#)

1.1 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.

1.2 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** - Informs 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.

1.3 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**.

```
DM4770# show alarm
Triggered on      Severity Source   Status   Name           Description
-----
2023-04-19 09:01:59 UTC-3 MAJOR    domain63 Active    EAPS_RING_FAILED EAPS domain changed state to 'Failed'
DM4770#
```

- **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.

1.4 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 possibles 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.

2 MIB

This chapter is about understanding the Management Information Base (MIB) supported by DmOS.

- [Exporting the SNMP MIBs](#)
- [Querying an SNMP object](#)

2.1 Exporting the SNMP MIBs

DmOS supports three versions of the Simple Network Management Protocol (SNMP), configuration examples can be seen in the manual **DmOS - Quick Configuration Guide**. The user can export a file with all SNMP MIBs supported by equipment to a TFTP or SCP server. The command below shall forward the MIBs file named **datacom-mibs.tar.gz** via TFTP protocol to the **172.1.1.1** server.

```
copy mibs tftp://172.1.1.1
```

2.2 Querying an SNMP object

The objective of this chapter is to explain the basic how the MIB works using as an example the **MIB DMOS-REBOOT-MIB.mib** file. A MIB has several other parameters and possible configurations, however, to facilitate understanding, a simple example will be used.

```
DMOS-REBOOT-MIB DEFINITIONS ::= BEGIN
... (Parts of file omitted)
rebootReason OBJECT-TYPE
    SYNTAX      String
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  ""
    ::= dmosRebootMIB 1
```

The module name is defined at the beginning of the file and is written in capital letters, and may contain numbers and hyphens. In the example, the name is defined on the first line, **DMOS-REBOOT-MIB**. In addition to the name of the MIB module, it is necessary to query the object's name for SNMP. This can be seen below in the file defined in the OBJECT-TYPE item. In this case it is **rebootReason**. Below is an example of an SNMP query on a Linux host regarding the reboot reason of the **10.0.0.1** equipment. The query is carried out using the module name and the object name separated by a double colon (::).

```
user@host$ snmpwalk -v2c -c public 10.0.0.1 DMOS-REBOOT-MIB::rebootReason
DMOS-REBOOT-MIB::rebootReason.0 = STRING: Reboot requested by user 'admin'
user@host$
```

3 Management

- CPU
- Environment
- Memory

3.1 CPU

3.1.1 Troubleshooting

DmOS forwards L2/L3/MPLS packets in hardware, as well as applying filters and QoS policies, ensuring wirespeed operation for any packet size, avoiding CPU usage for this purpose. Traffic destined to the CPU is used for establishment and resolution of configured protocols and services. Usually CPU-related events are originate from problems in protocol configuration, improper traffic or even the execution of some costly work requested by the user. To reduce incidents in this component, I read the item **CPU DoS Protect Configuration** in the Quick Configuration Guide.

3.1.2 Alarms

CPU_CORE_HIGH

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

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

- **Severity**
 - A. Major
 - B. Minor
- **Impact**
 1. Some protocols flapping.
 2. Some packets are dropped in normal requests such as: SNMP and ICMP Telnet or SSH sessions may be slow.
 3. Dropped packets or increased latency for packets routed.
 4. Dropped packets of user traffic.
- **Possible Cause**
 1. A large configuration being saved.
 2. Large number of simultaneous requests to CPU.
 3. Frequent or large number of requests to CPU processes.
 4. SNMP polling activities.
 5. ARP broadcast storms.

6. Ethernet broadcast storms.

- **Suggested Action**

1. Check Release Notes of software version to eliminate known issues.
2. Check status of CPU using **show system cpu** command.
3. Check logs about CPU using **show log component sysmon** command or only **show log**.
4. Check if the problem is caused by a system process or high network traffic, like a loop.
5. We recommend that you use the switch console for debugging on these cases.
6. Contact Support Team of DATACOM.

- **Trap**

cpuCoreHighTrap

CPU_LOAD_HIGH

A. The CPU usage average is higher than 80% during the last 5 minutes.

B. The CPU usage average is higher than 60% during the last 5 minutes.

- **Severity**

- A. Critical
- B. Major

- **Impact**

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

- **Possible Cause**

1. A large configuration being saved.
2. Large number of simultaneous requests to CPU.
3. Frequent or large number of requests to CPU processes.
4. SNMP polling activities.
5. ARP broadcast storms.
6. Ethernet broadcast storms.

- **Suggested Action**

1. Check Release Notes of software version to eliminate known issues.
2. Check status of CPU using **show system cpu** command.
3. Check logs about CPU using **show log component sysmon** command or only **show log**.
4. Check if the problem is caused by a system process or high network traffic, like a loop.
5. We recommend that you use the switch console for debugging on these cases.
6. Contact Support Team of DATACOM.

- **Trap**

cpuLoadHighTrap

3.2 Environment

3.2.1 Troubleshooting

Environment alarm is related to the place where the equipment is installed or also the replaceable parts of the equipment such as PSU, Fans and expansion card (Line Card). These alarms require immediate operator action to reduce the risk of further events.

3.2.2 Alarms

CARD_UNINITIALIZED

The line card could not be correctly initialized because it was inserted after the main board initialization.

- **Severity**

Major

- **Impact**

The line card is not programmed while in this state, rendering the line card unusable.

- **Possible Cause**

The line card was inserted after the main board initialization.

- **Suggested Action**

Reboot the system so that the line card is initialized together with the main board.

- **Trap**

cardUninitializedAlarmTrap

FAN_ERROR

FAN status could not be read.

- **Severity**
Major
- **Impact**
The equipment operation will try to operate normally.
- **Possible Cause**
Defect in FAN or FAN module.
- **Suggested Action**
 1. Check if the FAN module is installed correctly.
 2. Remove and insert the FAN module again.
- **Trap**
fanErrorAlarmTrap

FAN_FAIL

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

- **Severity**
Critical
- **Impact**
 1. The equipment operation will try to operate normally if the others FANS of FAN module will be normal.
 2. Possible interruption in equipment operation with possibility of permanent damage if all FANS go to fail.
- **Possible Cause**
 1. Object locking or blocking FAN operation.
 2. Defect in FAN or FAN module.
- **Suggested Action**
 1. Check if the FAN is broken.
 2. Check status of FAN using **show environment** command.
 3. Check if the FAN is clean (without dust).
 4. Check if there is something locking or blocking the FAN.
 5. Contact Support Team of DATACOM.

- **Trap**

fanFailAlarmTrap

FAN_MODULE_NOT_PRESENT

Removable FAN module has not been detected.

- **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.

- **Trap**

fanModuleNotPresentAlarmTrap

FAN_SPEED_LOW

FAN speed is below of secure speed threshold

- **Severity**

Major

- **Impact**

The equipment will operate near the minimum FAN speed supported.

- **Possible Cause**

1. Inadequate environment condition for equipment operation.
2. FAN module failure.

- **Suggested Action**

Replace the FAN module.

- **Trap**

fanLowAlarmTrap

PSU_ERROR

An error occurred when checking the PSU.

- **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**

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

- **Suggested Action**

1. Replace the PSU.
2. Contact Support Team of DATACOM.

- **Trap**

psuErrorAlarmTrap

PSU_FUSE_FAILURE

The PSU fuse is blown.

- **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.

- **Trap**

psuFuseFailureAlarmTrap

PSU_POWER_INPUT_FAILURE

The PSU has a power input problem.

- **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**

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

- **Suggested Action**

1. Connect the input cable.
2. Check the power source.

Contact Support Team of DATACOM.

- **Trap**

psuPowerInputFailureAlarmTrap

PSU_UNSUPPORTED

PSU module not supported in this product. Alarm will be generated for PSU with known model and not compatible with the product. For PSU with unknown model the alarm will not be generated.

- **Severity**

Major

- **Impact**

The use of unsupported PSUs may result in hardware malfunction.

- **Possible Cause**

PSU model not supported.

- **Suggested Action**

1. Replace the PSU with a supported module.
2. Contact Support Team of DATACOM.

- **Trap**

psuUnsupportedTrap

TEMP_ERROR

Temperature sensor could not be read.

- **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**

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

- **Suggested Action**

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

- **Trap**

tempErrorAlarmTrap

TEMP_HIGH

The temperature is higher than the recommended limit.

- **Severity**

Critical

- **Impact**

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

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

tempHighAlarmTrap

TEMP_LOW

The temperature is lower than the recommended limit.

- **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**

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

- **Trap**

tempLowAlarmTrap

3.3 Memory

3.3.1 Troubleshooting

Each equipment with the DmOS operating system has a certain amount of memory dimensioned for the product in question. The equipment has two types of memory, the FLASH memory where the operating system, configuration files,

firmware image and logs are stored. The RAM memory is used by applications and temporary log files. DmOS has an intelligent FLASH memory management system to avoid running out of space and thus allow the system to always have space to operate. The RAM memory is influenced by the configurations and actions performed by the operator and it can reach critical levels if the failure is not handled.

3.3.2 Alarms

MEMORY_AVAILABLE_LOW

A. Memory available is lower than 100 MB during the last 5 minutes.

B. Memory available is lower than 200 MB during the last 5 minutes.

- **Severity**

A. Critical

B. Major

- **Impact**

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

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

memAvailableLowTrap

4 OAM

- CFM
- EFM

4.1 CFM

4.1.1 Troubleshooting

Operations, Administration, and Maintenance (OAM) Connectivity Fault Management (CFM) provides end-to-end, point-to-point, or a LAN made up of several devices. Its design is hierarchical, with different levels and can be summarized as follows: The Maintenance Domain (MD) with names indicating the domain of action. For each MD level it is possible to have several Maintenance Association (MA) where the MEPs will communicate. The Maintenance End Point (MEP) is the main CFM entity that will know your specific MA within an MD level. MEPs can actively send and receive CCM frames, each MEP is configured to periodically transmit these messages. MEP can only be configured on the interfaces that delimit the border of a CFM domain. The Maintenance Intermediate Point (MIP) unlike the MEP is a passive entity. The MIP only sends CFM frames in response to a frame it has received. The Continuity Check Message (CCM) is responsible for the proactive monitoring of CFM connectivity, with the objective of detecting connection failures in the MA.

4.1.2 Alarms

CFM_ERROR_CCM

The MEP is receiving invalid CCMs.

- **Severity**
Major
- **Impact**
Unintended connectivity on the network.
- **Possible Cause**
 1. The MEP ID in the received CCM is not configured in the list of remote MEPs of the receiving MEP.
 2. The MEP ID in the received CCM matches the MEP ID of the receiving MEP.
 3. 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.
- **Trap**
None

CFM_ETH_AIS

The MEP is in Alarm Indication Signal condition.

- **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.

- **Trap**

None

CFM_RMEP_CCM

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

- **Severity**

Major

- **Impact**

The communication with the remote MEP is lost.

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

None

CFM_RMEP_INTF

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

- **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.

- **Trap**

None

CFM_RMEP_RDI

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

- **Severity**

Minor

- **Impact**

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

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

None

CFM_XCON_CCM

The MEP is receiving CCMs with wrong MD or MA names.

- **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.
- **Trap**
None

4.2 EFM

4.2.1 Troubleshooting

Ethernet in the First Mile (EFM) is an Operations, Administration, and Maintenance (OAM) mechanism/technology with the objective of monitoring the state of the point-to-point link, blocking the interface as soon as the communication is interrupted. Protocol information is transmitted through frame slow Protocol OAM Protocol Data Units (OAMPDUs). OAMPDUs are only exchanged between interfaces on the link and are not forwarded across switches, in case of using other encapsulation technologies such as L2VPN, L2TP the frames can be forwarded without being treated. OAMPDUs contain status and control information used to monitor, test, and troubleshoot the link for unidirectional communication and other problems.

4.2.2 Alarms

EFM_FAILURE

A failure was detected by EFM protocol in the interface.

- **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.

- **Trap**

efmFailureAlarmTrap

5 Interface

- Backup-Link

5.1 Backup-Link

5.1.1 Troubleshooting

Not available.

5.1.2 Alarms

BACKUPLINK_INTERFACE_DEFECT

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

- **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**.
- **Trap**
backuplinkInterfaceDefectAlarmTrap

BACKUPLINK_USING_BACKUP_INTERFACE

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

- **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**.

- **Trap**

backuplinkUsingBackupAlarmTrap

6 GPON

- OLT
- ONU

6.1 OLT

6.1.1 Troubleshooting

Not available.

6.1.2 Alarms

OLT_ADAPT_FAILURE

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

- **Severity**
Critical
- **Impact**
 1. It is possible that data traffic will keep working but control plane may not work correctly.
 2. It is likely that new ONUs will not be able to be provisioned.
- **Possible Cause**
 1. GPON underlying device failure.
 2. There are other possible causes for failure.
 3. Check user log.
- **Suggested Action**
 1. Reboot card to restore affected GPON services.
 2. Contact DATACOM support team.
- **Trap**
None

GPON_LOS

Loss of signal for PON link.

- **Severity**
Critical

- **Impact**

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

- **Possible Cause**

1. The GPON port without SFP.
2. The fiber that connects this PON was broken.
3. Attenuation of the very high signal. ONU was disconnected from OLT.
4. All previously activated ONUs are powered off or malfunctioning.

- **Suggested Action**

1. Check if the fiber between OLT and ONU or splitter is operational.
2. Check the GPON transceiver of PON port in OLT using **show interface transceivers gpon** command.
3. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
4. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

- **Trap**

None

GPON_TX_FAULT

TX Fault for PON Link.

- **Severity**

Minor

- **Impact**

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

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

None

GPON_TF

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

- **Severity**

Critical

- **Impact**

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

- **Possible Cause**

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

- **Suggested Action**

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

- **Trap**

gPonTFAlarm

6.2 ONU

6.2.1 Troubleshooting

The attenuation conditions are the cause of the majority of signal problems in the ONU. Higher attenuations cause the appearance of more alarms related to signal failures. In this scenario, the ONT can tune some parameters to improve the signal and to minimize these conditions. In adverse ONU or fiber conditions, alarms will appear in the following order:

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

6.2.2 Alarms

GPON_DOWi

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

- **Severity**

Critical

- **Impact**

Imperceptible to the customer.

- **Possible Cause**

Temporary unstable condition in the fiber. With environmental changes, e.g., temperature, humidity or even wind, the fiber can expand or contract, causing variations in its length, and consequently, the distance between the OLT and the ONU.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. 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.

- **Trap**

gPonDOWiAlarm

GPON_LOAi

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

- **Severity**

Minor

- **Impact**

User traffic.

- **Possible Cause**

Optical fiber is malfunctioning.

- **Suggested Action**

Check the fiber between ONU and OLT.

- **Trap**

gPonLOAiAlarm

GPON_SFi

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

- **Severity**

Critical

- **Impact**

User traffic.

- **Possible Cause**

1. Improper, damaged or dirty fiber connection.
2. High optical attenuation on the path to the ONU.
3. Too much attenuation of the optical signal.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the fiber between ONU and OLT is clean.

- **Trap**

gPonSFiAlarm

GPON_PEEi

Physical equipment error of ONU.

- **Severity**

Major

- **Impact**

User traffic. ONU services are stopped.

- **Possible Cause**

ONU is malfunctioning.

- **Suggested Action**

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

- **Trap**

gPonPEEiAlarm

GPON_LOSi

- **Description**

Signal loss of ONU.

- **Severity**

Critical

- **Impact**

User traffic. Data channel abnormal and cannot transmit data.

- **Possible Cause**

1. The fiber connection to this ONU is broken or malfunctioning.
2. The ONU is powered, but have a hardware failure that interferes with its transmission.
3. Too much attenuation of the optical signal.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. 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.

- **Trap**

gPonLOSiAlarm

GPON_ONU_EQUIP_FAILURE

The ONU has an internal problem/defect.

- **Severity**

Major

- **Impact**

User traffic.

- **Possible Cause**

ONU is malfunctioning.

- **Suggested Action**

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

- **Trap**

gPonOnuEquipmentFailureAlarm

GPON_ONU_DOWN

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

- **Severity**

Major

- **Impact**

Services of the ONU are interrupted.

- **Possible Cause**

1. ONU disconnected.
2. ONU turned off by the user.

- **Suggested Action**

1. Check if the ONU is operational and connected to OLT using **show interface gpon 1/1/1 onu 1 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
2. Check the link between ONU and OLT.
3. Replace ONU.

- **Trap**

None

GPON_Dfi

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

- **Severity**

Critical

- **Impact**

1. User traffic.
2. 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.

- **Trap**

gPonDFiAlarm

GPON_LOFi

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

- **Severity**

Critical

- **Impact**

User traffic. Data channel abnormal and cannot transmit data.

- **Possible Cause**

1. The fiber connection to this ONU is broken or malfunctioning.
2. The ONU is powered, but have a hardware failure that interferes with its transmission.
3. Too much attenuation of the optical signal.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the fiber between ONU and OLT is clean.
4. Replace ONU.

- **Trap**

gPonLOFiAlarm

GPON_LCDGi

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

- **Severity**

Major

- **Impact**

User traffic.

- **Possible Cause**

1. The fiber is defective. It may be improperly connected, aged, bent or damaged. Dirty or faulty connector.
2. Too much attenuation of the optical signal.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the fiber between ONU and OLT is clean.

- **Trap**

gPonLCDGiAlarm

GPON_LOAMi

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

- **Severity**

Minor

- **Impact**

1. User traffic.
2. ONU goes to operational state **down** (Inactive).

- **Possible Cause**

1. Power failure of the ONU.
2. This alarm could be shown during ONU's activation process. It is cleared after a successful activation.

- **Suggested Action**

1. Check if ONU is in rebooting process.
2. Check the link between ONU and OLT.

- **Trap**

gPonLOAMiAlarm

GPON_ONU_AUTO_PROV_FAIL

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

- **Severity**

Minor

- **Impact**

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

- **Possible Cause**

1. PON link reached the maximum number of ONUs.
2. No more service ports available.
3. There are other possible causes for failure. Check user log.

- **Suggested Action**

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

- **Trap**

gPonOnuAutoProvAddFailTrap

GPON_ONU_PASSWORD_MISMATCH

ONU password mismatch.

- **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.

- **Trap**

gPonOnuPasswordMismatchAlarm

GPON_SUFi

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

- **Severity**

Minor

- **Impact**

User traffic.

- **Possible Cause**

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

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the fiber between ONU and OLT is clean and without damaged fiber connector.

- **Trap**

gPonSUFiAlarm

GPON_MISi

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

- **Severity**

Major

- **Impact**

1. User traffic.
2. 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.

- **Trap**

gPonMISiAlarm

GPON_DGi

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

- **Severity**

Critical

- **Impact**

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

- **Possible Cause**

1. Power failure of ONU.
2. ONU is powered off.

- **Suggested Action**

Check if ONU is powered off or was reseted.

- **Trap**

gPonDGiAlarm

GPON_RDii

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

- **Severity**

Minor

- **Impact**

User traffic.

- **Possible Cause**

1. Signal optic is below acceptable limit.

2. Fiber with maximum length exceeded or excessive attenuation.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.

- **Trap**

gPonRDAlarm

GPON_SDi

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

- **Severity**

Major

- **Impact**

User traffic.

- **Possible Cause**

1. Improper, damaged or dirty fiber connection.
2. High optical attenuation on the path to the ONU.

- **Suggested Action**

1. Check if the TX-Power and RX-Power of PON link is within of recommended values using **show interface transceivers gpon** command.
2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the fiber between ONU and OLT is clean.

- **Trap**

gPonSDiAlarm

GPON_LOBi

1. Loss of burst for ONU.

2. Failure to delineate, for any reason, the specified number (default 4) of consecutive scheduled bursts from ONU, when not exempt by power management state machine.

- **Severity**

Critical

- **Impact**

User traffic. Abnormal data channel cannot transmit data.

- **Possible Cause**

1. The fiber connection to this ONU is broken or malfunctioning.
2. The ONU is powered, but have a hardware failure that interferes with its transmission.
3. Too much attenuation of the optical signal.

- **Note**

This alarm is only available to XGS ONU, and replaces the conditions known as LOSi and LOFi.

- **Suggested Action**

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

- **Trap**

gPonLOBiAlarm

GPON_LOPCi

1. Loss of PLOAM channel with ONU.
2. This is a generic defect indicating breakage of the PLOAM protocol: persistent MIC failure in the upstream; lack of acknowledgements or proper PLOAM responses from the ONU. Persistent means that the same irregular condition is observed consecutively at least three times.

- **Severity**

Major

- **Impact**

User traffic. Abnormal data channel cannot transmit data.

- **Possible Cause**

1. The fiber connection to this ONU is broken or malfunctioning.
2. The ONU is powered, but have a hardware failure that interferes with its transmission.
3. Too much attenuation of the optical signal.

- **Note**

This alarm is only available to XGS ONU.

- **Suggested Action**

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

- **Trap**

gPonLOPCiAlarm

GPON_LOOCi

1. Loss of OMCC channel with ONU.
2. Mananagement channel is not available.

- **Severity**

Major

- **Impact**

User traffic. Abnormal data channel cannot transmit data.

- **Possible Cause**

1. The fiber connection to this ONU is broken or malfunctioning.
2. The ONU is powered, but have a hardware failure that interferes with its transmission.
3. Too much attenuation of the optical signal.

- **Note**

This alarm is only available to XGS ONU.

- **Suggested Action**

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

2. 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 optical-info** and/or **show interface gpon 1/1/1 onu 1 rssi** commands. Where 1/1/1 is the chassi/slot/port and onu 1 is the ID of ONU.
3. Check if the link between OLT and ONU or splitter is operational.

- **Trap**

gPonLOOCiAlarm

GPON_ONU_SELF_TEST_FAILURE

Self Test Failure Indication ONU.

- **Severity**

Major

- **Impact**

Functioning of ONU.

- **Possible Cause**

ONU is malfunctioning.

- **Suggested Action**

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

- **Trap**

gPonOnuSelfTestFailureAlarm

7 Switching

- EAPS
- Loopback Detection

7.1 EAPS

7.1.1 Troubleshooting

Not available.

7.1.2 Alarms

EAPS_FAIL_TIMER_EXPIRED

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

- **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**
 1. EAPS misconfiguration in some Transit node of EAPS ring.
 2. 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.
 3. There is one or more link failures in EAPS ring.
 4. There is a unidirectional link.
 5. There is a storm-control limit configured on links of EAPS ring.
- **Suggested Action**
 1. Check equipments configuration of EAPS ring.
 2. Check the connectivity of links in EAPS ring.
- **Traps**
None

EAPS_RING_FAILED

EAPS domain entered on failed state.

- **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**

1. There is one or more link failures in EAPS ring.
2. Wrong configuration of Control VLAN in equipments of EAPS ring.

- **Suggested Action**

1. Check control-vlan configurations on equipments of EAPS ring.
2. Check the connectivity of links in EAPS ring.

- **Traps**

None

7.2 Loopback Detection

7.2.1 Troubleshooting

Not available.

7.2.2 Alarms

LOOPBACK_DETECTED

A network loop was detected by LBD protocol.

- **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 ports 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.

- **Trap**

loopbackDetectedAlarmTrap

8 MPLS

- L2VPN

8.1 L2VPN

8.1.1 Troubleshooting

Not available.

8.1.2 Alarms

VPWS_RED_MAIN_NEIGHBOR_FAIL

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

- **Severity**
Major
- **Impact**
The main neighbor pseudo-wire is not in use, the backup-neighbor is in use.
- **Possible Cause**
 1. There is one or more link failures in the main PW.
 2. There is a failure in the access interface of the remote device.
 3. Wrong configuration of local and remote neighbors.
- **Suggested Action**
Check VPWS information to detect failures.
- **Trap**
Indisponível.

Legal Note

In spite the fact that all the precautions were taken in development of the present document, DATACOM shall not be held responsible for eventual errors or omissions as well as no obligation is assumed due to damages resulting from the use of the information included in this guide. The specifications provided in this manual shall be subject to changes with no prior notification and are not acknowledged as any type of contract.

© 2023 DATACOM - All rights reserved.

Warranty

DATACOM's products are covered by a warranty against manufacturing defects during a minimum period of 12 (twelve) months including the legal term of 90 days, as from the date of issue of the supply Nota Fiscal (Invoice).

Our warranty is standard counter warranty, this means, for exercise of the warranty, the customer should send the product to DATACOM Authorized Technical Assistance with paid freight. The return freight of the equipment will be DATACOM responsibility.

To obtain additional information, see our warranty policy in <https://www.datacom.com.br/en>.

Telephone Number: **+55 51 3933-3094**