

# DATAKOM



## DmOS

DATAKOM OPERATING SYSTEM

Version 7.2.0

RELEASE NOTES

204.4295.52 - February 15, 2022

## 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:

**DATACOM**

**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

This report provides information regarding a new software release version for DmOS product. The Release Notes also intends to inform relevant changes that have occurred in software, hardware and documentation.

It is assumed the reader is familiar with network protocols concepts and has previous knowledge about DmOS products.

## Audience

This document is intended for Network Administrators, Engineers and any other qualified service personnel who are responsible for configuring and maintaining networks deployed with DmOS.

## 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.
<i>Object</i>	Indicates a reference to something. Used to emphasize this referenced object.
<b>Menu &gt; Path</b>	GUI (Graphic User Interface) menu paths.
[Key]	Keyboard buttons.

## Table of Contents

<b>Contacts</b>	<b>2</b>
<b>Product Documentation</b>	<b>3</b>
<b>Introduction to the document</b>	<b>4</b>
<b>1 Important Notes</b>	<b>6</b>
<b>2 Hardware and Software Compatibility</b>	<b>7</b>
2.1 Released Software . . . . .	7
2.2 Product Compatibility . . . . .	7
2.3 Compatibility Between Software Versions . . . . .	8
2.4 Compatibility of Electrical Modules . . . . .	11
2.5 Compatibility of Electrical Cables . . . . .	12
2.6 SSL Encryption Compatibility . . . . .	13
<b>3 New Features and Enhancements</b>	<b>14</b>
3.1 New Features . . . . .	14
3.2 Enhancements . . . . .	14
3.3 Changes in protocols management . . . . .	14
<b>4 Solved Issues and Restrictions</b>	<b>15</b>
4.1 Solved Issues . . . . .	15
4.2 DmOS Software Restrictions . . . . .	15
4.3 Hardware Platforms Restrictions . . . . .	22
<b>5 Document Versions</b>	<b>26</b>
5.1 Software Platform . . . . .	26
5.2 Hardware Platform . . . . .	26
<b>Legal Note</b>	<b>27</b>
<b>Warranty</b>	<b>27</b>

## 1 Important Notes

The table below provides important notes that should be observed when using the product.

Note	Product
Increasing the number of objects or decreasing the interval between SNMP requests might lead to management latency or SNMP errors.	All
DmOS devices support autocorrection for occurrences of data corruption in memory. There may be cases after power outages or swings where the system cannot perform data autocorrection and may cause loss of logs or configurations.	All
The memory can be allocated by internal processes due to successive link-flaps. After flap stop, the memory will return to initial state. It is recommended to use the Link-Flap-Detection feature in ethernet interfaces.	All
VPN configurations that use the default MTU size configuration before DmOS 3.0.0 must observe the change in the default value from 1500 to 9198, which may cause a configuration mismatch.	All
It is possible to update all ONUs in a PONLink simultaneously provided that all ONUs are model equivalent. If there are ONUs of different models in a PONLink, it is not recommended to use the “all” parameter in command request firmware onu install <image> interface gpon <id> .	DM461X
It is not recommended to configure the snmp real-time option for more than 128 ONUs. Large scale monitoring can cause performance impacts, such as an increase in ONU status update time. When using the DM461X products (OLT GPON) and operating near the maximum supported ONUs by the platform, it is recommended that the SNMP requests interval is no lower than 15 minutes.	DM461X

## 2 Hardware and Software Compatibility

This chapter lists hardware and software compatibility for this software release.

### 2.1 Released Software

This session presents the software release details:

Product	Release Version
DmOS	7.2.0



**DmOS 5.0** is the LTS release (Long-Term Support) for platform **DM4610 OLT 8GPON+8GX+4GT+2XS** (P/N 800.5081.xx). The platform will still receive maintenance releases based on DmOS 5.0, if necessary, with bug fixes. However, there will be no updates with new features. Other OLTs (DM4610-HW2 8-GPON and 4-GPON, DM4615), will still receive new features and bug fixes.



**DmOS 5.2** is the LTS release (Long-Term Support) for platform **DM4775 32CX** (P/N 820.0014.00). The platform will still receive maintenance releases based on DmOS 5.2, if necessary, with bug fixes. However, there will be no updates with new features.



For scalability values per platform, check document DmOS – DmOS Datasheet.

### 2.2 Product Compatibility



To use management via DmView with the DmOS version 7.2.0 it is necessary to update DmView to version 10.4.1 or greater.

The table below shows the product compatibility matrix stating the minimum hardware version, minimum software version and the minimum version of DmView (management software).

Product	Hardware Version	Software Version	DmView Version
DM4050 24GT+6XS	800.5189.00	2.2.0	10.3
DM4050 24GX+6XS	800.5190.00	2.2.0	10.3
DM4170 24GX+4XS+2QX	800.5184.01	3.0.0	10.3

Product	Hardware Version	Software Version	DmView Version
DM4170 24GX+12XS	800.5186.01	2.2.0	10.3
DM4250 24XS+2QX	800.5197.02	4.0.0	10.3
DM4270 24XS+2CX	800.5231.53	4.7.0	10.3
DM4270 48XS+6CX	800.5213.53	4.9.0	10.3
DM4360 4GT+4GX	800.5259.50	4.10.0	10.3
DM4370 4GT+4GX+4XS	800.5191.00	3.0.0	10.3
DM4380 12XS+3CX	800.5258.00	5.0.0	10.3
DM4610 OLT 8GPON+8GX+4GT+2XS	800.5081.03	1.4.0	10.3
DM4610 OLT 4GPON+4GX+2XS (HW2)	800.5193.01	2.4.0	10.3
DM4610 OLT 8GPON+8GX+4GT+2XS (HW2)	800.5165.01	2.2.0	10.3
DM4611 OLT 4GPON+2GT+2XS	800.5283.51	6.2.0	10.3
DM4612 OLT 8GPON+2GT+2XS	800.5285.51	6.2.0	10.3
DM4615 OLT 16GPON+4GT+4XS	800.5198.01	4.2.0	10.3
DM4770 16CX	800.5280.51	6.0.0	10.3
DM4770 32CX	800.5255.52	5.8.0	10.3
DM4775 32CX	820.0015.00 820.0016.00	4.9.0	10.3



**Bold itens - new hardware platform available in the current version of DmOS.**

## 2.3 Compatibility Between Software Versions

The tables below shows the compatibility matrix between firmware versions, including the notes for the firmware update process.

### Software Upgrade

For **DM4050** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4050	2.2.0	2.2.2	3.0.4	4.6.2	7.2.0



Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4050	2.2.2	-	3.0.4	4.6.2	7.2.0
DM4050	3.0.4 or higher	-	-	4.6.2	7.2.0
DM4050	4.6.2 or higher	-	-	-	7.2.0

For **DM4170** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4170	2.2.0	2.2.2	3.0.4	4.6.2	7.2.0
DM4170	2.2.2	-	3.0.4	4.6.2	7.2.0
DM4170	3.0.4 or higher	-	-	4.6.2	7.2.0
DM4170	4.6.2 or higher	-	-	-	7.2.0

For **DM4250** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4250	4.0.0 or higher	4.6.2			7.2.0
DM4250	4.6.2 or higher	-			7.2.0

For **DM4270 24XS+2CX** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4270 24XS+2CX	4.7.0 or higher	-			7.2.0

For **DM4270 48XS+6CX** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4270 48XS+6CX	4.9.0 or higher	-			7.2.0

For **DM4360** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4360	4.10.0 or higher	-			7.2.0

For **DM4370** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4370	3.0.0	3.0.4	4.6.2		7.2.0
DM4370	3.0.4 or higher	-	4.6.2		7.2.0
DM4370	4.6.2 or higher	-	-		7.2.0

For **DM4380** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4380	5.0.0 or higher	-			7.2.0

For **DM4610 HW1** platform, the DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions					Final Version
DM4610 HW1	1.8.0 or lower	1.8.2	2.2.2	3.0.4	4.0.2		5.0.2
DM4610 HW1	1.8.2 to 2.0.4	-	2.2.2	3.0.4	4.0.2		5.0.2
DM4610 HW1	2.2.2 to 3.0.2	-	-	3.0.4	4.0.2		5.0.2
DM4610 HW1	3.0.4 to 4.0.0	-	-	-	4.0.2		5.0.2
DM4610 HW1	4.0.2 or higher	-	-	-	-		5.0.2

For **DM4610 HW2** platform, the DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions					Final Version
DM4610 HW2	1.8.0 or lower	1.8.2	2.2.2	3.0.4	4.0.2		7.2.0
DM4610 HW2	1.8.2 to 2.0.4	-	2.2.2	3.0.4	4.0.2		7.2.0
DM4610 HW2	2.2.2 to 3.0.2	-	-	3.0.4	4.0.2		7.2.0
DM4610 HW2	3.0.4 to 4.0.0	-	-	-	4.0.2		7.2.0
DM4610 HW2	4.0.2 or higher	-	-	-	-		7.2.0

For **DM4611 and DM4612** platforms, the DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions			Final Version
DM4611 and DM4612	6.0.0 or higher	-			7.2.0

For **DM4615** platform, the DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions	Final Version
DM4615	4.0.0 or higher	-	7.2.0

For **DM4770 16CX** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions	Final Version
DM4770 16CX	6.0.0 or higher	-	7.2.0

For **DM4770 32CX** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions	Final Version
DM4770 32CX	5.8.0 or higher	-	7.2.0

For **DM4775** platform, DmOS has the following compatibility matrix:

Platform	Initial Version	Mandatory Intermediate Versions	Final Version
DM4775	4.9.0 or higher	-	5.2.0

#### Notes

It is always recommend save the configuration before firmware update process. To save the configuration use the **save <arquivo>** command.

In case of doubt, please call to DATACOM Technical Support.

## Software Downgrade

#### Notes

The database of the older version, if available, will be restored. Any configuration changes made after upgrade to version 4.x or higher will be lost in the downgrade process. If the equipment has never received firmware other than 4.x, when downgrading the equipment will start with the factory setting.

From version 2.4.0 it is only possible to perform firmware downgrade to version 2.0.0 or 2.2.2. Firmware downgrade to older versions is not allowed by the system.

## 2.4 Compatibility of Electrical Modules

The table below shows the matrix about electrical modules support (SFP Copper) by each product line and which version initiated its support. It's advised the use of **negotiation** on interfaces with copper SFPs.



The SFP Copper supported has **377.7000.00** DATACOM code. DATACOM does not guarantee compatibility with other modules. Contact us for more information.

Product Line	Software Version
DM4050	2.2.0
DM4170	2.2.0
DM4250	4.8.0
DM4270 24XS+2CX	4.8.0
DM4270 48XS+6CX	5.0.0 (forced only <sup>1</sup> )
DM4360	4.10.0
DM4370	3.0.0
DM4380	5.0.0
DM4610	2.2.0
DM4611	6.2.0
DM4612	6.2.0
DM4615	4.2.0
DM4770 16CX	6.0.0 (forced only <sup>1</sup> )
DM4770 32CX	5.8.0
DM4775	4.9.0



<sup>1</sup> **DM4270 48XS+6CX** and **DM4770 16CX** don't support negotiation on ten-gigabit interfaces and twenty-five-gigabit interfaces, but it's possible to make use of copper modules setting the interface to forced mode (no negotiation). The presence of a copper module makes the interface negotiate with the link partner advertising 1 Gbps speed only, with no support for pause frames or lower speeds, regardless of its current configuration. When operating in this mode, a link down status may take up to 10 seconds to be reported.

## 2.5 Compatibility of Electrical Cables

The table below shows the electrical cables support matrix recommended by Datacom.



The use of non recommended cables can cause performance problems.

Code	Description
710.0384.00	DAC Passive Cable 40GbE QSFP+ to QSFP+ (1m)
710.0391.00	DAC Passive Cable 40GbE QSFP+ to QSFP+ (3m)
710.0395.00	DAC Passive Cable 100GbE QSFP28 to QSFP28 (1m)
710.0396.00	DAC Passive Cable 100GbE QSFP28 to QSFP28 (3m)

## 2.6 SSL Encryption Compatibility

The table below lists the OpenSSL versions for each software version and which version initiated its support.

Software Version	OpenSSL Version
1.4.2	1.0.1f
1.10.x	1.0.2j
1.12.0 to 2.2.0	1.0.2k
2.4.0 to 3.0.4	1.0.2l
4.0.0 to 4.10.2	1.0.2o
5.0.0 or higher	1.0.2t

## 3 New Features and Enhancements

This chapter lists new features, enhancements and changes in commands introduced in this release.

### 3.1 New Features

Feature	Description
RSVP	Support to explicit path tunnels in RSVP.

### 3.2 Enhancements

Feature	Description	ID
-	-	-

### 3.3 Changes in protocols management

Feature	Description	ID
-	-	-

## 4 Solved Issues and Restrictions

This section lists solved issues and known restrictions for this software release.

- **Solved Issues:** Fixed bugs in this version.
- **DmOS Software Restrictions:** Feature restrictions which are valid for all hardware platforms.
- **Hardware Platforms Restrictions:** DmOS Software restrictions on specific hardware platforms.

### 4.1 Solved Issues

Feature	Description	ID
<b>GPON</b>	DHCPv6 packets does not pass through the N:1 service port. To use this service it is necessary to create a ip spoofing rule.	155891
<b>IP Routing</b>	If the equipment receives an ARP on an L3 interface asking for another L3 network and this host is reachable by some interface of this equipment, the equipment insert an entry in the host-table with the interface that the ARP was originated. This behavior causes traffic to this host to not be forwarded to the correct interface. There is still this issue in the case of GARP packet instead ARP.	150315
<b>OAM EFM</b>	Interface is not unlocked after returning from failure if the protocol is used in some topology that the equipment does not feel loss of the physical link.	154138
<b>L2VPN</b>	In some situations, backup pw does not return to main pw and occur a core-dump in vpn-mgr process.	156990
<b>L2VPN</b>	<i>show mpls l2vpn vpws group brief</i> command could generate core-dump in vpn-app process and L2VPN flapping.	156204
<b>RSVP</b>	In some scenarios, when explicit path tunnels converges a core-dump may occur into a LSR equipment.	154205
<b>RSVP</b>	Tunnel in headend may not work or respect CSPF information in the case of equipment has more than one OSPF area configured. Workaround is remove the excess OSPF areas and rebooting the equipment.	153877
<b>RSVP</b>	Tunnel using explicit path does not return to highest-priority path-option after restoring it.	154510
<b>Sensors</b>	Equipment restarting due to CPU sensor access not supported on DM4380 platform.	156793
<b>System</b>	In optical switches scenario a very fast link outage can happen does not signaled to the protocols. This issue only occurs on the DM4050 and DM4370 platforms.	156200

### 4.2 DmOS Software Restrictions

Feature	Description	ID
<b>ACL</b>	There is no support to access list in service-ports, only in PON links.	-
<b>ACL</b>	Broadcast and DLF traffic will be forwarded to CPU even when there is an ACL blocking it.	122376
<b>Aging Time</b>	There is no support to aging time configuration per interface, VLAN ID , Routed-MACs or specific MAC addresses.	-
<b>Assistant-task</b>	If there is a <b>show</b> command in the script, the next commands are not executed.	121680
<b>Banner</b>	On banner configuration, the \ character (backslash) operates as an escape character. To display this character, you must insert two backslash (\\).	-
<b>BFD</b>	BFD sessions are not shown in DmView.	127350
<b>BGP</b>	In BGP neighbors BGP with same IP address, in distinct VRF, it is not possible configure different passwords to the same neighbors.	-
<b>BGP</b>	Autocomplete does not work for <b>show ip bgp vrf neighbor</b> command.	114292
<b>BGP</b>	Possibility of coredump if user to run commands immediately after booting the system.	113454
<b>Booting Process</b>	During the initialization of equipment, if a commit is executed, it might show the "Database is Locked" message until all modules are applied	-
<b>CFM</b>	When adding a interface that blocked by CFM to a LAG that is also blocked by CFM, it can be unblocked.	124046
<b>CFM</b>	Communitication between MEPs may not work, being necessary to remove the CFM configuration and reapply it.	119632
<b>CLI</b>	"show" and "commit" commands may fail if executed shortly after booting the system due of software modules initialization.	116417
<b>CLI</b>	<b>show configuration diff</b> command can crash requiring the user execute a CTRL+C to return to the CLI.	-
<b>CLI</b>	The <b>compare file</b> command returns error when device has active license.	113068
<b>CLI</b>	The <b>select</b> option of CLI filter does not work for some commands.	95478
<b>DHCP Relay L3</b>	It does not supported in VRF.	-
<b>DmView</b>	Status of some protocols are not shown in DmView (Info/Config).	90961
<b>EAPS</b>	When several EAPS instances are operating, new instance activation might take several minutes to be applied after commit. In this time interval the CLI is blocked for the operator until the creation process and apply is finished.	88879
<b>EAPS</b>	It is not recommended using more than 8 EAPS instances in the same ring.	-



Feature	Description	ID
<b>EAPS/ERPS</b>	To have commuting times of about 50ms with protocols ERPS and EAPS, it should be used at most 4 instances in the same ring.	-
<b>GPON Autoprovisioning</b>	Alarm of autoprovisioning may get stuck under some configuration conditions of GPON interface.	99261
<b>GPON Autoprovisioning</b>	Automatic deprovisioning of ONUs is not supported.	-
<b>GPON Counters</b>	There is no support to VEIP counters.	-
<b>GPON Ethernet UNI</b>	ONU profiles do not automatically create the Ethernet interfaces.	-
<b>GPON Firmware Update</b>	After version 4.0.2 it may occur configuration loss of GPON interfaces when upgrading from a firmware version before 4.0.2. To prevent this situation, check Compatibility between software versions section must be followed. It is also possible that third-party tools reveals incompatibility issues when using NetConf protocol to access the equipment and, in these cases, the GPON interface keys must be adjusted.	-
<b>GPON Flood Blocking</b>	Support to flood blocking only in Service-VLAN type N:1.	-
<b>GPON IP Spoofing</b>	There is no support to disabling the IP Spoofing mechanism in GPON interfaces.	-
<b>GPON IP Spoofing</b>	Double tag traffic will only work with allowed ip all rule applied to the service-port.	-
<b>GPON IP Spoofing</b>	DHCP client negotiates and receives IP address, however, the rule is not created in allowed IP list because all filters are used in equipment.	-
<b>GPON Multicast</b>	IGMP is only possible in N:1 VLAN type.	-
<b>GPON MPLS</b>	VPWS port-based with Ethernet loop as access interface does not pass traffic.	-
<b>GPON MPLS</b>	PPPoE and DHCP circuit information is not sent over L2VPN with service-port access.	F1789
<b>GPON ONU</b>	Possibility of error like <b>Restarting CLI</b> when executing "shutdown" followed by "commit" in a UNI interface of ONU.	87508

Feature	Description	ID
<b>GPON ONU</b>	After several ONU firmware update executions using the parameter all, new firmware update commands are not processed until shut/no shut is performed in the PON links where the firmware update processes took place.	126539
<b>GPON ONU</b>	Dying Gasp is not supported for ONU SFP TEO-GNUK-S20B.	
<b>GPON ONU SNMP</b>	Monitoring of Ethernet ports ONU traffic by SNMP with flow greater than 38 Mbps does not work properly.	-
<b>GPON PON Interfaces</b>	It is not possible to execute some commands of GPON when using a range of GPON interfaces.	102236
<b>GPON PON Interfaces</b>	PONLINK LOS alarm generation eventually fails, without any further impact to the PONLINK, when the fiber is reconnected or other PONLINKs in the equipment. ONU LOSi alarms are generated normally during this error. The issue happens when there is an intermittent connection between the fiber and the ONT and after reconnecting the fiber to the PONLINK the system operates normally.	-
<b>GPON POTS</b>	There is no support to shutdown POTS UNI interface.	-
<b>GPON Service-Port</b>	Partial and not functional configuration of service port created using netconf in versions lower 5.6 can cause impossibility to update firmware to version 5.6 or above.	-
<b>GPON SIP Profile</b>	There is no support to Call ID and Call forwarding configuration.	-
<b>GPON SIP Profile</b>	SIP server port is fixed as 5060.	-
<b>GPON SIP Profile</b>	It is allowed to configure the field display-name in a SIP agent profile with a string greater than 25 character, but the only first 25 characters are used.	108932
<b>GPON SNMP</b>	Poor performance in GEM counters by SNMP.	144319
<b>Interfaces</b>	Commit warnings are not generated if changes are made to a range of interfaces rather than a specific interface.	99138
<b>Interfaces</b>	During the initialisation of DM4610 or DM4615 equipment, its interfaces may go to UP for 30 seconds even if the interfaces are in "shutdown" administratively.	-
<b>IP Routing</b>	Unable to execute "show ip ..." commands on two CLI sessions simultaneously. It is necessary to wait for the execution of the command before executing another.	M1253 M1254

Feature	Description	ID
<b>IP Routing</b>	If the equipment receives an ARP on an L3 interface asking for another L3 network and this host is reachable by some interface of this equipment, the equipment insert an entry in the host-table with the interface that the ARP was originated if receives an GARP when host is in failed state. This behavior causes traffic to this host to not be forwarded to the correct interface.	155887
<b>LAG</b>	If a equipment does not have MPLS settings and MPLS packets pass through a LAG of this equipment, the traffic will not be balanced properly.	US86449
<b>LAG</b>	A LAG stays up even it has less active interface than defined in minimum-active links if this setting is made only one side of the link. To operate correctly, the minimum-active links must be configured on both sides.	105313
<b>LDP</b>	There are no support to LDP Allocation mode Independent, LDP Encapsulation mode explicit-null, LDP Distribution mode On Demand, LDP Retention mode Conservative.	-
<b>LDP</b>	It is not possible the change the loopback IP address and enable the LDP protocol in a single commit.	US89105
<b>LDP</b>	When the ARP packets forwarded to the CPU is over than rate limit configured for the interface, the LDP sessions might not be established.	M43 M778
<b>LLDP</b>	When a packet with an invalid TLV is received, the valid content of the packet may be discarded and no neighbor information is displayed.	121683
<b>License</b>	In equipment with MPLS license enabled, it could occur a failure when loading a configuration file with load override.	106007
<b>License</b>	When disabled the MPLS license with an invalid key, it will be displayed a error messaged as if the user was trying to enable the license.	-
<b>L2VPN</b>	The <b>show mpls l2vpn counters</b> commands does not support autocomplete of the parameters.	M841
<b>L2VPN</b>	The <b>show mpls l2vpn hardware</b> command works only for VPWS.	US78815
<b>L2VPN</b>	During traffic convergence in network with interoperability with non Datacom equipment, the pseudowire may fail (L2VPN).	M1360
<b>L2VPN</b>	When there is a lag interface with LACP as a VPWS or VPLS access, the VPN counters are incremented by LACP control packets.	99727
<b>L2VPN</b>	Broadcast, multicast and unknown unicast packets are duplicate and counted twice in the VPN VPLS ingress counters. The duplicate packet is discard and the interface discarding counter is incremented.	-
<b>L2VPN</b>	VPN access interface counters can be incremented even when TX traffic is discarded.	121403

Feature	Description	ID
<b>L2VPN</b>	GMRP protocol BPDUs do not pass through VPLS, even with TLS enabled.	133639
<b>L2VPN</b>	Multicast packets encapsulated in L2VPNs are not registered in ingress counters of VPN uplink interfaces.	127464
<b>L2VPN</b>	L2VPN vlan-based and L2 circuit with QinQ enabled in the same interface access does not work.	-
<b>L2VPN</b>	The Backup PW uses the PW Status TLV to signal the main and backup PW information, for this reason it is necessary that neighbors have support for PW Status TLV and this TLV is enabled in L2VPN.	144471
<b>L3VPN</b>	It is not possible to change VRF name of an existing BGP instance.	113503
<b>MAC Addresses</b>	The <b>show mac-address-table</b> command presents invalid parameters in autocomplete of CLI.	91495
<b>MAC Addresses</b>	The <b>show mac-address-table type static</b> command shows all entries of MAC table.	91496
<b>MAC Addresses</b>	The repeat option was removed from <b>show mac-address-table</b> command due high CPU utilization.	140053
<b>OSPF</b>	It's not possible show details of a specific OSPF neighbor. Through of <b>show ip ospf neighbor detail</b> command, it is possible to check all neighbors simultaneously.	91647
<b>OSPF</b>	If OSPF configuration was removed and reinserted with area index changed in a single commit, it is need to reinserted the L3 interface in OSPF configuration.	96565
<b>OSPF</b>	OSPF agencies in the same physical port cannot have different passwords.	-
<b>QoS - Policer</b>	Policer egress counters do not work when there is an user-defined counter in the same VLAN.	-
<b>PBR</b>	It does not support PBR with ECMP.	138443
<b>Ping</b>	Ping does not for work for local address destination when it is specified a source interface.	105307
<b>Ping</b>	The IP address specified by the source interface parameter in the ping command is not respected when in VRFs.	120791
<b>Ping</b>	Ping does not for work for IPv6 local address destination in VRF.	152836
<b>Ping</b>	When a VRF interface is specified as a ping source, the IP address used as the source of the packet it not necessarily the address of the interface. The source interface will only specify in which VRF the ping will be executed.	-
<b>Ping</b>	In an equipment with VRF leaking and redistribute BGP in OSPF, it is not possible ping directly connected addresses.	123157

Feature	Description	ID
<b>Radius</b>	RADIUS authentication for IPv6 management is not supported.	F1618
<b>RDM</b>	After removing the RDM configuration from a slave equipment that had already established connection with a master RDM, show commands will keep displaying RDM informations that are not in the configuration anymore.	126618
<b>RSVP</b>	Tunnel establishment is supported only in the same OSPF area (intra-area).	-
<b>RSVP</b>	Tunnel in headend may not work if OSPF router-id was changed in tailend. Workaround is run <i>clear ospf process</i> command in the tailend equipment.	154174
<b>RSVP</b>	<i>Fast Reroute</i> and bandwidth reservation are not supported.	-
<b>SCP - Passwords</b>	When the password has special characters, you must enter the password in single quotation marks (") or use the wizard mode (enter the command without entering the password parameter so it will be prompted and then no quotation marks are needed).	-
<b>Sensors</b>	Possibility of error log from sensors of equipment.	117219
<b>SNMP</b>	When configuring a L3 interface in VRF with <i>snmp agent listen</i> , it is possible wich is allowed SNMP get using the loopback IP address if is configured in the same VRF of L3 interface.	-
<b>SNMP</b>	When configuring SNMP agent listen with loopback interface, the reply will be done with the loopback IP address and does not with the L3 interface IP address on which packet was sent.	-
<b>SNMP</b>	To get SNMP objects using IP address in VRFs it is necessary configure the <i>snmp agent listen interface</i> . If is not configured, the equipment will be reply using the global routing table if exists route in this table.	-
<b>SNMP</b>	If SNMP agent listen was configured in a L3/loopback interface and the IP/VRF configuration of this interface was changed, the SNMP get would not work. To workaround this issue it is necessary configure the interface before adding interface in SNMP agent listen.	125267
<b>SNTP</b>	Packet from SNTP SNTP server version 4 or earlier are discarded.	124339
<b>SSH</b>	It's possible occurs <b>Error: application timeout</b> message when to try generate SSH key. On retry the problem will not occur.	-
<b>Switching</b>	There is no support to TPID configuration.	-
<b>Switching</b>	The user cannot configure tagged or untagged members in VLAN ranges in a one-line CLI command.	-

Feature	Description	ID
<b>Switching</b>	Many time necessary for manipulation, show and commit of large amount of VLAN.	91367
		99040
		116112
		116179
		116724
<b>Syslog</b>	Possibility of coredumps when performing <b>load override</b> command for load some specific configuration.	117306
<b>Syslog</b>	Modification in l3 interfaces used for reaching the syslog server may cause the syslog server not to work. As a workaround, it is needed to remove the syslog configuration, commit it and configured it again.	127781
<b>TACACS+</b>	TACACS+ authentication for IPv6 management is not supported.	F1620
<b>TACACS+</b>	Command with more than 243 characters are not sent to the accounting server.	111614
<b>TACACS+</b>	Commands may not be registered in the accounting server when the command is executed and the user immediately logs out.	-
<b>TACACS+</b>	ERROR message generated in log when applying configuration of Banner using the multiline mode.	111616
<b>TACACS+</b>	Commanded reject by TACACS+ server are being registered in the accounting log.	122945
<b>Transceivers</b>	Order of transceivers is not displayed in ascending order on command <b>show interface transceivers</b> .	99257
<b>Transceivers</b>	Only are supported 100 Mbps optical transceivers in forced mode and only in GX interfaces.	-
<b>Transceivers</b>	Log of link UP is generated whenever an SFP Copper is inserted even without physical cable.	94344
<b>Transceivers</b>	Transceiver inventory informations are shown duplicated in DmView.	126537
<b>Transceivers</b>	Electrical transceiver negotiated in half-duplex shows full-duplex in DmOS.	US93493
<b>xSTP</b>	RSTP does not work if dot1q is not configured.	88154
<b>xSTP</b>	There is no support to BPDU options like: BPDU Guard and BPDU Filter.	F1131
<b>xSTP</b>	STP does not work with EAPS configured in the same interface.	-

### 4.3 Hardware Platforms Restrictions

DmOS has the following restrictions for affected platform:

Feature	Description	ID	Affected Platforms
<b>ACL</b>	ACL action of PCP set is not being performed when QinQ is configure an interface.	112774	DM4270
<b>BFD</b>	It does not support BFD.	-	DM4050, DM4250, DM461x
<b>Interfaces</b>	The MDIX works in reverse in interfaces gigabit-ethernet 1/1/1, 1/1/5, 1/1/9, 1/1/14, 1/1/17 e 1/1/21 if it is configured as forced. MDIX works as expected when in automatic mode.	93744	DM4050, DM4250
<b>Interfaces</b>	The MTU value in GT and GX interfaces is actually 4 bytes smaller than the configured value when the interface is untagged.	-	DM4050, DM4250
<b>L2CP</b>	L2 PDUs transparency in TLS services (service vlan type TLS) is enabled without the possibility of changing this behavior. For 1:1 and N:1 services (service vlan type 1:1 or n:1), L2 PDUs transparency is intrinsically disabled.	-	DM461x
<b>L2VPN</b>	MAC address limit is not supported in VPLS.	-	DM4270, DM4380, DM4775
<b>LAG</b>	Dynamic load-balancing (DLB) mode is not supported.	-	DM4360, DM4370, DM4611, DM4612
<b>LAG</b>	Equipment that do not support MPLS on the chipset do not consider MPLS labels on the traffic balancing.	-	DM4050, DM4250
<b>Management Out-Band</b>	It does not support 10Mbps in MGMT interface. For correct operation, 100 Mbps speed or higher must be used.	-	DM4050, DM4250
<b>MPLS</b>	It does not support MPLS.	-	DM4610-HW1, DM4611, DM4612
<b>MPLS</b>	To work the PDUs encapsulation in L2VPNs it is necessary to remove the remote-devices feature that is enabled in the default configuration. <i>configure; no remote-devices; commit.</i>	-	DM4360, DM4370

Feature	Description	ID	Affected Platforms
<b>PBR</b>	It does not support Policy Based Routing (PBR).	-	DM4360, DM4370, DM4611, DM4612
<b>HQoS</b>	It does not support Hierarchical Quality of Service (HQoS).	-	DM4170, DM4270, DM4380, DM4770
<b>QoS - Policer</b>	The ingress Policer matching filters do not consider possible packet modifications due to ACLs rules.	-	DM4050, DM4250
<b>QoS - Policer</b>	ARP Request packets can be dropped by the Ingress Policers.	-	DM4050, DM4250
<b>QoS - Policer</b>	Drop counters in egress stage policers are not supported in DM461x platforms.	-	DM461x
<b>QoS - Policer</b>	Packets discarded by egress policers are not incremented in user-defined egress counters in DM461x platform.	-	DM461x
<b>QoS - Policer</b>	Egress Policer does not limit the packets by VLAN on an untagged interfaces.	-	DM4270, DM4380, DM4775
<b>QoS - Scheduler</b>	The weights configured in a QoS Scheduler are not respected with average flow lower than 129 Bytes.	-	DM4050, DM4250
<b>RSVP</b>	It does not support RSVP.	-	DM461x
<b>SNMP</b>	Dying Gasp SNMP traps are not sent for SNMP targets associated to mgmt VRF or user VRFs.	US90189 US90190	DM4360, DM4370
<b>Switching</b>	It does not support in-Band management with a VLAN used in vlan-translate without having QinQ enabled in the interface.	-	DM4270
<b>Switching</b>	Double tagged packets do not add VLAN tag using VLAN mapping if QinQ is not enabled in interface.	-	DM4270, DM4380, DM4770
<b>Switching</b>	It does not support VLAN mapping.	-	DM4611, DM4612
<b>System</b>	It does not support CPU DoS Protect rate limit configuration.	-	DM4050, DM4250



Feature	Description	ID	Affected Platforms
<b>System</b>	In scenarios with a high number of ONUs the CPU can get high usage generating alarm.	148808	DM4610 HW2, DM4611, DM4612
<b>System</b>	The hostname size will be limited in less than 63 characters when the equipment has DHCP Relay L2 enabled and use hostname in circuit-id format.	-	DM461x
<b>Transceivers</b>	When enabling negotiation in 10G interface the link will transition from UP to DOWN and then returning to UP, remaining stable.	116953	DM4050, DM4250
<b>Transceivers</b>	Removal of a SFP and insertion of another one in an interface may not be identified if it is performed in less than 3 seconds.	109496	DM4170
<b>Transceivers</b>	The GX interfaces of DM4610 platform do not support Copper SFPs at speeds of 10 and 100 Mbps. Some models of Copper SFPs can operate at speeds of 1 Gbps, but are not homologated by DATACOM.	-	DM461x
<b>Transceivers</b>	The 10 Gbps interfaces do not support autonegotiation.	-	DM4270 48XS
<b>Transceivers</b>	The 25 Gbps interfaces do not support autonegotiation.	-	DM4770 16CX
<b>TWAMP</b>	It does not support TWAMP.	-	DM461x
<b>VRF</b>	It does not support VRF.	-	DM4050, DM461x

## 5 Document Versions

The following table lists all documents for DmOS products. DATACOM do not recommend the usage of previous versions.

### 5.1 Software Platform

Document	Version
DmOS - Troubleshooting Guide	204.4293.22
DmOS - Quick Configuration Guide	204.4292.30
DmOS - Command Reference	204.4284.38
DmOS - Datasheet	134.4918.19

### 5.2 Hardware Platform

Document	Version
DM4050 - Installation Guide	204.4317.03
DM4170 - Installation Guide	204.4308.05
DM4250 - Installation Guide	204.4312.01
DM4270 - Installation Guide	204.4331.07
DM4360 - Installation Guide	204.4337.01
DM4370 - Installation Guide	204.4314.02
DM4380 - Installation Guide	204.4336.00
DM4610 - Installation Guide	204.4291.04
DM4611 - Installation Guide	204.4349.01
DM4612 - Installation Guide	204.4350.01
DM4615 - Installation Guide	204.4323.03
DM4770 - Installation Guide	204.4339.10
DM4775 - Installation Guide (Portuguese only)	204.0337.00

## 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.

© 2022 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**