

DATACOM



DmOS

DmOS 7.2.0 - Command Reference

204.4284.38

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

DATACOM 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.

DATACOM 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:

DATACOM

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](#)).

INTRODUCING THE COMMAND REFERENCE

About this Guide

This guide provides command line interface (CLI) related information. This document describes how to use the CLI and it also covers initial configurations, those normally needed after hardware installation.

The document was designed to serve as a source of eventual queries. Therefore, it does not need be read sequentially. This guide provides command reference for each of the CLI commands available on the DmOS.

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


Intended Audience







The User Guide of each product is intended for Network Administrators and other qualified service personnel responsible for deploying, operating and maintaining the DmOS.

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	11
Chapter 2: Using the Command-Line Interface	12
Supported Platforms	12
Command Syntax	12
Common Parameter Values	13
Using the "No" Form of a Command	13
CLI Output Filtering	14
Command Modes	15
Command Completion and Abbreviation	15
CLI Error Messages	16
CLI Line-Editing Conventions	17
Using CLI Help	18
Accessing the CLI	20
Special Characters on CLI	20
Chapter 3: Management	22
CLI Settings	22
Interfaces	36
Configuration	41
Firmware	125
Diagnostics	129
SNMP	210
License	238
Chapter 4: Interfaces	243
Ethernet	243
L3	290
Loopback	310
Chapter 5: Layer 2 - Switching Protocols	316
MAC Learning	316
VLAN	334
Link Aggregation	360
Spanning-Tree	373
ERPS	386
EAPS	397
Control Protocols	406
Loopback Detection	417

Link Flap Detection	423
Hold Time	430
Backup Link	432
Chapter 6: Layer 3 - Routing	436
Basic	436
BFD	485
BGP	488
OSPF	678
OSPFv3	783
VRRP	849
PBR	881
VRF	889
Chapter 7: MPLS	899
Infra	899
L2VPN	917
L3VPN	1080
RSVP	1084
LDP	1135
Chapter 8: Multicast	1166
IGMP Snooping	1166
Chapter 9: Quality of Service	1229
QoS Policer	1229
QoS Packet Scheduler and Egress Shapers	1249
Storm Control	1259
Chapter 10: Access Lists	1263
Basic ACLs	1263
Chapter 11: Security	1288
AAA	1288
Port Security	1312
Chapter 12: OAM	1323
Continuity Check and Fault Management	1323
Activation Test	1372
EFM	1375
LLDP	1380
TWAMP	1395

sFlow	1451
Remote Devices Management	1461
Chapter 13: Synchronization	1466
NTP	1466
Chapter 14: GPON	1482
OLT	1482
ONU Profiles	1528
ONU	1574
Chapter 15: Services	1623
Management	1623
System	1658
DHCP	1685
PPP	1698
Chapter 16: Hardware	1704
Environment	1704
Resources	1713
Chapter 17: CPU Protection	1717
CPU DoS Protection	1717

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:

- [Supported Platforms](#)
- [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](#)

SUPPORTED PLATFORMS

Consult Hardware and Software Compatibility in Release Notes to check supported platforms.

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
syntax error: unknown command	Indicates that the command there is not in the CLI.
syntax error: unknown argument	Indicates that the argument there is not for the command.
syntax error: unknown element	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.

Table 2: CLI Editing Conventions

Key Sequence	Description
<Tab>	Command-line completion.
Exit	Go to next lower command prompt.
?	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.

specialCharactersCli

SPECIAL CHARACTERS ON CLI

Some characters have special interpretations for the command line.

Table 3: Special Characters on CLI

Character	Description
?	List available commands, keywords, or parameters.
! and #	It is interpreted as a comment.
\	It is interpreted as escape character.
	It is interpreted as output modifier. Used with output filtering commands.
;	Used to indicate end of a command line.
"	Used to delimit a string.

If it is necessary to use the characters above on a string, put the string between double-quotes (").

CHAPTER 3: MANAGEMENT

This chapter describes the commands related to management access in the DmOS CLI.

CLI SETTINGS

This topic describes the available settings used in a command-line interface (CLI) session. Changes on these settings are applied only to the current session.

debug

Description

This command is used to enable or to disable debug messages. The debug messages are printed only on the user session that enabled the debugs and these messages are not logged. After user logout, the user session is closed and all enabled debugs of that session are automatically disabled.

Supported Platforms

This command is supported in all platforms.

Syntax

debug { *enable* | *disable* } [*link-status*]*

Parameters

enable

Description: Enable the specified list of debug commands.

Value: N/A

Default Value: N/A

disable

Description: Disable the specified list of debug commands or disable all debug commands enabled in the current user session.

Value: N/A

Default Value: If none command is specified then the command “debug disable” will disable all debugs.

link-status

Description: Displays a debug message if a link status is changed.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Use the **debug enable** command to see the debug messages of a command or a list of commands. And use the **debug disable** to see no more debug messages of all commands or of some commands.

Impacts and precautions

The use of **debug enable** with many **commands** over serial interface may cause the session to become unresponsive to user intervention. Consider this before issuing the

respective command.

Hardware restrictions

N/A

display-defaults

Description

Shows default values as comments when showing the configuration. This setting is valid for the current session only.

Supported Platforms

This command is supported in all platforms.

Syntax

display-defaults *{true|false}*

Parameters

{true|false}

Description: Sets display-defaults to true (enabled) or false (disabled).

Value: true or false

Default Value: false

Default

The display of default values is disabled.

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.10	Command show-defaults was replaced by display-defaults

Usage Guidelines

If show-defaults is set to true, the default values, if available, are shown as comments after the actual parameter value:

Examples:

```
# display-defaults true
# show running-config aaa
aaa user admin
  password $1$SzCHCSOa$IiVcIUUino2s12Wk1Rdwa/
  group admin      ! audit
!
# show running-config mac-address-table
mac-address-table
  aging-time 600      ! 600
!
```

Note that even if the parameter is set to the default value, it is shown again in the comment.

Impacts and precautions

This command takes effect for the current session only, if the change is to be made persistent, use command “session display-defaults” or “user <username> session display-defaults” instead.

Hardware restrictions

N/A

screen-resize

Description

Adjust the screen size following the current size of screen being used. If the screen size is changed the command must be run again.

Supported Platforms

This command is supported in all platforms.

Syntax

screen-resize

Parameters

N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

Example:

```
# screen-resize
```

In configuration mode:

```
(config)# do screen-resize
```

Impacts and precautions

N/A

Hardware restrictions

N/A

session

Description

Configures global default CLI session parameters.

Supported Platforms

This command is supported in all platforms.

Syntax

session [**complete-on-space** {*true|false*}] [**ignore-leading-space** {*true|false*}] [**idle-timeout** *seconds*] [**paginate** {*true|false*}] [**history** *size*] [**display-defaults** {*true|false*}]

Parameters

complete-on-space {*true|false*}

Description: Controls if command completion should be attempted when <space> is entered. Entering <tab> always results in command completion.

Value: true or false

Default Value: false

ignore-leading-space {*true|false*}

Description: Controls if leading spaces should be ignored or not. This is useful to turn off when pasting commands into the CLI.

Value: true or false

Default Value: true

idle-timeout *seconds*

Description: Maximum idle time before being logged out. Use 0 (zero) for infinity.

Value: 0-8192

Default Value: 1800

paginate {*true|false*}

Description: Enables/Disables pagination of command output.

Value: true or false

Default Value: true

history *size*

Description: Size of CLI command history.

Value: 0-8192

Default Value: 100

display-defaults {*true*|*false*}

Description: Controls if defaults values should be shown when displaying the configuration. The default values are shown as comments after the configured value.

Value: true or false

Default Value: false

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release

Modification

1.0

This command was introduced.

5.4

The display-level option was removed.

Usage Guidelines

N/A

Impacts and precautions

This command sets the default settings for new sessions. It can be overridden by the corresponding configuration in operational mode or “user <username> session” commands. Use “show cli” command in operational mode to check the actual values.

Hardware restrictions

N/A

user

Description

Configures default CLI session parameters per user

Supported Platforms

This command is supported in all platforms.

Syntax

```
user user-name [description description] [alias alias_name expansion command]  
[session [complete-on-space {true|false}] [ignore-leading-space {true|false}] [idle-  
timeout seconds] [paginate {true|false}] [history size] [display-defaults {true|false}]]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

user-name

Description: Name of the user for which the CLI options are being set.

Value: Text

Default Value: N/A

description *description*

Description: Adds a description for the user.

Value: Text

Default Value: N/A

alias *alias_name*

Description: Creates a command alias.

Value: Text

Default Value: N/A

expansion *command*

Description:	Sets the original command to be replaced by the alias.
Value:	Text
Default Value:	N/A

session

Description:	Configures session parameters to be used as default for the specified user. These settings can be overridden by the corresponding configuration in operational mode. Use "show cli" command in operational mode to check the actual values.
Value:	N/A
Default Value:	N/A

complete-on-space {*true|false*}

Description:	Controls if command completion should be attempted when <space> is entered. Entering <tab> always results in command completion.
Value:	true or false
Default Value:	false

ignore-leading-space {*true|false*}

Description:	Controls if leading spaces should be ignored or not. This is useful to turn off when pasting commands into the CLI.
Value:	true or false
Default Value:	true

idle-timeout *seconds*

Description:	Maximum idle time before being logged out. Use 0 (zero) for infinity.
Value:	0-8192
Default Value:	1800

paginate {*true|false*}

Description:	Enables/Disables pagination of command output.
Value:	true or false
Default Value:	true

history *size*

Description: Size of CLI command history.

Value: 0-8192

Default Value: 100

display-defaults {*true*|*false*}

Description: Controls if defaults values should be shown when displaying the configuration. The default values are shown as comments after the configured value.

Value: true or false

Default Value: false

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

N/A

Impacts and precautions

This command sets the default settings for a specified user. It can be overridden by the corresponding configuration in operational mode. Use “show cli” command in operational mode to check the actual values. There is no check whether the user exists or not in database. This allows remote logged users to have a customized CLI environment.

Hardware restrictions

N/A

INTERFACES

This topic describes the commands related to management interfaces such as commands to configure console and Management-Ethernet (outband).

interface mgmt

Description

Configures management interface.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface mgmt interface [ vrf vrf-name | description if-description | ipv4 address a.b.c.d/x | ipv6 { enable | address x:x:x:x::x/y [ eui-64 ] | nd ra { suppress | max-interval | min-interval | prefix x:x:x:x::x/y [ no-advertise | no-autoconfig | off-link ] } } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface

Description: Management Ethernet interface in chassis/slot/port.

Value: chassis/slot/port

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this interface will be associated with. Currently, it is possible to configure only the VRF 'mgmt'.

Value: string.

Default Value: N/A

description *if-description*

Description: Specifies the description of the interface. It may point out a more meaningful text about its purpose.

Value: Must be a valid string.

Default Value: N/A

ipv4 address *a.b.c.d/x*

Description: Specifies an IPv4 address and prefix length, in CIDR notation, to be assigned to management interface.

Value: a.b.c.d/x.

Default Value: 192.168.0.25/24

ipv6 enable

Description: Enables/Disables IPv6 on management interface. When enabled, the system automatically configures an IPv6 link-local address to management interface.

Value: N/A

Default Value: Disabled.

ipv6 address *x:x:x:x::x/y*

Description: Specifies an IPv6 unicast address and prefix length to be assigned to management interface.

Value: x:x:x:x::x/y.

Default Value: N/A

eui-64

Description: Sets 64-bit Extended Unique Identifier for specific IPv6 prefix on management interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra suppress

Description: Suppresses Router Advertisements on the management interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x:x:x:x::x/y*

Description: Prefix Address to be advertised on the specified management interface.

Value: *x:x:x:x::x/y*.

Default Value: N/A

ipv6 nd ra prefix *x:x:x:x::x/y* **no-advertise**

Description: Disable this prefix on Router Advertisement of management interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x:x:x:x::x/y* **no-autoconfig**

Description: Disable auto configuration of hosts by management interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x:x:x:x::x/y* **off-link**

Description: When disabled, indicates that this prefix can be used for on-link determination on management interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra max-interval *max-interval*

Description: The maximum time allowed between sending unsolicited multi-cast router advertisements from the interface, in seconds.

Value: Must be no less than 4 seconds and no greater than 1800 seconds.

Default Value: 600

ipv6 nd ra min-interval *min-interval*

Description: The minimum time allowed between sending unsolicited multi-cast router advertisements from the interface, in seconds.

Value: Must be no less than 3 seconds and no greater than $0.75 * \text{MaxRtrAdvInterval}$.

Default Value: 198

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
2.4	IPv6 support. VRF support.
4.8.0	Support to IPv6 ND Router Advertisement.

Usage Guidelines

It is possible the use of only one IPv4 address and/or two IPv6 addresses on management interface.

Command to configure IPv6 addresses will be available only if `ipv6 enable` is set for interface. Example below shows that IPv6 address configuration option appears after `ipv6 enable` is set.

```
(config-mgmt-1/1/1)# ipv6 ?
Possible completions:
enable    Enable IPv6 on interface
!
(config-mgmt-1/1/1)# ipv6 enable
!
(config-mgmt-1/1/1)# ipv6 ?
Possible completions:
address   IPv6 address
enable    Enable IPv6 on interface
!
```

To find which management interface is configured with a specific IP address, it is possible

to use the commands showed in the example below.

Example:

This example shows all management interfaces:

```
# show running-config interface mgmt all
interface mgmt 1/1/1
ipv4 address 192.168.0.25/24
ipv6 enable
ipv6 address 2001:db8::10/32
!
```

Or in configuration mode:

```
(config)# show interface mgmt all
interface mgmt 1/1/1
ipv4 address 192.168.0.25/24
ipv6 enable
ipv6 address 2001:db8::10/32
!
```

If no VRF is explicitly associated with the mgmt interface, it is associated with the global VRF by default. The following example shows how to associate a management interface with the 'mgmt' VRF:

```
(config-mgmt-1/1/1)# ?
Possible completions:
vrf          Assign a VRF instance to the interface
!
(config-mgmt-1/1/1)# vrf ?
Possible completions:
<WORD>       VPN Routing/Forwarding instance name
mgmt
!
(config-mgmt-1/1/1)# vrf mgmt
(config-mgmt-1/1/1)# commit
Commit complete.
```

Impacts and precautions

Once the VRF associated with the mgmt interface is changed, any route in the previous VRF using it as output interface will be uninstalled. In order to keep the connectivity, you will need to configure the routes in the new VRF.

Hardware restrictions

N/A

CONFIGURATION

This topic describes the commands related to configuration management such as commands to backup or view the running-config content.

banner login

Description

This configuration represents the banner displayed when accessing the equipment via console, SSH or Telnet. This banner will be displayed before username and password prompts.

Supported Platforms

This command is supported in all platforms.

Syntax

banner login *banner-text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

banner-text

Description:	A text message representing the banner that will be shown before login on the equipment. The text can contain special characters including line breaks () and tabulations ().
Value:	Text with up to 3240 characters.
Default Value:	None

Default

None

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

It is possible to format the message using the following special characters:

- \n - New line
- \t - Horizontal tab
- \\ - Backslash

Example:

There are two ways to configure the login banner, the multiline mode and single line mode. In single line mode the banner text must be written in one line, if using spaces quotation marks will be required, to include line breaks use `\n` and to include tabs use `\t`. It is recommended to always include a line break at the end to avoid having the login prompt concatenated to the banner.

```
# config
Entering configuration mode terminal
(config)# banner login "***** BANNER *****"
(config)# commit
Commit complete.
```

It is possible to use the command `show banner login` to check how the banner will be displayed.

```
# show banner login
Login banner will be displayed as shown inside <>
<
*****
**  BANNER  **
*****
>
#
```

To use multi-line mode, press *Enter* after *banner login* and use *ctrl-D* when finished.

```
# config
Entering configuration mode terminal
(config)# banner login
(<Hit <cr> to enter in multi-line mode. Alternatively, enter a text between double quotes.
Remember to insert a line break at the end. See command reference for examples.
Maximum length of 3240 characters.>):
[Multiline mode, exit with ctrl-D.]
> *****
> ***    Only authorized personnel are allowed to access this piece of equipment. ***
> ***    Others are urged to log off IMMEDIATELY. ***
> ***
> ***    Somente pessoal autorizado pode acessar este equipamento. ***
> ***    Outros, por favor, desconectar IMEDIATAMENTE. ***
> ***
> *****
> ctrl-D
(config)# commit
Commit complete.
(config)# exit
# show banner login
Login banner will be displayed as shown inside <>
<
*****
***    Only authorized personnel are allowed to access this piece of equipment. ***
***    Others are urged to log off IMMEDIATELY. ***
***
***    Somente pessoal autorizado pode acessar este equipamento. ***
***    Outros, por favor, desconectar IMEDIATAMENTE. ***
***
*****
>
DM4610#
```

In multi-line mode, to use backslash, it is necessary include another backslash as escape character.

```
(config)# banner login
(<Hit <cr> to enter in multi-line mode. Alternatively, enter a text between double quotes.
Remember to insert a line break at the end. See command reference for examples.
Maximum length of 3240 characters.>):
[Multiline mode, exit with ctrl-D.]
>
|  _  \  / \ |  _  \  / \ |  _  \  / \ |  _  \  / \ | | | | | | | | |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
> ctrl-D
(config)# commit
Commit complete.
(config)# exit
# show banner login
Login banner will be displayed as shown inside <>
<
|  _  \  / \ |  _  \  / \ |  _  \  / \ |  _  \  / \ |
|  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |  |  |  /  \ |
```


clear

Description

Used to remove all configuration changes that were not committed, in other words, all uncommitted modifications made are discarded, returning the system to the state after the last commit.

Supported Platforms

This command is supported in all platforms.

Syntax

```
clear
```

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use the clear command. Modify the system configuration. In the example below, the management IP address is changed.

```
# config
Entering configuration mode terminal
(config)# show interface
interface mgmt 1/1/1
  ipv4 address 192.168.0.25/24
!
(config)# interface mgmt 1/1/1
(config-mgmt-1/1/1)# no ipv4 address
(config-mgmt-1/1/1)# ipv4 address 10.4.16.134/22
(config-mgmt-1/1/1)# exit
(config)# show interface
interface mgmt 1/1/1
  ipv4 address 10.4.16.134/22
!
(config)#
Clear all existing modifications.

(config)# clear
All configuration changes will be lost. Proceed? [yes, NO] yes
(config)#
(config)# show interface
interface mgmt 1/1/1
  ipv4 address 192.168.0.25/24
!
(config)#
```

Impacts and precautions

All uncommitted changes will be lost.

Hardware restrictions

N/A

commit

Description

Command used to confirm or abort a pending confirmed commit (see **commit confirmed** command for more details)

Supported Platforms

This command is supported in all platforms.

Syntax

```
commit { abort | confirm } { persist-id id }
```

Parameters

abort

Description: Aborts a pending confirmed commit

Value: N/A

Default Value: N/A

confirm

Description: Confirms a pending confirmed commit

Value: N/A

Default Value: N/A

persist-id *id*

Description: Specifies a **commit confirmed** to abort or confirm. This value is the same used in **commit confirmed persist** command

Value: Text

Default Value: N/A

Output Terms

Output	Description
Shows a message indicating the commit status	Examples of this command are displayed in the Usage Guidelines field

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced

Usage Guidelines

This command can be executed directly via CLI.

Examples:

The examples below shows how to use the command commit. Example 1 - Sequence of commands using commit confirm:

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
(config)# hostname TESTE-COMM
(config)# commit confirmed 1
Warning: The configuration will be reverted if you exit the CLI without
performing the commit operation within 1 minutes.
```

After applying a configuration using a specific timeout is possible to persist this configuration using the commit confirm command

```
TESTE-COMM(config)# end
TESTE-COMM# commit confirm
Commit complete. Configuration is now permanent
```

Example 2 - Sequence of commands using commit abort:

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
TESTE-COMM(config)# hostname DTC01
TESTE-COMM(config)# commit confirmed 1
Warning: The configuration will be reverted if you exit the CLI without
performing the commit operation within 1 minutes.
DTC01(config)# end

After applying a configuration using a specific timeout is possible to abort
this configuration using the commit abort command

DTC01# commit abort
Confirmed commit has been aborted. Old configuration will now be restored.
TESTE-COMM#
Message from system at 1970-01-01 02:37:53...
confirmed commit operation not confirmed by admin from cli
configuration rolled back
```

Impacts and precautions

N/A

Hardware restrictions

N/A

commit

Description

Copies configurations from candidate-config to running-config or confirms a pending commit. After that, the new configurations will be applied to the equipment.

Supported Platforms

This command is supported in all platforms.

Syntax

```
commit [and-quit | no-confirm] [ comment text ] [ label text ] [ persist-id id ] [ save-running file-name ]
```

Parameters

and-quit

Description: (Optional) Exits the configuration mode after completing the commit.

Value: N/A

Default Value: N/A

no-confirm

Description: (Optional) Commits without asking the user for confirmation when required.

Value: N/A

Default Value: N/A

comment *text*

Description: (Optional) Associates a comment with the commit. The comment can later be seen when examining rollback files.

Value: Text

Default Value: N/A

label *text*

Description: (Optional) Associates a label with the commit. The label can later be seen when examining rollback files.

Value: Text

Default Value: N/A

persist-id *id*

Description: (Optional) Specifies a pending commit to be confirmed.

Value: Text

Default Value: N/A

save-running *file-name*

Description: (Optional) Saves running-config into a file after the command completion.

Value: File name or path.

Default Value: N/A

Default

Copy candidate-config changes to running-config.

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

N/A

Impacts and precautions

N/A

Hardware restrictions

N/A

commit abort

Description

Aborts a pending confirmed commit.

Supported Platforms

This command is supported in all platforms.

Syntax

commit abort [**persist-id** *id*]

Parameters

persist-id *id*

Description: (Optional) Specifies a pending commit to be aborted.

Value: Text: **persist** *id* argument passed to **commit confirmed** command.

Default Value: N/A

Default

Abort pending confirmed commit.

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

N/A

Impacts and precautions

N/A

Hardware restrictions

N/A

commit check

Description

Used to validate the modifications made on the candidate-config. Syntax validation, integrity restrictions, YANG model validation points and coherence callbacks are assessed.

Supported Platforms

This command is supported in all platforms.

Syntax

commit check

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Examples:

This example shows how to use the commit check command. It includes a few additional steps only for better understanding.

Executing the command when everything is ok.

```
# config
(config)# hostname DmOS
(config)# commit check
Validation complete
(config)# commit
Commit complete.
```

Trying to configure mgmt interface ipv4 address as loopback address it is not allowed.

```
# config
DmOS(config)# interface mgmt 1/1/1
DmOS(config-mgmt-1/1/1)# show # existing configured IP
interface mgmt 1/1/1
    ipv4 address 10.4.16.129/22
!
DmOS(config-mgmt-1/1/1)# ipv4 address 127.0.0.1/8
DmOS(config-mgmt-1/1/1)# exit
DmOS(config)# commit check
Failed: 'interface mgmt 1/1/1 ipv4 address' (value "127.0.0.1/8"): IPv4 address
cannot be configured as loopback address
```

Impacts and precautions

N/A

Hardware restrictions

N/A

commit confirmed

Description

Used to copy the current candidate-config to the running-config with a timeout. If the **commit** command is not executed before the timeout expires, then the configuration will be reverted to the configuration that was active before the command was issued.

Supported Platforms

This command is supported in all platforms.

Syntax

```
commit confirmed [ timeout [persist id] [ comment text ] [ label text ] [ save-running file-name ] [persist-id id] ]
```

Parameters

timeout

Description: Sets the timeout (in minutes) to undo the commit.
Value: 0-71582788
Default Value: 10

persist *id*

Description: Creates a persistent confirmed commit to be used through different CLI sessions.
Value: Text
Default Value: N/A

comment *text*

Description: Associates a comment with the commit. The comment can be later verified when, for example, displaying the stored commit list.
Value: Text
Default Value: N/A

label *text*

Description: Associates a label with the commit. The label can be later verified when, for example, displaying the stored commit list.

Value: Text

Default Value: N/A

save-running *file-name*

Description: Saves running-config into a file after the command completion.

Value: File name.

Default Value: N/A

persist-id *id*

Description: Specifies an existing pending commit to be confirmed or updated.

Value: Text

Default Value: N/A

Default

Undo the committed changes after the default timeout (10 minutes).

Command Mode

Configuration mode

Required Privileges

Audit

History**Release****Modification**

1.0

This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Examples:

These examples show how to use the “commit confirmed” command.

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
(config)# hostname DTC001
(config)# commit confirmed 30
Warning: The configuration will be reverted if you exit the CLI without
performing the commit operation within 30 minutes.
DTC001(config)#
DTC001(config)# commit
Commit complete. Configuration is now permanent.
```

Commit confirmed without confirmation.

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
(config)# hostname DTC001
(config)# commit confirmed 2
Warning: The configuration will be reverted if you exit the CLI without
performing the commit operation within 2 minutes.
DTC001(config)#
(after 2 minutes)
Message from system at 1970-01-01 01:36:22...
confirmed commit operation not confirmed by admin from cli
configuration rolled back
(config)#
```

Persisting a **commit confirmed** through CLI sessions.

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
(config)# hostname DTC001
(config)# commit confirmed 300 persist commit-confirmed-label
Commit complete.
DTC001(config)# exit
DTC001# exit
Connection to 10.4.16.129 closed.
(open a new connection)
Welcome to the DmOS CLI
admin connected from 10.4.4.22 using ssh on DTC001
DTC001# config exclusive
Aborted: confirmed commit in progress
DTC001# commit persist-id commit-confirmed-label
Commit complete. Configuration is now permanent.
```

Impacts and precautions

Only available in exclusive mode.

To confirm the pending commit use the **commit** command.

To abort the pending commit use the **commit abort** command.

The pending commit will be aborted if the CLI session is terminated before confirming the commit, unless the **persist** argument is given. In the latter case, a future session may confirm the pending confirmed commit by supplying the **persist** *id* as an argument to the **commit** command using the **persist-id** parameter. During the period this pending commit exists, access to exclusive sessions are not allowed. Configurations from terminal sessions are allowed, but if the pending commit is aborted all changes will be lost.

Hardware restrictions

N/A

compare file

Description

Command used to compare the running-config with a configuration previously saved into a file. The differences are marked with diff notation:

- '+' means config is present in the file, not in running-config;
- '-' means config is present in the running-config, not in the file;

Supported Platforms

This command is supported in all platforms.

Syntax

compare file *config-file-name* [*pathfilter*]

Parameters

config-file-name

Description: Specifies the file to be compared with the running-config.

Value: Text

Default Value: N/A

pathfilter

Description: Filters a specific set of configuration for comparison.

Value: Text

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
4.4	The option 'brief' was removed. The command will always show only the differences, not the whole configuration.

Usage Guidelines

This example shows how to use the **compare file** command. It includes a few additional steps only for better understanding.

Example:

Saving the current configuration and comparing it after some changes:

```
DmOS# config
Entering configuration mode terminal
DmOS(config)# save current-cfg
DmOS(config)# alias alias_cmd01 expansion test1
DmOS(config-alias-alias_cmd01)# exit
DmOS(config)# alias alias_cmd02 expansion test2
DmOS(config-alias-alias_cmd02)# exit
DmOS(config)# alias alias_cmd03 expansion test3
DmOS(config-alias-alias_cmd03)# exit
DmOS(config)# commit
Commit complete.
DmOS(config)# exit

DmOS# compare file current-cfg
-alias alias_cmd01
- expansion test1
-!
-alias alias_cmd02
- expansion test2
-!
-alias alias_cmd03
- expansion test3
-!
```

Showing a removed config:

```
# config
(config)# no alias alias_cmd01
(config)# exit
# compare file current-cfg
+alias alias_cmd01
+ expansion test1
+!
```

Impacts and precautions

When TACACS+ authorization is enabled and the user is allowed to execute the command **compare file** the comparison will be performed in 2 different ways, depending on the config file format:

- a) If the config is stored in text format, which is the default format, the comparison will be done based on the user permission to execute each command present in the config-file. Thus, commands not allowed to be executed by the user will generate an error message in the comparison output.
- b) If the config is stored in XML format, no additional command authorization is needed for the user.

Hardware restrictions

N/A

config

Description

Used to enter the equipment configuration mode and change its configurations.

Supported Platforms

This command is supported in all platforms.

Syntax

config [**terminal** | **exclusive**]

Parameters

terminal

Description: Edits a private copy of the configuration without locking it.

Value: N/A

Default Value: N/A

exclusive

Description: Creates a lock in candidate-config allowing only one exclusive session. The access using a different mode is allowed but attempts to change the configurations will be denied.

Value: N/A

Default Value: N/A

Default

If no option is passed to the command **terminal** mode is used.

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
4.0	Removed 'config shared' command.

Usage Guidelines

This command can be executed directly via CLI.

Examples:

Accessing terminal mode.

```
# config
Entering configuration mode terminal
(config)#
```

Accessing exclusive mode.

```
# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
(config)#
```

Trying to open a second exclusive session.

```
# config exclusive
Error: configuration database locked by:
admin ssh (cli from 10.4.4.22) on since 1970-01-02 00:24:01
exclusive
Aborted: configuration locked
```

Impacts and precautions

Extra care must be taken with simultaneous edition (e.g. two or more opened sessions editing the same configuration) see **commit** command for more information.

Hardware restrictions

N/A

file

Description

Used to perform file operations (e.g. rm/ls/cat/nano unix commands).

Supported Platforms

This command is supported in all platforms.

Syntax

file { **delete** *file-name* | **list** | **show** *file-name* | **edit** *file-name* }

Parameters

delete *file-name*

Description: Deletes a file. The file name must be provided.

Value: File name.

Default Value: N/A

list

Description: Displays all the user-related files.

Value: N/A

Default Value: N/A

show *file-name*

Description: Displays the content of a file. The file name must be provided.

Value: File name.

Default Value: N/A

edit *file-name*

Description: Edits an existent file or creates a new one, if it does not already exist. The provided file name is limited to 255 characters and must not start with ".", "-", nor contain file paths.

Value: File name.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

5.0	The edit command was introduced.
-----	----------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Examples:

This example shows how to use the file command with each of the available parameters. It includes a few additional steps only for better understanding. List the system user files.

```
# file list
#
```

Save a user configuration file and then, use the “file list” command to check if it was saved.

```
# config
Entering configuration mode terminal
(config)# save users_cfg aaa user
```

```
Saving aaa user
(config)# exit
# file list
users_cfg
#
  Display the 'user_cfg' file contents.

# file show users_cfg
aaa user admin
  password $1$QAI4eb9Y$177HyfRcnuW.jY01DPG5M.
  group      admin
!
#
  Delete the 'user_cfg' file.

# file delete users_cfg
# file list
#
  Edit the 'user_cfg' file contents.

# file edit users_cfg
  The file editor will be opened. Use CTRL+s to save the file and CTRL+x to exit the editor
  and return to DmOS CLI.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

hostname

Description

This configuration represents the hostname of the equipment being configured. The configured value can be visualized in three different places. Consulting the equipment configuration through the protocols SNMP and NETCONF and looking at the CLI prompt.

Supported Platforms

This command is supported in all platforms.

Syntax

hostname *name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

name

Description: A value representing the hostname of equipment. This value must contains letters [a-zA-Z], numbers [0-9] and any of the following special characters: [~'@#\$\$%^&*()-_[]{}<>=+./"']. The host name can be up to 63 characters. Although allowed, the use of special characters is not recommended because it violates RFC 952 and RFC 1123, and therefore may cause problems in some applications.

Value: N/A

Default Value: DM4610

Default

DM4610

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
5.4	Underscore was introduced as a possible character for hostname.
5.6	Added support for the following characters [~'@#\$\$%^&*()[[]{}<>=+,. / "\].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use the hostname command. It includes a few additional steps only for better understanding.

```
DM4610# config
Entering configuration mode terminal
DM4610(config)# hostname HOST-001
DM4610(config)# commit
Commit complete.
HOST-001(config)#
HOST-001(config)# exit
HOST-001#
```

Impacts and precautions

Not available.

Hardware restrictions

Not available.

load factory-config

Description

Command used to load the factory configurations to the device.

Supported Platforms

This command is supported in all platforms.

Syntax

load factory-config

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use the load factory-config command and preserve the management configuration.

```
# config
Entering configuration mode terminal
(config)# load factory-config
Loading.
Done.
(config)# interface mgmt 1/1/1
(config-mgmt-1/1/1)# ipv4 address 192.0.2.10/24
(config)# commit
Commit complete.
```

Impacts and precautions

This command does not automatically commit the loaded configuration. The user must explicitly run the commit command in order to apply the loaded configuration on the running-config.

The user must be careful to apply the factory configuration. It may cause the loss of the device management, because the IP address will be reset to the default value (192.168.0.25/24).

Hardware restrictions

N/A

load merge

Description

Command used to merge the content of a file with the current configuration.

Supported Platforms

This command is supported in all platforms.

Syntax

load merge *file*

Parameters

file

Description:	Name of the file that contains the configuration to be loaded.
Value:	Text
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Examples:

This example shows how to use the 'load merge' command.

A new user 'datacom' is created and stored together with 'admin' in the 'users_cfg' file. This file contains only 'aaa user' settings.

```
(config)# aaa user datacom password 1234 group admin
(config-user-datacom)# exit
(config)# show
aaa user admin
password $1$uYMZohDj$gP/QPHc1kog5k6IopHNQh/
group admin
!
aaa user datacom
password $1$z9a2TqCc$23midDa3Bihf0Zlt86YfC1
group admin
!
...
(config)# save users_cfg aaa user
Saving aaa user
(config)#
```

A new user is created and the 'datacom' user is changed and the load merge command is used to restore its value. Note that the new user is not affected.

```
(config)# aaa user newuser group audit
(config-user-newuser)# show
aaa user newuser
password $1$z9a2dtIk$23midDa3Bihf0Zlt86YfC1
!
(config)# aaa user datacom group config
(config-user-datacom)# show
aaa user datacom
password $1$z9a2TqCc$23midDa3Bihf0Zlt86YfC1
group config
!
(config-user-datacom)# exit
(config)# load merge users_cfg
Loading.
188 bytes parsed in 0.09 sec (1.93 KiB/sec)
(config)# show
aaa user admin
password $1$uYMZohDj$gP/QPHc1kog5k6IopHNQh/
group admin
!
aaa user datacom
```

```
password $1$z9a2TqCc$23midDa3Bihf0Zlt86YfC1
group    admin
!
aaa user newuser
password $1$z9a2dtIk$23midDa3Bihf0Zlt86YfC1
!
...
(config) #
```

Impacts and precautions

This command does not automatically commit the loaded configuration. The user must explicitly run the commit command in order to apply the loaded configuration on the running-config.

A valid file must exist in order to execute this command. It can be a XML file or a text file with CLI commands.

Configuration not present in the file will not be affected by this command.

When TACACS+ authorization is enabled and the user is allowed to execute the command **load merge** the merging will be performed based on all commands present in the file if it is stored in xml format. Otherwise, if it is stored in text format, which is the default format, the merge will be done individually for each command present in the file based on the user permission to execute it. Thus, commands not allowed to be executed by the user can affect the merge requiring the operation to be aborted.

Hardware restrictions

N/A

load override

Description

The current configuration is deleted and a new configuration is loaded from file.

Supported Platforms

This command is supported in all platforms.

Syntax

load override *file*

Parameters

file

Description:	Name of the file that contains the configuration to be loaded.
Value:	Text
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Examples:

This example shows how to use the 'load override'.

The initial configuration of equipment is stored in the 'all_cfg' file and then the management IP is changed.

```
# config
Entering configuration mode terminal
(config)# show aaa
aaa user admin
  password $1$uYmZohDj$gP/QPHclkog5k6IopHNQh/
  group    admin
!
(config)# save all_cfg
```

A new user 'datacom' is created.

```
(config)# aaa user datacom password 1234 group admin
(config-user-datacom)# exit
(config)# show aaa
aaa user admin
  password $1$uYmZohDj$gP/QPHclkog5k6IopHNQh/
  group    admin
!
aaa user datacom
  password $1$z9a2TqCc$23midDa3Bihf0Zlt86YfC1
  group    admin
!
(config)#
```

The 'load override' command is used to restore the original configuration. Note that the new user is removed.

```
(config-user-datacom)# exit
(config)# load override all_cfg
Loading.
188 bytes parsed in 0.09 sec (1.93 KiB/sec)
(config)# show aaa
aaa user admin
  password $1$uYmZohDj$gP/QPHclkog5k6IopHNQh/
  group    admin
!
```

```
(config)#
```

Impacts and precautions

This command does not automatically commit the loaded configuration. The user must explicitly run the commit command in order to apply the loaded configuration on the running-config.

A valid file must exist in order to execute this command. It can be a XML file or a text file with CLI commands, but it **MUST** contain the complete configuration of the device, all missing configuration will be deleted, the equipment operation may be compromised. In some cases, the commit may fail if critical configuration is missing.

When TACACS+ authorization is enabled and the user is allowed to execute the command **load override** the overriding will be performed based on all commands present in the file if it is stored in xml format. Otherwise, if it is stored in text format, which is the default format, the overriding will be done individually for each command present in the file based on the user permission to execute it. Thus, commands not allowed to be executed will not remain in the candidate config, resulting in a partial configuration to be committed.

Hardware restrictions

N/A

resolved

Description

Used to resolve conflicts related to simultaneous configuration changes. For example, a conflict may occur if a user updates a configuration but another user commits an update in the same configuration before the first user can commit.

Supported Platforms

This command is supported in all platforms.

Syntax

resolved

Parameters

N/A

Output Terms

Output	Description
<code>Displays a warning message informing about the configuration conflict.</code>	Examples of this command are displayed in the Usage Guidelines field.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

Open 2 ssh sessions with the same equipment and access the configuration prompt from interface gigabit 1/1/1:

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

On ssh session 01, change the advertising-abilities as following:

```
(config-gigabit-ethernet-1/1/1)# advertising-abilities 1Gfull 100Mful
```

On ssh session 02, change the advertising-abilities as following and commit:

```
(config-gigabit-ethernet-1/1/1)# advertising-abilities 100Mfull
(config-gigabit-ethernet-1/1/1)# commit
Commit complete.
```

Go back to ssh session 01 and try to commit. The system shall return the following message:

```
(config-gigabit-ethernet-1/1/1)# commit
Aborted: there are conflicts.
```

Resolve needed before configuration can be committed. View conflicts with the command 'show configuration' and execute the command 'resolved' when done, or exit configuration mode to abort.

Conflicting configuration items are indicated with a leading '!'

Conflicting users: admin

It is possible to check the conflicting configuration by executing the command below:

```
(config-gigabit-ethernet-1/1/1)# show configuration
! advertising-abilities 100Mfull 1Gfull
```

Finally, to solve this conflict an apply the configuration, execute the command sequence below:

```
(config)# resolved
(config)# commit
Commit complete.
(config)# interface gigabit-ethernet 1/1/1
(config-gigabit-ethernet-1/1/1)# show
interface gigabit-ethernet 1/1/1
no shutdown
negotiation
duplex                full
speed                 1G
advertising-abilities 100Mfull 1Gfull
mdix                  normal
!
```

Impacts and precautions

N/A

Hardware restrictions

N/A

rollback configuration

Description

Used to return the current configuration to a previously committed configuration. All changes, from the selected number up to the newest, are rolled back. For example, if the rollback file number 5 is selected, the changes existing in the files 4, 3, 2, 1 and 0 are rolled back too.

Supported Platforms

This command is supported in all platforms.

Syntax

rollback configuration [*number*]

Parameters

number

Description:	Number that identifies the rollback file to be used.
Value:	0-64
Default Value:	0

Default

Return the current configuration to the most recently committed configuration, without activating it.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

These examples show how to use the rollback configuration command. It includes a few additional steps only for better understanding.

Examples:

Generating and visualizing the rollback files. First, it shows the configuration commit list to illustrate the system's current state.

```
# config
Entering configuration mode terminal
(config)# show configuration commit list
1970-01-01 07:28:32
SNo. ID      User      Client    Time Stamp      Label      Comment
~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~
0    10051    admin     cli       1970-01-01 07:28:12
1    10050    admin     cli       1970-01-01 07:01:59
2    10049    admin     cli       1970-01-01 06:29:00
3    10048    admin     cli       1970-01-01 06:28:36
4    10047    admin     cli       1970-01-01 05:36:01
5    10046    admin     cli       1970-01-01 01:49:10
6    10045    admin     cli       1970-01-01 01:45:42
7    10044    admin     cli       1970-01-01 01:42:42
8    10042    admin     cli       1970-01-01 01:32:03
9    10041    admin     cli       1970-01-01 01:30:24
10   10040    admin     cli       1970-01-01 01:24:45
...  .....
```

Then, it configures two different alias and commit them assigning a label. Next, it creates more two alias and also commit them with another label.

```
(config)# alias cmd-alias01 expansion test1
(config-alias-cmd-alias01)# exit
(config)# alias cmd-alias02 expansion test2
(config-alias-cmd-alias02)# exit
(config)# commit comment "add cmd-alias 1/2"
Commit complete.
(config)# alias cmd-alias03 expansion test3
(config-alias-cmd-alias03)# exit
(config)# alias cmd-alias04 expansion test4
(config-alias-cmd-alias04)# exit
(config)# commit comment "add cmd-alias 3/4"
Commit complete.
(config)# show configuration commit list
1970-01-01 07:30:56
SNo. ID      User      Client    Time Stamp      Label      Comment
~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~  ~~~~~
0    10053    admin     cli       1970-01-01 07:30:49
1    10052    admin     cli       1970-01-01 07:30:23
2    10051    admin     cli       1970-01-01 07:28:12
3    10050    admin     cli       1970-01-01 07:01:59
4    10049    admin     cli       1970-01-01 06:29:00
5    10048    admin     cli       1970-01-01 06:28:36
6    10047    admin     cli       1970-01-01 05:36:01
7    10046    admin     cli       1970-01-01 01:49:10
8    10045    admin     cli       1970-01-01 01:45:42
9    10044    admin     cli       1970-01-01 01:42:42
10   10042    admin     cli       1970-01-01 01:32:03
...  .....
```

The command below shows the resultant alias configuration.

```
(config)# show configuration running alias
alias cmd-alias01
  expansion test1
!
alias cmd-alias02
  expansion test2
!
alias cmd-alias03
  expansion test3
!
alias cmd-alias04
  expansion test4
!
```

Finally, the command sequence below uses the rollback command to return the current configuration to a previously committed configuration. In this case, the last 2 commits (0 and 1) are rolled back.

```
(config)# rollback configuration 1
(config)# commit
Commit complete.
```

As a result, all alias specific configurations (previously configured in this example) were removed from the system.

```
(config)# show configuration running alias
% No entries found.
```

Impacts and precautions

The system stores a limited number of rollback files (65). If the maximum number is reached, then the oldest configuration is removed before creating a new one. The most recently committed configuration (the running configuration) is number 0, the next most recent is number 1, etc.

This command does not automatically commit the rolled back configuration. The user must explicitly run the commit command in order to apply the configuration.

When a firmware upgrade is performed some commands might have been modified and the use of rollback command might fail if the rollback contains commands modified between firmware versions. In this case it is recommended to execute the configuration step by step again.

When TACACS+ authorization is enabled and the user is allowed to execute the command **rollback configuration** the operation will be done independent from the user permission to execute the commands in the rollback files.

Hardware restrictions

N/A

rollback selective

Description

Used to return the current configuration to a previously committed configuration. Only the changes existing in selected rollback file are rolled back.

Supported Platforms

This command is supported in all platforms.

Syntax

rollback selective [*number*]

Parameters

number

Description:	Number that identifies the rollback file to be used.
Value:	0-64
Default Value:	0

Default

Return the current configuration to the most recently committed configuration, without activating it.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

These examples show how to use the rollback selective command. It includes a few additional steps only for better understanding.

Examples:

Generating and visualizing the rollback files. First, it shows the configuration commit list to illustrate the system's current state.

```
# config
Entering configuration mode terminal
(config)# show configuration commit list
1970-01-01 07:28:32
SNo. ID User Client Time Stamp Label Comment
~~~ ~~~ ~~~~ ~~~~~~
0 10051 admin cli 1970-01-01 07:28:12
1 10050 admin cli 1970-01-01 07:01:59
2 10049 admin cli 1970-01-01 06:29:00
3 10048 admin cli 1970-01-01 06:28:36
4 10047 admin cli 1970-01-01 05:36:01
5 10046 admin cli 1970-01-01 01:49:10
6 10045 admin cli 1970-01-01 01:45:42
7 10044 admin cli 1970-01-01 01:42:42
8 10042 admin cli 1970-01-01 01:32:03
9 10041 admin cli 1970-01-01 01:30:24
10. 10040 admin cli 1970-01-01 01:24:45
...
```

Then, it configures two different alias and commit them assigning a label. Next, it creates more two alias and also commit them with another label.

```
(config)# alias cmd-alias01 expansion test1
(config-alias-cmd-alias01)# exit
(config)# alias cmd-alias02 expansion test2
(config-alias-cmd-alias02)# exit
(config)# commit comment "add cmd-alias 1/2"
Commit complete.
(config)# alias cmd-alias03 expansion test3
(config-alias-cmd-alias03)# exit
(config)# alias cmd-alias04 expansion test4
(config-alias-cmd-alias04)# exit
(config)# commit comment "add cmd-alias 3/4"
Commit complete.
(config)# show configuration commit list
1970-01-01 07:30:56
SNo. ID User Client Time Stamp Label Comment
~~~ ~~~ ~~~~ ~~~~~~
0 10053 admin cli 1970-01-01 07:30:49 add cmd-alias 3/4
1 10052 admin cli 1970-01-01 07:30:23 add cmd-alias 1/2
2 10051 admin cli 1970-01-01 07:28:12
3 10050 admin cli 1970-01-01 07:01:59
4 10049 admin cli 1970-01-01 06:29:00
5 10048 admin cli 1970-01-01 06:28:36
6 10047 admin cli 1970-01-01 05:36:01
7 10046 admin cli 1970-01-01 01:49:10
8 10045 admin cli 1970-01-01 01:45:42
9 10044 admin cli 1970-01-01 01:42:42
10. 10042 admin cli 1970-01-01 01:32:03
...
```

The command below shows the resultant alias configuration.


```
(config)# show configuration running alias
alias cmd-alias01
  expansion test1
!
alias cmd-alias02
  expansion test2
!
alias cmd-alias03
  expansion test3
!
alias cmd-alias04
  expansion test4
!
```

Finally, the command sequence below uses the rollback selective command to return the current configuration to a previously committed configuration. In this case, the “commit 1” is rolled back.

```
(config)# rollback selective 1
(config)# commit
Commit complete.
```

As a result, all configurations applied by “commit 1” (previously configured in this example) were removed from the system.

```
(config)# show configuration running alias
alias cmd-alias03
  expansion test3
!
alias cmd-alias04
  expansion test4
!
```

Impacts and precautions

The system stores a limited number of rollback files (65). If the maximum number is reached, then the oldest configuration is removed before creating a new one. The most recently committed configuration (the running configuration) is number 0, the next most recent is number 1, etc.

This command does not automatically commit the rolled back configuration. The user must explicitly run the commit command in order to apply the configuration.

When a firmware upgrade is performed some commands might have been modified and the use of rollback command might fail if the rollback contains commands modified between firmware versions. In this case it is recommended to execute the configuration step by step again.

When TACACS+ authorization is enabled and the user is allowed to execute the command **rollback selective** the operation will be done independent from the user permission to execute the commands present in the selected commit.

Hardware restrictions

N/A

save

Description

Used to save all or parts of the current configuration to a file.

Supported Platforms

This command is supported in all platforms.

Syntax

```
save file [xml] [pathfilter]
```

Parameters

file

Description: Name of the file where the configurations will be saved.

Value: Text

Default Value: N/A

xml

Description: Save the configuration in XML format. If this parameter is not used the configuration will be saved in text format as visualized in show command.

Value: N/A

Default Value: N/A

pathfilter

Description: Specify a filter to save only parts of the current configuration.

Value: Text

Default Value: N/A

Default

Save the whole configuration using the same format as visualized in show command.

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

The following examples show how to use the save command with each parameter.

Examples:

The command sequence below, shows how to save the current configuration into a file named cfg001.

```
# config
(config)# save cfg001
(config)# exit
# file show cfg001
aaa user admin
    password $1$BuQV.kcR$JkYGm./9vB8LJ5bjCjEpk1
    group admin
!
router static 0.0.0.0/0 next-hop 10.4.16.1
!
...
interface gpon 1/1/7
    upstream-fec
    downstream-fec
    no shutdown
!
interface gpon 1/1/8
    upstream-fec
    downstream-fec
    no shutdown
!
```

The command sequence below, shows how to save the current configuration into a file named cfg002, using xml format.

```
# config
(config)# save cfg002 xml
(config)# exit
# file show cfg002
<config xmlns="http://tail-f.com/ns/config/1.0">
<bfd xmlns="http://tail-f.com/ns/bfd-stub">
  <stub>
  </stub>
</bfd>
<config xmlns="urn:dmos">
  <interface>
    <gigabit-ethernet xmlns="urn:dmos:dmos-interface-ethernet">
      <id>1/1/1</id>
      <shutdown>false</shutdown>
      <negotiation>true</negotiation>
      <duplex>full</duplex>
      <speed>1G</speed>
      <advertising-abilities>1Gfull</advertising-abilities>
      <mdix>normal</mdix>
    </gigabit-ethernet>
  ...
</dot1q xmlns="http://tail-f.com/ns/example/vlan-manager">
  <vlan>
    <vlan-id>1</vlan-id>
    <interface>
      <interface-name>gigabit-ethernet 1/1/9</interface-name>
    </interface>
  </vlan>
</dot1q>
```

The command sequence below, shows how to save a partial configuration into a file named `cfg003`.

```
# config
(config)# save cfg003 dot1q
Saving dot1q
(config)# exit
# file show cfg003
dot1q
  vlan 1
    interface gigabit-ethernet 1/1/9
    !
  !
!
```

The command sequence below, shows how to save a partial configuration into a file named `cfg004`, using xml format.

```
# config
(config)# save cfg004 xml dot1q
Saving parts of the configuration.
(config)# exit
# file show cfg004
<config xmlns="http://tail-f.com/ns/config/1.0">
<dot1q xmlns="http://tail-f.com/ns/example/vlan-manager">
  <vlan>
    <vlan-id>1</vlan-id>
    <interface>
      <interface-name>gigabit-ethernet 1/1/9</interface-name>
    </interface>
  </vlan>
</dot1q>
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show

Description

Used to display all running configuration (applied by commits) without the default values. It can be used to display all fields when editing a subgroup configuration (e.g. a specific user in users configuration).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show { pathfilter }
```

Parameters

pathfilter

Description:	Specifies a filter to display only a specific configuration
Value:	Text
Default Value:	N/A

Output Terms

Output	Description
Displays information about the system configuration	Examples of this command are displayed in the Usage Guidelines field

Default

All running configuration are displayed

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

The examples below shows how to use the command show.

Examples:

Example 1:

```
(config)# show
aaa user admin
password $1$UoyZaDJS$aUxgMRkWXhhKCRmzqwasd/
group admin
!
alias bla
expansion bla7
!
bfd
!
interface mgmt 1/1/1
ipv4 address 10.4.16.132/22
!
router static 0.0.0.0/0 next-hop 10.4.16.1
!
snmp agent enabled
snmp agent version v2c
snmp agent version v3
snmp agent max-message-size 50000
snmp community public
sec-name public
!
snmp notify std_v1_trap
tag std_v1_trap
!
snmp notify std_v2_inform
tag std_v2_inform
type inform
!
snmp notify std_v2_trap
tag std_v2_trap
!
```


Example 2:

```
(config)# show aaa
aaa user admin
password $1$UoyZaDJS$aUxgMRkWXhhKCRmzqwasd/
group admin
!
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show banner login

Description

Display login banner.

Supported Platforms

This command is supported in all platforms.

Syntax

show banner login

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

login

Description: Display login banner.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Login banner	Displays the login banner formatted as it will be shown on login via console, SSH or Telnet.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.6	This command was introduced.

Usage Guidelines

```
DM4610# show banner login
Login banner will be displayed as shown inside <>
<
*****
***  Only authorized personnel are allowed to access this piece of equipment.  ***
***  Others are urged to log off IMMEDIATELY.                                ***
***  Somente pessoal autorizado pode acessar este equipamento.                ***
***  Outros, por favor, desconectar IMEDIATAMENTE.                          ***
***  *****                                                                    ***
>
DM4610#
```

Impacts and precautions

None.

Hardware restrictions

None.

show configuration

Description

Used to list all uncommitted configuration changes.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show configuration { this | diff | merge } [ pathfilter ]
```

Parameters

this

Description: Shows the configuration changes in CLI format.

Value: N/A

Default Value: N/A

diff

Description: Shows the changes using diff notation.

Value: N/A

Default Value: N/A

merge

Description: Shows the complete configuration merging the running configuration to the uncommitted changes.

Value: N/A

Default Value: N/A

pathfilter

Description: Specifies a filter to display only a specific configuration change.

Value: Text

Default Value: N/A

Output Terms

Output	Description
<code>Displays the difference between the candidate and committed configurations for the specified module.</code>	Examples of this command are displayed in the Usage Guidelines field

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

In order to check the “show configuration” command functionality, it is necessary to change the system default configuration and then execute:

`show configuration <path>.`

The example below, shows how to use the command show configuration.

Example:

If the candidate configuration is empty, the equipment shall return the message stated below:

```
(config)# show configuration diff
% No configuration changes found.
```

The same idea applies when a module is specified:

```
(config)# show configuration diff aaa
% No configuration changes found.
```

Now, to clarify the purpose and operation of this command, the example below will perform a change in the configuration. In this case, the gigabit-ethernet 1/1/1 interface was activated.

```
(config)# interface gigabit-ethernet 1/1/1
(config-gigabit-ethernet-1/1/1)# no shutdown
(config-gigabit-ethernet-1/1/1)# exit
```

Then, it is possible to verify the difference between the candidate and committed configuration.

```
(config)# show configuration this interface gigabit-ethernet 1/1/1
interface gigabit-ethernet 1/1/1
no shutdown
!
```

And if the user wants to check this difference using diff notation:

```
(config)# show configuration diff interface gigabit-ethernet 1/1/1
interface gigabit-ethernet 1/1/1
- shutdown
+ no shutdown
!
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show configuration commit changes

Description

Used to display the content of a commit file. A commit file is saved with new configurations any time a commit command is performed. These files can also be used in a rollback command.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show configuration commit changes [ diff ] [ id [ pathfilter ] ]
```

Parameters

diff

Description:	Marks the changes between running-config and rollback file using the diff notation.
Value:	N/A
Default Value:	N/A

id

Description:	For a valid value of id number, read the explanation example in the Usage Guidelines field.
Value:	Number
Default Value:	N/A

pathfilter

Description:	Specifies a filter to display only a specific configuration.
Value:	Text
Default Value:	N/A

Output Terms

Output	Description
<code>Displays the content of a commit file.</code>	Examples of this command are displayed in the Usage Guidelines field.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

These examples show how to use the `show configuration commit changes` command. It includes a few additional steps only for better understanding.

Examples:

In the first boot of system the commit list is empty:

```
Welcome to the DmOS CLI
admin connected from 127.0.0.1 using console on
# config
Entering configuration mode terminal
(config)# show configuration commit list
% no rollback files found
(config)#
```

If an invalid id is used the following message is displayed:

```
(config)# show configuration commit changes 10
Error: invalid rollback number
```

Now, just to illustrate a practical and valid command use, the command sequences below shall perform three configuration changes. First, the management IP address is changed and committed:

```
(config)# interface mgmt 1/1/1
(config-mgmt-1/1/1)# no ipv4 address
(config-mgmt-1/1/1)# ipv4 address 10.4.16.132/22
(config-mgmt-1/1/1)# exit
(config)# commit
Commit complete.
(config)#
```

Secondly, a static router is added and committed:

```
(config)# router static 0.0.0.0/0 next-hop 10.4.16.1
(config-static-0.0.0.0/0/10.4.16.1)# exit
(config)# commit
Commit complete.
(config)#
```

Finally, two new users are added and committed:

```
(config)# aaa user datacom_1 password 1234 group admin
(config-user-datacom_1)# exit
(config)# aaa user datacom_2 password 1234 group admin
(config-user-datacom_2)# exit
(config)# commit
Commit complete.
(config)#
```

Now the commit list has three items:

```
(config)# show configuration commit list
1970-01-01 00:09:02
SNo. ID      User      Client      Time Stamp      Label      Comment
~~~ ~~~~~
0      10002     admin     cli         1970-01-01 00:04:55
1      10001     admin     cli         1970-01-01 00:04:44
2      10000     admin     cli         1970-01-01 00:04:33
(config)#
```

Summary descriptions of the command:

```
(config)# show configuration commit ?
Possible completions:
  changes  Changes for a given rollback id
  list     Show commit history
(config)# show configuration commit changes ?
Possible completions:
  0        1970-01-01 00:04:55 by admin via cli
  1        1970-01-01 00:04:44 by admin via cli
  2        1970-01-01 00:04:33 by admin via cli
  __
  diff     Changes for a given rollback id
  <cr>     latest
(config)#
```

Using the command with its parameters:

```
(config)# show configuration commit changes
!
! Created by: admin
! Date: 1970-01-01 00:04:55
! Client: cli
!
aaa user datacom_1
password $1$VmUU06GU$Cf36xMHMikZBXDxgwYsXW0
group    admin
!
aaa user datacom_2
password $1$5dZ1FwQD$2SF8Q6K7pHMGnd7xGLWhS1
group    admin
!
```

Showing changes that were committed for a given commit id (id = 0):

```
(config)#
(config)# show configuration commit changes 0
!
! Created by: admin
! Date: 1970-01-01 00:04:55
! Client: cli
!
aaa user datacom_1
  password $1$VmUU06GU$Cf36xMHMikZBXDxgwYsXW0
  group    admin
!
aaa user datacom_2
  password $1$5dZ1FwQD$2SF8Q6K7pHMGnd7xGLWhs1
  group    admin
!
```

Showing changes that were committed for a given commit id (id = 1):

```
(config)#
(config)# show configuration commit changes 1
!
! Created by: admin
! Date: 1970-01-01 00:04:44
! Client: cli
!
router static 0.0.0.0/0 next-hop 10.4.16.1
!
```

Showing changes that were committed for a given commit id (id = 2):

```
(config)#
(config)# show configuration commit changes 2
!
! Created by: admin
! Date: 1970-01-01 00:04:33
! Client: cli
!
interface mgmt 1/1/1
  no ipv4 address
  ipv4 address 10.4.16.132/22
!
```

Showing the changes between running-config and rollback file (id = 0) using the diff notation:

```
(config)#
(config)# show configuration commit changes diff 0
!
! Created by: admin
! Date: 1970-01-01 00:04:55
! Client: cli
!
+aaa user datacom_1
+ password $1$VmUU06GU$Cf36xMHMikZBXDxgwYsXW0
+ group    admin
+!
+aaa user datacom_2
+ password $1$5dZ1FwQD$2SF8Q6K7pHMGnd7xGLWhs1
+ group    admin
+!
```

Showing the changes between running-config and rollback file (id = 0) to a specific configuration (aaa) using the diff notation:

```
(config)#
(config)# show configuration commit changes diff 0 aaa user datacom_2
!
! Created by: admin
! Date: 1970-01-01 00:04:55
! Client: cli
!
+aaa user datacom_2
+ password $1$5dZ1FwQD$2SF8Q6K7pHMGnd7xGLWhs1
+ group    admin
```

```
+!  
(config) #
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show configuration commit list.

Description

Shows a list including all configuration commits stored in the commit database.

Supported Platforms

This command is supported in all platforms.

Syntax

show configuration commit list { *num* | *pathfilter* }

Parameters

num

Description:	Number of commit IDs (beginning with the most recent commit) that will be displayed
Value:	Positive number
Default Value:	100

pathfilter

Description:	Specifies a filter to display only commit IDs that contain a specific configuration
Value:	Text
Default Value:	N/A

Output Terms

Output	Description
The output displays the commit IDs that are available for rollback	Examples of this command are displayed in the Usage Guidelines field

Default

Show all existing files

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced

Usage Guidelines

Use the show configuration commit list command to list the commit IDs (up to 65) that are available for rollback. The newest 65 commits are stored by the system. As new commit IDs are added, the oldest commit IDs are discarded.

Examples:

```
(config)# show configuration commit list
```

```

2016-01-01 09:02:07
SNo. ID      User      Client      Time Stamp      Label      Comment
~~~~~
0      10068    admin     cli         2015-03-26 16:17:40
1      10067    admin     cli         2015-03-26 16:15:03
2      10066    oper      cli         2015-03-26 16:13:35
3      10065    admin     cli         2015-03-26 14:43:03
4      10059    oper      cli         2015-03-26 14:09:34
5      10058    oper      cli         2015-03-26 13:55:31
6      10056    oper      cli         2015-03-26 13:54:25
7      10054    admin     cli         2015-03-26 13:45:39
8      10053    admin     cli         2015-03-26 13:45:00
9      10051    admin     cli         2015-03-26 13:43:26
10     10044    admin     cli         2015-03-25 14:33:31
11     10043    admin     cli         2015-03-25 14:32:47
12     10042    admin     cli         2015-03-25 11:30:25

```

It is also possible to limit the number of commits displayed in the command output, by using the **num** parameter. The example below, shows the last 3 configuration commits executed by the user.

```

(config)# show configuration commit list 3
2016-01-01 09:03:44
SNo. ID      User      Client      Time Stamp      Label      Comment
~~~~~
0      10068    admin     cli         2015-03-26 16:17:40
1      10067    admin     cli         2015-03-26 16:15:03
2      10066    oper      cli         2015-03-26 16:13:35

```

An example showing when a specific configuration filter is used:

```

(config)# show configuration commit list aaa
2016-01-01 09:04:14
SNo. ID      User      Client      Time Stamp      Label      Comment
~~~~~
0      10068    admin     cli         2015-03-26 16:17:40
1      10067    admin     cli         2015-03-26 16:15:03
12     10042    admin     cli         2015-03-25 11:30:25

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show configuration rollback changes

Description

Used to display the changes applied after a specific commit file is used in a rollback command.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show configuration rollback changes [ diff ] [ id ]
```

Parameters

diff

Description: Marks the changes using diff notation.

Value: N/A

Default Value: N/A

id

Description: For a valid value of id number, read the explanation example in the Usage Guidelines field.

Value: Number

Default Value: N/A

Output Terms

Output	Description
<code>Displays the changes applied after a specific commit file is used in a rollback command.</code>	Examples of this command are displayed in the Usage Guidelines field.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

These examples show how to use the show configuration rollback changes command. It includes a few additional steps only for better understanding.

Examples:

In the first boot of system the commit list is empty.

```
Welcome to the DmOS CLI
admin connected from 127.0.0.1 using console on
# config
```

```

Entering configuration mode terminal
(config)# show configuration commit list
% no rollback files found
(config)#

```

If an invalid id is used the following message is displayed.

```

(config)# show configuration rollback changes 10
Error: invalid rollback number

```

Now, just to illustrate a practical and valid command use, the command sequences below shall perform three configuration changes. First, the management IP address is changed and committed.

```

(config)# interface mgmt 1/1/1
(config-mgmt-1/1/1)# no ipv4 address
(config-mgmt-1/1/1)# ipv4 address 10.4.16.132/22
(config-mgmt-1/1/1)# exit
(config)# commit
Commit complete.
(config)#

```

Secondly, a static router is added and committed.

```

(config)# router static 0.0.0.0/0 next-hop 10.4.16.1
(config-static-0.0.0.0/0/10.4.16.1)# exit
(config)# commit
Commit complete.
(config)#

```

Now the commit list has two items.

```

(config)# show configuration commit list
1970-01-01 00:09:02
SNo. ID      User      Client      Time Stamp      Label      Comment
~~~ ~~~~    ~~~~    ~~~~~~    ~~~~~~
0      10001     admin     cli         1970-01-01 00:04:44
1      10000     admin     cli         1970-01-01 00:04:33

```

Summary descriptions of the command.

```

(config)# show configuration rollback ?
Possible completions:
  changes  Changes for rolling back last n commits
(config)# show configuration rollback changes ?
Possible completions:
  0          1970-01-01 00:04:44 by admin via cli
  1          1970-01-01 00:04:33 by admin via cli
  ---
  diff      Changes for rolling back last n commits
  <cr>      latest

```

Using the command with its parameters.

```

(config)# show configuration rollback changes
no router static 0.0.0.0/0 next-hop 10.4.16.1
(config)#
(config)# show configuration rollback changes 0
no router static 0.0.0.0/0 next-hop 10.4.16.1
(config)#
(config)# show configuration rollback changes 1
interface mgmt 1/1/1
no ipv4 address
ipv4 address 192.168.0.25/24
!
no router static 0.0.0.0/0 next-hop 10.4.16.1
(config)#
(config)# show configuration rollback changes diff 1
interface mgmt 1/1/1
- ipv4 address 10.4.16.132/22
+ ipv4 address 192.168.0.25/24
!
-router static 0.0.0.0/0 next-hop 10.4.16.1
-!
(config)#

```

Impacts and precautions

When a firmware upgrade is performed some commands might have been modified and the use of rollback command might fail if the rollback contains commands modified between firmware versions. In this case it is recommended to execute the configuration step by step again.

Hardware restrictions

N/A

show configuration running

Description

Used to display all running configurations without the default values.

Supported Platforms

This command is supported in all platforms.

Syntax

show configuration running [*pathfilter*]

Parameters

pathfilter

Description: Specifies a filter to display only a specific configuration.

Value: Text

Default Value: N/A

Output Terms

Output	Description
<code>Displays the running configuration without its default values.</code>	Examples of this command are displayed in the Usage Guidelines field.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples shows how to use the show configuration running command.

```
# config
Entering configuration mode terminal
(config)# show configuration running
aaa user admin
  password $1$DMOzVTxJ$pczOpWZo2hIU1Or0VUfce.
  group      admin
!
interface mgmt 1/1/1
  ipv4 address 192.168.0.25/24
!
snmp agent enabled
snmp agent version v2c
snmp agent version v3
snmp agent max-message-size 50000
snmp community public
  sec-name public
!
snmp vacm group public
  member public
  sec-model [ v2c ]
!
access v2c no-auth-no-priv
  read-view    root
  write-view   root
  notify-view  root
!
...
(config)#

# config
Entering configuration mode terminal
(config)# show configuration running interface
interface mgmt 1/1/1
```

```
ipv4 address 192.168.0.25/24
!  
(config) #
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show running-config

Description

Used to display all the current configurations (applied by commits). The configurations with default values will not be displayed.

Supported Platforms

This command is supported in all platforms.

Syntax

show running-config [*pathfilter*]

Parameters

pathfilter

Description: Specifies a filter to display only a specific configuration.

Value: Text

Default Value: N/A

Output Terms

Output	Description
<code>Displays the running configuration without its default values.</code>	Examples of this command are displayed in the Usage Guidelines field.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples shows how to use the show running-config command.

```
# show running-config
aaa user admin
  password $1$UoyZaDJS$aUxgMRkWXhhKCRmzLkolx/
  group admin
!
bfd
!
interface mgmt 1/1/1
  ipv4 address 10.4.16.132/22
!
router static 0.0.0.0/0 next-hop 10.4.16.1
!
snmp agent enabled
snmp agent version v2c
snmp agent version v3
snmp agent max-message-size 50000
snmp community public
  sec-name public
!
snmp notify std_v1_trap
  tag std_v1_trap
!
snmp notify std_v2_inform
  tag std_v2_inform
...
```

If a filter is specified, the command returns only the respective configuration. For instance, the command below shows all management interface configuration

```
# show running-config interface mgmt
```



```
interface mgmt 1/1/1
  ipv4 address 10.4.16.132/22
!
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

top

Description

Used to exit to the top level of configuration mode or execute a command at the top level of the configuration.

Supported Platforms

This command is supported in all platforms.

Syntax

top [*command*]

Parameters

command

Description:	It is an optional parameter that specifies a command to be executed at the top level of configuration.
Value:	Text
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This examples shows how to use the top command. Exit to the top level of configuration mode.

```
# config
Entering configuration mode terminal
(config)# aaa user config
(config-user-config)# top
(config)#
```

Execute a command at the top level of the configuration. In this example the command “interface l3 L3-name” is executed at the top of configuration creating a new interface but keep the actual configuration level.

```
# config
Entering configuration mode terminal
(config)#aaa user config
(config-user-config)# top interface l3 L3-name
(config-user-config)#
(config-user-config)# show interface l3
interface l3 L3-name
!
(config-user-config)#
```

Execute the command top and enter in other configuration level. In this example using “;” is possible to execute top command and enter at interface l3 configuration level.

```
# config
Entering configuration mode terminal
(config)#aaa user config
(config-user-config)# top ; interface l3 L3-name
(config-l3-L3-name)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

FIRMWARE

This topic describes the commands related to firmware management such as commands to identify current version or to execute an upgrade.

request firmware onu add

Description

This command is used to download a remotely stored ONU firmware file and store it locally.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

request firmware onu add *protocol://A.B.C.D/path/fw_name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

protocol://A.B.C.D/path/fw_name

Description: Download and store an ONU firmware file in the local device to be used in a remote device ONU update. This parameter specifies the 'protocol' (available protocol is TFTP); the remote server address 'A.B.C.D' (IPv4 address); and the path and name 'path/fw_name' of the firmware stored in the remote server.

Value: Max. Length 765

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.4	This command was introduced.
2.0	The command was modified to remove remote option
4.9	Added text to Impacts and precautions about ONU FW available flash memory.

Usage Guidelines

Use the `request firmware onu add` command to download and store a new ONU firmware file in the local device.

Impacts and precautions

There is up to 106 MB available for ONU firmware files in the equipment flash memory.

Hardware restrictions

N/A

request firmware onu remove

Description

This command is used to remove a ONU firmware file stored in the local device.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

request firmware onu remove *filename*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

filename

Description: Delete an ONU firmware file stored in the local device. This parameter specifies the name of the ONU firmware file to be removed.

Value: Max. Length 255

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

1.4	This command was introduced.
-----	------------------------------

Usage Guidelines

Use the `request firmware onu remove` command to delete a downloaded ONU firmware file from the local device.

Impacts and precautions

N/A

Hardware restrictions

N/A

DIAGNOSTICS

This topic describes the commands related to management diagnostic such as commands to verify some interface connection, to check CPU usage or to execute a traffic mirror.

clear core-dump

Description

Deletes a core-dump file of the list. Uses the file name.

Supported Platforms

This command is supported in all platforms.

Syntax

clear core-dump *filename*

Parameters

filename

Description:	Name of core dump file to be deleted
Value:	File name or 'all' to delete all core dumps
Default Value:	No default value.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To clear existing core-dump file, as in the example below.

```
DM4610# clear core-dump core-file.5407.111222333.core.gz
Success!
DM4610#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

clear counters

Description

Clear statistics counters for User-Defined Counter instances. If no parameters are given all user-defined counters will be cleared.

Supported Platforms

This command is supported in all platforms.

Syntax

```
clear counters [ { ingress | egress } [ id counter-id ] ]
```

Parameters

ingress

Description: Clear counters of ingress stage. If no IDs are given all counters of ingress stage will be cleared.

Value: N/A

Default Value: N/A

egress

Description: Clear counters of egress stage. If no IDs are given all counters of egress stage will be cleared.

Value: N/A

Default Value: N/A

id counter-id

Description: Counter ID to be cleared. It supports multiple IDs by using range/list syntax (e.g. 1-3,5).

Value: 1 - 512

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.9	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has ingress counters 1, 3, 5 and 7 and egress counters 2, 4, 6 and 8 configured.

```
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One          6546   octets
3   Three         47984  octets
5   Five          1321   octets
7   Seven         71211  octets

EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two          19655  octets
4   Four          75203  octets
6   Six           5616   octets
8   Eight         39458  octets
```

Let's clear ingress counter 1:

```
# clear counters ingress id 1
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One          0       octets
3   Three         47984  octets
5   Five          1321   octets
7   Seven         71211  octets
```

```
EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two           19655  octets
4   Four           75203  octets
6   Six            5616   octets
8   Eight          39458  octets
```

Now let's clear ingress counters 3 and 7 by using list syntax:

```
# clear counters ingress id 3,7
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One           0       octets
3   Three          0       octets
5   Five          1321   octets
7   Seven          0       octets

EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two           19655  octets
4   Four           75203  octets
6   Six            5616   octets
8   Eight          39458  octets
```

It is possible to clear multiple counters by using range syntax, so let's clear egress counters from ID 4 up to ID 8. Note that in that range there are non-existent counters and they are going to be ignored:

```
# clear counters egress id 4-8
Counter ID 5 doesn't exist. Skipping...
Counter ID 7 doesn't exist. Skipping...
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One           0       octets
3   Three          0       octets
5   Five          1321   octets
7   Seven          0       octets

EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two           19655  octets
4   Four           0       octets
6   Six            0       octets
8   Eight          0       octets
```

To clear all counter of a given stage just omit the ID:

```
# clear counters egress
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One           0       octets
3   Three          0       octets
5   Five          1321   octets
7   Seven          0       octets

EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two           0       octets
4   Four           0       octets
6   Six            0       octets
8   Eight          0       octets
```

To clear all counters of all stages just omit all parameters:

```
# clear counters
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   One          0      octets
3   Three        0      octets
5   Five         0      octets
7   Seven        0      octets

EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
2   Two          0      octets
4   Four         0      octets
6   Six          0      octets
8   Eight        0      octets
```

Impacts and precautions

The clear operation is valid for all user interfaces. That means that a clear operation done through CLI, for example, will affect the values shown in all other user interfaces too i.e. SNMP and NETCONF.

Hardware restrictions

None

clear statistics

Description

This command clears the statistics counters of an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

clear statistics *interface-name*

Parameters

interface-name

Description:	Interface id referencing chassis/slot/port respectively or an id referencing a specified LAG.
Value:	{ { gigabit-ethernet ten-gigabit-ethernet twenty-five-g-ethernet forty-gigabit-ethernet hundred-gigabit-ethernet } <i>c/s/p</i> lag <i>id</i> }
Default Value:	None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.2	This command was introduced.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G and LAG interfaces.
5.0	Added support for 25G.

Usage Guidelines

The CLI and Netconf values are subject to this command and should not be used for accounting or billing.

Impacts and precautions

Once issued, this command will set all counters to 0 on the network interface *interface-name*, on the CLI and NetConf access interfaces. Other access interfaces will not be cleared by this command. The values on these access interfaces should not be used for accounting or billing (see usage guidelines).

Hardware restrictions

N/A

copy core-dump

Description

Copies a core-dump file using the TFTP or SCP protocol to valid host.

Supported Platforms

This command is supported in all platforms.

Syntax

```
copy core-dump filename protocol://ip-address/ [username login] [password pass]  
[source {ip-address | interface}]
```

Parameters

filename

Description: Name of core dump file to be copied
Value: File name or 'all' to copy all core dumps
Default Value: No default value.

protocol

Description: Protocol to be used to upload core dump file
Value: tftp or scp
Default Value: None.

ip-address

Description: IP address of destination host.
Value: a.b.c.d or X:X:X:X::X
Default Value: None.

username

Description: The username is required by SCP protocol.
Value: Max. Length 40
Default Value: N/A

password

Description: The password is required by SCP protocol.
If omitted in the command, the system will ask for the password.

Value: Max. Length 40

Default Value: N/A

source {*ip-address* | *interface*}

Description: Specify the source ip address or the interface name where core dump file should be send through.

Value: *ip-address* - IP address from a configured interface in a.b.c.d or X:X:X:X::X format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
2.2	Changed parameters order and included 'scp' option for protocol parameter.
2.4	Included IPv6 and VRF support.

Usage Guidelines

To copy core-dump file to existing remote host using TFTP protocol as in the example below.

```
DM4610# copy core-dump core-file.5407.111222333.core.gz tftp://172.22.110.12
Transfer complete.
DM4610#
```

To copy core-dump file to existing remote host using SCP protocol as in the example below.

```
DM4610# copy core-dump core-file.5407.111222333.core.gz scp://172.22.110.12/~
User name: user
Password: *****
Transfer complete.
DM4610#
```

To copy core-dump file to existing remote host using SCP protocol and IPv6 as in the example below.

```
DM4610# copy core-dump core-file.5407.111222333.core.gz scp://2001:db8::10/~
User name: user
Password: *****
Transfer complete.
DM4610#
```

To copy core-dump file to existing remote host using TFTP protocol and source ip address as in the example below.

```
DM4610# copy core-dump core-file.540.1.core.gz tftp://172.22.110.12 source 10.1.1.1
Transfer complete.
DM4610#
```

To copy core-dump file to existing remote host using TFTP protocol and source interface

as in the example below.

```
DM4610# copy core-dump core-file.540.1.core.gz tftp://172.22.110.12 source 13-vlan200
Transfer complete.
DM4610#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

copy file

Description

Copy file using TFTP or SCP protocol to/from valid host.

Supported Platforms

This command is supported in all platforms.

Syntax

copy file { *local-filename* | *protocol://ip-address/remote-path* } { *protocol://ip-address/remote-path* | *remote-filename* } [**username** *login* | **password** *pass* | **port** *number* | **rename** *name* | **source** {*ip-address* | *interface*}]*

Parameters

local-filename

Description:	Name of local file to be copied to remote host. Names are limited to 255 characters and must not start with '.' and '-'.
Value:	File name.
Default Value:	N/A

protocol

Description:	Protocol to be used to upload/download file
Value:	tftp or scp
Default Value:	N/A

ip-address

Description:	IP address of the host.
Value:	a.b.c.d or X:X:X:X::X.
Default Value:	N/A

remote-path

Description:	Remote file path.
---------------------	-------------------

Value: File path.

Default Value: N/A

remote-filename

Description: Name of remote file to be copied from remote host.

Value: File name.

Default Value: N/A

username *login*

Description: Specifies the login name to access a remote host. Use this only when protocol is scp.

Value: Login name.

Default Value: N/A

password *pass*

Description: Specifies the login password to access a remote host. Use this only when protocol is scp.

Value: Login password.

Default Value: N/A

port *number*

Description: Specifies the port number to access a remote host.

Value: 0-65535.

Default Value: For tftp protocol is 69 and scp protocol is 22.

rename *name*

Description: Specifies the name to save file on device or remote host. Names are limited to 255 characters and must not start with '.' and '-'.

Value: File name.

Default Value: N/A

source {*ip-address* | *interface*}

Description: Specifies the source ip address or the interface name from which transfer should be started.

Value: *ip-address* - IP address from a configured interface in a.b.c.d or X:X:X:X::X format;

or
interface - name of the management or I3 interface in I3-<name>,
mgmt-<c>/<s>/<p> format.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

To copy file to existing remote host using TFTP protocol.

```
# copy file test tftp://1.2.1.1
Transfer complete.
#
```

To copy file to existing remote IPv6 host using TFTP protocol.

```
# copy file test tftp://2001:DB8::10
Transfer complete.
#
```

To copy file to existing remote host using SCP protocol in a specific folder.

```
# copy file test scp://1.2.1.1/dir/ username user password pass
Transfer complete.
#
```

To copy file to existing remote host using SCP protocol in a specific folder and a specific port.

```
# copy file test scp://1.2.1.1/dir/ username user password pass port 200
Transfer complete.
#
```

To copy file to existing remote host using TFTP protocol in a specific folder.

```
# copy file test tftp://1.2.1.1/dir/
Transfer complete.
#
```

To copy file to existing remote host using TFTP protocol and rename the file.

```
# copy file test tftp://1.2.1.1 rename test_renamed
Transfer complete.
#
```

To copy file from existing remote host using TFTP protocol without rename.

```
# copy file tftp://1.2.1.1 test
Transfer complete.
#
```

To copy file from existing remote host using TFTP protocol and rename the file.

```
# copy file tftp://1.2.1.1 test rename test_renamed
Transfer complete.
#
```

To copy file from existing remote host using TFTP protocol with source IPv4 address.

```
# copy file tftp://1.2.1.1 test source 1.1.1.1
Transfer complete.
#
```

To copy file from existing remote host using TFTP protocol with source interface-name.

```
# copy file tftp://1.2.1.1 test source mgmt-1/1/1
Transfer complete.
#
```

To copy file from existing remote IPv6 host using TFTP protocol with source IPv6 address.

```
# copy file tftp://2001::DB8::10 test source 2001:DB8::1
Transfer complete.
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

copy mibs

Description

Copies a compressed file containing the device MIB files via the TFTP or SCP protocol to a remote host.

Supported Platforms

This command is supported in all platforms.

Syntax

```
copy mibs protocol://ip-address/ [username login] [password pass] [source {ip-address | interface}]
```

Parameters

protocol

Description: Protocol to be used to upload the compressed file.
Value: tftp or scp
Default Value: None.

ip-address

Description: IP address of destination host.
Value: a.b.c.d or X:X:X:X::X
Default Value: None.

username

Description: The username is required by the SCP protocol.
Value: Max. Length 40
Default Value: N/A

password

Description: The password is required by the SCP protocol.
If omitted in the command, the system will prompt for the password.

Value: Max. Length 40

Default Value: N/A

source {*ip-address* | *interface*}

Description: Specifies the source IP address or the interface name from which the transfer should be initiated.

Value: *ip-address* - IP address of a configured interface in a.b.c.d or X:X:X:X::X format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
5.4	This command was introduced.
5.6	The parameter 'source' was added.

Usage Guidelines

Copying MIBs to a remote host using the TFTP protocol:

```
DM4610# copy mibs tftp://172.22.110.12
File 'datacom-mibs.tar.gz' successfully transferred.
DM4610#
```

Copying MIBs to a remote host using the SCP protocol:

```
DM4610# copy mibs scp://172.22.110.12/dir
User name: user
Password: *****
File 'datacom-mibs.tar.gz' successfully transferred.
DM4610#
```

Copying MIBs to a remote host using IPv6 and the SCP protocol:

```
DM4610# copy mibs scp://2001:db8::10/dir
User name: user
Password: *****
File 'datacom-mibs.tar.gz' successfully transferred.
DM4610#
```

Copying MIBs to a remote host using the TFTP protocol and a source IP address:

```
DM4610# copy mibs tftp://172.22.110.12 source 1.1.1.1
File 'datacom-mibs.tar.gz' successfully transferred.
DM4610#
```

Copying MIBs to a remote host using the SCP protocol and a source interface name:

```
DM4610# copy mibs scp://172.22.110.12/dir source mgmt-1/1/1
User name: user
Password: *****
File 'datacom-mibs.tar.gz' successfully transferred.
DM4610#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

copy pcap

Description

Copies the pcap file generated by tcpdump using the TFTP or SCP protocol to valid host.

Supported Platforms

This command is supported in all platforms.

Syntax

```
copy pcap protocol://ip-address/ [username login] [password pass] [source {ip-address | interface}]
```

Parameters

protocol

Description: Protocol to be used to upload pcap file
Value: tftp or scp
Default Value: None.

ip-address

Description: IP address of destination host.
Value: a.b.c.d or X:X:X:X::X
Default Value: None.

username

Description: The username is required by SCP protocol.
 If omitted in the command, the system will ask for the user-name.
Value: Max. Length 40
Default Value: N/A

password

Description: The password is required by SCP protocol.
If omitted in the command, the system will ask for the password.

Value: Max. Length 40

Default Value: N/A

source {*ip-address* | *interface*}

Description: Specify the source IP address or the interface name where pcap file should be send through.

Value: *ip-address* - IP address from a configured interface in a.b.c.d or X:X:X:X::X format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

6.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To copy pcap file to existing remote host using TFTP protocol as in the example below.

```
# copy pcap tftp://172.22.110.12
Transfer complete.
#
```

To copy pcap file to existing remote host using SCP protocol as in the example below.

```
# copy pcap scp://172.22.110.12/~
User name: user
Password: *****
Transfer complete.
#
```

To copy pcap file to existing remote host using SCP protocol and IPv6 as in the example below.

```
# copy pcap scp://2001:db8::10/~
User name: user
Password: *****
Transfer complete.
#
```

To copy pcap file to existing remote host using TFTP protocol and source ip address as in the example below.

```
# copy pcap tftp://172.22.110.12 source 10.1.1.1
Transfer complete.
#
```

To copy pcap file to existing remote host using TFTP protocol and source interface as in the example below.

```
# copy pcap tftp://172.22.110.12 source l3-vlan200
Transfer complete.
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

counters

Description

Create a User-Defined Counter instance.

Supported Platforms

This command is supported in all platforms.

Syntax

counters {**ingress** | **egress**} **id** *counter-id* **type** **octets** [**description** *counter-description*] {**vlan** *vlan-id* [**inner-vlan** *vlan-id*] | **interface** *interface-name*}*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

ingress

Description:	This parameter configures ingress user defined counters.
Value:	N/A
Default Value:	N/A

egress

Description:	This parameter configures egress user defined counters.
Value:	N/A
Default Value:	N/A

id *counter-id*

Description:	User defined counter identifier.
Value:	1 - 512
Default Value:	N/A

type **octets**

Description:	Define the type of data counted by this counter.
---------------------	--

Value: octets

Default Value: octets

description *counter-description*

Description: User defined counter description, used to identification.

Value: String with a maximum of 128 characters.

Default Value: N/A

vlan *vlan-id*

Description: Apply this counter only in specific outer VLAN ID.

Value: 1 - 4094

Default Value: N/A

inner-vlan *vlan-id*

Description: Apply this counter only in specific inner VLAN ID.

Value: 1 - 4094

Default Value: N/A

interface *interface-name*

Description: Apply this counter only in specific interface. Multiple interface may be specified, and the counter will aggregate all these interfaces.

Value: *interface-type-chassis/slot/port | lag-id*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet and hundred-gigabit-ethernet.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.9	This command was introduced.
5.1	Added support for 25G interfaces.

Usage Guidelines

Counters can be created specifying multiple interfaces to count only the traffic in the specified interfaces.

Examples:

The following example creates one counter instance to count the number of octets on the ingress side of VLAN 100 and interfaces gigabit-ethernet-1/1/4 and gigabit-ethernet-1/1/5.

```
# config
Entering configuration mode terminal
(config)# counters
(counters)# ingress id 12
(counters-ingress-12)# vlan 100
(counters-ingress-12)# interface gigabit-ethernet-1/1/4
(counters-ingress-12)# interface gigabit-ethernet-1/1/5
(counters-ingress-12)# commit
Commit complete.
(counters-ingress-12)#
```

Impacts and precautions

With ACL: Ingress counters increment even for packets dropped by Ingress ACLs.

With VLAN Mapping: For packets which Action Replace has been applied the inner-VLAN considered by the Ingress Counter is the VLAN that has just been replaced.

Hardware restrictions

On DM4611 and DM4612 series: Ingress Counters are not supported.

On DM4270, DM4770 and DM4380 series: it is not allowed to create an egress counter

for an interface + VLAN when the interface is an untagged member of the VLAN.

On DM4270, DM4770 and DM4380 series: Layer 2 Control Protocol tunneled packets are counted twice on matching ingress counters.

interface utilization

Description

This command shows the port utilization bandwidth.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface utilization *interface-name* [I1] [I2]

Parameters

interface-name

Description: Single interface or a group of interfaces using regular expression.

Value: String with a maximum of 64 characters. It accepts a string to match a single interface or a regular expression to match more than one interface (See Usage Guidelines).

Default Value: N/A

I1

Description: Displays L1 bandwidth utilization.

Value: N/A

Default Value: N/A

I2

Description: Displays L2 bandwidth utilization.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
L1 TX Bandwidth	L1 bandwidth TX utilization.
L1 RX Bandwidth	L1 bandwidth RX utilization.
L2 TX Bandwidth	L2 bandwidth TX utilization.
L2 RX Bandwidth	L2 bandwidth RX utilization.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

Example:

Display L1 and L2 bandwidth of all available interfaces.

```
#show interface utilization
```

Display L1 bandwidth of all available interfaces.

```
#show interface utilization l1
```

Display L2 bandwidth of all available interfaces

```
#show interface utilization l2
```

Repetition Mode

For monitoring the bandwidth it is useful to use this command within the <repeat> command:

- Repeat the command every 2 seconds (default is 1 second):

```
#show interface utilization forty* | repeat 2
```

Filtering interfaces:

This command also has a property to refine and only display some interfaces.

Some filters are:

```
^      | Matches the beginning of a string.
[abc]  | Character class, which matches any of the characters abc. Character
        | ranges are specified by a pair of characters separated by a .
r*     | Matches zero or more rs.
```

Common filters examples:

- Match exactly an interface (pressing <tab> button will display all possible interfaces):

```
#show interface utilization gigabit-ethernet-1/1/1
```

- Filter for forty-gigabit-ethernet interfaces (when available):

```
#show interface utilization forty*
```

- Filter for interfaces presents in chassis 1 and slot 2 (when available):

```
#show interface utilization *1/2/*
```

- Filter for forty-gigabit-ethernet interfaces and ten-gigabit-ethernet (when available):

```
#show interface utilization [ft]*
```

- Filter for any interfaces presents in chassis 1 and any slot (when available):

```
#show interface utilization *1/*/*
```

- Filter for a range of interfaces presents in chassis 1 and slot 2 (when available):

```
#show interface utilization *1/2/2-5
```

- Filter for some interfaces presents in chassis 1 and slot 2 (when available):

```
#show interface utilization *1/2/2,7,10
```

Impacts and precautions

When the interval between the two last executions of this command is less than 1 minute, the measured and displayed bandwidth is the mean bandwidth during this interval. When the interval is greater than 1 minute, the displayed value is the instantaneous

bandwidth. When this command is executed in more than one user session at the same time, the bandwidth value displayed is not guaranteed to be accurate. For more accurate results, use this command with <repeat> option in a single user session (See Usage Guidelines).

Hardware restrictions

N/A

monitor session

Description

Create a monitor session and configure its parameters.

Supported Platforms

This command is supported in all platforms.

Syntax

monitor session *id*

monitor session *id* **destination interface** *interface-name*

monitor session *id* **source interface** *interface-name* [*traffic-type*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

monitor session *id*

Description: Sets the monitor session id.

Value: 1

Default Value: None

destination interface *interface-name*

Description: Sets the destination port for the monitoring session.

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: None

source interface *interface-name*

Description: Adds a source port to the monitoring session.

Value: *interface-type-chassis/slot/port | lag-id*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: None

traffic-type

Description: Sets the traffic type to monitor on a source interface.

Value: *rx | tx | all*

Default Value: rx (monitor the received traffic only)

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.2	This command was introduced.
5.0	Added support for 25G interfaces.

Usage Guidelines

Example:

This example shows how to create a monitor session.


```
#config
Entering configuration mode terminal
(config)# monitor session 1
(monитор-session-1)# destination interface gigabit-ethernet-1/1/1
(monитор-session-1-destination)# exit
(monитор-session-1)# source interface ten-gigabit-ethernet-1/1/1 tx
(monитор-session-source-interface-gigabit-ethernet-1/1/1)# top
(config)# commit
Commit complete.
(config)#
```

When adding a source interface to the monitor session, the default behaviour is to monitor its received traffic. Inside the interface configuration tree, the command *tx* or *all* will change the monitored traffic type.

Impacts and precautions

- Only one monitor session is available for configuration.
- Only pre-existing interfaces will be accepted when entering an interface name.
- A LAG cannot be used as the session destination interface.
- A LAG and its members cannot be used as source interfaces in the same monitor session.
- The mirrored traffic is subjected to the QoS and shaping rules of the destination interface.

Hardware restrictions

N/A

ping

Description

Ping is a utility that uses the ICMP protocol to test connectivity between IP networks devices.

Supported Platforms

This command is supported in all platforms.

Syntax

ping *ipv4-address* [**vrf** *name* | **size** *number* | **count** *number* | **interval** *time* | **fragment** *type* | **tos** *number* | **source** {*ip-address* | *interface*}]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

ipv4-address

Description: The IPv4 address destination to verify the reachability.

Value: a.b.c.d

Default Value: None.

vrf *name*

Description: The name of VRF to use.

Value: Any VRF created.

Default Value: None.

size *number*

Description: ICMP payload size.

Value: 0 - 65507

Default Value: 56.

count *number*

Description: Number of packets to be sent.

Value: 1 - 1000000000

Default Value: 5.

interval *number*

Description: Time interval in seconds to generate each packet.

Value: 1.0 - 86400.0

Default Value: 1.0

fragment *type*

Description: Set the Path MTU Discovery strategy:
The value *prohibit* prohibits fragmentation, even local one.
The value *discover* does PMTU discovery, fragment locally when packet size is large.
The value *permit* does not change fragmentation mode.

Value: {prohibit | discover | permit}

Default Value: permit.

tos *number*

Description: Set Type of Service bits.

Value: 0 - 255

Default Value: None.

source {*ip-address* | *interface*}

Description: Specify the source IP address or the interface name from which packets should be sent.

Value: *ip-address* - IP address from a configured interface in a.b.c.d format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
5.4	Added VRF support.

Usage Guidelines

The following example demonstrates how to use the ping command without any parameter. It will send 5 ICMP probes to the destination host.

```
# ping 10.0.121.80
PING 10.0.121.80 (10.0.121.80) 56(84) bytes of data.
64 bytes from 10.0.121.80: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 10.0.121.80: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 10.0.121.80: icmp_seq=3 ttl=64 time=0.019 ms
64 bytes from 10.0.121.80: icmp_seq=4 ttl=64 time=0.033 ms
64 bytes from 10.0.121.80: icmp_seq=5 ttl=64 time=0.036 ms
--- 10.0.121.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.015/0.027/0.036/0.009 ms
```

The following example demonstrates how to use the ping command with the “count” parameter:

```
# ping 10.0.121.80 count 2
```

```
PING 10.0.121.80 (10.0.121.80) 56(84) bytes of data.
64 bytes from 10.0.121.80: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 10.0.121.80: icmp_seq=2 ttl=64 time=0.034 ms

--- 10.0.121.80 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.023/0.028/0.034/0.007 ms
```

The following example demonstrates how to use the ping command with the “size” parameter:

```
# ping 10.0.121.80 size 1500
PING 10.0.121.80 (10.0.121.80) 1500(1528) bytes of data.
1508 bytes from 10.0.121.80: icmp_seq=1 ttl=64 time=0.018 ms
1508 bytes from 10.0.121.80: icmp_seq=2 ttl=64 time=0.035 ms
1508 bytes from 10.0.121.80: icmp_seq=3 ttl=64 time=0.034 ms
1508 bytes from 10.0.121.80: icmp_seq=4 ttl=64 time=0.035 ms
1508 bytes from 10.0.121.80: icmp_seq=5 ttl=64 time=0.037 ms

--- 10.0.121.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.018/0.031/0.037/0.009 ms
```

The following example demonstrates how to use the ping command with the “source” parameter using ip address:

```
# ping 10.0.121.80 source 200.20.136.10
PING 10.0.121.80 (10.0.121.80) from 200.20.136.10 : 56(84) bytes of data.
64 bytes from 10.0.121.80: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.0.121.80: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 10.0.121.80: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 10.0.121.80: icmp_seq=4 ttl=64 time=0.035 ms
64 bytes from 10.0.121.80: icmp_seq=5 ttl=64 time=0.037 ms

--- 10.0.121.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.018/0.031/0.037/0.009 ms
```

The following example demonstrates how to use the ping command with the “source” parameter using interface name:

```
# ping 10.0.121.80 source mgmt-1/1/1
PING 10.0.121.80 (10.0.121.80) from 11.12.0.14 eth0: 56(84) bytes of data.
64 bytes from 10.0.121.80: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.0.121.80: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 10.0.121.80: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 10.0.121.80: icmp_seq=4 ttl=64 time=0.035 ms
64 bytes from 10.0.121.80: icmp_seq=5 ttl=64 time=0.037 ms

--- 10.0.121.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.018/0.031/0.037/0.009 ms
```

Impacts and precautions

N/A

Hardware restrictions

N/A

ping6

Description

Ping6 is a utility that uses the ICMPv6 protocol to test connectivity between IP networks devices.

Supported Platforms

This command is supported in all platforms.

Syntax

ping6 *ipv6-address* [**vrf** *name* | **size** *number* | **count** *number* | **interval** *time* | **tos** *number* | **source** {*ip-address* | *interface*}]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

ipv6-address

Description: The IPv6 address destination to verify the reachability.

Value: X:X:X:X::X.

Default Value: None.

vrf *name*

Description: The name of VRF to use.

Value: Any VRF created.

Default Value: None.

size *number*

Description: ICMPv6 payload size.

Value: 0 - 65507

Default Value: 56.

count *number*

Description: Number of packets to be sent.

Value: 1 - 1000000000

Default Value: 5.

interval *number*

Description: Time interval in seconds to generate each packet.

Value: 1.0 - 86400.0

Default Value: 1.0

tos *number*

Description: Set Traffic Class bits.

Value: 0 - 255

Default Value: None.

source {*ip-address* | *interface*}

Description: Specify the source IP address or the interface name from which packets should be sent.

Value: *ip-address* - IP address from a configured interface in X:X:X:X::X format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
2.4	This command was introduced.
6.0	Added VRF support.

Usage Guidelines

The following example demonstrates how to use the ping6 command without any parameter. It will send 5 ICMPv6 probes to the destination host:

```
# ping6 2001:DB8::1
PING 2001:DB8::1(2001:DB8::1) 56 data bytes
64 bytes from 2001:DB8::1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 2001:DB8::1: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from 2001:DB8::1: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=5 ttl=64 time=0.051 ms

--- 2001:DB8::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.027/0.036/0.051/0.010 ms
```

The following example demonstrates how to use the ping6 command with the “count” parameter:

```
# ping6 2001:DB8::1 count 2
PING 2001:DB8::1(2001:DB8::1) 56 data bytes
64 bytes from 2001:DB8::1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 2001:DB8::1: icmp_seq=2 ttl=64 time=0.037 ms

--- 2001:DB8::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.028/0.032/0.037/0.007 ms
```

The following example demonstrates how to use the ping6 command with the “size” parameter:

```
# ping6 2001:DB8::1 size 1500
PING 2001:DB8::1(2001:DB8::1) 1500 data bytes
```

```

1508 bytes from 2001:DB8::1: icmp_seq=1 ttl=64 time=0.050 ms
1508 bytes from 2001:DB8::1: icmp_seq=2 ttl=64 time=0.073 ms
1508 bytes from 2001:DB8::1: icmp_seq=3 ttl=64 time=0.039 ms
1508 bytes from 2001:DB8::1: icmp_seq=4 ttl=64 time=0.037 ms
1508 bytes from 2001:DB8::1: icmp_seq=5 ttl=64 time=0.040 ms

--- 2001:DB8::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.037/0.047/0.073/0.015 ms

```

The following example demonstrates how to use the ping6 command with the “source” parameter using ip address:

```

# ping6 2001:DB8::1 source 3001:AFF::2
PING 2001:DB8::1(2001:DB8::1) from 3001:AFF::2 : 56 data bytes
64 bytes from 2001:DB8::1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 2001:DB8::1: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from 2001:DB8::1: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=5 ttl=64 time=0.051 ms

--- 2001:DB8::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.027/0.036/0.051/0.010 ms

```

The following example demonstrates how to use the ping6 command with the “source” parameter using interface name:

```

# ping6 2001:DB8::1 source mgmt-1/1/1
PING 2001:DB8::1(2001:DB8::1) from 11:12::14 eth0 : 56 data bytes
64 bytes from 2001:DB8::1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 2001:DB8::1: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from 2001:DB8::1: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from 2001:DB8::1: icmp_seq=5 ttl=64 time=0.051 ms

--- 2001:DB8::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.027/0.036/0.051/0.010 ms

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show alarm

Description

Display the current active alarms.

Supported Platforms

This command is supported in all platforms.

Syntax

show alarm

Parameters

N/A

Output Terms

Output	Description
Triggered on	Time of when the alarm was triggered.
Severity	Severity of the alarm, can be either MINOR, MAJOR or CRITICAL.
Source	Source interface which triggered the alarm.
Status	Status of the alarm.
Name	Name of the alarm, prefixed with '*' when the alarm is unstable.
Description	Description of the alarm.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

N/A

Impacts and precautions

N/A

Hardware restrictions

N/A

show core-dump

Description

Show list core dump files.

Supported Platforms

This command is supported in all platforms.

Syntax

show core-dump

Parameters

N/A

Output Terms

Output	Description
Filename, size and timestamp	Filename, size and timestamp of the core dump file.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
2.0	The format of timestamp was changed to include the timezone offset information.

Usage Guidelines

To show core-dump file list. Maximun files in list: 10

```
DM4610# show core-dump
Filename | Size | Date created
-----|-----|-----
core-file.5407.1493214178.core.gz 0.99 MB 2017-04-26 13:42:58 UTC+0
DM4610#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show counters

Description

Displays statistics counters for User-Defined Counter instances.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show counters [ { ingress | egress } [ id counter-id ] ]
```

Parameters

ingress

Description: This parameter displays ingress user defined counters only.

Value: N/A

Default Value: N/A

egress

Description: This parameter displays egress user defined counters only.

Value: N/A

Default Value: N/A

id *counter-id*

Description: User defined counter identifier.

Value: 1 - 256

Default Value: N/A

Output Terms

Output	Description
ID	The user defined counter identifier.
DESCRIPTION	The user defined counter description.
VALUE	The current value of the user defined counter.
TYPE	The unit of the user defined counter current value.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.9	This command was introduced.

Usage Guidelines

Given the equipment has an ingress and an egress user defined counter configured, the command could result in the following output:

```
# show counters
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   vlan100      1024   octets
```



```
EGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   vlan100      2048   octets
```

The output of the command when the user specifies the ingress counter-id 1 could look like this:

```
# show counters ingress id 1
INGRESS COUNTERS
ID  DESCRIPTION  VALUE  TYPE
-----
1   vlan100      1024   octets
```

Impacts and precautions

The values presented by this command are accumulated since the last time the operator issued a clear command.

Hardware restrictions

The maximum counter value is restricted by the width of the hardware counter storage.

show interface statistics

Description

This command displays the statistics counters for an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface *interface-name* **statistics**

Parameters

interface-name

- Description:** Interface id referencing chassis/slot/port respectively or an id referencing a specified LAG.
- Value:** { { **gigabit-ethernet** | **ten-gigabit-ethernet** | **twenty-five-g-ethernet** | **forty-gigabit-ethernet** | **hundred-gigabit-ethernet** } *c/s/p* } | **lag** *id* }
- Default Value:** None

Output Terms

Output	Description
In Octets	The amount of octets that entered the network interface
In Unicast Pkts	The amount of packets that entered the network interface to a unicast address
In Broadcast Pkts	The amount of packets that entered the network interface to a broadcast address

Output	Description
In Multicast Pkts	The amount of packets that entered the network interface to a multicast address
In Discards	The amount of packets discarded by the network interface
In Errors	The amount of packets that entered the network interface with errors
In Unknown Protos	The amount of packets whose protocol was unknown that entered the network interface
Out Octets	The amount of octets that exited the network interface
Out Unicast Pkts	The amount of packets that exited the network interface to a unicast address
Out Broadcast Pkts	The amount of packets that exited the network interface to a broadcast address
Out Multicast Pkts	The amount of packets that exited the network interface to a multicast address
Out Discards	The amount of packets discarded by the network interface in the egress block
Out Errors	The amount of packets with errors in the egress block

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.2	This command was introduced.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G and LAG interfaces.
5.0	Added support for 25G.

Usage Guidelines

The values presented by this command are accumulated since the last time the operator issued a **clear statistics** *interface-name* command. Because of this, these values should not be used for accounting or billing. A sample usage of the command is presented below:

```
> show interface gigabit-ethernet 1/1/1 statistics
```

Counter	Value
In Octets	: 0
In Unicast Pkts	: 0
In Broadcast Pkts	: 0
In Multicast Pkts	: 0
In Discards	: 0
In Errors	: 0
In Unknown Protos	: 0
Out Octets	: 0
Out Unicast Pkts	: 0
Out Broadcast Pkts	: 0
Out Multicast Pkts	: 0
Out Discards	: 0
Out Errors	: 0

Impacts and precautions

The values presented via CLI and Netconf should not be used for accounting or billing (see usage guidelines for more information).

Hardware restrictions

The maximum counter value is restricted by the width of the hardware counter storage.

show system cpu

Description

Displays information about CPU usage including the overall CPU load per chassis and slot on the equipment.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show system cpu [ detail | chassis chassis-id [ slot slot-id [ { load | core [ core-id ] } ] ]
```

Parameters

detail

Description: Show the CPU usage of all process.

Value: None.

Default Value: None.

chassis *chassis-id*

Description: Chassis identification.

Value: 1.

Default Value: None.

slot *slot-id*

Description: Slot identification.

Value: 1.

Default Value: None.

load

Description: Load information.

Value: None.

Default Value: None.

core *core-id*

Description: Core information.

Value: 0-1.

Default Value: None.

Output Terms

Output	Description
user	Statistics for CPU time spent in user mode.
system	Statistics for CPU time spent in system mode.
nice	Statistics for CPU time spent in user mode with low priority.
wait	Statistics for CPU time spent awaiting for I/O to complete.
irq	Statistics for CPU time spent in hardware interrupts.
softirq	Statistics for CPU time spent in software interrupts.
active	Statistics for active CPU time spent.
idle	Statistics for idle CPU time spent.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.6	This command was introduced.
-----	------------------------------

Usage Guidelines

Displaying load average of all CPUs, in particular slot, in different interval of time:

```
DM4610# show system cpu chassis 1 slot 1 load
CPU load information:
---      5 seconds  1 minute  5 minutes
active   60.0%      4.4%      100.0%
idle     40.0%      96.6%      0.0%
```

Displaying detailed information about a specific CPU core:

```
DM4610# show system cpu chassis 1 slot 1 core 0
CPU core 0 information:
---      5 seconds  1 minute  5 minutes
user      0.8%      1.0%      0.8%
system    0.3%      0.8%      0.3%
nice      0.0%      0.0%      0.0%
wait      2.0%      5.6%      2.0%
interrupt 0.0%      0.0%      0.0%
softirq   0.0%      0.2%      0.0%
active    1.0%      1.0%      1.0%
idle      96.9%     92.4%     96.9%
```

Displaying the load average, and also detailed information per-core for each chassis and slot:

```
DM4610# show system cpu
Chassis/Slot: 1/1

CPU load information:
---      5 seconds  1 minute  5 minutes
active    0.0%      2.9%      2.9%
idle      100.0%     95.1%     97.3%

CPU core 0 information:
---      5 seconds  1 minute  5 minutes
user      0.2%      0.8%      0.2%
system    0.3%      1.7%      0.3%
nice      0.0%      0.0%      0.0%
wait      0.0%      1.9%      0.0%
interrupt 0.0%      0.0%      0.0%
softirq   0.2%      0.2%      0.2%
active    0.5%      0.5%      0.5%
idle      99.4%     95.4%     99.4%
```

Impacts and precautions

Some minutes after system initialization, the percentage is zero because no information was generated yet.

Hardware restrictions

None.

show system memory

Description

Displays system memory information and usage statistics useful for monitoring and troubleshooting.

Supported Platforms

This command is supported in all platforms.

Syntax

show system memory [**detail** | **chassis** *chassis-id* [**slot** *slot-id*]]

Parameters

detail

Description: Show the memory usage of all process.

Value: None.

Default Value: None.

chassis *chassis-id*

Description: Chassis identification.

Value: 1.

Default Value: None.

slot *slot-id*

Description: Slot identification.

Value: 1.

Default Value: None.

Output Terms

Output	Description
<code>total</code>	Statistics for total usable RAM.
<code>used</code>	Statistics for memory in use by processes.
<code>available</code>	Statistics for memory available for starting new applications (not including swap memory).
<code>free</code>	Statistics for memory available for use by userspace programs, kernel data structures and the pagecache.
<code>buffered</code>	Statistics for buffered memory, used as temporary storage for raw disk blocks lower than 20 MiB.
<code>cached</code>	Statistics for cached memory, which is an in-memory cache for files read from disk (the page cache).
<code>slab_recl</code>	Statistics for reclaimable slab memory, which is a reclaimable in-kernel cache for data structures.
<code>slab_unrecl</code>	Statistics for non-reclaimable slab memory, which is a non-reclaimable in-kernel cache for data structures.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.8	This command was introduced.

Release	Modification
---------	--------------

4.4	Adds the '1 minute' memory interval
-----	-------------------------------------

Usage Guidelines

Report detailed memory information of the line card on slot 1 of chassis 1. There are four consolidation intervals expressing the trend line of memory consumption in the last thirty minutes. On non-modular equipments the values for chassis and slot are fixed at 1.

```
DM4610# show system memory chassis 1 slot 1
Memory information:
---      5 seconds  1 minute   5 minutes   30 minutes
```

Report detailed memory information of line cards on chassis 1. There are four consolidation intervals expressing the trend line of memory consumption in the last thirty minutes

```
DM4610# show system memory chassis 1
Memory information:
---      5 seconds  1 minute   5 minutes   30 minutes
```

Report detailed memory information of the entire system. There are four consolidation intervals expressing the trend line of memory consumption in the last thirty minutes.

```
DM4610# show system memory
Chassis/Slot: 1/1

Memory information:
---      5 seconds  1 minute   5 minutes   30 minutes
```

Impacts and precautions

None.

Hardware restrictions

None.

show system uptime

Description

Shows the system uptime.

Supported Platforms

This command is supported in all platforms.

Syntax

show system uptime

Parameters

N/A

Output Terms

Output	Description
Current uptime of system	Shows the time that the system is operational in “<Current time> up <uptime>, <Number of logged users>, load average: <in 1 minute>, <in 5 minutes>, <in 15 minutes>” format

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.10	The command “uptime” was replaced by “show system uptime”. The old command was kept for compatibility.

Usage Guidelines

N/A

Impacts and precautions

N/A

Hardware restrictions

N/A

show tech-support

Description

Shows relevant information to be used by technical support.

Supported Platforms

This command is supported in all platforms.

Syntax

show tech-support [gpon | infra | I2 | I3 | mpls | no-running]

Parameters

tech-support

Description: Show all technical support informations.

Value: No range value.

Default Value: No default value.

gpon

Description: Show gpon information more infrastructure informations.

Value: No range value.

Default Value: No default value.

infra

Description: Show infrastructure informations.

Value: No range value.

Default Value: No default value.

I2

Description: Show layer 2 information more infrastructure informations.

Value: No range value.

Default Value: No default value.

I3

Description: Show layer 3 information more infrastructure informations.

Value: No range value.

Default Value: No default value.

mpls

Description: Show mpls information more infrastructure informations.

Value: No range value.

Default Value: No default value.

no-running

Description: Show technical information without the running-config.

Value: No range value.

Default Value: No default value.

Output Terms

Output	Description
Status	Shows relevant information to be used by technical support

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
6.0	Added parameter 'no-running' to exclude show running-config from tech-support.

Usage Guidelines

The following example shows how to use the show tech-support without parameters, it will show all technical support informations:

```
hostname# show tech-support
```

The following example shows how to use the show tech-support with gpon option, it will show gpon information more infrastructure informations:

```
hostname# show tech-support gpon
```

The following example shows how to use the show tech-support with infra option, it will show infrastructure informations:

```
hostname# show tech-support infra
```

The following example shows how to use the show tech-support with l2 option, it will show layer 2 information more infrastructure informations:

```
hostname# show tech-support l2
```

The following example shows how to use the show tech-support with l3 option, it will show layer 3 information more infrastructure informations:

```
hostname# show tech-support l3
```

Impacts and precautions

N/A

Hardware restrictions

N/A

tcpdump

Description

Start a debug session to capture network traffic received or transmitted by the CPU. Only inband management packets are captured, i.e., all traffic received or sent by out-band management interfaces (such as mgmt 1/1/1) are not captured. Please note that simultaneous debug sessions are not allowed.

Supported Platforms

This command is supported in all platforms.

Syntax

```
tcpdump packet-direction [ interface name ] [ count number ] [ verbosity-level level ]
[ print-link-level-header ] [ print-data format ] [ print-timestamp format ] [ filter
tcpdump-filter ] [ save-pcap ]
```

Parameters

packet-direction

Description: Packet direction (received, transmitted or both).
Value: List of supported directions: rx, tx, and rx-and-tx.
Default Value: None.

interface *name*

Description: Name of the interface to be sniffed.
Value: Name of the interface.
Default Value: Listen all interfaces.

count *number*

Description: Number of packets to be sniffed.
Value: Integer number greater than zero.
Default Value: None.

verbosity-level *level*

Description: Level of verbosity of packet dump.

Value: 1 - 3

Default Value: Use non-verbose packet dump.

print-link-level-header

Description: Print link-level header of each packet.

Value: N/A;

Default Value: Do not print link-level header information.

print-data *format*

Description: Print the data of each packet in hex and/or ASCII format.

Value: List of supported formats: hex, link-level-hex, hex-ascii, and link-level-hex-ascii.

Default Value: None.

print-timestamp *format*

Description: Print timestamp of each packet.

Value: List of supported formats and examples:

- no: no timestamp is printed
- utc: 1612286218.939735
- h-m-s: 2021-02-02 14:16:58.939735
- delta-current-previous: 00:00:00.000051
- delta-current-first: 00:00:00.001741

Default Value: If not specified, time is shown for each packet. For instance: 14:16:58.939735.

filter *tcpdump-filter*

Description: Tcpdump filter expression. Note that tcpdump filter presents an unusual behaviour when using “vlan” in the expression because “vlan” always causes an offset of 4 bytes to the following parameters of the filter. If a filter is passed as “vlan and arp”, tcpdump will correctly filter VLAN-encapsulated ARP packets. But “vlan or arp” instead of looking for VLAN-encapsulated packets or ARP (without VLAN) packets, will also look for VLAN-encapsulated ARP packets.

Value: A Berkeley Packet Filter (BPF) expression.

Default Value: None.

save-pcap

Description: Save captured packets to a pcap file, which has a maximum size of 2MB. When this limit is reached, the file will be rotated, removing ~1MB associated with the oldest packets. When a new capture is started, the pcap file is removed, and data from previous capture sessions are thus discarded. If no packet is captured, no capture file is generated.

Value: N/A;

Default Value: Do not save dump to pcap file.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

The following example demonstrates how to use tcpdump only with direction parameter:

```
# tcpdump rx-and-tx
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
[TX Mode: INTERFACE, TX] - 13:53:51.378208 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 13:53:52.407735 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 13:53:53.431732 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
```

The following example demonstrates how to use tcpdump with interface parameter:

```
# tcpdump rx interface gigabit-ethernet-1/1/1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on gigabit-ethernet-1/1/1, link-type EN10MB (Ethernet), capture size 262144 bytes
[Interface: gigabit-ethernet-1/1/1, RX] - 15:31:56.661166 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/1, RX] - 15:31:56.770118 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/1, RX] - 15:31:56.878792 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
```

The following example demonstrates how to use tcpdump with interface parameter when there is a LAG interface:

```
# tcpdump rx interface gigabit-ethernet-1/1/1 count 20
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on gigabit-ethernet-1/1/1, link-type EN10MB (Ethernet), capture size 262144 bytes
[Physical interface: gigabit-ethernet-1/1/1, Interface: lag-1, RX] - 15:28:42.143215 ARP, Reply...
[Physical interface: gigabit-ethernet-1/1/1, Interface: lag-1, RX] - 15:28:42.263215 ARP, Reply...
[Physical interface: gigabit-ethernet-1/1/1, Interface: lag-1, RX] - 15:28:42.363215 ARP, Reply...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
# tcpdump rx interface lag-1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lag-1, link-type EN10MB (Ethernet), capture size 262144 bytes
[Physical interface: gigabit-ethernet-1/1/3, Interface: lag-1, RX] - 15:28:42.205291 IP 5.5.5.1...
[Physical interface: gigabit-ethernet-1/1/1, Interface: lag-1, RX] - 15:28:42.263215 ARP, Reply...
[Physical interface: gigabit-ethernet-1/1/3, Interface: lag-1, RX] - 15:28:42.306467 IP 5.5.5.1...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
```

The following example demonstrates how to use the tcpdump command with the “count” parameter:

```
# tcpdump rx-and-tx count 1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 16:42:51.186861 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
```

```

1 packet captured
4 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates how to use the `tcpdump` command with the “`verbosity-level`” parameter:

```

# tcpdump rx-and-tx verbosity-level 1
tcpdump: listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 16:44:02.866870 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has...
^C
1 packet captured
1 packet received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates how to use the `tcpdump` command with the “`print-timestamp`” parameter:

```

# tcpdump rx-and-tx print-timestamp h-m-s
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 2015-10-21 07:28:28.275022 ARP, Request who-has 1.1.1.1 tell 192.168...
[TX Mode: INTERFACE, TX] - 2015-10-21 07:28:29.298877 ARP, Request who-has 1.1.1.1 tell 192.168...
[TX Mode: INTERFACE, TX] - 2015-10-21 07:28:30.322868 ARP, Request who-has 1.1.1.1 tell 192.168...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates how the timestamp is printed when “`print-timestamp`” is “`delta-current-previous`”:

```

# tcpdump rx-and-tx print-timestamp delta-current-previous
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 00:00:00.000000 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
[TX Mode: INTERFACE, TX] - 00:00:01.024301 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
[TX Mode: INTERFACE, TX] - 00:00:01.023696 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates how the timestamp is printed when “`print-timestamp`” is “`delta-current-first`”:

```
# tcpdump rx-and-tx print-timestamp delta-current-first
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 00:00:00.000000 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
[TX Mode: INTERFACE, TX] - 00:00:01.024301 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
[TX Mode: INTERFACE, TX] - 00:00:02.047997 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, len...
^C
3 packets captured
3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
```

The following example demonstrates how to use the tcpdump command with the “filter” parameter:

```
# tcpdump rx-and-tx filter "arp"
tcpdump: verbose output suppressed, use verbosity-level 1, 2 or 3 for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 16:04:10.991225 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:12.019647 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:13.043746 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:14.067979 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:15.091813 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
^C
5 packets captured
5 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
# tcpdump rx-and-tx filter "vlan and arp"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[Interface: gigabit-ethernet-1/1/3, RX] - 14:28:49.226863 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/3, RX] - 14:28:49.327539 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/3, RX] - 14:28:49.428315 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/3, RX] - 14:28:49.528865 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
[Interface: gigabit-ethernet-1/1/3, RX] - 14:28:49.629842 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
^C
5 packets captured
5 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
# tcpdump rx-and-tx filter "ether proto 0x0806"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
[TX Mode: INTERFACE, TX] - 16:04:10.991225 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:12.019647 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:13.043746 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:14.067979 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
[TX Mode: INTERFACE, TX] - 16:04:15.091813 ARP, Request who-has 1.1.1.1 tell 192.168.1.80, leng...
^C
5 packets captured
5 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
```

The following example demonstrates how to use the tcpdump command with the “save-pcap” parameter:

```
# tcpdump rx-and-tx save-pcap
tcpdump: listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
^C3 packets captured
```



```

3 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates how to use tcpdump and filter by VLAN ID:

```

# tcpdump rx filter "vlan 20"
[Interface: gigabit-ethernet-1/1/1, RX] - 14:28:49.423160 ARP, Reply 5.5.5.1 is-at 52:54:00:81:...
^C
1 packets captured
1 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
# tcpdump rx print-link-level-header filter "vlan 20"
...9:06 (oui Unknown), ethertype 802.1Q (0x8100), length 64: vlan 20, p 0, ethertype ARP, Reply...
^C
1 packets captured
1 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

The following example demonstrates what happens when try to open a second tcpdump session:

```

# tcpdump rx-and-tx
Error: already running by:
    admin ssh (cli from 192.168.1.127) on since 2021-03-02 14:27:29

```

The following example demonstrates the unusual behaviour of tcpdump when using filter with “vlan”:

```

# tcpdump rx print-link-level-header filter "vlan and arp"
tcpdump: verbose output suppressed, use verbosity-level 1, 2 or 3 for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
...9:06 (oui Unknown), ethertype 802.1Q (0x8100), length 64: vlan 30, p 0, ethertype ARP, Reply...
^C
1 packets captured
1 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel
# tcpdump rx print-link-level-header filter "vlan or arp"
tcpdump: verbose output suppressed, use verbosity-level 1, 2 or 3 for full protocol decode
listening on any, link-type EN10MB (Ethernet), capture size 262144 bytes
...9:06 (oui Unknown), ethertype 802.1Q (0x8100), length 64: vlan 20, p 0, ethertype ARP, Reply...
^C
1 packets captured
1 packets received by filter
0 packets dropped by metadata filters
0 packets dropped by kernel

```

Impacts and precautions

None.

Hardware restrictions

None

traceroute

Description

Traceroute is a utility for displaying all the hops to reach a destination and measuring transit delays of packets across an Internet Protocol (IP) network.

Supported Platforms

This command is supported in all platforms.

Syntax

```
traceroute ipv4-address [ vrf name | source {ip-address | interface} ]
```

Parameters

ipv4-address

Description: The IPv4 address destination.

Value: a.b.c.d

Default Value: None.

vrf *name*

Description: The name of VRF to use.

Value: Any VRF created.

Default Value: None.

source {*ip-address* | *interface*}

Description: Specify the source IP address or the interface name from which packets should be sent.

Value: *ip-address* - IP address from a configured interface in a.b.c.d format;
or
interface - name of the management or I3 interface in I3-<name>, mgmt-<c>/<s>/<p> format.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.0	This command was introduced.
5.2	Added source support.
5.4	Added VRF support.

Usage Guidelines

The following example demonstrates how to use the traceroute command.

```
# traceroute 10.1.147.55
traceroute to 10.1.147.55 (10.1.147.55), 30 hops max, 60 byte packets
 1  10.1.8.1 (10.1.8.1)  1.255 ms  5.530 ms  6.095 ms
 2  10.1.63.18 (10.1.63.18)  1.172 ms  2.871 ms  3.436 ms
 3  10.1.63.110 (10.1.63.110)  5.423 ms  10.524 ms  12.045 ms
 4  10.1.147.55 (10.1.147.55)  0.321 ms  0.326 ms  0.313 ms
```

The following example demonstrates how to use the traceroute command with the “source” parameter using interface name:

```
# traceroute 10.1.8.173 source mgmt-1/1/1
traceroute to 10.1.8.173 (10.1.8.173), 30 hops max, 38 byte packets
 1  10.1.147.254 (10.1.147.254)  10.175 ms  7.070 ms  3.228 ms
 2  10.1.63.109 (10.1.63.109)  1.139 ms  1.142 ms  1.251 ms
```

```
3 10.1.63.17 (10.1.63.17) 1.204 ms 1.245 ms 2.664 ms
4 10.1.8.173 (10.1.8.173) 0.334 ms 0.313 ms 0.295 ms
```

The following example demonstrates how to use the traceroute command with the “source” parameter using IP address:

```
# traceroute 10.1.8.173 source 10.1.147.11
traceroute to 10.1.8.173 (10.1.8.173) from 10.1.147.11, 30 hops max, 38 byte packets
 1 10.1.147.254 (10.1.147.254) 6.749 ms 5.596 ms 3.289 ms
 2 10.1.63.109 (10.1.63.109) 1.286 ms 1.088 ms 1.484 ms
 3 10.1.63.17 (10.1.63.17) 1.037 ms 1.221 ms 1.206 ms
 4 10.1.8.173 (10.1.8.173) 0.557 ms 0.294 ms 0.261 ms
```

The following example demonstrates how to use the traceroute command with the “vrf” parameter:

```
# traceroute 31.1.1.2 vrf yellow
traceroute to 31.1.1.2 (31.1.1.2), 30 hops max, 38 byte packets
 1 21.1.1.1 (21.1.1.1) 1.687 ms 1.494 ms 1.455 ms
 2 31.1.1.2 (31.1.1.2) 2.526 ms 0.859 ms 0.849 ms
```

Impacts and precautions

N/A

Hardware restrictions

N/A

traceroute6

Description

Traceroute is a utility for displaying all the hops to reach a destination and measuring transit delays of packets across an Internet Protocol version 6 (IPv6) network.

Supported Platforms

This command is supported in all platforms.

Syntax

```
traceroute6 ipv6-address [ vrf name ]
```

Parameters

ipv6-address

Description: The IPv6 address destination.

Value: X:X:X:X::X

Default Value: None.

vrf *name*

Description: The name of VRF to use.

Value: Any VRF created.

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.0	This command was introduced.
6.0	Added VRF support.

Usage Guidelines

The following example demonstrates how to use the traceroute command.

```
# traceroute6 2002::1
traceroute to 2002::1 (2002::1) from 2001::1, 30 hops max, 16 byte packets
 1  2001::2 (2001::2)  11.438 ms  2.072 ms  1.962 ms
 2  2002::1 (2002::1)  1.172 ms  1.327 ms  1.113 ms
```

The following example demonstrates how to use the traceroute command with the “vrf” parameter:

```
# traceroute6 2002::1 vrf yellow
traceroute to 2002::1 (2002::1) from 2001::1, 30 hops max, 16 byte packets
 1  2001::2 (2001::2)  11.438 ms  2.072 ms  1.962 ms
 2  2002::1 (2002::1)  1.172 ms  1.327 ms  1.113 ms
```

As link-local addresses are not routable, the traceroute command with this kind of address must fail.

```
# traceroute6 fe80::204:dfff:fecc:25cb
connect: Invalid argument
```

Impacts and precautions

N/A

Hardware restrictions

N/A

SNMP

This topic describes the commands related to configuration and use of Simple Network Management Protocol (SNMP) such as commands to configure communities or to enable traps.

snmp agent

Description

Configures the SNMP agent.

Supported Platforms

This command is supported in all platforms.

Syntax

```
snmp agent { [ context vrf-name]* | [ disabled | enabled ] | engine-id { enterprise-number number | [ from-ip { a.b.c.d | x:x:x:x::x } | from-mac-address mac-address | from-text text | other string ] }* | ip { a.b.c.d | x:x:x:x::x } | max-message-size size | udp-port port | version { v1 | v2c | v3 }* }* snmp agent [ listen { interface interface-name } | [ udp-port port ] ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

context *vrf-name*

Description:	Creates a context for SNMP requests enabling logical network entity mapping. SNMP contexts may be used to access MIB data within a VRF/VPN context. It must be used along snmp community context-map configuration in case of SNMPv1 and SNMPv2.
Value:	VRF name
Default Value:	None.

[**disabled** | **enabled**]

Description: Disables or enables the SNMP agent.

Value: disabled or enabled.

Default Value: disabled.

engine-id

Description: Configures the SNMP agent Engine ID. It is a local and unique identifier to be used for communication with SNMPv3 Agents and Managers.

Value: { **enterprise-number** *number* | [**from-ip** { a.b.c.d | x:x:x:x::x } | **from-mac-address** *mac-address* | **from-text** *text* | **other** *string*] }*

Default Value: None.

enterprise-number *number*

Description: Assigns an Enterprise ID to assemble the Engine ID octets.

Value: 0-4294967295.

Default Value: 3709.

from-ip { a.b.c.d | x:x:x:x::x }

Description: Assigns an IPv4 or IPv6 address to assemble the Engine ID octets.

Value: a.b.c.d or x:x:x:x::x.

Default Value: None.

from-mac-address *mac-address*

Description: Assigns a MAC address to assemble the Engine ID octets.

Value: xx:xx:xx:xx:xx:xx.

Default Value: None.

from-text *text*

Description: Assigns a text to assemble the Engine ID octets.

Value: String - maximum 27 characters.

Default Value: None.

other *string*

Description: Configures the engine ID based on a specified string pattern in accordance to RFC3411.

Value: pattern “[0-9a-fA-F]{2}(:[0-9a-fA-F]{2}){0,27}”

Default Value: None.

ip { a.b.c.d | x:x:x:x::x }

Description: Configures an IPv4 or IPv6 as local SNMP agent address.

Value: a.b.c.d or x:x:x:x::x.

Default Value: None.

max-message-size *size*

Description: Configures the maximum SNMP agent message size that can be sent or received.

Value: 484-214748364.

Default Value: 50000.

udp-port *port*

Description: Sets the UDP protocol port to be used for communication with the SNMP Agents and Managers.

Value: UDP port.

Default Value: 161.

version { **v1** | **v2c** | **v3** }

Description: Configures the SNMP agent version. The options are SNMP version 1, SNMP version 2c and SNMP version 3. More than one option can be configured.

Value: { **v1** | **v2c** | **v3** }

Default Value: **v2c** and **v3**.

listen interface *interface-name* [**udp-port** *port*]

Description: List of interfaces to listen for SNMP requests.

Value: Interface name in format I3-<name> or loopback-<name>.

Default Value: None.

udp-port *port*

Description: Port on which SNMP will listen for requests on this interface.

Value: UDP port.
Default Value: 161.

Default

disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
2.4	Supported extra-list parameter in SNMP agent.
4.4	Removed the option no for SNMP agent enabled and disabled.
5.0	Command extra-listen replaced by listen .
5.8	Added parameter context in SNMP agent command.
6.0	Added support to loopback interface on SNMP agent listen configuration.

Usage Guidelines

This command can be executed directly via CLI. The *listen interface* allows the configuration of a list of interfaces to listen for SNMP requests. This configuration can be used

for managing SNMP on a VRF.

Example:

This example shows how to configure the SNMP agent using version 2c.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp agent version v2c
(config)# snmp agent ip 10.1.0.1
(config)# snmp agent enabled
(config)# commit
Commit complete.
```

This example shows how to configure the SNMP agent listen interfaces.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp agent listen interface l3-vrf-blue
(config-interface-l3-vrf-blue)# commit
Commit complete.
```

Impacts and precautions

The SNMP version 3 requires an engine ID.

The Enterprise number 3709 is assigned by IANA to Teracom Telematica Ltda.

Be very careful when using a different udp-port for SNMP agent listen interface in order to avoid conflicts with other protocols, such as DHCP (67/68), TFTP (69). In these cases SNMP agent listen interface might work but it can interfere in other protocols. The exception is NTP port (123), that is forbidden to be used, since it will not work.

For SNMP listen interface without VRF, SNMP agent will always listen on 161 port, even when a listen interface is configured for another port. In such cases, both ports can be used for SNMP service. For listen interfaces with VRF, only the configured udp-port works.

In order to use SNMP agent with VRF mgmt, use SNMP agent IP with the same IPv4 address as configured in out-of-band management interface (interface mgmt X/Y/Z).

SNMP agent listen interface will only use the L3 interface primary IPv4 address. Secondary IPv4 address is not supported for L3 interfaces. Also, only the first IPv6 address will be used for L3 or loopback interface.

SNMP agent listen interface only supports VRF with IPV4 address. VRF with IPv6 is not supported yet (L3 or loopback interfaces).

Hardware restrictions

N/A

snmp community

Description

Configures the SNMP communities to be used with managers and agents using version SNMPv1 or SNMPv2c.

Supported Platforms

This command is supported in all platforms.

Syntax

snmp community *index* [**context-map** *context* | **name** *community_name* | **sec-name** *security-name* | **target-tag** *identifier*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

index

Description: Specifies the community index.
Value: String - maximum 32 characters.
Default Value: None.

context-map *context*

Description: Specifies the context mapping.
SNMP requests for the related community will address MIB data within the VRF pointed by the SNMP context.
Value: SNMP agent context.
Default Value: Empty.

name *community_name*

Description: Specifies the community name. It should be used in case it is different from the *index*.
Value: String.

Default Value: None.

sec-name *security-name*

Description: Specifies the community security name corresponding to the community name in a security model independent format.

Value: String - maximum 32 characters.

Default Value: None.

target-tag *identifier*

Description: Specifies the target tag to be used as an identifier to restrict access for this community.

Value: String.

Default Value: None.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
5.8	The parameter context-map was introduced.

Usage Guidelines

This command can be executed directly via CLI. Up to 32 communities can be created.

Example:

This example shows how to configure an SNMP community.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp community private name private-comm sec-name pvt
(config)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

snmp notify

Description

Configures the SNMP notification for a specific target defined by tag identifier.

Supported Platforms

This command is supported in all platforms.

Syntax

snmp notify *name* **tag** *identifier* [**type** { **inform** | **trap** }]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

name

Description: Specifies the notification name.
Value: String - maximum 32 characters.
Default Value: None.

tag *identifier*

Description: Specifies the notification target tag identifier.
Value: String.
Default Value: None.

type { **inform** | **trap** }

Description: Specifies the notification type.
Value: **inform** or **trap**.
Default Value: **trap**.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI. Up to 32 entries can be created. SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

Example:

This example shows how to configure the SNMP notification for the target std_v1_trap.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp notify std_v1_trap
(config-notify-std_v1_trap)# tag std_v1_trap
(config-notify-std_v1_trap)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

snmp system

Description

Configures the SNMP system parameters.

Supported Platforms

This command is supported in all platforms.

Syntax

snmp system { **contact** *text* **location** *loc* }*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

contact *text*

Description: Sets the system contact information.
Value: String - maximum 255 characters.
Default Value: None.

location *loc*

Description: Sets the system location.
Value: String - maximum 255 characters.
Default Value: None.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the SNMP system parameters.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp system location Curitiba
(config)# snmp system contact "Teracom Telematica Ltda"
(config)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

snmp target

Description

Configures a SNMP target list.

Supported Platforms

This command is supported in all platforms.

Syntax

```
snmp target name ip { a.b.c.d | x:x:x:x::x } { usm user-name name sec-level {  
auth-no-priv | auth-priv | no-auth-no-priv } | { v1 | v2c } sec-name security-name  
} [ engine-id end-id | retries num-retries | tag tag-list | timeout time | udp-port port  
| vrf vrf-name | source { ipv4 address IPv4address | interface interface-name } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

name

Description: Specifies the target name.
Value: String - maximum 32 characters.
Default Value: None.

ip { *a.b.c.d* | *x:x:x:x::x* }

Description: Specifies the target IPv4 or IPv6 address.
Value: a.b.c.d or x:x:x:x::x.
Default Value: None.

usm

Description: Configures the target to use SNMPv3 user based parameters.
Value: **user-name** *name* **sec-level** { **auth-no-priv** | **auth-priv** | **no-auth-no-priv** }
Default Value: None.

user-name *name***Description:** Specifies the SNMPv3 user name.**Value:** String - maximum 32 characters.**Default Value:** None.**sec-level** { **auth-no-priv** | **auth-priv** | **no-auth-no-priv** }**Description:** Specifies the minimum SNMPv3 security level.**Value:** **auth-no-priv**, **auth-priv** or **no-auth-no-priv**.**Default Value:** None.{ **v1** | **v2c** }**Description:** Configures the target to use SNMPv1 or SNMPv2c parameters.**Value:** **v1** or **v2c**.**Default Value:** None.**sec-name** *security-name***Description:** Specifies the SNMP target security name.**Value:** String - maximum 32 characters.**Default Value:** None.**engine-id** *end-id***Description:** (Optional) Specifies the target remote engine ID to receive SNMPv3 informs.**Value:** pattern "[0-9a-fA-F]{2}(:[0-9a-fA-F]{2}){0,27}".**Default Value:** None.**retries** *num-retries***Description:** (Optional) Specifies the number of retries to receive SNMPv3 informs.**Value:** 0 - 255.**Default Value:** 3.**tag** *tag-list***Description:** (Optional) Specifies the target tag list. A list must be between brackets "[" and "]".**Value:** String.

Default Value: None.

timeout *time*

Description: (Optional) Specifies the timeout in hundreds of seconds to receive SNMPv3 informs.

Value: 0-4294967295.

Default Value: 1500.

udp-port *port*

Description: (Optional) Sets the UDP protocol port to be used for communication with the SNMP target entity.

Value: 0-65532.

Default Value: 162.

vrf *vrf-name*

Description: (Optional) Specifies the name of VRF which the target can be reached.

Value: String.

Default Value: None.

source ipv4 address *IPv4address*

Description: (Optional) Specifies the source IPv4 address to send SNMP notifications to target.

Value: a.b.c.d

Default Value: None.

source interface *interface-name*

Description: (Optional) Specifies the interface used to send SNMP notifications to target.

Value: Interface name in format I3-<name> or loopback-<id>

Default Value: None.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
5.0	Add vrf option.
6.0	Add source ipv4 address and source interface options.

Usage Guidelines

This command can be executed directly via CLI. Up to 32 entries can be created.

Example:

This example shows how to configure a SNMP target entry.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp target outband
(config-target-outband)# ip 192.168.10.1
(config-target-outband)# tag [ std_v2_trap std_v3_trap ]
(config-target-outband)# usm user-name public
(config-target-outband)# usm sec-level no-auth-no-priv
(config-target-outband)# vrf red
(config-target-outband)# source ipv4 address 5.5.5.5
(config-target-outband)# commit
Commit complete.
```

Impacts and precautions

The parameter **engine-id** must indicate an Engine ID identifier present in the **snmp usm remote** configuration.

Take special care when configuring a different UDP port from default (162), since it must not conflict with well-known protocols or services, such as SNTP (123) and Syslog (514).

Hardware restrictions

N/A

snmp traps

Description

This configuration allows the selection of traps that will be sent to the snmp target.

Supported Platforms

This command is supported in all platforms.

Syntax

snmp traps [config-commit | cpu-core | cpu-load | link-status | login-fail | login-success]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

config-commit

Description:	Enable the configCommit trap.
Value:	N/A
Default Value:	N/A

cpu-core

Description:	Enable the cpuCoreHighTrap trap.
Value:	N/A
Default Value:	N/A

cpu-load

Description:	Enable the cpuLoadHighTrap trap.
Value:	N/A
Default Value:	N/A

link-status

Description:	Enable the IF-MIB linkDown/linkUp traps.
---------------------	--

Value: N/A

Default Value: N/A

login-fail

Description: Enable the loginFail trap.

Value: N/A

Default Value: N/A

login-success

Description: Enable the loginSuccess trap.

Value: N/A

Default Value: N/A

Default

The following configuration are enabled: config-commit, cpu-core, cpu-load, link-status and login-success.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.6	This config was introduced.
5.12	New configuration available: config-commit, cpu-core, cpu-load, login-fail and login-success.

Usage Guidelines

The generation of traps can be enabled or disabled with this configuration.

Impacts and precautions

Netconf connections don't generate login traps.

Hardware restrictions

N/A

snmp usm

Description

Configures the SNMP user based security model.

Supported Platforms

This command is supported in all platforms.

Syntax

```
snmp usm { local | remote engine-id } user name [ auth { md5 | sha } { key hexlist | password pw } [ priv { aes | des } { key hexlist | password pw } ] | security-name sec-name ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

{ **local** | **remote** *engine-id* }

Description: Configures a local or remote user.

Value: Remote user requires an engine ID according to the pattern “[0-9a-fA-F]{2}(:[0-9a-fA-F]{2}){0,27}”.

Default Value: None.

user *name*

Description: Specifies the user name.

Value: String - maximum 32 characters.

Default Value: None.

auth { **md5** | **sha** } { **key** *hexlist* | **password** *pw* }

Description: (Optional) Enables user authentication based on **md5** or **sha** mode.

Value: **md5** or **sha**.

Default Value: None.

key *hexlist***Description:** Specifies the authentication key in hexadecimal format.**Value:** pattern “((((([0-9A-Fa-f]{2}))*([0-9A-Fa-f]{2}))) {0,1}”.**Default Value:** None.**password** *pw***Description:** Specifies the authentication password.**Value:** String (length 8-255).**Default Value:** None.**priv** { **aes** | **des** }**Description:** (Optional) Enables encryption for the authentication process.**Value:** AES or DES encryption.**Default Value:** None.**security-name** *sec-name***Description:** (Optional) Specifies the user security name in case it should be different from the user name.**Value:** String - maximum 32 characters.**Default Value:** None.**Default**

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI. Up to 32 local and remote entries can be created.

Example:

This example shows how to configure a local user based security model.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp usm local user public
(config-user-public)# auth sha password 12345678
(config-user-public)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

snmp vacm

Description

Configures the SNMP group or MIB view based access control model.

Supported Platforms

This command is supported in all platforms.

Syntax

```
snmp vacm { group grp-name { member member-name sec-model { id | usm | v1 | v2c }* }* [ access { context } { sec-model-num | any | usm | v1 | v2c } { auth-no-priv | auth-priv | no-auth-no-priv } [ { notify-view | read-view | write-view } view-name ]* ]* | view view-name subtree oid { excluded | included }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

group *grp-name*

Description: Specifies the group name.

Value: String - maximum 32 characters.

Default Value: None.

member *member-name*

Description: Configures a member list for the group.

Value: String - maximum 32 characters.

Default Value: None.

sec-model { *id* | **usm** | **v1** | **v2c** }*

Description: Configures the group security model list.

Value: 1 .. 2147483647, usm, v1 or v2c. A list must be between brackets "[" and "]".

Default Value: None.

access { *context* }

Description: Configures the SNMP context under which the access rights are applied. If no VRF is used, leave it in blank using "" (Two double quotes).

Value: SNMP agent context.

Default Value: None.

access { *sec-model-num* | **any** | **usm** | **v1** | **v2c** }

Description: (Optional) Configures the group access list under which the access rights are applied based on the security model.

Value: 1 .. 2147483647, any, usm, v1 or v2c.

Default Value: None.

{ **auth-no-priv** | **auth-priv** | **no-auth-no-priv** }

Description: Defines the access rights priviledge mode.

Value: auth-no-priv, auth-priv or no-auth-no-priv.

Default Value: None.

{ **notify-view** | **read-view** | **write-view** }* *view-name*

Description: (Optional) Defines the access rights for notification, read or write based on the MIB view name.

Value: Mode and MIB view name.

Default Value: None.

view *view-name*

Description: Configures a MIB view based access control model.

Value: String - maximum 32 characters.

Default Value: None.

subtree *oid*

Description: Configures the SNMP family subtree to be excluded or included in this MIB view.

Value: pattern '(((0-1*)|([2*].((0|([1-9]*)|[*])))' + '(.((0|([1-9]*)|[*])))*'.

Default Value: None.

{ **excluded** | **included** }

Description:	The SNMP family subtree action for this MIB view.
Value:	excluded or included.
Default Value:	None.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
5.8	The parameter context was introduced.
7.0	Add a pattern to VRF context allowing only the use of a-z, A-z, 0-9, _ and -.

Usage Guidelines

This command can be executed directly via CLI. Up to 32 groups or views can be created.

Example:

This example shows how to configure a SNMP group access control.

```
# configure terminal
Entering configuration mode terminal
```

```
(config)# snmp vacm group public
(config-group-public)# member public
(config-member-public)# sec-model [ usm v2c ]
(config-member-public)# commit
Commit complete.
```

This example shows how to configure a SNMP MIB view access control.

```
# configure terminal
Entering configuration mode terminal
(config)# snmp vacm view root
(config-view-root)# subtree 1.3
(config-subtree-1.3)# included
(config-subtree-1.3)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

LICENSE

This topic describes the commands to manage licenses.

license

Description

This command is used to disable or enable a licensed feature.

Supported Platforms

This command is supported only in the following platforms: DM4170.

Syntax

license *feature* { **disabled** | **enabled** } **key** *key*

Parameters

license *feature*

Description: Specifies the feature to be disabled or enabled.

Value: String of the licensed feature.

Default Value: None.

{ **disabled** | **enabled** }

Description: Disables or enables the specified licensed feature.

Value: disabled or enabled.

Default Value: None.

key *key*

Description: Specifies the key to disable or enable the licensed feature.

Value: String.

Default Value: None.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

3.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI. Please contact the support to consult the licensable features and how to obtain a key to disable or enable them.

Example:

This example shows how to enable the MPLS features.

```
# configure terminal
Entering configuration mode terminal
(config)# license mpls enabled key 416195f4bd3a73243352aaf4e3eb06abfd35c9ed6f99c7f336ef37d263fd59970137c
(config)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show license

Description

This command shows the list of licensed features.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

show license

Parameters

N/A

Output Terms

Output	Description
Feature	Displays the feature name.
Status	Displays the license status.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Access level audit

History

Release	Modification
2.2	This command was introduced.
4.9	The show command was modified to include the number of licenses available for a given feature.

Usage Guidelines

To show the list of licensed features available the following command can be used:

If the number of licenses is not applicable to the feature, "N/A" is displayed.

```
#show license
Feature          Status          Number of Licenses
-----
mpls              enabled         N/A
speed-100g-ports enabled         5
```

The example below shows the command output when the license is disabled:

```
#show license
Feature          Status          Number of Licenses
-----
mpls              disabled        N/A
speed-100g-ports disabled        N/A
```

Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 4: INTERFACES

This chapter describes the commands related to management of interfaces in the DmOS CLI.

ETHERNET

This topic describes the commands related to management of Ethernet interfaces such as commands to configure speed or to disable the interface.

dwdm interface

Description

Configure DWDM QSFP on hundred gigabit ethernet ports.

Supported Platforms

This command is supported only in the following platforms: DM4770.

Syntax

dwdm interface *interface-name* [**grid-50ghz** { *frequency* { 191.30 .. 196.10 } } | **grid-100ghz** { *frequency* { 191.3 .. 196.1 } } | **tx-power** { range -20.0 .. 0 }]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Configures a hundred gigabit ethernet port that supports DWDM QSFP.

Value: N/A

Default Value: N/A

grid

Description: Configure DWDM grid in GHz.

Value: 50GHz or 100GHz

Default Value: 100GHz

frequency

Description: Configures the DWDM frequency. It's dependent on the grid choice:
0.05 THz steps for 50GHz grid;
0.1 THz steps for 100GHz grid.

Value: range from 191.3 to 196.1

Default Value: 193.7

tx-power

Description: Set the DWDM transmission power in dBm with 0.1 steps.

Value: range from -20.0 to 0.0

Default Value: 0.0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release

Modification

6.4

This command was introduced.

Usage Guidelines

This command should be used to configure hundred gigabit Ethernet interfaces with DWDM QSFP support.

Examples:

These examples show the DWDM configuration for interface hundred gigabit interface 1/1/16.

To configure the grid with 50GHz and its frequency.

```
DM4770(config)# dwdm interface hundred-gigabit-ethernet-1/1/16
DM4770(dwdm-hundred-gigabit-ethernet-1/1/16)# grid-50ghz frequency 191.35
DM4770(dwdm-hundred-gigabit-ethernet-1/1/16)# commit
Commit complete.
```

To configure the grid with 100GHz and its frequency.

```
DM4770(config)# dwdm interface hundred-gigabit-ethernet-1/1/16
DM4770(dwdm-hundred-gigabit-ethernet-1/1/16)# grid-100ghz frequency 191.4
DM4770(dwdm-hundred-gigabit-ethernet-1/1/16)# commit
Commit complete.
```

To set tx-power

```
DM4770(config)# dwdm interface hundred-gigabit-ethernet-1/1/16
DM4770(dwdm-hundred-gigabit-ethernet-1/1/16)# tx-power -2.0
```

Impacts and precautions

The tx-power must be set with caution, higher configuration values could damage partner transceiver optical receiver.

The tx-power parameter allow the provision of a transmit power lower or equal to the module physical internal laser power capability. This is useful for leveling of several transceivers on a DWDM system, to normalize all channels power to the EDFA without the need of individual external optical attenuators. Since each module have its own maximum power capability and the tx-power command has a range from -20 to 0 dBm, it may occur that the physical output power may not match tx-power definition, specially on higher tx-power configuration.

Hardware restrictions

DM4770 16CX supports QSFP-DD only for hundred gigabit ethernet ports 10, 12, 14 and 16.

interface forty-gigabit-ethernet

Description

Configure forty gigabit Ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface forty-gigabit-ethernet id [ shutdown | speed { 40G } | duplex { full }  
| mdix { normal } | flow-control { rx-pause | tx-pause } | advertising-abilities {  
40Gfull* | rx-pause | tx-pause } | description { string* }* ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Configures the forty-gigabit-ethernet interface. The ID is composed by chassis/slot/port.

Value: *chassis/slot/port*
Chassis is equal to 1, slot is equal to 1 and port needs to be 1 or 2.

Default Value: N/A

shutdown

Description: Turn the interface down administratively (the interfaces startup is *no shutdown* by default).

Value: N/A

Default Value: N/A

speed

Description: Set speed (for forty-gigabit-ethernet is only available 40G).

Value: 40G.

Default Value: 40G.

duplex

Description: Set a duplex mode (for forty-gigabit-ethernet is only available full mode).

Value: full.

Default Value: full.

mdix

Description: Set MDIX mode (for forty-gigabit-ethernet is only available normal mode).

Value: normal.

Default Value: normal.

flow-control

Description: Set a flow control mode.

Value: rx-pause and tx-pause.

Default Value: rx-pause and tx-pause.

advertising-abilities

Description: Set the speed, duplex and flow control modes that will be advertised on negotiation protocol (for forty-gigabit-ethernet this option is not available).

Value: 40Gfull, rx-pause and tx-pause.

Default Value: N/A

description

Description: Set a textual description of the interface, according to the network manager's choice.
Valid characters are A-Z, a-z, 0-9 and - _ / + * @.

Value: The interface description.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command should be used to configure the forty gigabit Ethernet interfaces.

Example:

This example is applied to *id* equal to *1/1/1*. This *id* corresponds to chassis 1, slot 1 and port 1.

To set flow control

```
DM4170(config)# interface forty-gigabit-ethernet 1/1/1
DM4170(config-forty-gigabit-ethernet-1/1/1)# flow-control rx-pause tx-pause
```

To set description

```
DM4170(config)# interface gigabit-ethernet 1/1/9
DM4170(config-gigabit-ethernet-1/1/9)# description "test interface name"
```

Impacts and precautions

Changes in interfaces configuration could result in link connection loss.

The interface description is set using CLI and the maximum number of characters is 128. This description is available in SNMP through IF-MIB::ifAlias, but it is truncated in 64 characters.

Hardware restrictions

According to SFP+ inserted, these configurations could be available or not.

interface gigabit-ethernet

Description

Configure gigabit Ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface gigabit-ethernet id [ shutdown | negotiation | speed { 10M | 100M | 1G }
| duplex { full } | mdix { normal | xover | auto } | flow-control { rx-pause | tx-pause } |
advertising-abilities { 10Mfull* | 100Mfull | 1Gfull | rx-pause | tx-pause } | description
{ string* }* ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Configures the gigabit-ethernet interface. The ID is composed by chassis/slot/port.

Value: chassis/slot/port
Chassis is equal to 1, slot is equal to 1 and port needs to be in the range 1 to 12.

Default Value: N/A

shutdown

Description: Turn the interface down administratively (the interfaces startup is *no shutdown* by default).

Value: N/A

Default Value: N/A

negotiation

Description: Enable auto negotiation.

Value: N/A

Default Value: N/A

speed

Description: Set a speed to be used when negotiation is disabled.

Value: 1G, 10M or 100M.

Default Value: 1G for optical ports and 100M for electrical ports.

duplex

Description: Set a duplex mode to be used when negotiation is disabled.

Value: full.

Default Value: full.

mdix

Description: Set MDIX mode to be used when negotiation is disabled.

Value: normal, xover or auto.

Default Value: normal for ports from 1 to 8.
auto for ports from 9 to 12.

flow-control

Description: Set a flow control mode to be used when negotiation is disabled.

Value: rx-pause and tx-pause.

Default Value: N/A

advertising-abilities

Description: Set the speed, duplex and flow control modes that will be advertised on negotiation protocol.

Value: 10Mfull, 100Mfull, 1Gfull, rx-pause and tx-pause.

Default Value: 1Gfull.

description

Description: Set a textual description of the interface, according to the network manager's choice.

Valid characters are A-Z, a-z, 0-9 and - _ / + * @.

Value: The interface description.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.10	Removed the configurations “duplex half”, “advertising-abilities 10Mhalf” and “advertising-abilities 100Mhalf”.
1.12	The configuration to set the description of interfaces was added.

Usage Guidelines

This command should be used to configure the gigabit Ethernet interfaces.

Examples:

These examples are applied to *id* equal to *1/1/9*. This *id* correspond to chassis 1, slot 1 and port 9.

To shutdown port

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# shutdown
```

To enable negotiation

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# negotiation
```

To set speed equal to 1 gigabit

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# speed 1G
```

To set duplex

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# duplex full
```

To set advertising abilities

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# advertising-abilities 1Gfull rx-pause
```

To set description

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# description "test interface name"
```

Or

```
DM4610(config) interface gigabit-ethernet 1/1/9 DM4610(config-gigabit-ethernet-1/1/9) de-
scription testinterface_name
```

Impacts and precautions

Changes in interfaces configuration could result in link connection loss.

The interface description is set using CLI and the maximum number of characters is 128. This description is available in SNMP through IF-MIB::ifAlias, but it is truncated in 64 characters.

Hardware restrictions

According to SFP inserted, these configurations could be available or not.

interface hundred-gigabit-ethernet

Description

Configure hundred gigabit Ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface hundred-gigabit-ethernet id [ shutdown | negotiation | speed { 40G | 100G } | duplex { full } | mdix { normal } | flow-control { rx-pause | tx-pause } | mtu { range } | description { string } | fec { off | cl91 } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Configures the hundred-gigabit-ethernet interface. The ID is composed by chassis/slot/port.

Value: *chassis/slot/port*
Chassis is equal to 1, slot is equal to 1 and port needs to be 1 or 2.

Default Value: N/A

shutdown

Description: Turn the interface down administratively (the interfaces startup is *no shutdown* by default).

Value: N/A

Default Value: N/A

negotiation

Description: Enable autonegotiation.

Value: N/A

Default Value: N/A

speed

Description: Set interface speed to 100G or to 40G.

Value: 40G, 100G.

Default Value: 100G.

duplex

Description: Set a duplex mode (for hundred-gigabit-ethernet it is only available full mode).

Value: full.

Default Value: full.

mdix

Description: Set MDIX mode (for hundred-gigabit-ethernet it is only available normal mode).

Value: normal.

Default Value: normal.

flow-control

Description: Set a flow control mode.

Value: rx-pause and tx-pause.

Default Value: rx-pause and tx-pause.

mtu

Description: Set MTU (Maximum Transmission Unit) in bytes. Packets that surpass the limit are dropped.

Value: From 64 bytes to the maximum supported on the product.

Default Value: The maximum supported on the product.

description

Description: Set a textual description of the interface, according to the network manager's choice.
Valid characters are A-Z, a-z, 0-9 and - _ / + * @.

Value: The interface description.

Default Value: N/A

fec

Description: Enable/disable Forward Error Correction.

Value: off, cl91.

Default Value: off.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

This command should be used to configure the hundred gigabit Ethernet interfaces.

Example:

This example is applied to *id* equal to *1/1/1*. This *id* correspond to chassis 1, slot 1 and port 1.

To set flow control

```
DM4270(config)# interface hundred-gigabit-ethernet 1/1/1
DM4270(config-hundred-gigabit-ethernet-1/1/1)# flow-control rx-pause tx-pause
```

To set description

```
DM4270(config)# interface hundred-gigabit-ethernet 1/1/1
DM4270(config-hundred-gigabit-ethernet-1/1/1)# description "test interface name"
```

To set mtu

```
DM4270(config)# interface hundred-gigabit-ethernet 1/1/1
DM4270(config-hundred-gigabit-ethernet-1/1/1)# mtu 1500
```

To set fec

```
DM4270(config)# interface hundred-gigabit-ethernet 1/1/1
DM4270(config-hundred-gigabit-ethernet-1/1/1)# fec cl91
```

Impacts and precautions

Changes in interfaces configuration could result in link connection loss.

The interface description is set using CLI and the maximum number of characters is 128. This description is available in SNMP through IF-MIB::ifAlias, but it is truncated in 64 characters.

The MTU configuration considers an Ethernet frame with the maximum headers size of 26 bytes, which is the case for frames tagged with VLAN (4 bytes) and QinQ (4 bytes). Therefore, untagged frames with a payload that exceeds the MTU configuration by at most 8 bytes will not be dropped.

Hardware restrictions

According to SFP+ inserted, these configurations could be available or not.

interface ten-gigabit-ethernet

Description

Configure ten gigabit Ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface ten-gigabit-ethernet id [ shutdown | speed { 10G } | duplex { full }  
| mdix { normal } | flow-control { rx-pause | tx-pause } | advertising-abilities {  
10Gfull* | rx-pause | tx-pause } | description { string* }* ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Configures the ten-gigabit-ethernet interface. The ID is composed by chassis/slot/port.

Value: *chassis/slot/port*
Chassis is equal to 1, slot is equal to 1 and port needs to be 1 or 2.

Default Value: N/A

shutdown

Description: Turn the interface down administratively (the interfaces startup is *no shutdown* by default).

Value: N/A

Default Value: N/A

speed

Description: Set speed (for ten-gigabit-ethernet is only available 10G).

Value: 10G.

Default Value: 10G.

duplex

Description: Set a duplex mode (for ten-gigabit-ethernet is only available full mode).

Value: full.

Default Value: full.

mdix

Description: Set MDIX mode (for ten-gigabit-ethernet is only available normal mode).

Value: normal.

Default Value: normal.

flow-control

Description: Set a flow control mode.

Value: rx-pause and tx-pause.

Default Value: rx-pause and tx-pause.

advertising-abilities

Description: Set the speed, duplex and flow control modes that will be advertised on negotiation protocol (for ten-gigabit-ethernet this option is not available).

Value: 10Gfull, rx-pause and tx-pause.

Default Value: N/A

description

Description: Set a textual description of the interface, according to the network manager's choice.
Valid characters are A-Z, a-z, 0-9 and - _ / + * @.

Value: The interface description.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.12	The configuration to set the description of interfaces was added.

Usage Guidelines

This command should be used to configure the ten gigabit Ethernet interfaces.

Example:

This example is applied to *id* equal to *1/1/1*. This *id* corresponds to chassis 1, slot 1 and port 1.

To set flow control

```
DM4610(config)# interface ten-gigabit-ethernet 1/1/1
DM4610(config-ten-gigabit-ethernet-1/1/1)# flow-control rx-pause tx-pause
```

To set description

```
DM4610(config)# interface gigabit-ethernet 1/1/9
DM4610(config-gigabit-ethernet-1/1/9)# description "test interface name"
```

Or

DM4610(config) interface gigabit-ethernet 1/1/9 DM4610(config-gigabit-ethernet-1/1/9) description test_i*interface*_n*ame*

Impacts and precautions

Changes in interfaces configuration could result in link connection loss.

The interface description is set using CLI and the maximum number of characters is 128. This description is available in SNMP through IF-MIB::ifAlias, but it is truncated in 64 characters.

Hardware restrictions

According to SFP+ inserted, these configurations could be available or not.

interface twenty-five-g-ethernet

Description

Configure twenty-five gigabit Ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface twenty-five-g-ethernet id [ shutdown | speed { 1G | 10G | 25G } | duplex { full } | mdix { normal } | flow-control { rx-pause | tx-pause } | mtu { range } | description { string } | fec { off | cl74 | cl108 } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Configures the twenty-five-g-ethernet interface. The ID is composed by chassis/slot/port.

Value: *chassis/slot/port*
Chassis is equal to 1, slot is equal to 1 and port needs to be 1 or 2.

Default Value: N/A

shutdown

Description: Turn the interface down administratively (the interfaces startup is *no shutdown* by default).

Value: N/A

Default Value: N/A

speed

Description: Set interface speed to 25G, 10G or to 1G.

Value: 1G, 10G, 25G.

Default Value: 25G.

duplex

Description: Set a duplex mode (for twenty-five-g-ethernet it is only available full mode).

Value: full.

Default Value: full.

mdix

Description: Set MDIX mode (for twenty-five-g-ethernet it is only available normal mode).

Value: normal.

Default Value: normal.

flow-control

Description: Set a flow control mode.

Value: rx-pause and tx-pause.

Default Value: rx-pause and tx-pause.

mtu

Description: Set MTU (Maximum Transmission Unit) in bytes. Packets that surpass the limit are dropped.

Value: From 64 bytes to the maximum supported on the product.

Default Value: The maximum supported on the product.

description

Description: Set a textual description of the interface, according to the network manager's choice.
Valid characters are A-Z, a-z, 0-9 and - _ / + * @.

Value: The interface description.

Default Value: N/A

fec

Description: Enable/disable Forward Error Correction.

Value: off, cl74, cl108.

Default Value: off.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.
6.0	The configuration to set FEC CL74 and CL108 was added.

Usage Guidelines

This command should be used to configure the twenty-five gigabit Ethernet interfaces.

Example:

This example is applied to *id* equal to *1/1/1*. This *id* correspond to chassis 1, slot 1 and port 1.

To set flow control

```
DM4770(config)# interface twenty-five-g-ethernet 1/1/1
DM4770(config-twenty-five-g-ethernet-1/1/1)# flow-control rx-pause tx-pause
```

To set description

```
DM4770(config)# interface twenty-five-g-ethernet 1/1/1
DM4770(config-twenty-five-g-ethernet-1/1/1)# description "test interface name"
```

To set mtu

```
DM4770(config)# interface twenty-five-g-ethernet 1/1/1
DM4770(config-twenty-five-g-ethernet-1/1/1)# mtu 1500
```

To set fec

```
DM4770(config)# interface twenty-five-g-ethernet 1/1/1
DM4770(config-twenty-five-g-ethernet-1/1/1)# fec c174
```

Impacts and precautions

Changes in interfaces configuration could result in link connection loss.

The interface description is set using CLI and the maximum number of characters is 128. This description is available in SNMP through IF-MIB::ifAlias, but it is truncated in 64 characters.

The MTU configuration considers an Ethernet frame with the maximum headers size of 26 bytes, which is the case for frames tagged with VLAN (4 bytes) and QinQ (4 bytes). Therefore, untagged frames with a payload that exceeds the MTU configuration by at most 8 bytes will not be dropped.

Hardware restrictions

According to SFP+ inserted, these configurations could be available or not.

show dwdm channels

Description

Shows DWDM QSFP tabular information about channels, frequency and wavelength.

Supported Platforms

This command is supported only in the following platforms: DM4770.

Syntax

show dwdm channels

Parameters

show dwdm channels

Description:	Show information about the channels, wavelengths and frequencies.
Value:	None
Default Value:	None

Output Terms

Output	Description
CHANNEL (ID)	Identification of the channel
FREQUENCY (THz)	Value of the channel frequency measured in THz
WAVELENGTH (nm)	Value of the channel wavelength measured in nm

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

7.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Examples:

Show the DWDM table channels

```
DM4770# show dwdm channels
CHANNEL  FREQUENCY  WAVELENGTH
 (ID)      (THz)      (nm)
-----
 13       191.3       1567.13
 14       191.4       1567.19
 ...
```

Impacts and precautions

N/A

Hardware restrictions

DM4770 16CX supports QSFP-DD only for hundred gigabit ethernet ports 10, 12, 14 and 16. DM4770 32CX does not support this command.

show interface description

Description

Description of interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface description interface-type

Parameters

interface-type

Description: Interface type to filter.

Value: { **gigabit-ethernet** | **ten-gigabit-ethernet** | **twenty-five-g-ethernet** | **forty-gigabit-ethernet** | **hundred-gigabit-ethernet** }

Default Value: None

Output Terms

Output	Description
CHASSIS ID/SLOT ID/ PORT ID	Interface id referencing chassis/slot/port respectively.
Description	The textual description of the interface, according to the network manager's choice.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

Use this command to display an overview of all interfaces;

Example:

```
# show interface description
Gigabit Ethernet Interfaces:
CHASSIS
ID/SLOT
ID/PORT
ID      Description
-----
1/1/1   My_pretty_name_for_this_interface
1/1/2   LINK_X
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  -
1/1/13  -
1/1/14  -
1/1/15  -
1/1/16  -
1/1/17  -
1/1/18  -
1/1/19  -
1/1/20  -
1/1/21  -
1/1/22  -
1/1/23  -
1/1/24  -

Ten Gigabit Ethernet Interfaces:
ID/SLOT
```

```
ID/PORT
ID      Description
-----
1/1/1   A_short_description
1/1/2   -
1/1/3   -
1/1/4   -

Forty Gigabit Ethernet Interfaces:
ID/SLOT
ID/PORT
ID      Description
-----
1/1/1   UPLINK
1/1/2   -
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface forty-gigabit-ethernet

Description

Display status and configuration of forty-gigabit-ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface forty-gigabit-ethernet *id*

Parameters

id

Description: Interface id referencing chassis/slot/port respectively.

Value: chassis/slot/port

Default Value: N/A

Output Terms

Output	Description
Port admin	The configured administrative state.
Negotiation	The configured autonegotiation mode.
Speed	The configured speed mode.
Duplex	The configured duplex mode.
Flow-Control	The configured flow control mode.

Output	Description
MDIX	The configuration and status of MDIX mode.
MTU	The configured MTU (Maximum Transmission Unit) in bytes.
Description	The configured textual description of the interface.
Link status	The current interface link state (Up/Down).
Speed/Duplex	The current speed/duplex state.
Flow Control	The current flow control state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

Use this command to display status and configuration of forty-gigabit-ethernet interfaces.

Example:

```
DM4270# show interface forty-gigabit-ethernet 1/1/1
interface forty-gigabit-ethernet 1/1/1
Configuration:
-----
Port admin           : Enabled
Negotiation          : Disabled
Speed                : 40G
Duplex                : full
Flow-Control         : Disabled
MDIX                  : normal
MTU                   : 12262

Status:
-----
Link Status          : Up
Speed/Duplex         : 40Gfull
Flow Control         : Disabled
MDIX                  : Normal
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface gigabit-ethernet

Description

Display status and configuration of gigabit-ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface gigabit-ethernet *id*

Parameters

id

Description: Interface id referencing chassis/slot/port respectively.

Value: chassis/slot/port

Default Value: N/A

Output Terms

Output	Description
Port admin	The configured administrative state.
Negotiation	The configured autonegotiation mode.
Advertising Abilities	The configured advertising abilities.
MDIX	The configuration and status of MDIX mode.
MTU	The configured MTU (Maximum Transmission Unit) in bytes.

Output	Description
Description	The configured textual description of the interface.
Link status	The current interface link state (Up/Down).
Speed/Duplex	The current speed/duplex state.
Flow Control	The current flow control state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to display status and configuration of gigabit-ethernet interfaces.

Example:

```
DM4050# show interface gigabit-ethernet 1/1/24
interface gigabit-ethernet 1/1/24
  Configuration:
  -----
```

```
Port admin          : Enabled
Negotiation         : Enabled
Advertising Abilities : [ 10Mfull 100Mfull 1Gfull ]
MDIX                : auto
MTU                 : 16338

Status:
-----
Link Status         : Up
Speed/Duplex        : 1Gfull
Flow Control        : Disabled
MDIX                : Xover
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface hundred-gigabit-ethernet

Description

Display status and configuration of hundred-gigabit-ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface hundred-gigabit-ethernet *id*

Parameters

id

Description: Interface id referencing chassis/slot/port respectively.

Value: chassis/slot/port

Default Value: N/A

Output Terms

Output	Description
Port admin	The configured administrative state.
Negotiation	The configured autonegotiation mode.
Speed	The configured speed mode.
Duplex	The configured duplex mode.
Flow-Control	The configured flow control mode.

Output	Description
MDIX	The configuration and status of MDIX mode.
FEC	The configured FEC (Forward Error Correction) mode.
MTU	The configured MTU (Maximum Transmission Unit) in bytes.
Description	The configured textual description of the interface.
Link status	The current interface link state (Up/Down).
Speed/Duplex	The current speed/duplex state.
Flow Control	The current flow control state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.6	This command was introduced.

Usage Guidelines

Use this command to display status and configuration of hundred-gigabit-ethernet interfaces.

Example:

```
DM4270# show interface hundred-gigabit-ethernet 1/1/1
interface hundred-gigabit-ethernet 1/1/1
Configuration:
-----
Port admin           : Enabled
Negotiation          : Disabled
Speed                : 100G
Duplex               : full
Flow-Control         : Disabled
MDIX                 : normal
FEC                  : off
MTU                  : 12262

Status:
-----
Link Status          : Up
Speed/Duplex         : 100Gfull
Flow Control         : Disabled
MDIX                 : Normal
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface link

Description

Overview of interfaces status.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface link interface-type

Parameters

interface-type

Description: Interface type to filter.

Value: { **gigabit-ethernet** | **ten-gigabit-ethernet** | **twenty-five-g-ethernet** | **forty-gigabit-ethernet** | **hundred-gigabit-ethernet** }

Default Value: None

Output Terms

Output	Description
CHASSIS ID/SLOT ID/ PORT ID	Interface id referencing chassis/slot/port respectively.
Link	The current interface link state (Up/Down).
Shutdown	The configured administrative state.
Speed	The current speed state.

Output	Description
Duplex	The current duplex state.
Disabled by	Protocol name that is disabling the port.
Blocked by	Names of protocols blocking the port.
Parent LAG	LAG ID, if the port belongs to any LAG.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.7	This command was introduced.
4.8	Added Speed/Duplex information. Interface type was added as parameters, in order to filters the output. Removed <i>Disabled</i> column.
5.0	Added support to 25G.

Release	Modification
---------	--------------

5.2	Added information of which protocols blocked interfaces.
-----	--

Usage Guidelines

Use this command to display an overview of all interfaces;

Example:

```
# show interface link
Gigabit Ethernet Interfaces:
CHASSIS
ID/SLOT
ID/PORT
ID      Link  Shutdown Speed Duplex Disabled Blocked Parent
by      by      LAG
-----
1/1/1   Down  false   -      -      [ LAG ] -      lag-1
1/1/2   Down  false   -      -      -      -      -
1/1/3   Down  false   -      -      -      -      -
1/1/4   Down  false   -      -      -      -      -
1/1/5   Down  false   -      -      -      -      -
1/1/6   Down  false   -      -      -      -      -
1/1/7   Down  false   -      -      -      -      -
1/1/8   Down  false   -      -      -      -      -
1/1/9   Down  false   -      -      -      -      -
1/1/10  Down  false   -      -      -      -      -
1/1/11  Down  false   -      -      -      -      -
1/1/12  Down  false   -      -      -      -      -
1/1/13  Down  false   -      -      -      -      -
1/1/14  Down  false   -      -      [ LAG ] -      lag-1
1/1/15  Down  false   -      -      [ LAG ] -      lag-1
1/1/16  Up     false   1G     full   -      [ LBD ] -
1/1/17  Down  false   -      -      -      -      -
1/1/18  Up     false   1G     full   -      -      -
1/1/19  Down  false   -      -      -      -      -
1/1/20  Up     false   1G     full   -      [ CFM ] -
1/1/21  Down  false   -      -      -      -      -
1/1/22  Down  false   -      -      -      -      -
1/1/23  Down  false   -      -      -      -      -
1/1/24  Down  false   -      -      -      -      -

Ten Gigabit Ethernet Interfaces:
CHASSIS
ID/SLOT
ID/PORT
ID      Link  Shutdown Speed Duplex Disabled Blocked Parent
by      by      LAG
-----
1/1/1   Down  false   -      -      [ LAG ] -      lag-2
1/1/2   Down  false   -      -      -      -      -
1/1/3   Down  false   -      -      -      -      -
1/1/4   Down  false   -      -      [ LAG ] -      lag-2

Forty Gigabit Ethernet Interfaces:
CHASSIS
ID/SLOT
ID/PORT
ID      Link  Shutdown Speed Duplex Disabled Blocked Parent
by      by      LAG
-----
1/1/1   Up     false   40G    full   -      [ EFM, CFM ] -
1/1/2   Up     false   40G    full   -      -      -
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface ten-gigabit-ethernet

Description

Display status and configuration of ten-gigabit-ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface ten-gigabit-ethernet *id*

Parameters

id

Description: Interface id referencing chassis/slot/port respectively.

Value: chassis/slot/port

Default Value: N/A

Output Terms

Output	Description
Port admin	The configured administrative state.
Negotiation	The configured autonegotiation mode.
Speed	The configured speed mode.
Duplex	The configured duplex mode.
Flow-Control	The configured flow control mode.

Output	Description
MDIX	The configuration and status of MDIX mode.
MTU	The configured MTU (Maximum Transmission Unit) in bytes.
Description	The configured textual description of the interface.
Link status	The current interface link state (Up/Down).
Speed/Duplex	The current speed/duplex state.
Flow Control	The current flow control state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to display status and configuration of ten-gigabit-ethernet interfaces.

Example:

```
DM4270# show interface ten-gigabit-ethernet 1/1/2
interface ten-gigabit-ethernet 1/1/2
Configuration:
-----
Port admin           : Enabled
Negotiation          : Disabled
Speed                : 10G
Duplex               : full
Flow-Control         : Disabled
MDIX                 : normal
MTU                  : 12262

Status:
-----
Link Status          : Up
Speed/Duplex         : 10Gfull
Flow Control         : Disabled
MDIX                 : Normal
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface twenty-five-g-ethernet

Description

Display status and configuration of twenty-five-g-ethernet interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show interface twenty-five-g-ethernet *id*

Parameters

id

Description: Interface id referencing chassis/slot/port respectively.

Value: chassis/slot/port

Default Value: N/A

Output Terms

Output	Description
Port admin	The configured administrative state.
Negotiation	The configured autonegotiation mode.
Speed	The configured speed mode.
Duplex	The configured duplex mode.
Flow-Control	The configured flow control mode.

Output	Description
MDIX	The configuration and status of MDIX mode.
FEC	The configured FEC (Forward Error Correction) mode.
MTU	The configured MTU (Maximum Transmission Unit) in bytes.
Description	The configured textual description of the interface.
Link status	The current interface link state (Up/Down).
Speed/Duplex	The current speed/duplex state.
Flow Control	The current flow control state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.0	This command was introduced.

Release	Modification
---------	--------------

6.0	Added support to FEC CL74 and CL108.
-----	--------------------------------------

Usage Guidelines

Use this command to display status and configuration of twenty-five-g-ethernet interfaces.

Example:

```
DM4665# show interface twenty-five-g-ethernet 1/1/1
interface twenty-five-g-ethernet 1/1/1
Configuration:
-----
Port admin           : Enabled
Negotiation          : Disabled
Speed                : 25G
Duplex               : full
Flow-Control         : Disabled
MDIX                 : normal
FEC                  : off
MTU                  : 12262

Status:
-----
Link Status          : Up
Speed/Duplex         : 25Gfull
Flow Control         : Disabled
MDIX                 : Normal
```

Impacts and precautions

N/A

Hardware restrictions

N/A

L3

This topic describes the commands related to management of L3 logical interfaces such as commands to configure IP address and bind it to lower layer interface, e.g., VLAN.

interface l3

Description

Configures L3 logical interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

```
interface l3 if-name [ description if-description | ipv4 address { a.b.c.d/x | secondary a.b.c.d/x } | ipv6 { enable | address x:x:x:x::x/y [ eui-64 ] | ip-mtu mtu-size | nd ra { lifetime | max-interval | min-interval | mtu suppress | prefix x:x:x:x::x/y [ no-advertise | no-autoconfig | off-link ] | suppress } } | lower-layer-if if-type if-id | vlan-link-detect { enabled | disabled } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

if-name

Description: Specifies the name of the interface.

Value: Must be a valid string.

Default Value: N/A

description *if-description*

Description: Specifies the description of the interface. It may point out a more meaningful text about its purpose.

Value: Must be a valid string.

Default Value: N/A

ipv4 address *a.b.c.d/x*

Description: Specifies an IPv4 address and prefix length, in CIDR notation, to be assigned to logical interface.

Value: a.b.c.d/x.

Default Value: N/A

ipv4 address secondary *a.b.c.d/x*

Description: Specifies a secondary IPv4 address and prefix length, in CIDR notation, to be assigned to logical interface.

Value: a.b.c.d/x.

Default Value: N/A

ipv6 enable

Description: Enables/Disables IPv6 on the L3 interface. When enabled, the system automatically configures an IPv6 link-local address to the L3 interface.

Value: N/A

Default Value: Disabled.

ipv6 address *x:x:x:x::x/y*

Description: Specifies an IPv6 unicast address and prefix length to be assigned to logical interface.

Value: x:x:x:x::x/y.

Default Value: N/A

eui-64

Description: Sets 64-bit Extended Unique Identifier for specific IPv6 prefix on logical interface.

Value: N/A

Default Value: Disabled.

ip-mtu *mtu-size*

Description: Specifies the Control Plane IP MTU size of the interface.

Value: 68-9198.

Default Value: 1500

lower-layer-if *if-type*

Description: Specifies the lower layer interface type to be associated to logical interface.

Value: { vlan }

Default Value: N/A

if-id

Description: Specifies the identifier associated to **lower-layer-if** *if-type* selected.

Value: ID of a configured VLAN.

Default Value: N/A

vlan-link-detect enabled

Description: Enables VLAN link detection on the L3 interface.

Value: N/A

Default Value: N/A

vlan-link-detect disabled

Description: Disables VLAN link detection on the L3 interface.

Value: N/A

Default Value: N/A

ipv6 nd ra suppress

Description: Suppresses Router Advertisements on the L3 interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x:x:x:x::x/y*

Description: Prefix Address to be advertised on the specified L3 interface.

Value: *x:x:x:x::x/y*.

Default Value: N/A

ipv6 nd ra prefix *x:x:x:x::x/y* **no-advertise**

Description: Disables this prefix on Router Advertisement of this L3 interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x::x:x::x/y* no-autoconfig

Description: Disables auto configuration of hosts by this L3 interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra prefix *x::x:x::x/y* off-link

Description: When disabled, indicates that this prefix can be used for on-link determination on L3 interface.

Value: N/A

Default Value: Disabled.

ipv6 nd ra lifetime *lifetime*

Description: Sets Router Advertisement lifetime of this L3 interface.

Value: Must be either zero or between max-interval and 9000 seconds.

Default Value: 1800

ipv6 nd ra max-interval *max-interval*

Description: The maximum time allowed between sending unsolicited multi-cast router advertisements from the interface, in seconds.

Value: Must be no less than 4 seconds and no greater than 1800 seconds.

Default Value: 600

ipv6 nd ra min-interval *min-interval*

Description: The minimum time allowed between sending unsolicited multi-cast router advertisements from the interface, in seconds.

Value: Must be no less than 3 seconds and no greater than $0.75 * \text{MaxRtrAdvInterval}$.

Default Value: 198

ipv6 nd ra mtu suppress

Description: Suppresses Router Advertisement's MTU option.

Value: N/A

Default Value: Enabled.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.
2.2	VLAN link detect support.
2.4	IPv6 support.
4.5.0	Support for secondary IPv4 address.
4.8.0	Support for IPv6 ND Router Advertisement.
4.9.0	Support for MTU configuration. Support for IPv6 ND RA MTU option suppression.
6.2	Maximum IP MTU value was increased to 9198.

Usage Guidelines

The name of L3 logical interface must be unique across interfaces and it will be used as key to be referenced from other features.

It is possible the use of one primary IPv4 address, up to three secondary IPv4 addresses and two IPv6 addresses per L3 logical interface. The products DM4360, DM4370, DM4611 and DM4612 support only one secondary IPv4 address.

Command to configure IPv6 addresses will be available only if `ipv6 enable` is set for interface. Example below shows that IPv6 address configuration option appears after `ipv6 enable` is set.

```
(config-l3-test)# ipv6 ?
Possible completions:
enable    Enable IPv6 on interface
!
(config-l3-test)# ipv6 enable
!
(config-l3-test)# ipv6 ?
Possible completions:
address   IPv6 address
enable    Enable IPv6 on interface
!
```

Currently it is only possible to associate the logical interface with lower layer of type VLAN.

To find which L3 logical interface is configured with a specific IPv4 address or a specific VLAN ID, it is possible to use the commands showed in the example below.

Example:

This example shows how to find an L3 logical interface using an IPv4 address as parameter:

```
# show running-config interface l3 | include -b 2 192.168.1.1
5-interface l3 example2
6- lower-layer-if vlan 200
7: ipv4 address 192.168.1.1/24
```

Or in configuration mode:

```
(config)# show interface l3 | include -b 2 192.168.1.1
5-interface l3 example2
6- lower-layer-if vlan 200
7: ipv4 address 192.168.1.1/24
```

This example shows how to find an L3 logical interface using a VLAN ID as parameter:

```
# show running-config interface l3 | include -b 1 -a 1 "vlan 300"
9-interface l3 example3
10: lower-layer-if vlan 300
11- ipv4 address 192.168.2.1/24
```

Or in configuration mode:

```
(config)# show interface l3 | include -b 1 -a 1 "vlan 300"  
9-interface l3 example3  
10: lower-layer-if vlan 300  
11- ipv4 address 192.168.2.1/24
```

Impacts and precautions

The ip-mtu is restricted to control plane. Therefore, it does not have any effect on the data plane.

Hardware restrictions

N/A

interface l3 vrf

Description

Configures VRF on L3 logical interfaces.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615.

Syntax

interface l3 *if-name* **vrf** *vrf-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

if-name

Description:	Specifies the name of the interface.
Value:	Must be a valid string.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this interface will be associated with. It is not possible to associate the VRF 'mgmt' to an L3 interface. Also, the VRF 'global' cannot be directly configured as it is the default VRF when no VRF is associated.
Value:	string.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
5.12	Introduced VRF support on L3 interfaces with IPv6.

Usage Guidelines

If no VRF is explicitly associated with the L3 interface, it is associated with the global VRF by default. The following example shows how to associate an L3 interface with the 'test_vrf' VRF:

```
(config-l3-vlan100)# ?
Possible completions:
vrf          Assign a VRF instance to the interface
!
(config-l3-vlan100)# vrf ?
Possible completions:
<WORD>       VPN Routing/Forwarding instance name
test_vrf
!
(config-l3-vlan100)# vrf test_vrf
(config-l3-vlan100)# commit
Commit complete.
```

Impacts and precautions

Once the VRF associated with an L3 interface is changed, any route in the previous VRF using it as output interface will be uninstalled. In order to keep the connectivity, you will need to configure the routes in the new VRF.

Hardware restrictions

N/A

show ip interface

Description

Shows the list of interfaces configured with IPv4 addresses and associated information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip interface [vrf {<vrf-name> | all}] { brief }
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information

Default Value: N/A

brief

Description: Displays brief information about IPv4 addresses associated with each interface and its status.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
VRF name	Displays the VRF name.
Interface name	Displays the interface name.

Output	Description
Logical interface	Displays the logical interface.
Address	Displays the IPv4 addresses.
Type	Type of IPv4 address. Type Codes: P - primary, S - secondary, V - VRRP virtual address.
State	Displays the state of IPv4 addresses.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.4	This command was introduced.
4.5.0	Added Type column.

Usage Guidelines

To simply show the global IPv4 interfaces, the following command can be used:

Example:

```
# show ip interface brief
```

Type Codes: P - primary, S - secondary, V - VRRP virtual address

VRF-name	Interface-name	Logical-interface	Address	Type	State
global	mgmt 1/1/1	mgmt-1/1/1	192.168.0.1/24	P	active
global	loopback 0	loopback 0	192.168.1.1/24	P	active
global	intf_l3_1	13-vlan 10	192.168.10.10/24	P	active
global	intf_l3_1	13-vlan 10	192.168.10.11/24	S	active
global	intf_l3_5	13-vlan 50	192.168.50.50/24	PV	active
global	intf_l3_6	13-vlan 60	192.168.60.60/24	P	active
global	intf_l3_6	13-vlan 60	192.168.60.61/24	V	active

To show interfaces configured with IPv4 addresses in all VRFs, the following command can be used:

Example:

```
# show ip interface vrf all brief
```

Type Codes: P - primary, S - secondary, V - VRRP virtual address

VRF-name	Interface-name	Logical-interface	Address	Type	State
global	mgmt 1/1/1	mgmt-1/1/1	192.168.0.1/24	P	active
global	loopback 0	loopback 0	192.168.1.1/24	P	active
global	intf_l3_1	13-vlan 10	192.168.10.10/24	P	active
global	intf_l3_5	13-vlan 50	192.168.50.50/24	PV	active
global	intf_l3_6	13-vlan 60	192.168.60.60/24	P	active
global	intf_l3_6	13-vlan 60	192.168.60.61/24	V	active
GREEN	intf_l3_2	13-vlan 20	192.168.20.20/24	P	active
GREEN	intf_l3_3	13-vlan 30	192.168.30.30/24	P	active
RED	intf_l3_4	13-vlan 40	192.168.40.40/24	P	active

To show interfaces configured with IPv4 addresses in a specific VRF, the following command can be used:

Example:

```
# show ip interface vrf GREEN brief
```

Type Codes: P - primary, S - secondary, V - VRRP virtual address

VRF-name	Interface-name	Logical-interface	Address	Type	State
GREEN	intf_l3_2	13-vlan 20	192.168.20.20/24	P	active
GREEN	intf_l3_3	13-vlan 30	192.168.30.30/24	P	active

Impacts and precautions

N/A

Hardware restrictions

N/A

show ipv6 interface

Description

Shows the list of interfaces configured with IPv6 addresses and associated information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ipv6 interface [vrf {<vrf-name> | all}] { brief }
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information

Default Value: N/A

brief

Description: Displays brief information about IPv6 addresses associated with each interface and its status.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
VRF name	Displays the VRF name.
Interface name	Displays the interface name.

Output	Description
<code>Logical interface</code>	Displays the logical interface.
<code>Address</code>	Displays the IPv6 addresses.
<code>Scope</code>	Displays the scope of IPv6 addresses.
<code>State</code>	Displays the state of IPv6 addresses.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.
2.4	IPv6 support.
5.12	Introduced VRF support.

Usage Guidelines

To simply show the IPv6 interface brief, the following command can be used:

Example:

```
# show ipv6 interface brief
VRF-name  Interface-name  Logical-interface  Address                               Scope      State
-----
global    intf_l3_1             13-vlan 300       fe80::204:dfff:feb3:f42a/64         link-local active
global    intf_l3_1             13-vlan 300       fd01::1/16                          global     active
```

To show interfaces configured with IPv6 addresses in all VRFs, the following command can be used:

Example:

```
# show ipv6 interface vrf all brief
VRF-name  Interface-name  Logical-interface  Address                               Scope      State
-----
global    intf_l3_1             13-vlan 300       fe80::204:dfff:feb3:f42a/64         link-local active
global    intf_l3_1             13-vlan 300       fd01::1/16                          global     active
green     intf_l3_2             13-vlan 400       fe80::204:dfff:feb3:f42a/64         link-local active
green     intf_l3_2             13-vlan 400       fd02::1/16                          global     active
```

To show interfaces configured with IPv6 addresses in a specific VRF, the following command can be used:

Example:

```
# show ipv6 interface vrf green brief
VRF-name  Interface-name  Logical-interface  Address                               Scope      State
-----
green     intf_l3_2             13-vlan 400       fe80::204:dfff:feb3:f42a/64         link-local active
green     intf_l3_2             13-vlan 400       fd02::1/16                          global     active
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show router vrrp

Description

Shows the list of routers VRRP protecting L3 interfaces address(es).

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show router vrrp { brief }
```

Parameters

brief

Description: Displays brief operational information about router VRRP.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Interface name	Display the L3 interface name with addresses protected by the router VRRP.
Afi	Display the address family of the router VRRP.
VR-ID	Display virtual router ID of the router VRRP.
Priority	Display the priority of the router VRRP.
State	Display state of the router VRRP.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

To simply show router VRRP operational information brief, the following command can be used:

Example:

```
# show router vrrp brief
Interface-name  Afi    VR-ID  Priority  State
-----
test_backup    ipv6   100    100      backup
test_init      ipv4   1       50       initialize
test_master    ipv6   200    255      master
```

Impacts and precautions

N/A

Hardware restrictions

N/A

LOOPBACK

This topic describes the commands related to management of Loopback logical interfaces such as commands to configure IP address.

interface loopback

Description

Configures Loopback logical interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

interface loopback *id* [**description** *if-description* | **ipv4 address** *a.b.c.d/x* | **ipv6** { **enable** | **address** *x:x:x:x::x/y* [**eui-64**] }]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Specifies the ID of the interface.

Value: 0-7.

Default Value: N/A

description *if-description*

Description: Specifies the description of the interface. It may point out a more meaningful text about its purpose.

Value: Must be a valid string.

Default Value: N/A

ipv4 address *a.b.c.d/x*

Description: Specifies an IPv4 address and prefix length, in CIDR notation, to be assigned to logical interface.

Value: a.b.c.d/x.

Default Value: N/A

ipv6 enable

Description: Enables/Disables IPv6 on interface loopback. When enabled, the system allows configuration of IPv6 unicast addresses.

Value: N/A

Default Value: Disabled.

ipv6 address x:x:x:x::x/y

Description: Specifies an IPv6 unicast address and prefix length to be assigned to interface loopback.

Value: x:x:x:x::x/y.

Default Value: N/A

eui-64

Description: Sets 64-bit Extended Unique Identifier for specific IPv6 prefix on interface loopback.

Value: N/A

Default Value: Disabled.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.8	This command was introduced.
2.4	IPv6 support.

Usage Guidelines

The identifier of Loopback logical interface must be within the valid range of 0 and 7. It is possible the use of only one IPv4 per Loopback logical interface and two IPv6 addresses

To find which Loopback logical interface is configured with a specific IPv4 address, it is possible to use the commands showed in the example below.

Example:

This example shows how to find a Loopback logical interface using address as parameter:

```
# show running-config interface loopback all | include -b 2 200.200.200.1
3-interface loopback 3
4: ipv4 address 200.200.200.1/32
```

Or in configuration mode:

```
(config)# show interface loopback all | include -b 2 200.200.200.1
3-interface loopback 3
4: ipv4 address 200.200.200.1/32
```

```
(config)# show interface loopback all | include 2001:db8::1/32
ipv6 address 2001:db8::1/32
```

This example shows how to find Loopback logical interface IPv6 addresses:

```
# show ipv6 interface brief
Interface-name Logical-interface Address Scope State
-----
loopback 0      loopback 0      2001:db8::1/32 global active
```

Command to configure IPv6 addresses will be available only if `ipv6 enable` is set for interface. Example below shows that IPv6 address configuration option appears after `ipv6 enable` is set.

```
(config-loopback-4)# ipv6 ?
Possible completions:
enable    Enable IPv6 on interface
!
(config-loopback-4)# ipv6 enable
```

```
!  
(config-loopback-4)# ipv6 ?  
Possible completions:  
address    IPv6 address  
enable      Enable IPv6 on interface  
!
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface loopback vrf

Description

Configures VRF on Loopback logical interfaces.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615.

Syntax

interface loopback *id* **vrf** *vrf-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description:	Specifies the ID of the interface.
Value:	0-7.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this interface will be associated with. It is not possible to associate the VRF 'mgmt' to a loop-back interface. Also, the VRF 'global' cannot be directly configured as it is the default VRF when no VRF is associated.
Value:	string.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
5.12	Introduced VRF support on loopback interfaces with IPv6.

Usage Guidelines

If no VRF is explicitly associated with the loopback interface, it is associated with the global VRF by default. The following example shows how to associate a loopback interface with the 'test_vrf' VRF:

```
(config-loopback-7)# ?
Possible completions:
vrf          Assign a VRF instance to the interface
!
(config-loopback-7)# vrf ?
Possible completions:
<WORD>      VPN Routing/Forwarding instance name
test_vrf
!
(config-loopback-7)# vrf test_vrf
(config-loopback-7)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 5: LAYER 2 - SWITCHING PROTOCOLS

This chapter describes the commands related to management of Layer 2 protocols in the DmOS CLI.

MAC LEARNING

This topic describes the commands related to management of learning conditions such as commands to configure the aging or to inspect the MAC address table.

clear mac-address-table

Description

The **clear mac-address-table** command is used to clear entries learned by the switch.

Supported Platforms

This command is supported in all platforms.

Syntax

clear mac-address-table

clear mac-address-table interface *interface-name*

Parameters

interface *interface-name*

Description: Interface on which to delete L2 entries.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id }

Default Value: None

Default

N/A. There is no default profile.

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.4	This command was introduced.
1.6	Clear by type blocked and clear by interface were added.
2.2	Remove clear by type blocked.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
5.0	Added support for 25G interfaces.

Usage Guidelines

To clear the entire table:

```
# clear mac-address-table
```

To clear the entries on a gigabit-ethernet interface:

```
# clear mac-address-table interface gigabit-ethernet-1/1/9
```

To clear the entries on a service-port:

```
# clear mac-address-table interface service-port-1
```

Impacts and precautions

Clear confirmation will be asked for the user, once this is a permanent action.

Hardware restrictions

N/A

mac-address-table aging-time

Description

The **mac-address-table aging-time** command is used to set the global maximum time that MAC table entries will be stored in the MAC address table without a hit.

Supported Platforms

This command is supported in all platforms.

Syntax

mac-address-table aging-time *aging time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

aging-time

Description:	Maximum time, in seconds, to exclude dynamic MAC table entries. Value of 0 indicates that MAC table entries will never be aged.
Value:	20 to 2000000 0 disables MAC address aging
Default Value:	600

Default

N/A. There is no default profile.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.6	This command was introduced.
-----	------------------------------

Usage Guidelines

Setting the global MAC address aging time to 500 seconds:

```
(config)#  
(config)# mac-address-table aging time 500
```

To disable MAC address aging time:

```
(config)#  
(config)# mac-address-table aging time 0
```

To go back to the default MAC address aging time:

```
(config)#  
(config)# no mac-address-table aging time
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mac-address-table interface learning

Description

The **mac-address-table interface** *interface-name* **learning** command is used to disable MAC address learning for the specified interface.

Supported Platforms

This command is supported in all platforms.

Syntax

mac-address-table interface *interface-name* **learning**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Interface on which to configure dynamic MAC table entries learning.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: None

learning

Description: Enable/disable dynamic MAC table entries learning on interface.

Value: enabled | disabled

Default Value: enabled

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
5.0	Added support for 25G interfaces.

Usage Guidelines

Enabling the MAC address learning on interface gigabit-ethernet-1/1/1 :

```
(config)#
```

```
(config)# mac-address-table interface gigabit-ethernet-1/1/1 learning enabled
```

To disable MAC address learning:

```
(config)#
```

```
(config)# mac-address-table interface gigabit-ethernet-1/1/1 learning disabled
```

Impacts and precautions

This command clears all dynamically learned MAC entries on the configured interface. Be careful disabling MAC address learning when storm control unicast is configured on the same interface, it may occur a data loss due to DLF packet flood.

Hardware restrictions

N/A

mac-address-table interface limit

Description

The **mac-address-table interface** *interface-name* **limit** command is used to set the maximum MAC address table entries that can be learned for the specified interface.

Supported Platforms

This command is not supported in the following platforms: DM4270, DM4770, DM4380.

Syntax

mac-address-table interface *interface-name* **limit maximum** *entries*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Interface on which to limit MAC table entries.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: None

entries

Description: Maximum number of dynamic MAC table entries learned on interface. Value of 0 indicates that MAC address table entries will never be learned and traffic will be discarded.

Value: 0 to 16000
0 to disable MAC address learning and data traffic

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
3.0	Added support for 40G interfaces.
4.0	Maximum value of parameter limit increased.
4.6	Added support for 100G interfaces.
5.0	Added support for 25G interfaces.

Usage Guidelines

Setting the maximum MAC address to 10 entries on interface gigabit-ethernet-1/1/1 :

```
(config)#
```

```
(config)# mac-address-table interface gigabit-ethernet-1/1/1 limit maximum 10
```

To disable MAC address limit:

```
(config)#
```

```
(config)# (config)# no mac-address-table interface gigabit-ethernet-1/1/1 limit maximum
```

Impacts and precautions

This command clears all dynamically learned MAC entries on the configured interface, so a momentaneous data loss can occur.

When used within the vlan mac-limit, the most restrictive rule will be considered.

Hardware restrictions

N/A

mac-address-table vlan limit

Description

The **mac-address-table vlan *vlan-id* limit** command is used to set the maximum MAC address table entries that can be learned for the specified VLAN.

Supported Platforms

This command is not supported in the following platforms: DM4270, DM4770, DM4380.

Syntax

mac-address-table vlan *vlan-id* limit maximum *entries*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: VLAN on which to limit MAC table entries.

Value: { 1 to 4094 }

Default Value: None

entries

Description: Maximum number of dynamic MAC table entries learned on VLAN. Value of 0 indicates that MAC address table entries will never be learned and traffic will be discarded.

Value: 0 to 16000
0 to disable MAC address learning and data traffic

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.
4.0	Maximum value of parameter limit increased.

Usage Guidelines

Setting the maximum MAC address to 10 entries on VLAN 15 :

```
(config)#
```

```
(config)# mac-address-table vlan 15 limit maximum 10
```

To disable MAC address limit:

```
(config)#
```

```
(config)# (config)# no mac-address-table vlan 15 limit maximum
```

Impacts and precautions

This command clears all dynamically learned MAC entries on the configured VLAN, so a momentaneous data loss can occur.

When used within the interface mac-limit, the most restrictive rule will be considered.

Hardware restrictions

N/A

show mac-address-table

Description

The **show mac-address-table** command is used to display entries learned by the switch.

Supported Platforms

This command is supported in all platforms.

Syntax

show mac-address-table

show mac-address-table [[**interface** *interface-name*] | [**mac-address** *address*] | [**vlan** *vlan-id*] | [**type** *entry-type*]]

Parameters

None

Description: This parameter displays all entries learned by the switch.

Value: N/A

Default Value: N/A

interface *interface-name*

Description: This parameter displays entries learned by the switch filtered by interface.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id }

Default Value: N/A

mac-address *address*

Description: This parameter displays entries learned by the switch filtered by MAC address.

Value: XX:XX:XX:XX:XX:XX

Default Value: N/A

vlan *vlan-id*

Description: This parameter displays entries learned by the switch filtered by vlan-id.

Value: 1-4094

Default Value: N/A

type *entry-type*

Description: This parameter displays entries learned by the switch filtered by entry type.

Value: dynamic | static

Default Value: N/A

Output Terms

Output	Description
INTERFACE	Interface identifier in the system.
MAC ADDRESS	MAC Address in hexadecimal presentation.
VLAN	VLAN identifier in the system.
TYPE	<ul style="list-style-type: none"> dynamic: dynamic learn MAC address. static: static MAC address entry inserted in MAC address table.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.4	This command was introduced.
2.4	Column chassis/slot removed from show.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
5.0	Added support for 25G interfaces.

Usage Guidelines

To show the entire table:

```
# show mac-address-table
INTERFACE                               MAC ADDRESS          VLAN  TYPE
-----
gigabit-ethernet-1/1/1                  a4:88:01:34:c8:a6    100   dynamic
gigabit-ethernet-1/1/2                  dc:71:48:42:f7:a4    102   dynamic
gigabit-ethernet-1/1/3                  4c:9b:94:26:08:9c    130   dynamic
gigabit-ethernet-1/1/4                  2c:77:29:26:fd:e2    100   dynamic
gigabit-ethernet-1/1/5                  50:8a:9f:15:46:78    104   dynamic
ten-gigabit-ethernet-1/1/4              a0:8f:f7:16:8f:02    105   dynamic
ten-gigabit-ethernet-1/1/5              e6:30:97:4a:4a:fc    160   dynamic

Total MAC Addresses for this criterion: 7
```

Impacts and precautions

N/A

Hardware restrictions

Maximum number of entries that can be learned depends on hardware used.

VLAN

This topic describes the commands related to the management of 802.1Q Virtual Bridged LAN and to the management of VLAN extensions such as commands to configure Q-in-Q, dynamic VLANs and VLAN Translations.

dot1q vlan

Description

Enables configuration mode for a given VLAN or a range of VLANs

Supported Platforms

This command is supported in all platforms.

Syntax

dot1q vlan *vlan-id* [**name** *vlan-name*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: Single, range or list of VLAN IDs to be configured.

Value: 1 - 4094

Default Value: N/A

name *vlan-name*

Description: VLAN name.

Value: 1 - 32 characters

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

When entering the VLAN configuration tree, the VLAN itself is created if it does not exist. VLANs can be created in ranges, or list. The following command will create VLANs from 10 to 20 and VLAN 30 and assing a name to all of them:

```
(config)#dot1q vlan 10-20,30 name example
```

The following command will destroy the VLAN and its members:

```
(config)# no dot1q vlan 1
```

Impacts and precautions

VLANs must be created before being used by others features on their configurations.

Hardware restrictions

N/A

dot1q vlan interface

Description

Adds an interface as a member of the configured VLAN.

Supported Platforms

This command is supported in all platforms.

Syntax

dot1q vlan *vlan-id* **interface** *interface-name* [*tag-mode*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: ID of VLAN to be configured.

Value: 1 - 4094

Default Value: N/A

interface *interface-name*

Description: Interface name to be configured.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id }

Default Value: N/A

tag-mode

Description: Frames are forwarded with or without VLAN tag.
The value *tagged* configures frames with tag by this VLAN interface.
The value *untagged* configures frames without tag by this VLAN interface.

Value: { tagged | untagged }

Default Value: tagged

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
4.6	Added support to 40 Gigabit Ethernet and 100 Gigabit Ethernet.
5.0	Added support to 25 Gigabit Ethernet.

Usage Guidelines

The following command adds gigabit-ethernet 1/1/1 interface *tagged* in the VLAN 1:

```
(config)# dot1q vlan 1 interface gigabit-ethernet-1/1/1
```

When adding an interface as a member of a VLAN, the default behaviour is to add it as tagged. Inside the interface configuration tree, the command *untagged* will change it.

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name.

Interfaces added as a member of a link aggregation group(LAG) cannot be added to VLAN membership. The LAG itself should be configured instead.

Service-port interfaces cannot be added untagged to VLAN. All VLAN manipulations for this interface can be done by the service-port command itself.

Hardware restrictions

N/A

show vlan

Description

Used to display VLAN information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show vlan { brief [vlan id] | membership { brief | detail } }
```

Parameters

brief

Description: Display VLAN brief information.

Value: N/A

Default Value: N/A

membership

Description: Display VLAN membership information.

Value: N/A

Default Value: N/A

detail

Description: Display membership detailed information.

Value: N/A

Default Value: N/A

vlan id

Description: Display information of a specific VLAN.

Value: 1-4094

Default Value: N/A

Output Terms

Output	Description
VLAN ID	VLAN identifier in the system.
NAME	Textual name of the VLAN.
INTERFACE	Interface identifier in the system.
INTERFACE COUNT	Display the summarized information about VLAN members.
TYPE	Type attribute describes how it was created. Static entries means that users have created it through configuration.
STATUS	Operational state of the interface. The possible states are Up and Down.
PORT STATE	Port state of the interface for this vlan. Can be set by protocols such as RSTP, EAPS and ERPS. The possible states are Disabled, Learning, Forwarding and Blocked.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced
4.2	Removed parameter detail. Added parameters status and port state. Show vlan membership detail is now presented as table by default.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples shows how to use the show vlan commands.

```
# show vlan brief

VLAN          INTERFACE
ID    NAME    TYPE    COUNT
-----
100    MyVlan    static    1
200                static    1

# show vlan membership brief

VLAN
ID    INTERFACE
-----
100    gigabit-ethernet-1/1/1
200    gigabit-ethernet-1/1/2

# show vlan membership detail

VLAN          TYPE    STATUS    PORT STATE
ID    INTERFACE
-----
100    gigabit-ethernet-1/1/1    static    down    forwarding
200    gigabit-ethernet-1/1/2    static    down    forwarding
```

Impacts and precautions

N/A

Hardware restrictions

N/A

switchport acceptable-frame-types

Description

This configuration allows the interface to choose between tagged, untagged and all frames to be accepted. By default all frames either tagged with a IEEE 802.1Q header or not are accepted.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface { *interface-name* } **acceptable-frame-types** { *type-value* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to set the acceptable frame type.

Value: *interface-type-chassis/slot/port | lag-id*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.

Default Value: N/A

acceptable-frame-types *type-value*

Description: Configure acceptable frame types in the interface.

Value: { all | tagged | untagged }

Default Value: all

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.2	This command was introduced.

Usage Guidelines

The example below shows the configuration of acceptable-frame-types for a given interface.

```
# config
Entering configuration mode terminal
(config)# switchport interface gigabit-ethernet-1/1/1
(config-switchport-gigabit-ethernet-1/1/1)# acceptable-frame-types tagged
(config-switchport-gigabit-ethernet-1/1/1)# commit
Commit complete.
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name.

Interfaces added as a member of a link aggregation group(lag) cannot have acceptable-frame-types configured.

The lag itself should be configured instead.

Hardware restrictions

N/A

switchport native-vlan

Description

Defines a native VLAN ID to be added in all untagged packets received in ingress mode in the given interface.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface { *interface-name* } **native-vlan vlan-id** { *native-vlan-id* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to set the native-vlan.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

vlan-id *native-vlan-id*

Description: VLAN ID to be added in incoming untagged packets in the interface.

Value: 1 - 4094

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.8	This command was introduced.

Usage Guidelines

To configure a native-vlan the interface must be either valid and untagged member of the VLAN ID being used for native vlan. The VLAN ID which will be added must exists. The example below shows the creation of a native-vlan for the given interface.

```
# config
Entering configuration mode terminal
(config)# dot1q vlan 100
(config-vlan-100)# interface gigabit-ethernet-1/1/1
(config-dot1q-interface-gigabit-ethernet-1/1/1)# untagged
(config-vlan-100)# top
(config)# switchport interface gigabit-ethernet-1/1/1
(config-switchport-gigabit-ethernet-1/1/1)# native-vlan vlan-id 100
(config-switchport-interface-native-vlan)# commit
Commit complete.
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name. Interfaces added as a member of a link aggregation group(lag) cannot have native vlan configured. The lag itself should be configured instead. VLANs to be added on the packets need to pre-exists, so configuration will be committed

successfully.

When an invalid interface or VLAN ID is used, the user is warned about the error during commit step.

Hardware restrictions

N/A

switchport pcsp

Description

Defines a 802.1p priority (PCP) to be added for untagged packets or for QinQ packets within the native VLAN-ID.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface { *interface-name* } **pcsp** { *pcsp-value* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to set the pcsp.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

pcsp *pcsp-value*

Description: PCP to be added for incoming packets in the interface within the native VLAN-ID

Value: 0 - 7

Default Value: 0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.6	This command was introduced.

Usage Guidelines

The example below shows the configuration of a pcpc for the given interface.

```
# config
Entering configuration mode terminal
(config)# dot1q vlan 100
(config-vlan-100)# interface gigabit-ethernet-1/1/1
(config-dot1q-interface-gigabit-ethernet-1/1/1)# untagged
(config-vlan-100)# top
(config)# switchport interface gigabit-ethernet-1/1/1
(config-switchport-gigabit-ethernet-1/1/1)# native-vlan vlan-id 100
(config-switchport-interface-native-vlan)# exit
(config-switchport-gigabit-ethernet-1/1/1)# pcpc 2
(config-switchport-interface-pcpc)# commit
Commit complete.
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name.

Interfaces added as a member of a link aggregation group(lag) cannot have pcpc configured. The lag itself should be configured instead.

PCP configuration has no effect without native-vlan configuration.

Hardware restrictions

N/A

switchport qinq

Description

Enables VLAN QinQ mode for the packets received on this interface. When enabled, the received packets will get an extra IEEE 802.1Q header, that is created using the native VLAN ID and default values for TPID (0x8100), priority code point(0) and drop eligible information (0). Usually this enclosing VLAN ID is usually referred as S-VLAN.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface { *interface-name* } **qinq**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to set the QinQ.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

qinq

Description: Enable QinQ in the interface.

Value: N/A

Default Value: Disabled

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.

Usage Guidelines

The interface must have a valid configuration for native VLAN. The example below shows the configuration of QinQ for a given interface and its pre-conditions.

```
# config
Entering configuration mode terminal
(config)# dot1q vlan 50
(config-vlan-50)# interface gigabit-ethernet-1/1/1 untagged
(config-dot1q-interface-gigabit-ethernet-1/1/1)# top
(config)# switchport interface gigabit-ethernet-1/1/1
(config-switchport-gigabit-ethernet-1/1/1)# native-vlan vlan-id 50
(config-switchport-interface-native-vlan)# exit
(config-switchport-gigabit-ethernet-1/1/1)# qinq
(config-switchport-gigabit-ethernet-1/1/1)# commit
Commit complete.
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name.

Interfaces added as a member of a link aggregation group(lag) cannot have qinq configured. The lag itself should be configured instead.

VLANs to be added on the packets need to pre-exists, so configuration will be committed successfully.

When an invalid interface or VLAN ID is used, the user is warned about the error during commit step.

Hardware restrictions

N/A

switchport tpid

Description

Configures tag protocol identifier(TPID) accepted for VLAN tagged frames. Only frames received with the configured TPID are considered as tagged frames. Also, tagged frames sent by the configured interface will have the configured TPID.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface { *interface-name* } **tpid** { *tpid-value* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to set the TPID.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

tpid *tpid-value*

Description: Configure TPID in the interface.

Value: { 0x8100 | 0x88a8 | 0x9100 }

Default Value: 0x8100

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

The example below shows the configuration of TPID for a given interface.

```
# config
Entering configuration mode terminal
(config)# switchport interface gigabit-ethernet-1/1/1
(config-switchport-gigabit-ethernet-1/1/1)# tpid 0x88a8
(config-switchport-gigabit-ethernet-1/1/1)# commit
Commit complete.
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name.

Interfaces added as a member of a link aggregation group(lag) cannot have TPID configured. The lag itself should be configured instead.

When an invalid interface is used, the user is warned about the error during commit step.

Hardware restrictions

N/A

vlan-mapping

Description

Create or update VLAN mapping rules to add or replace a VLAN tags when match criteria is met.

Supported Platforms

This command is supported in all platforms.

Syntax

```
vlan-mapping interface { interface-name } { stage } rule { rule-name } match vlan
vlan-id { vlan-id-match } action { add | replace } vlan vlan-id { vlan-id-action } [pcp
{ pcp } ] [ inner-action replace inner-vlan vlan-id { vlan-id-action } [pcp { pcp } ] ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Name of interface to install the rule.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

stage

Description: Specify the stage the VLAN-mapping rule refers to (ingress or egress data).

Value: ingress | egress

Default Value: N/A

rule *rule-name*

Description:	Name of the rule being created/updated. Only accepts alphanumeric characters and '_', '+' and '-'.
Value:	String with maximum 48 characters
Default Value:	N/A

match

Description:	Parameters after match and before action describe the type of flow selected to be modified.
Value:	N/A
Default Value:	N/A

vlan vlan-id *vlan-id-match*

Description:	Single, range or list of VLAN ID that will be matched.
Value:	1 - 4094
Default Value:	N/A

action { *add* | *replace* }

Description:	<p>Selects the action to be applied to the outer VLAN.</p> <p><i>replace</i> will replace the outer VLAN tag of packets that meet match criteria.</p> <p><i>add</i> will add a new outer VLAN tag to packets that meet match criteria.</p> <p>The action is only available after the match is configured.</p>
Value:	add replace
Default Value:	N/A

inner-action *replace*

Description:	<p>Selects the action to be applied to the inner VLAN.</p> <p><i>replace</i> will replace the inner VLAN tag of packets that meet match criteria.</p> <p>When the action is <i>add</i> (for the outer VLAN), then the new added VLAN is considered the outer VLAN, and the inner-action will act over the previous outer VLAN tag.</p> <p>The inner-action is only available after the action is configured.</p> <p>The combination of action <i>add</i> and inner-action <i>replace</i> is only valid when <i>switchport qinq</i> is enabled for the interface.</p>
---------------------	--

The combination of **action** *replace* and **inner-action** *replace* is only valid when *switchport qinq* is disabled for the interface.

Value: replace

Default Value: N/A

vlan vlan-id *vlan-id-action*

Description: VLAN ID that will be added or replaced into the outer VLAN tag of the packet.

Value: 1 - 4094

Default Value: N/A

inner-vlan vlan-id *vlan-id-action*

Description: VLAN ID that will be replaced into the inner VLAN tag of the packet.

The value *copy* may be configured, and it will keep the current VLAN ID in the inner VLAN tag.

Value: 1 - 4094 | copy

Default Value: N/A

pcp *pcp*

Description: VLAN PCP (802.1p) field value that will be added into packet for outer or inner VLAN tag. It can be the numeric priority value or the copy from the PCP value from the existing VLAN tag.

Value: 0-7 | copy

Default Value: 0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.
4.6	Added pcp action. Added support for 100G interfaces.
4.8	Added inner-action.
5.0	Added support for 25G interfaces.
5.10	Remove restriction of using action add without QinQ enabled for DM4270, DM4770 and DM4380 series.

Usage Guidelines

To configure a VLAN mapping rule the interface must be a valid one. Also, the VLAN that will replace the original one in the VLAN tag must exist. The example below shows the creation of a rule with *replace* action.

```
# config
(config)# dot1q vlan 100
(config-vlan-100)# interface gigabit-ethernet-1/1/1
(config-interface-gigabit-ethernet-1/1/1)# top
(config)# vlan-mapping interface gigabit-ethernet-1/1/1 ingress rule RULE1
(config-rule-RULE1)# match vlan vlan-id 1 action replace vlan vlan-id 100
(config-rule-RULE1)# commit
Commit complete.
(config-rule-RULE1)# end
#
```

Impacts and precautions

Only pre-existing interfaces will be accepted when entering an interface name. Interfaces added as members of a link aggregation group (LAG) cannot be added to vlan-mapping rules. The LAG itself should be configured instead.

VLANs to be added on the packets need to pre-exist, so configuration will be committed successfully.

Hardware restrictions

DM4611 and DM4612 series do not support VLAN Mapping.

DM4050 and DM4250 series do not support PCP copy on ingress rules.

DM4050 and DM4250 series do not support *inner-action*.

On DM4270, DM4770 and DM4380 series, VLAN mapping rules do not act over packets modified by ACL.

On DM4270, DM4770 and DM4380 series, VLANs associated with L3 interfaces cannot be used for ingress VLAN Mapping rules when there is no QinQ enabled, except when both the match and action VLANs are the same.

On DM4270, DM4770 and DM4380 series, VLAN mapping rules with action add do not act over double-tagged packets when the ingress interface has QinQ disabled.

LINK AGGREGATION

This topic describes the commands related to management of interface aggregations such as commands to configure static and dynamic aggregations.

clear lacp

Description

The **clear lacp** command is used to reset statistics about Link Aggregation Control Protocol (LACP).

Supported Platforms

This command is supported in all platforms.

Syntax

clear lacp statistics {**all** | **lag id** *id* }

Parameters

all

Description: Reset statistics for all link-aggregations.

Value: N/A

Default Value: N/A

lag id *id*

Description: Reset statistics for a specific link-aggregation. The actual maximum number of link-aggregations depends on the product model.

Value: 1-32

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.12	This command was introduced
2.4	Number of LAG-IDs increased to eight

Usage Guidelines

To clear all LAGs statistics:

```
# clear lacp statistics all
```

To clear a single LAG statistics:

```
# clear lacp statistics lag id 1
```

Impacts and precautions

It is only possible to clear statistics for link-aggregations controlled by LACP, i.e., link-aggregations configured in active or passive modes.

Hardware restrictions

N/A

link-aggregation

Description

Link aggregation bundles individual ethernet links into a single logical link. It may be used for redundancy or to expand bandwidth capacity. It is controlled by Link Aggregation Control Protocol (LACP).

Supported Platforms

This command is supported in all platforms.

Syntax

link-aggregation [**system-priority** *priority*]

link-aggregation [**load-balance hash-function** *hash*]

link-aggregation interface lag *lag-id* [**load-balance** *type*] [**maximum-active** *links*] [**minimum-active** *links*] [**mode** *lACP-mode*] [**period** *period-interval*] **interface** *interface-name* [**port-priority** *priority*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

system-priority *priority*

Description: Sets a priority to the LACP system.

Value: 0-65535

Default Value: 32768

load-balance hash-function *hash*

Description: Sets the global load balance hash function for enhanced and dynamic mode.

Value: { crc16xor8 | crc16xor4 | crc16xor2 | crc16xor1 | crc16 | xor16 | crc16ccitt | crc32lo | crc32hi | crc32ethlo | crc32ethhi | crc32koopmanlo | crc32koopmanhi }

Default Value: crc16xor8

interface lag *lag-id*

Description: Creates a Link Aggregation Group with a specific identifier. The actual maximum number of link-aggregations depends on the product model.

Value: 1-32

Default Value: N/A

load-balance *type*

Description: Sets the load balancing algorithm to apply to traffic forwarded on this LAG interface.

The dynamic balance type provides an evenly load distribution across the LAG members. By taking into account the instant values for the load of the LAG members, flows are dynamically moved from links with lower loads.

Other types are hash-based, where the packet order is always maintained. However, as the output interface is selected according to the traffic (using an XOR of packet fields), bandwidth usage might not be uniform among the LAG members. Eventually, some LAG members present heavy loading while others are underused.

Value: { dst-ip | dst-mac | dynamic | enhanced | src-dst-ip | src-dst-mac | src-ip | src-mac }

Default Value: enhanced

maximum-active *links*

Description: Sets the maximum number of links allowed to be simultaneously active on this LAG interface.

If more interfaces are configured than the maximum-active links, the exceeding interfaces with higher port-priority will remain inactive. The maximum value for this parameter may be lower depending on the product model. The default value for this parameter is equal to the maximum value, which may be lower depending on the product model.

Value: 1-16

Default Value: 16

minimum-active *links*

Description:	Sets the minimum number of links required to bring up this LAG interface. If less interfaces are active than the minimum-active links, the LAG interface itself will be considered inactive. The maximum value for this parameter may be lower depending on the product model.
Value:	1-16
Default Value:	1

mode *lacp-mode*

Description:	Sets the mode of LACP operation for this LAG. If set to Static, LACP is disabled. If set to Passive, the remote node must be set to Active.
Value:	{ static active passive }
Default Value:	static

period *period-interval*

Description:	Sets the interval period of LACP for this LAG, short (1s) or long (30s). Short option allows a faster link detection/recovery. Preferably both nodes must be set with the same value.
Value:	{ short long }
Default Value:	long

description

Description:	Sets a textual description of the interface, according to the network manager's choice. Valid characters are A-Z, a-z, 0-9 and - _ / + * @.
Value:	The interface description.
Default Value:	N/A

interface *interface-name*

Description:	Interface to be added to LAG. Each interface may appear in only one LAG at time.
---------------------	--

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port }

Default Value: N/A

port-priority *priority*

Description: Sets a port priority for a LAG member.

Value: 0-65535

Default Value: 32768

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced
1.12	Implemented support to LACP
2.4	Added description parameter and number of LAG-IDs increased to eight
3.0	Added support for 40G interfaces
4.5	Added maximum-active and minimum-active parameters

Release	Modification
4.6	Added support for 100G interfaces
4.9	Added support for load-balance command
5.0	Added support for 25G interfaces
5.10	Added support for load-balance hash-function command

Usage Guidelines

Commands for configure the link-aggregation.

Example:

This example shows how to configure a simple static link-aggregation.

```
# config terminal
Entering configuration mode terminal
(config)# link-aggregation interface lag 1
(config-lag-if-lag-1)# interface gigabit-ethernet-1/1/1
(config-lag-if-gigabit-ethernet-1/1/1)#
```

Impacts and precautions

Each interface may appear in only one LAG at time.

Only interfaces with the same nominal speed can be aggregated together. Interfaces with half-duplex configuration cannot be members of a LAG.

Each LAG must contain at least one and no more than eight aggregatable interfaces.

If the LAG interface has more physical interfaces than the configured maximum-active parameter, in static mode the interfaces with higher value at port-priority parameter will be maintained inactive as standby.

In active or passive modes the interface selection criteria follows the following path of comparisons: System Priority -> System MAC -> Port Priority -> Port ID. In priority comparisons, numerically lower values have higher priority.

This means that the interfaces of the equipment with lower System Priority will be used

for standby selection, according to it's Port Priority and Port ID. If System Priority is the same on both equipments, the equipment with lower System MAC will use it's interfaces to decide standby selection, according to it's Port Priority and Port ID.

Maximum-links and minimum-links are independent configuration options. They can be used in any mode of operation (static, active or passive).

Hardware restrictions

When load-balance enhanced is used, the platform DM4050 only supports non-unicast (broadcast, multicast and unknown unicast) load-balance based on source and destination MAC addresses. Others load-balance criteria like source and destination IP and TCP/UDP ports are not available.

Load-balance dynamic is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4050, DM4250 and DM4370.

Load-balance hash-function parameter is not supported in the DM4050 platform.

show link-aggregation

Description

Used to display link-aggregation information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show link-aggregation [ brief | interfaces brief | lacp [ brief | statistics | extensive ] ]
```

Parameters

brief

Description: Display brief information about link-aggregations.

Value: N/A

Default Value: N/A

extensive

Description: Display detailed information about link-aggregations.

Value: N/A

Default Value: N/A

interfaces

Description: Display information about members of link-aggregations.

Value: N/A

Default Value: N/A

lacp

Description: Display information about dynamic aggregations controlled by Link Aggregation Control Protocol (LACP).

Value: N/A

Default Value: N/A

statistics

Description: Display information about PDU exchange in dynamic aggregations controlled by Link Aggregation Control Protocol (LACP).

Value: N/A

Default Value: N/A

Output Terms

Output	Description
LAG interface	Identifier of link-aggregation instance in the system.
State	LAG operational state. Up means that at least 1 interface member has link status up. Down means no member has active link.
Aggregation Status	<p>Indicates whether this LAG member is active in the LAG. The possible values are:</p> <ul style="list-style-type: none"> • active - the member is aggregated in the LAG. • inactive - the member is not aggregated in the LAG. • inactive: too few links - the member is not active due to minimum-active links configuration. • inactive: standby - the member is not active due to maximum-active links configuration. • inactive: max-active lower than min-active - the member is inactive due to a misconfiguration.
Mode	<p>Indicates the operation mode for a LAG, three options are available:</p> <ul style="list-style-type: none"> • static - LAG is configured statically by user; • active - LAG is controlled by LACP in active mode; • passive - LAG is controlled by LACP in passive mode.

Output	Description
Rate	Indicates the PDUs rate requested by protocol: <ul style="list-style-type: none">• slow - PDUs sent at long intervals of 30 seconds;• fast - PDUs sent at short intervals of 1 second.
Port Prio	Indicates the configured priority for this interface.
Port ID	Indicates the port identifier in the system.
Key	Indicates the link-aggregation key used by LACP to establish LAGs.
System Prio	Indicates the system priority used by LACP.
LACPDUs Sent/Received	Indicates the number of sent or received PDUs in an interface.
Pkt Errors	Indicates the number of invalid PDUs received in an interface.
Cleared(s)	Indicates the elapse time (in seconds) since the statistics of this interface were cleared.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced
1.12	The LACP parameter was introduced
4.6	New aggregation states added

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples shows how to use the show link-aggregation commands.

```
# show link-aggregation brief

State codes: down - no link up; up - at least 1 member up;

LAG interface   State   Mode
-----
lag-1           up      static
lag-3           down    static

# show link-aggregation interfaces brief

Aggregation Status:
  active - member is aggregated;
  inactive - member is not aggregated;
  inactive: too few links - member is inactive due to minimum-active links;
  inactive: standby - member is inactive due to maximum-active links;
  inactive: max-active lower than min-active - member is inactive due to a ...

LAG interface: lag-1
Members
-----
gigabit-ethernet-1/1/1      Oper Status  Aggregation Status
gigabit-ethernet-1/1/3      down         inactive

LAG interface: lag-3
Members
-----
ten-gigabit-ethernet-1/1/1  Oper Status  Aggregation status
ten-gigabit-ethernet-1/1/1  down         inactive
```

Impacts and precautions

N/A

Hardware restrictions

N/A

SPANNING-TREE

This topic describes the commands related to management of Spanning-Tree topologies such as commands to configure the spanning-tree mode, to change the path cost or to inspect the interface roles.

show spanning-tree

Description

Used to display spanning-tree information.

Supported Platforms

This command is supported in all platforms.

Syntax

show spanning-tree [brief | detail | extensive]

Parameters

brief

Description: Display spanning tree brief information.

Value: N/A

Default Value: N/A

detail

Description: Display spanning tree detailed information.

Value: N/A

Default Value: N/A

extensive

Description: Display spanning tree extensive information.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Priority	Spanning tree priority of the STP instance.
Address	Mac address of STP instance.
Cost (Root ID)	The cost configured for a port from Root.
Port (Root ID)	Display the port id from Root.
Hello Time	Time interval that the root bridge will generate BPDUs.
Max Age	The maximum length of time that passes before a bridge port saves its configuration BPDU information.
Forward Delay	Time interval that interfaces of all bridges should wait to change from its listening and learning states to forwarding state.
Interface	Spanning tree interface name.
Port	Display port number.
Prio	Display the port priority.
Cost	The path cost configured for a port.
Sts	Port state from STP instance.
Cost	Designated path cost configured for a port.
Bridge ID	Designated Bridge ID used for sending and receiving STP BPDUs.
Port	Designated Port from STP instance.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.6	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples shows how to use the show spanning-tree command.

```
# show spanning-tree
Spanning tree enabled protocol rstp
Root ID    Priority: 32768; Address: 00:00:00:00:00:00;
           Cost: 0; Port: global;
           Hello Time: 2sec; Max Age: 20sec; Forward Delay: 15sec;

Bridge ID  Priority: 32768; Address: n/a;
           Hello Time: 2sec; Max Age: 20sec; Forward Delay: 15sec;
```

Interface	Port	Prio	Cost	Sts	Cost	Designated Bridge ID	Port
gigabit-ethernet-1/1/1	0	128	100	DIS	0	0 00:00:00:00:00:00	0

```
# show spanning-tree brief
Spanning tree enabled protocol rstp
Root ID    Priority: 32768; Address: 00:00:00:00:00:00;
           Cost: 0; Port: global;
           Hello Time: 2sec; Max Age: 20sec; Forward Delay: 15sec;

Bridge ID  Priority: 32768; Address: n/a;
           Hello Time: 2sec; Max Age: 20sec; Forward Delay: 15sec;
```

Interface	Port	Prio	Cost	Sts	Cost	Designated Bridge ID	Port
gigabit-ethernet-1/1/1	0	128	100	DIS	0	0 00:00:00:00:00:00	0

```
# show spanning-tree detail
Spanning tree enabled protocol: rstp
  Bridge Identifier has priority: 32768; address: n/a;
  Configured: hello time: 2sec; max age: 20sec; forward delay: 15sec;
  Topology flag not set;
  Number of topology changes 0, last change occurred 0 seconds ago;
  Times: hold: 6; hello: 2; max age: 20; forward delay: 15;

Port 0 (gigabit-ethernet-1/1/1) is discarding
  Path cost: 100; Priority: 128;
  Designated root: priority: 0; address: 00:00:00:00:00:00;
  Designated bridge: priority: 0; address: 00:00:00:00:00:00;
  Designated port: 0; designated path cost: 0;
  Number of transitions to forwarding state: 0;
```

```
# show spanning-tree extensive
Spanning tree enabled protocol: rstp
  Administrative state: up; Operational state: failed;
  Bridge Identifier has priority: 32768; address: n/a;
  Configured: hello time: 2sec; max age: 20sec; forward delay: 15sec;
  Topology flag not set;
  Number of topology changes 0, last change occurred 0 seconds ago;
  Times: hold: 6; hello: 2; max age: 20; forward delay: 15;

Port 0 (gigabit-ethernet-1/1/1) is discarding
  Operational state: down;
  Forwarding state: discarding; Role: disabled;
  Path cost: 100; Priority: 128;
  P2p: no; Edge: no; Up-time: 0; Disputed: false;
  Designated root: priority: 0; address: 00:00:00:00:00:00;
  Designated bridge: priority: 0; address: 00:00:00:00:00:00;
  Designated port: 0; designated path cost: 0;
  Number of transitions to forwarding state: 0;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

spanning-tree

Description

The Spanning Tree Protocol (STP) is a network protocol that prevents loops from occurring in the network topology. Spanning tree also allows a network design to include redundant links to provide automatic backup paths.

Supported Platforms

This command is supported in all platforms.

Syntax

spanning-tree [**bridge-priority** *priority*] [**forward-delay** *seconds*] [**hello-time** *seconds*] [**maximum age** *seconds*] [**mode** *version*] [**name** *identifier*] [**revision** *number*] [**transmit hold-count** *number*] [**maximum** {[**age** *number*] [**hops** *number*] }] **interface** *name* { [**cost** *number*] [**port-priority** *number*] [**link-type** *type*] [**restricted-role**] [**restricted-tcn**] [{**edge-port** | **auto-edge**}] [**bpdu-guard**] }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

bridge-priority *priority*

Description: The bridge priority for this instance. When using the MSTP mode, this parameter is used as the CIST bridge priority.

Value: 0-61440

Default Value: 32768

forward-delay *seconds*

Description: Used by root to set the number in seconds, that interfaces of all bridges should wait to change from its listening and learning states to forwarding state.

Value: 4-30

Default Value: 15

hello-time *seconds*

Description: Value that all bridges will use for the hello time if this bridge is acting as root.

Value: 1-10

Default Value: 2

maximum age *seconds*

Description: Value that all bridges will use for the max age of BPDUs if this bridge is acting as root.

Value: 6-40

Default Value: 20

mode *version*

Description: Spanning Tree Protocol version selection.

Value: rstp, mstp

Default Value: rstp

name *identifier*

Description: The Configuration Name part of the STP Configuration Identifier.

Value: Name - maximum 32 characters

Default Value: N/A

revision *number*

Description: The Configuration Revision level part of the MSTP Configuration Identifier. Only available when mode is MSTP.

Value: 0-65535

Default Value: 0

transmit hold-count *number*

Description: The value used by port to limit the maximum BPDU transmission rate.

Value: 1-10

Default Value: 6

maximum age *number*

Description: Value that all bridges will use for the max age of BPDUs if this bridge is acting as root.

Value: 6-40

Default Value: 20

maximum hops *number*

Description: The maximum number of hops across an MST region. Only available when mode is MSTP.

Value: 6-40

Default Value: 20

interface *name*

Description: Interface name to be configured.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

cost *number*

Description: Path cost configuration for the port.

Value: 1-2000000000

Default Value: 20000

port-priority *number*

Description: Priority configuration for the port.

Value: 0-240

Default Value: 128

link-type *type*

Description: Link type configuration for the port.

Value: auto, not-point-to-point, point-to-point

Default Value: auto

restricted-role

Description: Restricted role configuration for the port. Also known as root guard. When enable for an interface that would be chosen as root port, this interface will be blocked instead.

Value: N/A

Default Value: N/A

restricted-tcn

Description: Restricts the propagation of topology changes for the port. Topology change notifications received on the interface are not propagated to other interfaces.

Value: N/A

Default Value: N/A

edge-port

Description: Administrative edge port configuration for the port. When configured, auto-edge configuration is ignored.

Value: N/A

Default Value: N/A

auto-edge

Description: Automatic edge port detection on this port.

Value: N/A

Default Value: N/A

bpdu-guard

Description: Enables bpdu-guard for the port. When enable, if an edge port receives a BPDU, the port role is set to disable and port state is set to discarding. Bpdu-guard parameter only can be set if edge-port is also set.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced
1.12	Spanning-tree supports configuration in link-aggregations.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
4.8	Added support for MSTP mode. Added parameters restricted-role, restricted-tcn and bpdu-guard.
5.0	Added support for 25G interfaces.
5.2	The cist-bridge-priority parameter was deprecated and unified with the bridge-priority parameter.

Usage Guidelines

Commands for configure the spanning-tree.

Example:

This example shows how to configure the spanning-tree protocol.

```
# config terminal
Entering configuration mode terminal
(config)# spanning-tree forward-delay 20
(config)# spanning-tree hello-time 5
```

```
(config)# spanning-tree transmit hold-count 10
(config-spanning-tree)# spanning-tree interface gigabit-ethernet 1/1/1
(config-stp-interface-gigabit-ethernet-1/1/1)# cost 2000
(config-stp-interface-gigabit-ethernet-1/1/1)# port-priority 100
(config-stp-interface-gigabit-ethernet-1/1/1)# link-type auto
(config-stp-interface-gigabit-ethernet-1/1/1)# edge-port
```

Impacts and precautions

The maximum age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. The switch that is at the periphery of the network does not time out the root information under stable conditions. So, the maximum age requires the coherence $(2 \times (\text{hello-time}) \leq \text{age} \leq 2 \times (\text{forward-delay} - 1))$.

Hardware restrictions

N/A

spanning-tree mst

Description

Spanning-tree mst allows multiples instances of spanning-tree, according to IEEE 802.1Q, 2011. This command is only available when spanning-tree mode is set to *mstp*.

Supported Platforms

This command is supported in all platforms.

Syntax

spanning-tree mst *id* [**priority** *priority*] [**vlan** *vlangs*] [**interface** *name* [**cost** *number*] [**port-priority** *number*]]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mst *id*

Description: The id of this MST instance.

Value: 1-64

Default Value: N/A

priority *priority*

Description: The bridge priority for this MST instance.

Value: 0-61440

Default Value: 32768

vlan *vlangs*

Description: Sets the list of protected VLANs of this MST instance. Ranges of VLANs or single VLAN are allowed and can be combined to specify the set of protected VLANs

Value: 1-4094

Example: **protected-vlans 1-3,5,7-9**

Default Value: None

interface *name*

Description: Interface name to be configured in this MST instance. The interface must also be configured in the CIST instance.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: N/A

cost *number*

Description: Path cost configuration for the port in this MST instance.

Value: 1-2000000000

Default Value: 20000

port-priority *number*

Description: Priority configuration for the port in this MST instance.

Value: 0-240

Default Value: 128

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced
-----	-----------------------------

5.0	Add support for 25G interfaces
-----	--------------------------------

Usage Guidelines

Commands for configure the spanning-tree.

Example:

This example shows how to configure a spanning-tree instance.

```
# config terminal
Entering configuration mode terminal
(config)# spanning-tree mode mstp
(config-spanning-tree)# interface gigabit-ethernet-1/1/1
(config-stp-gigabit-ethernet-1/1/1)# port-priority 240
(config-stp-gigabit-ethernet-1/1/1)# cost 2000
(config-stp-gigabit-ethernet-1/1/1)# exit
(config-spanning-tree)# interface gigabit-ethernet-1/1/2
(config-stp-gigabit-ethernet-1/1/2)# cost 2000
(config-stp-gigabit-ethernet-1/1/2)# port-priority 240
(config-stp-gigabit-ethernet-1/1/2)# exit
(config-spanning-tree)# spanning-tree mst 1
(config-stp-mst1)# priority 1
(config-stp-mst1)# interface gigabit-ethernet-1/1/1
(config-stp-mst-gigabit-ethernet-1/1/1)# port-priority 16
(config-stp-mst-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

ERPS

This topic describes the commands related to management of G.8032 ERPS topologies such as commands to configure the RPL or to inspect the protection status.

erps ring

Description

The current implementation follows ERPS version 2 specification, as described in ITU-T G.8032.

Supported Platforms

This command is supported in all platforms.

Syntax

erps ring *ring-name*

erps ring *ring-name* **ring-id** *id*

erps ring *ring-name* **control-vlan** *vlan-id*

erps ring *ring-name* **protected-vlans** *vlans*

erps ring *ring-name* **r-aps-level** *level*

erps ring *ring-name* { **port0** | **port1** } { **interface** *interface-name* | **virtual-channel** **control-vlan** *vlan-id* }

erps ring *ring-name* { **port0** | **port1** } **interface** *interface-name* **rpl-role** *role*

erps ring *ring-name* **timers** [**guard** *milliseconds* | **hold-off** *milliseconds* | **wtr** *minutes*]*

erps ring *ring-name* **type** *ring-type*

erps ring *ring-name* **node** *ring-node*

erps ring *ring-name* **parent-ring** *ring-name*

erps ring *ring-name* **propagate-tc**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

erps ring *ring-name*

Description: Sets a textual name for this ERPS ring instance, according to the network manager's choice. Valid characters are A-Z, a-z, 0-9 and + _ - ".

Value: An identifier with up to 48 characters.

Default Value: None

erps ring *ring-name* **ring-id** *id*

Description: Sets the ring identifier used for control traffic (ERPS PDUs).

Value: 1-239

Default Value: None

erps ring *ring-name* **control-vlan** *vlan-id*

Description: Sets the VLAN used for control traffic (ERPS PDUs).

Value: 1-4094

Default Value: None

erps ring *ring-name* **protected-vlans** *vlangs*

Description: Sets the list of VLANs protected by this ERPS ring instance. VLAN ranges or single VLANs are allowed and can be combined to specify the set of protected VLANs.

Value: 1-4094
Example: *protected-vlans 1-3,5,7-9*

Default Value: None

erps ring *ring-name* **r-aps-level** *level*

Description: Sets the R-APS level of PDUs exchanged by this ring instance.

Value: 0-7

Default Value: 0

erps ring *ring-name* **port0 interface** *interface-name*

Description: Sets the first ring instance's port.

Value: *interface-type-chassis/slot/port*
 Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, lag.**

Default Value: None

erps ring *ring-name* **port1 interface** *interface-name*

Description: Sets the second ring instance's port.

Value: *interface-type-chassis/slot/port*
 Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, lag.**

Default Value: None

erps ring *ring-name* **port1 virtual-channel control-vlan** *vlan-id*

Description: Sets the ring instance's virtual-channel. Only *port1* can be set as virtual-channel. This configuration is available only when *ring-type* parameter is set to *sub-ring* and *node* parameter is set to *interconnection*.

Value: 1-4094

Default Value: None

erps ring *ring-name* **port0 interface** *interface-name* **rpl-role** *role*

Description: Sets the RPL role of the first ring instance's port.

Value: *owner | neighbor | none*

Default Value: none (the interface is not an end of the RPL).

erps ring *ring-name* **port1 interface** *interface-name* **rpl-role** *role*

Description: Sets the RPL role of the second ring instance's port.

Value: *owner | neighbor | none*

Default Value: none (the interface is not an end of the RPL).

erps ring *ring-name* **timers guard** *milliseconds*

Description: Sets the guard timer value.

Value: 10-2000 in steps of 10

Default Value: 500

erps ring *ring-name* **timers hold-off** *milliseconds***Description:** Sets the hold-off timer value.**Value:** 0-10000 in steps of 100**Default Value:** 0**erps ring** *ring-name* **timers wtr** *minutes***Description:** Sets the wait-to-restore timer value.**Value:** 1-12**Default Value:** 5**erps ring** *ring-name* **type** *ring-type***Description:** Sets the ring-type for this ring instance.**Value:** *major-ring* | *sub-ring***Default Value:** *major-ring***erps ring** *ring-name* **node** *node-type***Description:** Sets the node-type for this ring instance. This configuration is available only when *ring-type* parameter is set to *sub-ring*.**Value:** *interconnection* | *non-interconnection***Default Value:** *non-interconnection***erps ring** *ring-name* **parent-ring** *ring-name***Description:** Sets the parent-ring for this ring instance. This configuration is available only when *ring-type* parameter is set to *sub-ring*.**Value:** An already created ring-name.**Default Value:** None**erps ring** *ring-name* **propagate-tc****Description:** Allows the *sub-ring* instance to propagate topology changes to the *parent-ring* instance. This configuration is available only when *ring-type* parameter is set to *sub-ring*.**Value:** N/A**Default Value:** N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.
4.6	Added support for 100G interfaces.
5.6	Added sub-ring support.
5.1	Added support for 25G interfaces.

Usage Guidelines

Example:

This example shows how to create an ERPS ring instance.

```
#config
Entering configuration mode terminal
(config)#dot1q vlan 100
(config-vlan-100)# interface lag-1
(config-dot1q-interface-lag-1)# exit
(config-vlan-100)# interface ten-gigabit-ethernet-1/1/1
(config-vlan-100)#top
(config)#erps ring Foo
(erps-ring-Foo)#ring-id 10
(erps-ring-Foo)#control-vlan 100
(erps-ring-Foo)#protected-vlans 1-4,100-400,1024
(erps-ring-Foo)#r-aps-level 5
(erps-ring-Foo)#timers
(erps-ring-timers)#wtr 7
(erps-ring-timers)#guard 600
```

```
(erps-ring-timers)#hold-off 2000
(erps-ring-timers)#exit
(erps-ring-Foo)#port0 interface ten-gigabit-ethernet-1/1/1
(erps-ring-port0)#exit
(erps-ring-Foo)#port1 interface lag-1
(erps-ring-port1)#top
(config)#commit
Commit complete.
(config)#
```

Impacts and precautions

- Changes on specific configurations will cause a protocol reset for the affected rings, namely: ring ID and control VLAN. Traffic on the protected VLANs will be affected.

Considerations to prevent network loops during maintenance procedures:

- Before mounting a physical ring, please consider disabling, in the node that is going to be designated as the RPL owner node, the port that represents the RPL end point.
- To add a new protected VLAN, you must add it to the protected VLANs list of the ERPS ring before adding the ring ports to the VLAN domain (*dot1q vlan id interface name*).
- Before removing a VLAN from the ERPS list of protected VLANs, you must first remove the ring ports from that VLAN domain (*no dot1q vlan id interface name*).
- To physically add a new node in the ERPS ring, it is recommended to disable (*shutdown*) the adjacent port of the neighbors' nodes of the ring node that is being added. After making all the connections and configurations of the new ring node, enable (*no shutdown*) the adjacent ports to finish the procedure.
- To physically remove a node from the ERPS ring, it is recommended to disable (*shutdown*) the adjacent port of the neighbors' nodes of the ring node that is being removed. After the ring node removal, enable (*no shutdown*) the adjacent ports to finish the procedure.

Considerations to create a valid ERPS configuration:

- ERPS cannot be configured in a port that is member of an EAPS domain or is protected by STP.
- The minimum configuration of an ERPS ring must contain a ring-id, a control-vlan, at least one protected-vlan and two different ports (port0 and port1) as members of the ring.
- At least one of the ring member ports' rpl-role must be 'none'.
- The ports of an ERPS ring must be members, and the only members, of its control-vlan.

- A control-vlan of an ERPS ring cannot exist in the protected-vlan list of any ERPS ring or EAPS domain.
- The protected-vlan list of an ERPS ring cannot overlap the protected-vlan list of another ERPS ring or EAPS domain.
- The same protected-vlan list can be used in different ERPS rings or EAPS domains as long as the protected ports are different.

Hardware restrictions

N/A

show erps

Description

Display ERPS status information.

Supported Platforms

This command is supported in all platforms.

Syntax

show erps [brief] [detail]

Parameters

brief

Description: This parameter displays a summary information about ring instances, including name, ring ID, control VLAN, and state.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays all that the **brief** parameter displays plus a table listing the the number of protected VLANs, the ring ports, and their RPL roles. When no parameter is given the show command displays the same content of **detail** parameter.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
NAME	The name of the ring.

Output	Description
RING ID	The ring identifier.
CONTROL VLAN	The VLAN used for ERPS control packets, in this ring instance.
STATE	The current state of the ring instance. The possible states are Init, Idle, Protection, ManualSwitch, ForcedSwitch, and Pending.
PROTECTED VLANS	The number of VLANs protected by this ring instance.
PORT0	The first ring instance's port.
PORT0 RPL ROLE	The RPL role of the second ring instance's port. Possible values are <i>owner</i> , <i>neighbor</i> , and <i>none</i> .
PORT0 STATE	The state of the port. Possible values are <i>Forward</i> , <i>Blocked</i> , <i>Data Blocked</i> , <i>Control Channel Blocked</i> and <i>Unknown</i> .
PORT0 LOCAL FAILURE	Inform if the port has a local failure. Possible values are <i>Yes</i> and <i>No</i> .
PORT1	The second ring instance's port.
PORT1 RPL ROLE	The RPL role of the second ring instance's port. Possible values are <i>owner</i> , <i>neighbor</i> , and <i>none</i> .
PORT1 STATE	The state of the port. Possible values are <i>Forward</i> , <i>Blocked</i> , <i>Data Blocked</i> , <i>Control Channel Blocked</i> and <i>Unknown</i> .
PORT1 LOCAL FAILURE	Inform if the port has a local failure. Possible values are <i>Yes</i> and <i>No</i> .
Default	
N/A	

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has 5 ring instances, the **brief** status command could result in the following output:

```
# show erps brief
```

NAME	RING ID	CONTROL VLAN	STATE	PORT0 STATE	PORT1 STATE
MyRing1	1	11	Protection	Forward	Blocked
MyRing2	2	21	Idle	Forward	Blocked
MyRing3	15	151	Protection	Forward	Forward
MyRing4	15	152	Protection	Forward	Forward
MyRing5	3	31	Pending	Forward	Blocked

```
#
```

The output of a **detail** status command would look like this:

```
# show erps detail
```

NAME	RING ID	CONTROL VLAN	STATE	PROTECTED VLANs	PORT0	...
MyRing1	1	11	Protection	10	gigabit-ethernet-1/1/1	...
MyRing2	2	21	Idle	5	gigabit-ethernet-1/1/3	...
MyRing3	15	151	Protection	5	gigabit-ethernet-1/1/9	...
MyRing4	15	152	Protection	8	lag-1	...
MyRing5	3	31	Pending	20	gigabit-ethernet-1/1/5	...

PORT0 RPL ROLE	PORT0 LOCAL FAILURE	PORT0 STATE	PORT1	PORT1 RPL ROLE	PORT1 LOCAL FAILURE	PORT1 STATE
owner	Yes	Forward	gigabit-ethernet-1/1/2	none	No	Blocked
none	No	Forward	gigabit-ethernet-1/1/4	owner	No	Blocked
owner	Yes	Forward	gigabit-ethernet-1/1/10	none	No	Forward
none	No	Forward	lag-2	neighbor	Yes	Forward
none	No	Forward	gigabit-ethernet-1/1/6	none	No	Blocked

```
#
```

Impacts and precautions

None

Hardware restrictions

None

EAPS

This topic describes the commands related to management of EAPS topologies such as commands to configure the protected VLANs or to inspect the protection status.

eaps

Description

The current implementation follows the EAPS version 1.3 described as a Internet-Draft, which includes some enhancements over the EAPS version 1 described by RFC 3619.

Supported Platforms

This command is supported in all platforms.

Syntax

```
eaps domain { control-vlan vlan-id | port { primary interface-name | secondary interface-name }* | protected-vlans vlans }*  
eaps domain [name identifier]  
eaps domain {mode {transit | master}}  
eaps domain [ failtime seconds | failtime-action action-type | hellotime seconds ]*
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

eaps *domain*

Description: Domain identification

Value: 0-63

Default Value: None

control-vlan *vlan-id*

Description: Sets the VLAN used for control traffic (EAPS PDUs). This VLAN cannot be used for data traffic.

Value: 1-4094

Default Value: None

failtime *seconds*

Description: Only relevant for the Master node.
After received health check PDUs, a timer with this value is started and upon its expiration the ring will take the failtime-action. The timer is restarted on receipt of any health check PDU.

Value: 1-60

Default Value: 3

failtime-action *action-type*

Description: Only relevant for the Master node.
Use action **send-alert** to log the failure and query the link status of all Transit nodes and then force a network converge through the secondary port if some failure is reported.

Value: { send-alert }

Default Value: send-alert

hellotime *seconds*

Description: Only relevant for the Master node.
Sets the interval for transmission of health check PDUs.

Value: 1-60

Default Value: 1

mode { master | transit }

Description: Sets the EAPS mode of this ring node. A ring is allowed to have a single Master node and multiple Transit nodes.

Value: { master | transit }

Default Value: transit

name *identifier*

Description: Set a textual name for this EAPS domain, according to the network manager's choice. Valid characters are A-Z, a-z, 0-9 and + _ - "

Value: An identifier with at most 48 characters.

Default Value: None

port { **primary** *interface-name* | **secondary** *interface-name* }*

Description: Defines both primary and secondary ports of EAPS ring.

Value: NA

Default Value: NA

primary *interface-name*

Description: Sets a specific port as primary.

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, lag.**

Default Value: None

secondary *interface-name*

Description: Sets a specific port as secondary

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, lag.**

Default Value: None

protected-vlans *vlans*

Description: Sets the list of protected VLANs of this EAPS domain. Ranges of VLANs or single VLAN are allowed and can be combined to specify the set of protected VLANs

Value: 1-4094
Example: **protected-vlans 1-3,5,7-9**

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced
3.0	Added support on 40G interfaces
4.6	Added support on 100G interfaces
5.0	Added support on 25G interfaces

Usage Guidelines

Example:

This example shows how to create an EAPS master domain.

```
#config
Entering configuration mode terminal
(config)#dot1q vlan 100
(config-vlan-100)# interface lag-1
(config-dot1q-interface-lag-1)# exit
(config-vlan-100)# interface ten-gigabit-ethernet-1/1/1
(config-vlan-100)#top
(config)#eaps 0
(config-eaps-1)#control-vlan 100
(config-eaps-1)#mode master
(config-eaps-1)#protected-vlans 1-4,100-400,1024
(config-eaps-1)#port
(config-eaps-1-port)#primary ten-gigabit-ethernet-1/1/1
(config-eaps-1-port)#secondary lag-1
(config-eaps-1)#top
(config)#commit
Commit complete.
(config)#
```

Impacts and precautions

- Changes on specific configurations will cause a protocol reset for the affected domains, namely: primary or secondary **port**, **control-vlan** and **mode**. Traffic on the protected VLANs will be affected.

Considerations to prevent network loops during maintenance procedures:

- Before mounting a physical ring, please consider disabling the secondary port of the Master node.
- To add a new protected VLAN, you must add it to the protected VLAN list of the EAPS domain before adding the ring ports to the VLAN domain (*dot1q vlan id interface name*).
- Before removing a VLAN from the EAPS list of protected VLANs, you must first remove the ring ports from that VLAN domain (*no dot1q vlan id interface name*).
- To physically add a new node in the EAPS ring, it is recommended to disable (*shutdown*) the adjacent port of the neighbors nodes of the ring node that is being added. After making all the connections and configurations of the new ring node, enable (*no shutdown*) the adjacent ports to finish the procedure.
- To physically remove a node from the EAPS ring, it is recommended to disable (*shutdown*) the adjacent port of the neighbors nodes of the ring node that is being removed. After the ring node removal, enable (*no shutdown*) the adjacent ports to finish the procedure.

Hardware restrictions

N/A

show eaps

Description

Display information about EAPS status and statistics.

Supported Platforms

This command is supported in all platforms.

Syntax

show eaps [brief] [detail]

Parameters

brief

Description: This parameter displays a summary information about the domains, including domain's ID, name, state, mode and status of both primary and secondary ports.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays all that the **brief** parameter displays plus a table listing the protected VLANs and both the primary and secondary ports. When no parameter is given the show command displays the same content of **detail** parameter.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
ID	The ID number of the domain.
Name	The name of the domain.
State	The current state of the domain. The possible states are Idle, Init, Complete, Failed, Pre Forwarding, Links Down and Links Up.
Primary port state	The state of the domain's primary port, where Up and Down refer to port link status and Enable and Blocked refer to the port traffic block state.
Secondary port state	The state of the domain's secondary port, where Up and Down refer to port link status and Enable and Blocked refer to the port traffic block state.
Primary port	The primary port configured in the domain.
Secondary port	The secondary port configured in the domain.
Protected VLANs	The list of protected VLANs configured in the domain.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has the domains 0, 1, 2, 3, 4, 5 and 63 created, let's see the **brief** information:

```
# show eaps brief
```

ID	NAME	STATE	MODE	PRIMARY PORT STATE	SECONDARY PORT STATE
0	My-Eaps-Domain-0	Idle	transit	Down Blocked	Down Blocked
1	My-Eaps-Domain-1	Init	master	Up Enabled	Up Blocked
2	My-Eaps-Domain-2	Complete	master	Up Enabled	Up Blocked
3	My-Eaps-Domain-3	Failed	master	Down Enabled	Up Blocked
4	My-Eaps-Domain-4	Pre Forwarding	transit	Up Enabled	Up Blocked
5	My-Eaps-Domain-5	Links Down	transit	Up Enabled	Down Blocked
63	My-Eaps-Domain-63	Links Up	transit	Up Enabled	Up Enabled

```
#
```

Now let's see the detailed information:

```
# show eaps detail
```

ID	NAME	STATE	MODE	PRIMARY PORT STATE	SECONDARY PORT STATE
0	My-Eaps-Domain-0	Idle	transit	Down Blocked	Down Blocked
1	My-Eaps-Domain-1	Init	master	Up Enabled	Up Blocked
2	My-Eaps-Domain-2	Complete	master	Up Enabled	Up Blocked
3	My-Eaps-Domain-3	Failed	master	Down Enabled	Up Blocked
4	My-Eaps-Domain-4	Pre Forwarding	transit	Up Enabled	Up Blocked
5	My-Eaps-Domain-5	Links Down	transit	Up Enabled	Down Blocked
63	My-Eaps-Domain-63	Links Up	transit	Up Enabled	Up Enabled

ID	PRIMARY PORT	SECONDARY PORT	PROTECTED VLANS
0	ten-gigabit-ethernet-1/1/1	gigabit-ethernet-1/1/1	10,20,30
1	ten-gigabit-ethernet-1/1/2	gigabit-ethernet-1/1/2	31-35,39
2	ten-gigabit-ethernet-1/1/3	gigabit-ethernet-1/1/3	40
3	ten-gigabit-ethernet-1/1/4	gigabit-ethernet-1/1/4	45-50
4	ten-gigabit-ethernet-1/1/5	gigabit-ethernet-1/1/5	51-55,60-65
5	ten-gigabit-ethernet-1/1/6	gigabit-ethernet-1/1/6	70,75
63	ten-gigabit-ethernet-1/1/7	gigabit-ethernet-1/1/7	100,105-110

```
#
```

Impacts and precautions

None

Hardware restrictions

None

CONTROL PROTOCOLS

This topic describes the commands related to management of control protocol such as commands to enable PDU tunnel, drop, peer and forward of some specific protocol.

layer2-control-protocol interface protocols action action-type

Description

Allows actions for L2 control protocols (PDUs) received by an interface.

The action tunnel is based on destination MAC address modification for protocol packets. PDUs received on a port that has tunneling enabled will have their destination address changed to another address. With that destination address the packets will be transparently forwarded (flooded) through the network until some other port with tunneling enabled is reached. You must use this command on access ports that will convert protocol packets into tunneled packets and/or convert tunneled packets into protocol packets. The intermediate ports on the tunneling path must not have this command enabled so that they will only forward tunneled packets without modifications.

If no action is specified for an interface, the PDUs will be dropped, forwarded or treated according with the protocol standards.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
layer2-control-protocol { interface interface-name [ protocols { action action-type } ] }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Interface to be configured.

Value: { gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id }

Default Value: None

protocols

Description: Protocol or group of protocols.
The value *extended* configures the following group of protocols: IEEE, Cisco, EAPS and RRPP.
Other protocols can be configured with its respective name and they take precedence over the extended tunneling.

Value: { extended | lacp | marker | oam | stp | pvst | lldp | pagp | udd | cdp | vtp | eaps | erps | gvrp | dot1x }

Default Value: None

action *action-type*

Description: PDU packet action.
The value *tunnel* configures Layer 2 protocols tunneling for Ethernet interfaces. The value *forward* is only available for *extended* protocols and configures Layer 2 protocols to be switched transparently for Ethernet interfaces.

Value: { tunnel | forward }

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
4.7	Added support for new protocols tunneling.
4.9	Added support for LLDP tunneling and action Forward for extended tunneling.
5.0	Added support for 25G interfaces.
5.2	Added support for tunneling protocols PAGP, UDLD, CDP and VTP.
5.4	Added support for tunneling protocols EAPS, ERPS, GVRP and Dot1x.

Usage Guidelines

To configure protocols to tunnel:

```
(config)# layer2-control-protocol
(l2cp)# interface gigabit-ethernet-1/1/1
(l2cp-interface-gigabit-ethernet-1/1/1)# extended action tunnel
(l2cp-interface-gigabit-ethernet-1/1/1)# lacp action tunnel
(l2cp-interface-gigabit-ethernet-1/1/1)# stp action tunnel
```

To remove protocol configuration:

```
(config)# layer2-control-protocol
(l2cp)# interface gigabit-ethernet-1/1/1
(l2cp-interface-gigabit-ethernet-1/1/1)# no extended
(l2cp-interface-gigabit-ethernet-1/1/1)# no stp
```

Impacts and precautions

When action parameter is configured as tunnel, the equipment will not be in accordance with the “Frame Filtering” section from IEEE 802.1Q standard.

Features such as STP, EAPS and others that have their controls protocols packets impacted will not work together with action tunnel.

ACL action “deny” does not affect tunneled packets.

When enabling Protocol tunnelings for an access interface, it is recommended to configure the same tunneling modes for all access interfaces within the same VLAN.

Hardware restrictions

N/A

layer2-control-protocol tunnel-mac

Description

Allows to set the destination MAC address for tunneled packets on modes *LACP*, *Marker*, *OAM* and *STP*.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

layer2-control-protocol tunnel-mac *mac*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

tunnel-mac *mac*

Description:	Set destination MAC Address for per-protocol tunneled packets.
Value:	{ datacom interop }
Default Value:	datacom

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.7	This command was introduced.
-----	------------------------------

Usage Guidelines

To configure the destination MAC address for tunneled packets:

```
(config)# layer2-control-protocol
```

```
(l2cp)# tunnel-mac interop
```

To reset the configuration to default:

```
(config)# layer2-control-protocol
```

```
(l2cp)# no tunnel-mac
```

Impacts and precautions

N/A

Hardware restrictions

N/A

layer2-control-protocol tunnel-priority

Description

Allows to set the PCP (802.1p) and QoS Scheduler Queue for tunneled packets.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

layer2-control-protocol tunnel-priority *priority*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

tunnel-priority *priority*

Description:	Set PCP (802.1p) and QoS Scheduler Queue for tunneled packets.
Value:	{ 0-7 }
Default Value:	None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.

Usage Guidelines

To configure priority for tunneled packets:

```
(config)# layer2-control-protocol
```

```
(l2cp)# tunnel-priority 7
```

To remove configuration:

```
(config)# layer2-control-protocol
```

```
(l2cp)# no tunnel-priority
```

Impacts and precautions

The tunnel-priority takes precedence over the priority from ACL action “set pcp”.

Hardware restrictions

N/A

layer2-control-protocol vlan protocols action action-type

Description

Command used to configure PDU on preexisting VLAN configured with service/VLAN TLS.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

layer2-control-protocol { **vlan** *vlan-id* [*protocols* { **action** *action-type* }] }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: VLAN ID to be configured.

Value: 1 - 4094

Default Value: None

protocols

Description: Protocol or group of protocols.
The value *extended* configures the following group of protocols: IEEE, Cisco, EAPS and RRPP.

Value: extended

Default Value: None

action *action-type*

Description: PDU packet action.
The value *drop* discards the packet.
The value *forward* sends the packet without any change.

Value: {drop | forward}

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
4.2	This command was deprecated. From this version on, all service VLAN TLS have forward action by default.

Usage Guidelines

VLAN must be created and configured as service/VLAN TLS to use this functionality. The commit of a configuration with a PDU action (drop or forward) with a non existing VLAN or with a VLAN not configured properly (without service/VLAN TLS configuration) will result in an error message and the configuration will not be applied. This command supports up to 186 actions, however it depends on platform and services configured.

To configure extended protocols to forward:

```
(config)# layer2-control-protocol
```

```
(l2cp)# vlan 100
```

```
(l2cp-vlan-100)# extended action forward
```

To configure extended protocols to drop:

```
(config)# layer2-control-protocol
```

```
(l2cp)# vlan 100
(l2cp-vlan-100)# extended action drop
```

To remove configuration:

```
(config)# layer2-control-protocol
(l2cp)# no vlan 100
```

Impacts and precautions

When action parameter is configured as forward (transparent), the equipment will not be in accordance with the “Frame Filtering” section from IEEE 802.1Q standard.

Hardware restrictions

N/A

LOOPBACK DETECTION

This topic describes the commands related to loopback detection.

loopback-detection

Description

Enable Loopback Detection

Supported Platforms

This command is supported in all platforms.

Syntax

loopback-detection destination-address *address* **interface** *interface-name* **timer** *time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

destination-address *address*

- Description:** Destination MAC address to be used on Loopback Detection frames.
- Value:** *alternative* is the only value currently supported. It means that the alternative MAC address of slow protocols (01:04:DF:10:00:02) will be used.
- Default Value:** *alternative*

interface *interface-name*

- Description:** Ethernet interface where Loopback Detection is being enabled.
- Value:** *interface-type-chassis/slot/port*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.
- Default Value:** N/A

timer *time*

Description: Set the time interval to be waited before unblock the interface.

Value: 2-86400 seconds

Default Value: 30 seconds

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.7	This command was introduced.
-----	------------------------------

5.10	Added support for 25G interfaces.
------	-----------------------------------

Usage Guidelines

The Loopback Detection can be enabled on Ethernet interfaces to detect loop failures caused by RX/TX fiber loop or loops in neighbor networks.

```
# config
(config)# loopback-detection interface gigabit-ethernet-1/1/1
(config-lbd-interface-gigabit-ethernet-1/1/1)# timer 30
(config-lbd-interface-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-lbd-interface-gigabit-ethernet-1/1/1)# end
#
```

One-line like command is also supported.

```
# config
(config)# loopback-detection interface ten-gigabit-ethernet-1/1/1 timer 45
```

```
(config-lbd-interface-ten-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-lbd-interface-ten-gigabit-ethernet-1/1/1)# end
#
```

Impacts and precautions

- Loopback Detection is not supported on interfaces added as members of a Link Aggregation Group (LAG) or LAG interfaces themselves. In this case LACP can be used to prevent loops.

Hardware restrictions

N/A

show loopback detection

Description

Display information about Loopback Detection status and configuration. This show only present ports that are configured for Loopback Detection.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show loopback-detection [ { port | all } ] [ loopback ] [ timeout ] [ unblock-time ]
```

Parameters

port

Description: The Interface with Loopback Detection whose status is desired to show.

Value: N/A

Default Value: N/A

all

Description: Shows the Loopback Detection status for *all* enabled interfaces.

Value: N/A

Default Value: N/A

loopback

Description: Shows only the Loopback Detection status for the desired port.

Value: N/A

Default Value: N/A

timeout

Description: Shows only the time that the port still needs to wait in non-loop status to unblock.

Value: N/A

Default Value: N/A

unblock-time

Description: Shows only the configured time to unblock a port after the loop state clearance.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
INTERFACE	The Interface that is configured for Loopback Detection.
UNBLOCK TIME	The configured time to unblock a port after the loop state clearance.
TIMEOUT	The time that the port still needs to wait in non-loop status to unblock.
LOOPBACK	The status of loopback detection for the port. Can be YES for looped, or NO for non-loop.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.7	This command was introduced.
5.10	Added support for 25G interfaces.

Usage Guidelines

Given the equipment has the following ports configured for Loopback detection.

```
# show running-config loopback-detection
loopback-detection
destination-address alternative
interface ten-gigabit-ethernet-1/1/1
timer 10
!
```

A show will present:

```
# show loopback-detection
                                UNBLOCK
INTERFACE-----TIME-----TIMEOUT  LOOPBACK
ten-gigabit-ethernet-1/1/1  10       3       yes
#
```

Impacts and precautions

None

Hardware restrictions

None

LINK FLAP DETECTION

This topic describes the commands related to link flap detection.

link-flap

Description

Configure Link Flap Detection

Supported Platforms

This command is supported in all platforms.

Syntax

link-flap interface *interface-name* **detection transitions** *value* **interval** *time* **restore-timeout** *time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Ethernet interface where Link Flap Detection is being enabled.

Value: *interface-type-chassis/slot/port*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.

Default Value: N/A

detection transitions *value*

Description: Set the transitions to be detected during the interval before blocking the interface.

Value: 2-100 transitions

Default Value: 10 transitions.

detection interval *time*

Description: Set the time interval to monitor the transitions of interface link state after the first one.

Value: 1-3600 seconds

Default Value: 40 seconds.

detection restore-timeout *time*

Description: Set the time interval without new transitions to wait before restoring the interface to the previous state.

Value: 1-86400 seconds

Default Value: 30 seconds.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

4.7	This command was introduced.
-----	------------------------------

5.10	Added support for 25G interfaces.
------	-----------------------------------

Usage Guidelines

The Link Flap Detection can be enabled on Ethernet interfaces to avoid link status propagation on unstable links.

```
# config
(config)# link-flap interface gigabit-ethernet-1/1/1
```

```
(config-lfd-interface-gigabit-ethernet-1/1/1)# detection transitions 4
(config-lfd-interface-gigabit-ethernet-1/1/1)# detection interval 20
(config-lfd-interface-gigabit-ethernet-1/1/1)# detection restore-timeout 60
(config-lfd-interface-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-lfd-interface-gigabit-ethernet-1/1/1)# end
#
```

One-line like command is also supported .

```
# config
(config)# link-flap interface gigabit-ethernet-1/1/1 detection transitions 4 detection
interval 20 detection restore-timeout 60
(config-lfd-interface-ten-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-lfd-interface-ten-gigabit-ethernet-1/1/1)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show link-flap

Description

Displays information about Link Flap Detection status and configuration. This command only shows interfaces that are configured for Link Flap Detection.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show link-flap [ { interface | all } ] [ config-interval ] [ config-restore-timeout ] [ config-transitions ] [ detected-transitions ] [ detection-timeout ] [ link-flap ] [ restore-timeout ]
```

Parameters

interface

Description:	The interface whose Link Flap Detection status should be shown.
Value:	N/A
Default Value:	N/A

all

Description:	Shows the Link Flap Detection status for <i>all</i> enabled interfaces.
Value:	N/A
Default Value:	N/A

config-interval

Description:	Shows the configured detection time interval for the specified interface.
Value:	N/A
Default Value:	N/A

config-restore-timeout

Description: Shows the configured restore time interval for the specified interface.

Value: N/A

Default Value: N/A

config-transitions

Description: Shows the configured number of transitions to be detected before blocking the specified interface.

Value: N/A

Default Value: N/A

detected-transitions

Description: Shows the number of transitions detected for the specified interface.

Value: N/A

Default Value: N/A

detection-timeout

Description: Show the remaining time before resetting the transitions counter if the specified interface does not enter link flap state.

Value: N/A

Default Value: N/A

link-flap

Description: Shows the Link Flap Detection state for the specified interface.

Value: N/A

Default Value: N/A

restore-timeout

Description: Shows the remaining time without transitions before unblocking the specified interface.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Interface	The interface that is configured for Link Flap Detection.
Configured Transitions	The configured number of transitions to be detected before blocking the interface.
Configured Interval	The configured detection time interval.
Configured restore timeout	The configured restore timeout.
Detected Transitions	The number of transitions detected.
Detection Timeout	Remaining time before resetting the transitions counter if the interface does not enter link flap state.
Restore Timeout	Remaining time without transitions before unblocking the interface.
Link Flap	The Link Flap Detection state.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has the following interface configured for Link Flap Detection.

```
# show running-config link-flap
link-flap
interface ten-gigabit-ethernet-1/1/1
  detection transitions 5
  detection interval 25
  detection restore-timeout 65
!
```

A show command will display the following information:

```
# show link-flap
```

Interface	Configured Transitions	Configured Interval	Configured Restore Timeout	
ten-gigabit-ethernet-1/1/1	5	25	65	...

Detected Transitions	Detection Timeout	Restore Timeout	Link Flap
0	0	0	no

Impacts and precautions

None

Hardware restrictions

None

HOLD TIME

This topic describes the commands related to hold time feature.

hold-time

Description

Configure a delay for processing a link event on a interface.

Supported Platforms

This command is supported in all platforms.

Syntax

hold-time interface *interface-name* **down** *time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description:	Ethernet interface where hold-time is being enabled.
Value:	<i>interface-type-chassis/slot/port</i> Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.
Default Value:	N/A

down *time*

Description:	Delay for processing a link down event on an interface. When a link down happens, a timer will be started. If the timer expires, the link down will be notified. If a link up happens before it expires, the timer is reset. The administrative shutdown of a interface may be affected by this configuration, therefore a “no shutdown” may prevent a link down notification if executed before the timer expiring.
Value:	50-5000 milliseconds in steps of 50 milliseconds.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.10	This command was introduced.
------	------------------------------

Usage Guidelines

The hold-time configuration can be enabled on Ethernet interfaces to delay the link down processing.

```
# config
(config)# hold-time interface gigabit-ethernet-1/1/1
(config-interface-gigabit-ethernet-1/1/1)# down 500
(config-interface-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-interface-gigabit-ethernet-1/1/1)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

BACKUP LINK

This topic describes the commands related to backup link protection.

backup-link

Description

Create an alternative interface to the main interface (Backup-Link pair). That is, in case of link problems (link down, blocked due to link-flap detection, EFM, loopback detection, etc.) in the main interface, the backup interface takes its place, preventing packet loss. The main interface assumes again when a link problem occurs with the backup interface (and the state of the main interface link is up) or when the revertive mode is configured. The Backup-Link can be configured on ethernet and LAG interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

backup-link *id* {**main** *interface-name*} {**backup** *interface-name*} [**action** {**block** | **shutdown**}] [**reversion** [**mode** {**revertive** | **non-revertive**}] [**delay** *time*]] [**description** *text*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

id

Description: Unique identification number of the Backup-Link pair.

Value: 0 - 65535

Default Value: N/A

main *interface-name*

Description: Main ethernet or LAG interface where Backup-Link is being enabled.

Value: Name of the interface.

Default Value: N/A

backup *interface-name*

Description: Backup ethernet or LAG interface where Backup-Link is being enabled.

Value: Name of the interface.

Default Value: N/A

action {**block** | **shutdown**}

Description: Configuration of the link state of the Backup-Link pair interfaces. On block mode operation, when one or both interfaces have the link up, the other must be blocked, and, when both are down, both must be blocked. On shutdown mode operation, when one or both interfaces have the link up, the other must be administratively down, and, when both are down, both must be administratively down. With shutdown action, it's not possible to configure the **revertive** mode.

Value: List of supported actions: **block** and **shutdown**.

Default Value: block.

reversion mode {**revertive** | **non-revertive**}

Description: With the link status in **block**, it's possible to configure the automatic reversion to the main interface. That is, when setting the mode to revertive, if a link problem occurs to the main interface and the backup interface takes its place, the main, when fully recovered, will assume again automatically after the configured delay. In non-revertive mode, the main interface will only assume again if the backup interface link goes down. Reversion is not supported with **shutdown** action.

Value: List of supported reversion modes: **revertive** and **non-revertive**.

Default Value: non-revertive.

reversion delay *time*

Description: When in **revertive** mode, set the delay interval before reactivating the main interface. After the delay ends and the main interface link is up, the Backup-Link interfaces are switched back.

Value: 1 - 300 seconds.

Default Value: 35 seconds.

description *text*

Description: Optional description of the Backup-Link pair.

Value: String with a maximum of 128 characters. It only accepts alphanumeric characters and '*', '@', '/', '_', '.', '+' and '-'.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

6.2	This command was introduced.
-----	------------------------------

Usage Guidelines

The following example shows how to create a Backup-Link pair with non-revertive block configuration.

```
# config
(config)# backup-link 1
(config-backup-link-1)# main gigabit-ethernet-1/1/1
(config-backup-link-1)# backup gigabit-ethernet-1/1/2
(config-backup-link-1)# commit
Commit complete.
(config-backup-link-1)#
```

The following example shows how to create a Backup-Link pair with revertive block configuration and delay of 30 seconds.

```
# config
(config)# backup-link 2
(config-backup-link-2)# main ten-gigabit-ethernet-1/1/1
(config-backup-link-2)# backup ten-gigabit-ethernet-1/1/2
(config-backup-link-2)# action block
(config-backup-link-2)# reversion mode revertive
(config-backup-link-2)# reversion delay 30
(config-backup-link-2)# commit
Commit complete.
(config-backup-link-2)#
```

The following example shows how to create a Backup-Link pair with shutdown configuration.

```
# config
(config)# backup-link 3
(config-backup-link-3)# main lag-1
(config-backup-link-3)# backup lag-2
(config-backup-link-3)# action shutdown
(config-backup-link-3)# commit
Commit complete.
(config-backup-link-3)#
```

Impacts and precautions

None.

Hardware restrictions

None.

CHAPTER 6: LAYER 3 - ROUTING

This chapter describes the commands related to management of Layer 3 protocols in the DmOS CLI.

BASIC

This topic describes the commands related to management of basic routing such as commands to configure the ARP behavior or Static Routes.

clear ip host-table

Description

Clears the neighbor cache table of the system.

Supported Platforms

This command is supported in all platforms.

Syntax

clear ip host-table [**intf** *l3-if*]

clear ip host-table [**vrf** {*vrf-name* | **all**} | **ip-address** *a.b.c.d* | **port** *port-if*]*

Parameters

ip-address *a.b.c.d*

Description: Clear host with specified IPv4 address from system ARP cache.

Value: a.b.c.d.

Default Value: N/A

intf *l3-if*

Description: Clear all hosts with specified L3 interface from system ARP cache.

Value: Name of L3 interface.

Default Value: N/A

port *port-if*

Description: Clear all hosts with specified physical port interface from system ARP cache.

Value: Name of physical port.

Default Value: N/A

vrf *vrf-name*

Description: Clear all hosts with specified VRF name from system ARP cache. When no VRF is specified, the clear will be performed on the global VRF.

Value: Name of the VRF.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10.0	This command was introduced.
4.4	VRF parameter support.

Usage Guidelines

Clearing the neighbor cache table of the system forces the deletion of all dynamically learned entries, except those that are next-hop. Next-hop entries will be probed and refreshed. After executing this command it is possible to ensure the correct mapping between learned IP addresses with their corresponding MAC addresses.

This command clears IPv4 and IPv6 hosts, but the ip-address parameter only accepts IPv4 addresses at the moment.

Impacts and precautions

Clearing hosts may cause temporary traffic disruption.

Hardware restrictions

N/A

ip arp aging-time

Description

Configures aging-time for ARP entries

Supported Platforms

This command is supported in all platforms.

Syntax

ip arp aging-time *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

value

Description:	Specifies the time in seconds that an ARP entry stays in cache.
Value:	200-10000000.
Default Value:	3600.

Default

Aging-time of 3600 seconds.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.10.0	This command was introduced.
--------	------------------------------

Usage Guidelines

The aging-time ensures that the ARP cache does not retain learned entries that are no longer used.

To configure ARP aging-time the following command can be used:

Example:

```
DM4610(config)# ip arp aging-time 500
```

If 'no' command is used, the default value is applied:

```
DM4610(config)# no ip arp aging-time
```

Impacts and precautions

For longer aging-time periods, the ARP cache can retain entries that are no longer used. And as you reduce the ARP timeout, your network resolution traffic can increase. The general recommended value for aging-time is the configured default value, which is 1 hour (3600 seconds).

Hardware restrictions

N/A

prefix-list

Description

Prefix list configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

prefix-list *name* **seq** *seq-number* **action** { **permit** | **deny** } [**address** *prefix*] [**le** *prefix-len*] [**ge** *prefix-len*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

prefix-list *name*

Description: Creates a prefix list with the given *name*.

Value: N/A

Default Value: N/A

seq *seq-number*

Description: Apply the sequence number to the prefix list entry.

Value: 1-4294967295.

Default Value: N/A

action

Description: The **action permit** allows a matched prefix. The **action deny** denies a matched prefix.

Value: permit - deny.

Default Value: permit.

address *prefix*

Description: A unicast IP/IPv6 prefix/mask format.

Value: <a.b.c.d/x> or <x:x:x:x::x/x>.

Default Value: N/A

le prefix-len

Description: The maximum prefix length to match.

Value: 1-128.

Default Value: N/A

ge prefix-len

Description: The minimum prefix length to match.

Value: 1-128.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

4.6	This command was introduced.
-----	------------------------------

4.8	Added support to IPv6.
-----	------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a prefix list that only permits the network address 50.50.50.0/24.

```
(config)# prefix-list TEST
(config-prefix-list-TEST)# seq 10
(config-seq-10)# address 50.50.50.0/24
(config-seq-10)# commit
Commit complete.
```

This example shows how to configure a prefix list which allows both prefixes 60.60.60.0/24 and 60.60.60.0/25.

```
(config)# prefix-list TEST_RANGE
(config-prefix-list-TEST_RANGE)# seq 20
(config-seq-20)# address 60.60.60.0/24 ge 24 le 25
(config-seq-20)# commit
Commit complete.
```

This example shows how to configure a prefix list that denies the network address 60.60.60.0/24 but allows the others.

```
(config)# prefix-list TEST_DENY
(config-prefix-list-TEST_DENY)# seq 20
(config-seq-20)# action deny
(config-seq-20)# address 60.60.60.0/24
(config-seq-20)# exit
(config-prefix-list-TEST_DENY)# seq 30
(config-seq-30)# address 0.0.0.0/0 le 32
(config-seq-30)# commit
Commit complete.
```

This example shows how to configure a prefix list that denies the network address 2001::/64 but allows the others.

```
(config)# prefix-list TEST_DENY
(config-prefix-list-TEST_DENY)# seq 20
(config-seq-20)# action deny
(config-seq-20)# address 2001::/64
(config-seq-20)# exit
(config-prefix-list-TEST_DENY)# seq 30
(config-seq-30)# address ::/0 le 128
(config-seq-30)# commit
Commit complete.
```

Impacts and precautions

When the prefix list is associated with a route map the permit or deny action configuration of the prefix list entry is ignored.

In case of prefix list directly associated with a BGP neighbor and no permit action matches are found, all routes will be denied. Therefore, it is necessary to add an additional sequence with a clause to permit the other routes by setting a matching all address (0.0.0.0/0 le 32).

Notice that a route policy associated with a neighbor have precedence over a prefix list directly associated with it.

If there is no route refresh capability support any update on the prefix list configuration that is associated with a BGP neighbor will cause its BGP session to be restarted.

Updates on prefix-lists associated with a neighbor or with a route map will trigger either route-refresh or update messages. Route-refresh messages request to the neighbor the sending of all its prefixes. Differently from a route-refresh message the sending of update messages is an optimization because only the prefixes not included on the previous BGP update will be advertised.

Hardware restrictions

N/A

router static address-family ipv4

Description

Configures an IPv4 static route.

Supported Platforms

This command is supported in all platforms.

Syntax

```
router static [ vrf vrf-name ] address-family ipv4 a.b.c.d/x { { next-hop a.b.c.d  
[administrative-distance distance] [administrative-status status] [interface interface-  
name] } | { black-hole } }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF this IPv4 route will be associated with.

Value: N/A

Default Value: N/A

a.b.c.d/x

Description: Specifies the IPv4 network address for the destination.

Value: Must be a valid IPv4 network address and prefix length.

Default Value: N/A

next-hop *a.b.c.d*

Description: Specifies the IPv4 address of the next hop for this static route.

Value: Must be a valid IPv4 address.

Default Value: N/A

administrative-distance *distance*

Description: Specifies the administrative distance for the static route.

Value: 1-255.

Default Value: 1.

administrative-status *status*

Description: Activates (up) or deactivates (down) the static route.

Value: {*up* | *down*}.

Default Value: *up*.

interface *interface-name*

Description: Specifies the L3 interface to be used as output interface for the static route.

Value: Must be a valid L3 interface name.

Default Value: N/A

black-hole

Description: Specifies that all traffic to IPv4 network address must be discarded.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced supporting only IPv4 routes
2.4	This command was changed to support IPv6, VRF and output interface.
3.0	This command was changed to support administrative distance.
5.4	Added support for black-hole.

Usage Guidelines

Currently are supported up to 1000 IPv4 static routes. If IPv6 static routes are configured, the following constraint must be considered:

$$(\text{number of IPv6 static routes} \times 2) + \text{number of IPv4 routes} \leq 1000$$

Example:

This example shows how to configure an IPv4 static route.

```
(config)# router static address-family ipv4
(config-static-ipv4)# 203.0.113.0/24 next-hop 198.51.100.254
(config-static-ipv4-203.0.113.0/24-198.51.100.254)# commit
Commit complete.
```

Example:

This example shows how to configure an IPv4 static route in VRF *green*.

```
(config)# router static vrf green address-family ipv4
(config-static-vrf-ipv4)# 203.0.113.0/24 next-hop 198.51.100.254
(config-static-vrf-ipv4-203.0.113.0/24-198.51.100.254)# commit
Commit complete.
```

Example:

This example shows how to configure an IPv4 static route with administrative distance.

```
(config)# router static address-family ipv4
(config-static-ipv4)# 203.0.113.0/24 next-hop 198.51.100.254
(config-static-ipv4-203.0.113.0/24-198.51.100.254)# administrative-distance 2
```

```
(config-static-ipv4-203.0.113.0/24-198.51.100.254)# commit  
Commit complete.
```

Example:

This example shows how to configure an IPv4 static route with black-hole.

```
(config)# router static address-family ipv4  
(config-static-ipv4)# 203.0.113.0/24 black-hole  
(config-static-ipv4-203.0.113.0/24-black-hole)# commit  
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

Some platforms may have VRF restrictions, only supporting 'global' and 'mgmt' VRFs.

router static address-family ipv6

Description

Configures an IPv6 static route.

Supported Platforms

This command is supported in all platforms.

Syntax

router static [**vrf** *vrf-name*] **address-family ipv6** *x:x:x:x::x/y* { { **next-hop** *x:x:x:x::x* [**administrative-distance** *distance*] [**administrative-status** *status*] [**interface** *interface-name*] } | { **black-hole** } }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF this IPv6 route will be associated with.

Value: N/A

Default Value: N/A

x:x:x:x::x/y

Description: Specifies the IPv6 network address for the destination.

Value: Must be a valid IPv6 network address and prefix length.

Default Value: N/A

next-hop *x:x:x:x::x*

Description: Specifies the IPv6 address of the next hop for this static route.

Value: Must be a valid IPv6 address.

Default Value: N/A

administrative-distance *distance*

Description: Specifies the administrative distance for the static route.

Value: 1-255.

Default Value: 1.

administrative-status *status*

Description: Activates (up) or deactivates (down) the static route.

Value: {*up* | *down*}.

Default Value: *up*.

interface *interface-name*

Description: Specifies the L3 interface to be used as output interface for the static route.

Value: Must be a valid L3 interface name.

Default Value: N/A

black-hole

Description: Specifies that all traffic to IPv6 network address must be discarded.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
3.0	This command was changed to support administrative distance.
5.4	Added support for black-hole.
6.0	Introduced VRF support.

Usage Guidelines

Currently are supported up to 500 IPv6 static routes. If IPv4 static routes are configured, the following constraint must be considered:

$$(\text{number of IPv6 static routes} \times 2) + \text{number of IPv4 routes} \leq 1000$$

Example:

This example shows how to configure an IPv6 static route.

```
(config)# router static address-family ipv6
(config-static-ipv6)# 2001:db8::/64 next-hop 2001:db8:1::1
(config-static-ipv6-2001:db8::/64-2001:db8:1::1)# commit
Commit complete.
```

Example:

This example shows how to configure an IPv6 static route in VRF *green*.

```
(config)# router static vrf green address-family ipv6
(config-static-vrf-ipv6)# 2001:db8::/64 next-hop 2001:db8:1::1
(config-static-vrf-ipv6-2001:db8::/64-2001:db8:1::1)# commit
Commit complete.
```

Example:

This example shows how to configure an IPv6 static route with administrative distance.

```
(config)# router static address-family ipv6
(config-static-ipv6)# 2001:db8::/64 next-hop 2001:db8:1::1
(config-static-ipv6-2001:db8::/64-2001:db8:1::1)# administrative-distance 2
```

```
(config-static-ipv6-2001:db8::/64-2001:db8:1::1)# commit  
Commit complete.
```

Example:

This example shows how to configure an IPv6 static route with black-hole.

```
(config)# router static address-family ipv6  
(config-static-ipv6)# 2001:db8::/64 black-hole  
(config-static-ipv6-2001:db8::/64-black-hole)# commit  
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

Some platforms may have VRF restrictions, only supporting 'global' and 'mgmt' VRFs.

show ip fib

Description

Displays IPv4 route information from Forwarding Information Base (FIB).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip fib [ vrf { vrf-name | all } ] { brief } [ network ip-address | state route-state ]
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information.

Default Value: N/A

brief

Description: Displays brief information about IPv4 route from FIB.

Value: N/A

Default Value: N/A

network *ip-address*

Description: IPv4 address and mask network used to filter the output.

Value: a.b.c.d/x

Default Value: N/A

state *route-state*

Description: Route state used to filter the output.

Value: active | inactive | pending

Default Value: N/A

Output Terms

Output	Description
VRF-name	Display the VRF name associated with the IPv4 route.
Network	Display the destination IPv4 address and mask of the remote network.
Next-hop	Display the IPv4 address of the next router to the remote network.
Logical-interface	Display the output logical interface to reach the remote network, or display <code>black-hole</code> for routes that discard traffic.
State	Display the route state. The active state represents installed routes, the inactive state represents unsupported routes that will not be installed and the pending state represents valid routes currently not installed due to a hardware limitation.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

3.0	This command was introduced.
4.0	Route state 'inactive' created.
4.6	Filter by VRF changed.
5.4	Black-hole route support was added.

Usage Guidelines

To simply show IPv4 FIB information, the following command can be used:

Example:

```
# show ip fib brief
VRF-name  Network      Next-hop    Logical-interface  State
-----
global    10.1.30.0/24    10.1.30.10  13-vlan 30        active
global    10.1.40.0/24    10.1.40.10  13-vlan 40        inactive
global    10.1.100.0/24   10.1.100.10 13-vlan 100       pending
global    10.1.200.0/24   10.1.200.10 13-vlan 200       active
global    10.1.201.0/24   0.0.0.0     black-hole        active
```

It is possible to filter the output by Network, State and VRF.

Filter by Network:

Example:

```
# show ip fib brief network 10.1.100.0/24
VRF-name  Network      Next-hop    Logical-interface  State
-----
global    10.1.100.0/24 10.1.100.10 13-vlan 100       pending
```

Filter by State:

Example:

```
# show ip fib brief state pending
VRF-name  Network      Next-hop    Logical-interface  State
-----
global    10.1.100.0/24 10.1.100.10 13-vlan 100       pending
```

Filter by VRF:

Example:

```
# show ip fib vrf all brief
VRF-name  Network      Next-hop      Logical-interface  State
-----
global    10.1.30.0/24    10.1.30.10    13-vlan 30        active
global    10.1.40.0/24    10.1.40.10    13-vlan 40        inactive
global    10.1.100.0/24   10.1.100.10   13-vlan 100       pending
global    10.1.200.0/24   10.1.200.10   13-vlan 200       active
black     10.1.200.0/24   10.1.200.10   13-vlan 201       active
red       10.1.200.0/24   10.1.200.10   13-vlan 202       active
```

Impacts and precautions

Depending on the number of routes installed, the execution of the command may take a while.

Hardware restrictions

N/A

show ip host-table

Description

Shows the list of hosts present in the system.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip host-table [ vrf { vrf-name | all } ] { brief } [ address ip-address | mac {  
mac-address | incomplete } | type host-type ]
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information.

Default Value: N/A

brief

Description: Displays brief information about IP hosts.

Value: N/A

Default Value: N/A

address *ip-address*

Description: IP address used to filter the output.

Value: a.b.c.d

Default Value: N/A

mac *mac-address*

Description: MAC address used to filter the output.

Value: XX:XX:XX:XX:XX:XX | incomplete

Default Value: N/A

type *host-type*

Description: Type of host to filter the output.

Value: dynamic | local | static | unknown

Default Value: N/A

Output Terms

Output	Description
VRF-name	Display the VRF name associated with the host.
Address	Display the IP addresses associated with host.
MAC	Display the MAC addresses associated with host IP addresses.
Logical interface	Display the logical interface on which the respective host is associated.
Physical interface	Display the physical interface on which the respective host is associated.
Type	Display the type of the host entry.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.8	This command was introduced.
4.4	Added VRF-name column and filter by VRF.

Usage Guidelines

To simply show the list of hosts the following command can be used:

Example:

```
# show ip host-table brief
```

To show the the list of hosts of all VRFs the following command can be used:

Example:

```
# show ip host-table vrf all brief
```

To show the the list of hosts of an specific VRF the following command can be used:

Example:

```
# show ip host-table vrf vrf-test brief
```

It is possible to filter the results by IP address, MAC address and Type.

Filter by IP:

Example:

```
# show ip host-table brief address 1.1.10.1
```

Filter by MAC:

Example:

```
# show ip host-table brief mac 00:11:22:33:44:55
```

Filter by Type:

Example:

```
# show ip host-table brief type local
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip rib

Description

Displays route information from Routing Information Base (RIB).

Supported Platforms

This command is supported in all platforms.

Syntax

show ip rib [**bgp** | **connected** | **destination** *ip-address* | **ospf** | **static** | **vrf** *name*]

Parameters

bgp

Description: Displays route information filtering by BGP routes.

Value: N/A

Default Value: N/A

connected

Description: Displays route information filtering by connected routes and local IP addresses.

Value: N/A

Default Value: N/A

destination *ip-address*

Description: Displays route information filtering by exact match of destination IP address and mask.

Value: a.b.c.d/x

Default Value: N/A

ospf

Description: Displays route information filtering by OSPF routes.

Value: N/A

Default Value: N/A

static

Description: Displays route information filtering by static routes.

Value: N/A

Default Value: N/A

vrf *name*

Description: Displays route information for VRF *name*.

Value: Name of VRF.

Default Value: N/A

Output Terms

Output	Description
Type	Indicates the type and the protocol that derived the route. The legend codes are displayed at the beginning of each report.
Dest Address/Mask	Indicates the destination IP address and mask of the remote network.
Next-hop	Indicates the address of the next router to the remote network.
Age	Indicates the time period since this route was last updated.
AD	Indicates the administrative distance value of the route.
Metric	Indicates the routing metric value of the route.
Output Interface	Indicates the output interface through which the specified network can be reached. It may display <code>black-hole</code> for routes that discard traffic.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.8	This command was introduced.
2.0	The command was modified to have OSPF input/output.
2.4	The command was modified to have VRF.
4.0	The command was modified to have BGP filter.
5.4	Black-hole route support was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use the show ip rib command.

```
# show ip rib
```

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,

Output Interface Codes: DC - directly connected

Type	Dest Address/Mask	Next-hop	Age	AD	Metric	Output Interface
S	192.0.2.0/25	0.0.0.0	00:46:42	1	0	black-hole
S	192.0.2.128/25	0.0.0.0	00:46:42	1	0	black-hole
S	198.51.100.0/26	198.51.100.66	00:46:42	1	0	loose-next-hop
C	198.51.100.64/26	198.51.100.65	01:15:48	0	0	mgmt-1/1/1
L	198.51.100.65/32	0.0.0.0	01:15:48	0	0	DC
C	198.51.100.128/26	198.51.100.129	00:05:48	0	0	13-vlan 100

```

L      198.51.100.129/32  0.0.0.0          00:05:48 0   0   DC
# show ip rib vrf red
Type Codes:  C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,
Output Interface Codes: DC - directly connected
-----
Type   Dest Address/Mask  Next-hop      Age          AD  Metric Output Interface
-----
C      198.51.100.64/26  198.51.100.65 00:02:26 0   0      13-vlan 101
L      198.51.100.65/32  0.0.0.0       00:02:26 0   0      DC
S      198.51.100.99/32  0.0.0.0       00:00:48 1   0      black-hole
S      203.0.113.0/25   198.51.100.66 00:00:48 1   0      loose-next-hop
# show ip rib destination 192.0.2.0/25
Routing entry for 192.0.2.0 (mask 255.255.255.128)
Known via 'static', distance 1, metric 0
  Redistributing via static
  Last update from 0.0.0.0 00:00:02 ago
Routing Descriptor Blocks:
0.0.0.0 directly connected, via black-hole 00:00:02 ago
Route metric is 0
#

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip route

Description

Display route information based on Forwarding Information Base (FIB).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip route [bgp | connected | destination ip-address | ospf | static | summary  
| vrf name ]
```

Parameters

bgp

Description: Displays route information filtering by BGP routes.

Value: N/A

Default Value: N/A

connected

Description: Displays route information filtering by connected routes and local IP addresses.

Value: N/A

Default Value: N/A

destination *ip-address*

Description: Displays route information filtering by exact match of destination IP address and mask.

Value: a.b.c.d/x

Default Value: N/A

ospf

Description: Displays route information filtering by OSPF routes.

Value: N/A

Default Value: N/A

static

Description: Displays route information filtering by static routes.

Value: N/A

Default Value: N/A

summary

Description: Displays summary route information.

Value: N/A

Default Value: N/A

vrf *name*

Description: Displays route information for VRF *name*.

Value: Name of VRF.

Default Value: N/A

Output Terms

Output	Description
Type	Indicates the type and the protocol that derived the route. The legend codes are displayed at the beginning of each report.
Dest Address/Mask	Indicates the destination IP address and mask of the remote network.
Next-hop	Indicates the address of the next router to the remote network.
Age	Indicates the time period since this route was last updated.
AD	Indicates the Administrative Distance value of the route.
Metric	Indicates the routing metric value of the route.

Output	Description
Output Interface	Indicates the output interface through which the specified network can be reached. It may display <code>black-hole</code> for routes that discard traffic.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.8	The command output was improved.
2.0	The command was modified to have OSPF input/output.
2.4	The command was modified to have VRF.
4.0	The command was modified to have BGP filter.
5.4	Black-hole route support was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use the show ip route command.

```
# show ip route

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,
Output Interface Codes: DC - directly connected

Type  Dest Address/Mask  Next-hop  Age  AD  Metric  Output Interface
-----
S      192.0.2.0/25         0.0.0.0   00:46:42  1    0      black-hole
S      192.0.2.128/25        0.0.0.0   00:46:42  1    0      black-hole
S      198.51.100.0/26        198.51.100.66  00:46:42  1    0      mgmt-1/1/1
C      198.51.100.64/26      198.51.100.65  01:15:48  0    0      mgmt-1/1/1
L      198.51.100.65/32       0.0.0.0   01:15:48  0    0      DC
C      198.51.100.128/26     198.51.100.129  00:05:48  0    0      13-vlan 100
L      198.51.100.129/32     0.0.0.0   00:05:48  0    0      DC

# show ip route vrf red

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,
Output Interface Codes: DC - directly connected

Type  Dest Address/Mask  Next-hop  Age  AD  Metric  Output Interface
-----
C      198.51.100.64/26      198.51.100.65  00:02:26  0    0      13-vlan 101
L      198.51.100.65/32       0.0.0.0   00:02:26  0    0      DC
S      198.51.100.99/32       0.0.0.0   00:00:48  1    0      black-hole
S      203.0.113.0/25        203.0.113.200  00:00:48  1    0      13-vlan 101

# show ip route destination 192.0.2.0/25

Routing entry for 192.0.2.0 (mask 255.255.255.128)
Known via 'static', distance 1, metric 0
  Redistributing via static
  Last update from 0.0.0.0 00:00:02 ago
Routing Descriptor Blocks:
  0.0.0.0 directly connected, via black-hole 00:00:02 ago
Route metric is 0

#
```

Impacts and precautions

Right after switch initialization the route table will be empty, because it takes a while to be populated.

Hardware restrictions

N/A

show ipv6 fib

Description

Displays IPv6 route information from Forwarding Information Base (FIB).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ipv6 fib [ vrf { vrf-name | all } ] { brief } [ network ipv6-address | state route-state ]
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information.

Default Value: N/A

brief

Description: Displays brief information about IPv6 routes from FIB.

Value: N/A

Default Value: N/A

network *ipv6-address*

Description: IPv6 address and mask network used to filter the output.

Value: *x:x:x:x::x/y*

Default Value: N/A

state *route-state*

Description: Route state used to filter the output.

Value: active | inactive | pending

Default Value: N/A

Output Terms

Output	Description
VRF-name	Display the VRF name associated with the IPv6 route.
Network	Display the destination IPv6 address and mask of the remote network.
Next-hop	Display the IPv6 address of the next router to the remote network.
Logical-interface	Display the output logical interface to reach the remote network, or display <code>black-hole</code> for routes that discard traffic.
State	Display the route state. The active state represents installed routes, the inactive state represents unsupported routes that will not be installed and the pending state represents valid routes currently not installed due to a hardware limitation.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

3.0	This command was introduced.
4.0	Route state 'inactive' created.
4.6	Filter by VRF changed.
5.4	Black-hole route support was added.

Usage Guidelines

To simply show IPv6 FIB information, the following command can be used:

Example:

```
# show ipv6 fib brief
VRF-name  Network                Next-hop                Logical-interface  State
-----
global    2001:db8:aaaa::/48          2001:db8:c3af::1       l3-vlan 100        pending
global    2001:db8:bbbb::/48          2001:db8:bbbb::1       l3-vlan 200        active
global    2001:db8:cccc::/48          2001:db8:alf::1        l3-vlan 300        active
global    2001:db8:dddd::/48          2001:db8:alf3::1       l3-vlan 400        inactive
global    2001:db8:eeee::/48          ::                      black-hole           active
```

It is possible to filter the output by Network, State and VRF.

Filter by Network:

Example:

```
# show ipv6 fib brief network 2001:db8:cccc::/48
VRF-name  Network                Next-hop                Logical-interface  State
-----
global    2001:db8:cccc::/48          2001:db8:alf::1        l3-vlan 300        active
```

Filter by State:

Example:

```
# show ipv6 fib brief state active
VRF-name  Network                Next-hop                Logical-interface  State
-----
global    2001:db8:bbbb::/48          2001:db8:bbbb::1       l3-vlan 200        active
global    2001:db8:cccc::/48          2001:db8:alf::1        l3-vlan 300        active
```

Filter by VRF:

Example:

```
# show ipv6 fib vrf all brief
VRF-name  Network-----Next-hop-----Logical-interface  State-----
global    2001:db8:aaaa::/48  2001:db8:c3af::1  l3-vlan 100      pending
global    2001:db8:bbbb::/48  2001:db8:bbbb::1  l3-vlan 200      active
global    2001:db8:cccc::/48  2001:db8:a1f::1   l3-vlan 300      active
global    2001:db8:dddd::/48  2001:db8:a1f3::1  l3-vlan 400      inactive
```

Impacts and precautions

Depending on the number of routes installed, the execution of the command may take a while.

Hardware restrictions

N/A

show ipv6 host-table

Description

Shows the list of IPv6 hosts present in the system.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ipv6 host-table [ vrf { vrf-name | all } ] { brief } [ address ipv6-address | mac  
{ mac-address | incomplete } | type host-type ]
```

Parameters

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information.

Default Value: N/A

brief

Description: Displays brief information about IPv6 hosts.

Value: N/A

Default Value: N/A

address *ipv6-address*

Description: IPv6 address used to filter the output.

Value: x:x:x:x::x/y

Default Value: N/A

mac *mac-address*

Description: MAC address used to filter the output.

Value: XX:XX:XX:XX:XX:XX | incomplete

Default Value: N/A

type *host-type*

Description: Type of host to filter the output.

Value: dynamic | local | static | unknown

Default Value: N/A

Output Terms

Output	Description
VRF-name	Display the VRF name associated with the host.
Address	Display the IPv6 addresses associated with host.
MAC	Display the MAC addresses associated with host IPv6 addresses.
Logical interface	Display the logical interface on which the respective host is associated.
Physical interface	Display the physical interface on which the respective host is associated.
Type	Display the type of the host entry.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.4	This command was introduced.
4.4	Added VRF-name column and filter by VRF.

Usage Guidelines

To simply show the list of hosts the following command can be used:

Example:

```
# show ipv6 host-table brief
```

To show the the list of hosts of all VRFs the following command can be used:

Example:

```
# show ipv6 host-table vrf all brief
```

To show the the list of hosts of an specific VRF the following command can be used:

Example:

```
# show ipv6 host-table vrf vrf-test brief
```

It is possible to filter the results by IPv6 address, MAC address, and Type.

Filter by IPv6 address:

Example:

```
# show ipv6 host-table brief address 2001:db8::1
```

Filter by MAC:

Example:

```
# show ipv6 host-table brief mac 00:11:22:33:44:55
```

Filter by Type:

Example:

```
# show ipv6 host-table brief type local
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ipv6 rib

Description

Displays IPv6 route information based on Routing Information Base (RIB).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ipv6 rib [bgp | connected | destination ip-address | ospf | static | vrf vrf-name ]
```

Parameters

bgp

Description: Displays route information filtering by BGP routes.

Value: N/A

Default Value: N/A

connected

Description: Displays IPv6 route information filtering by connected routes and local IP addresses.

Value: N/A

Default Value: N/A

destination *ip-address*

Description: Displays IPv6 route information filtering by exact match of destination IPv6 address and mask.

Value: x:x:x:x::x/x

Default Value: N/A

ospf

Description: Displays route information filtering by OSPFv3 routes.

Value: N/A

Default Value: N/A

static

Description: Displays IPv6 route information filtering by static routes

Value: N/A

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information

Default Value: N/A

Output Terms

Output	Description
Type	Indicates the type and the protocol that derived the route. The legend codes are displayed at the beginning of each report.
Dest Address/Mask	Indicates the destination IPv6 address and mask of the remote network.
Next-hop	Indicates the address of the next router to the remote network.
Age	Indicates the time period since this route was last updated.
AD	Indicates the Administrative Distance value of the route.
Metric	Indicates the routing metric value of the route.
Output Interface	Indicates the output interface through which the specified network can be reached. It may display <code>black-hole</code> for routes that discard traffic.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.4	This command was introduced.
4.0	OSPF and BGP parameters were added.
5.4	Black-hole route support was added.
5.12	Introduced VRF support.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use the show ipv6 rib command.

```
# show ipv6 rib
```

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,

Output Interface Codes: DC - directly connected

Type	Dest Address/Mask	Next-hop	Age	AD	Metric	Output Interface
C	2001:db8:100::/64	2001:db8:100::1	00:11:45 0	0		13-vlan 100
L	2001:db8:100::1/128	::	00:11:45 0	0		DC

```

S      2001:db8:2010::/64      ::      00:00:20 1 0      black-hole
C      2001:db8:2020::/64      2001:db8:2020::1 00:00:20 0 0      mgmt-1/1/1
L      2001:db8:2020::1/128    ::      00:00:20 0 0      DC
S      2001:db8:2030::/64      2001:db8:2020::2 00:00:20 1 0      loose-next-hop

# show ipv6 rib destination 2001:db8:2010::/64

Routing entry for 2001:db8:2010:: (mask 64)
Known via 'static', distance 1, metric 0
  Redistributing via static
  Last update from :: 00:00:03 ago
Routing Descriptor Blocks:
:: directly connected, via black-hole 00:00:03 ago
Route metric is 0

# show ipv6 rib vrf green

Type Codes:  C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,
Output Interface Codes: DC - directly connected

Type  Dest Address/Mask  Next-hop  Age      AD  Metric  Output Interface
-----
C      fd01::/16             fd01::1   00:04:16 0   0       13-vlan 101
L      fd01::1/128       ::        00:04:16 0   0       DC
#

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ipv6 route

Description

Displays IPv6 route information based on Forwarding Information Base (FIB).

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ipv6 route [bgp | connected | destination ip-address | ospf | static | summary | vrf vrf-name ]
```

Parameters

bgp

Description: Displays route information filtering by BGP routes.

Value: N/A

Default Value: N/A

connected

Description: Displays IPv6 route information filtering by connected routes and local IP addresses.

Value: N/A

Default Value: N/A

destination *ip-address*

Description: Displays route information filtering by exact match of destination IPv6 address and mask.

Value: x:x:x:x::x/x

Default Value: N/A

ospf

Description: Displays route information filtering by OSPFv3 routes.

Value: N/A

Default Value: N/A

static

Description: Displays IPv6 route information filtering by static routes

Value: N/A

Default Value: N/A

summary

Description: Displays summary IPv6 route information

Value: N/A

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF to filter displayed information.

Value: Name of VRF to display information

Default Value: N/A

Output Terms

Output	Description
Type	Indicates the type and the protocol that derived the route. The legend codes are displayed at the beginning of each report.
Dest Address/Mask	Indicates the destination IPv6 address and mask of the remote network.
Next-hop	Indicates the address of the next router to the remote network.
Age	Indicates the time period since this route was last updated.
AD	Indicates the Administrative Distance value of the route.
Metric	Indicates the routing metric value of the route.

Output	Description
Output Interface	Indicates the output interface through which the specified network can be reached. It may display <code>black-hole</code> for routes that discard traffic.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.4	This command was introduced.
4.0	OSPF and BGP parameters were added.
5.4	Black-hole route support was added.
5.12	Introduced VRF support.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use the show ipv6 route command.

```
# show ipv6 route

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,

Output Interface Codes: DC - directly connected

Type  Dest Address/Mask  Next-hop  Age      AD  Metric  Output Interface
-----
C      2001:db8:100::/64      2001:db8:100::1  00:11:29 0  0      13-vlan 100
L      2001:db8:100::1/128    ::              00:11:29 0  0      DC
S      2001:db8:2010::/64      ::              00:00:03 1  0      black-hole
C      2001:db8:2020::/64      2001:db8:2020::1  00:00:03 0  0      mgmt-1/1/1
L      2001:db8:2020::1/128  ::              00:00:03 0  0      DC
S      2001:db8:2030::/64      2001:db8:2020::2  00:00:04 1  0      mgmt-1/1/1

# show ipv6 route summary

IPv6 routing table name is Default-IPv6-Routing-Table
Family          Total routes
ipv6             6

# show ipv6 route destination 2001:db8:2010::/64

Routing entry for 2001:db8:2010:: (mask 64)
Known via 'static', distance 1, metric 0
  Redistributing via static
    Last update from :: 00:00:03 ago
Routing Descriptor Blocks:
:: directly connected, via black-hole 00:00:03 ago
Route metric is 0

# show ipv6 route vrf green

Type Codes: C - connected, S - static, L - local, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2, IA - OSPF inter area,

Output Interface Codes: DC - directly connected

Type  Dest Address/Mask  Next-hop  Age      AD  Metric  Output Interface
-----
C      fd01::/16          fd01::1   00:03:03 0  0      13-vlan 101
L      fd01::1/128        ::         00:03:04 0  0      DC

#
```

Impacts and precautions

Right after switch initialization the route table will be empty, because it takes a while to be populated.

Hardware restrictions

N/A

BFD

This topic describes the commands related to management of BFD such as commands to configure the BFD parameters or to inspect the sessions status.

show bfd session

Description

Shows information about the BFD sessions.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

show bfd session brief

Parameters

brief

- Description:** Shows summarized information about BFD sessions.
- Value:** N/A
- Default Value:** N/A

Output Terms

Output	Description
Proto	Indicates the client protocol which is protected by this BFD session.
Local-address	Indicates the local address used in the monitored link.

Output	Description
<code>Remote-address</code>	Indicates the address of remote endpoint in the monitored link.
<code>Output interface</code>	Indicates the L3 interface used to communicate to the other endpoint.
<code>State</code>	Indicates the state of monitored link (up or down).

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show bfd session brief
Protocol Codes: 0 - OSPF
```

```
Proto Local-address Remote-address Output interface State
-----
O 172.16.100.1 172.16.100.2 l3-vlan 100 up
O 172.16.101.1 172.16.101.2 l3-vlan 101 down

2 BFD sessions found.
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

BGP

This topic describes the commands related to management of BGP topologies such as commands to configure the BGP parameters or to inspect the protocol status.

clear bgp neighbor

Description

Restart BGP neighbors via Notification Cease message.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
clear bgp [vrf name] neighbor [ip IP address]
```

Parameters

vrf *name*

Description: Specifies a VRF name (only in supported platforms).

Value: Name of an existent VRF, *global* or *all*.

Default Value: N/A

ip *IP address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.
4.6	Added VRF support.
7.0	Added support for IPv6 on VRF.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to restart a BGP neighbor from a BGP router specifying a neighbor ip address.

```
# clear bgp neighbor ip 50.50.50.1
```

```
# clear bgp neighbor ip 2001:db8::1
```

This example shows how to restart all BGP neighbors from a BGP router.

```
# clear bgp neighbor
```


If no VRF parameter is included, the action will be executed only for the BGP on the global VRF. The VRF parameter accepts a *VRF name*, the *global* VRF or *all* VRFs.

This example shows how to restart all BGP neighbors on a specific VRF.

```
# clear bgp vrf GREEN neighbor
```

It is also possible to specify a neighbor IP address on that VRF.

```
# clear bgp vrf GREEN neighbor ip 50.50.50.1
```

```
# clear bgp vrf GREEN neighbor ip 2001:db8::1
```

To restart all BGP neighbors for all VRFs, the following command can be used.

```
# clear bgp vrf all neighbor
```

Impacts and precautions

This command will restart the connections to the neighbors.

Hardware restrictions

N/A

clear bgp soft

Description

Performs soft reset in BGP sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
clear bgp [vrf name] soft [ip IP address]
```

Parameters

vrf *name*

Description: Specifies a VRF name (only in supported platforms).

Value: Name of an existent VRF, *global* or *all*.

Default Value: N/A

ip *IP address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.
4.6	Added VRF support.
7.0	Added support for IPv6 on VRF.

Usage Guidelines

This command can be executed directly via CLI.

It requires route refresh capability in router BGP.

Example:

This example shows how to perform soft reset in a specific BGP neighbor.

```
# clear bgp soft ip 50.50.50.1
```

```
# clear bgp soft ip 2001:db8::1
```

This example shows how to perform a soft reset in all BGP sessions.

```
# clear bgp soft
```

If no VRF parameter is included, the action will be executed only for the BGP on the global VRF. The VRF parameter accepts a *VRF name*, the *global* VRF or *all* VRFs.

This example shows how to soft restart all BGP sessions on a specific VRF.

```
# clear bgp vrf GREEN soft
```

It is also possible to specify a neighbor IP address on that VRF.

```
# clear bgp vrf GREEN soft ip 50.50.50.1
```

```
# clear bgp vrf GREEN soft ip 2001:db8::1
```

To soft restart all BGP sessions for all VRFs, the following command can be used.

```
# clear bgp vrf all soft
```

Impacts and precautions

For neighbors that do not support the route refresh capability a Cease Notification message will be sent instead causing BGP session to restart.

Hardware restrictions

N/A

router bgp

Description

Configures a BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a BGP router.

```
(config)# router bgp 65000
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp address-family

Description

Enables the router BGP VPNv4/VPNv6 address family support.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **address-family** { **vpn4** | **vpn6** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

address-family { **vpn4** | **vpn6** }

Description: Selects the address family (AFI).

Value: **vpn4**. VPNv4 address family.
vpn6. VPNv6 address family.

Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast**. VPNv4/VPNv6 unicast routes.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.0	Added VPNv6 Address Family

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

The disabling of a router BGP address family support is only possible if it is not configured in any BGP neighbor. Thus, the removal of all BGP neighbors address family configuration is required before disabling the address family on the router BGP.

Dual-stack can be enabled.

Example:

This example shows how to enable the router BGP VPNv4 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# address-family vpnv4 unicast
(config-address-family-vpnv4/unicast)# commit
Commit complete.
```


Example:

This example shows how to enable the router BGP VPNv6 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# address-family vpnv6 unicast
(config-address-family-vpnv6/unicast)# commit
Commit complete.
```

Impacts and precautions

Changes on the address family will impact the router BGP capabilities. It also causes a flap in the established BGP sessions.

Hardware restrictions

N/A

router bgp address-family

Description

Enables the router BGP address family support.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **address-family** { **ipv4** | **ipv6** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

address-family { **ipv4** | **ipv6** }

Description: Selects the address family (AFI).

Value: **ipv4** or **ipv6**. IPv4 or IPv6 address family.

Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast**. IPv4 or IPv6 unicast routes.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

The disabling of a router BGP address family support is only possible if it is not configured in any BGP neighbor. Thus, the removal of all BGP neighbors address family configuration is required before disabling the address family on the router BGP.

Example:

This example shows how to enable the router BGP IPv4 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# address-family ipv4 unicast
(config-address-family-ipv4/unicast)# commit
Commit complete.
```

This example shows how to enable the router BGP IPv6 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# address-family ipv6 unicast
(config-address-family-ipv6/unicast)# commit
Commit complete.
```

Impacts and precautions

Changes on the address family will impact the router BGP capabilities. It also causes a flap in the established BGP sessions.

Hardware restrictions

N/A

router bgp administrative-status

Description

Configures the desired administrative status of a BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

administrative-status *status*

Description: Activate (up) or deactivate (down) the BGP router.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
(config)# router bgp 65000 administrative-status down
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp as-size

Description

Configures the Router BGP Autonomous system(AS) size.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **as-size** *length*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

as-size *length*

Description:	Specifies the Router BGP Autonomous System(AS) size.
Value:	two-octets four-octets.
Default Value:	four-octets.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the Router BGP Autonomous system(AS) size.

```
(config)# router bgp 65000 as-size two-octets
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp bgp cluster-id

Description

Configures the Router Cluster-ID.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **bgp cluster-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

bgp cluster-id *id*

Description:	Specifies the BGP Cluster-ID for this Router in IPv4 address format.
Value:	a.b.c.d.
Default Value:	0.0.0.0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP Cluster-ID.

```
(config)# router bgp 65000 bgp cluster-id 1.1.1.1
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp bgp default-local-preference

Description

Configures the Router BGP Default Local Preference.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **bgp default-local-preference** *local-preference*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.
Value: 1-4294967295.
Default Value: N/A

bgp default-local-preference *local-preference*

Description: Specifies the default local preference for this Router.
Value: 0-4294967295.
Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP default local preference.

```
(config)# router bgp 65000 bgp default-local-preference 150
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor

Description

Configures a neighbor for a BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a neighbor for a BGP router.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor address-family

Description

Enables the BGP neighbor address family support and enters in mode configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **address-family** { **ipv4** | **ipv6** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

address-family { **ipv4** | **ipv6** } **unicast**

Description: Enables the BGP neighbor address family mode support and enters in mode configuration.

Value: **ipv4** or **ipv6 unicast**. IPv4 or IPv6 address family.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

The enabling of a BGP neighbor address family support is only possible if it is already configured in router BGP.

Example:

This example shows how to enable the BGP neighbor IPv4 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-address-family-ipv4/unicast)# commit
Commit complete.
```

This example shows how to enable the BGP neighbor IPv6 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 2222::2
(config-neighbor-2222::2)# address-family ipv6 unicast
(config-address-family-ipv6/unicast)# commit
Commit complete.
```


Impacts and precautions

Changes on the address family will impact the BGP neighbor capabilities. It also causes a flap in the established BGP neighbor session.

Hardware restrictions

N/A

router bgp neighbor address-family prefix-list

Description

Associates a prefix list with a BGP neighbor for export or import based on the address family.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **address-family ipv4 unicast** [**export-prefix-list** *prfx-name*] [**import-prefix-list** *prfx-name*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

address-family ipv4 unicast

Description: Enters in the BGP neighbor address family mode configuration.

Value: **ipv4 unicast**. IPv4 unicast address family.

Default Value: N/A

export-prefix-list *prfx-name*

- Description:** Specifies the prefix list for export to be directly associated with the BGP neighbor. Use the **no** form to remove this parameter.
- Value:** Name of a prefix list.
- Default Value:** N/A

import-prefix-list *prfx-name*

- Description:** Specifies the prefix list for import to be directly associated with the BGP neighbor. Use the **no** form to remove this parameter.
- Value:** Name of a prefix list.
- Default Value:** N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
3.0	Changes on the behavior when a prefix list and a route policy are associated with a neighbor.

Usage Guidelines

This command can be executed directly via CLI.

Notice that a route policy associated with a neighbor have precedence over a prefix list directly associated with it.

This command is only supported in IPv4 address family mode configuration.

Example:

This example shows how to associate the prefix list for export named PRX_LIST_EXPORT with a BGP neighbor. This prefix list must be previously created.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-address-family-ipv4/unicast)# export-prefix-list PRX_LIST_EXPORT
(config-address-family-ipv4/unicast)# commit
```

This example shows how to associate the prefix list for import named PRX_LIST_IMPORT with a BGP neighbor. This prefix list must be previously created.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-address-family-ipv4/unicast)# import-prefix-list PRX_LIST_IMPORT
(config-address-family-ipv4/unicast)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor address-family vpn

Description

Enables the BGP neighbor VPNv4/VPNv6 address family support and enters in mode configuration.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **address-family** { **vpn***nv4* | **vpn***nv6* } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 address format.

Value: a.b.c.d

Default Value: N/A

address-family { **vpn***nv4* | **vpn***nv6* } **unicast**

Description: Enables the BGP neighbor address family mode support and enters in mode configuration.

Value: **vpn***nv4 unicast*. VPNv4 unicast address family.
vpn*nv6 unicast*. VPNv6 unicast address family.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.0	Added VPNv6 Address Family

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

The enabling of a BGP neighbor address family support is only possible if it is already configured in router BGP.

IPv4 neighbors support both VPNv4 (L3VPN) and VPNv6 (6VPE) address families. IPv6 neighbors don't support VPN address families.

Dual-stack can be enabled.

Example:

This example shows how to enable the BGP neighbor VPNv4 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family vpnv4 unicast
(config-address-family-vpnv4/unicast)# commit
Commit complete.
```

This example shows how to enable the BGP neighbor VPNv6 unicast address family support.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family vpnv6 unicast
(config-address-family-vpnv6/unicast)# commit
Commit complete.
```

This example shows how to enable dual-stack on BGP neighbor.

```
(config)# router bgp 65000
(config-bgp-65000)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# address-family vpnv4 unicast
(config-address-family-vpnv4/unicast)# address-family vpnv6 unicast
(config-address-family-vpnv6/unicast)# commit
Commit complete.
```

Impacts and precautions

Changes on the address family will impact the BGP neighbor capabilities. It also causes a flap in the established BGP neighbor session.

Hardware restrictions

N/A

router bgp neighbor administrative-status

Description

Configures the desired administrative status of a BGP neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

administrative-status *status*

Description:	Activate (up) or deactivate (down) the BGP neighbor.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP neighbor administrative status in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# administrative-status down
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor description

Description

Configures the BGP neighbor description.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **description** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

description *text*

Description:	A textual string containing information about the BGP neighbor.
Value:	string.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a BGP neighbor description in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# description "Remote bgp peer"
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor ebgp-multihop

Description

Configure the maximum hop count to reach a BGP neighbor not directly connected.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number neighbor address ebgp-multihop hop-count
```

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.
Value: 1-4294967295.
Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value: a.b.c.d or x:x:x:x::x.
Default Value: N/A

ebgp-multihop *hop-count*

Description: Specifies the maximum hop count to reach the neighbor.
Value: 1-255.
Default Value: 1 for eBGP sessions. 255 for iBGP sessions.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP neighbor ebgp-multihop in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1 remote-as 66000
(config-neighbor-50.50.50.1)# ebgp-multihop 2
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

For security reasons, please note that this parameter is automatically configured to 1 for eBGP and 255 for iBGP sessions, unless it was manually configured. But if neighbor mode changes (to iBGP or eBGP) and ebgp-multihop has not been changed, it will be automatically updated according to the new mode.

Hardware restrictions

N/A

router bgp neighbor next-hop-self

Description

Configures the BGP neighbor to use its own address as next hop in the advertised routes.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **next-hop-self**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

next-hop-self

Description:	Enables the neighbor option to use itself as next-hop.
Value:	N/A
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP neighbor next hop self in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# next-hop-self
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor password

Description

Configures the neighbor to use Message-Digest algorithm 5 (MD5) authentication on the TCP connection between BGP peers.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **password** *pwd*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

password *pwd*

Description: Specifies the BGP neighbor case-sensitive password to be used between the TCP peer connection.

Value: string (length 2 - 80).

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI. The same password must be applied for both BGP peers.

Example:

This example shows how to configure the BGP neighbor password in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# password pwdTest
(config-neighbor-50.50.50.1)# commit
```

This example shows the configuration of a neighbor password using an already encrypted password.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# password "hls:2922743918:337ZpL=Z"
(config-neighbor-50.50.50.1)# commit
```

This example shows the configuration of a neighbor password using special characters (i.e: " " , "?" , "!" , ";"). Please note that it is necessary to use double quotation marks in this case.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# password "pwd?test:2"
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

Password must be enclosed in double quotation marks if special characters were used (i.e: " " , "?" , "!" , ";"). Note that in an established BGP session if password is configured or changed the session will be restarted.

Hardware restrictions

N/A

router bgp neighbor remote-as

Description

Configures the BGP neighbor remote Autonomous System(AS) number.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **remote-as** *as-number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

remote-as *as-number*

Description:	Specifies the BGP neighbor remote Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a neighbor remote Autonomous System(AS) number after entering in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# remote-as 65001
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor route-policy

Description

Associates a route policy with the BGP neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **route-policy** *rp-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

route-policy *rp-name*

Description:	Specifies the route policy to be associated with the BGP neighbor.
Value:	Route policy name.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

It is only supported by IPv4 BGP neighbors.

The route refresh capability in router BGP is required to avoid BGP sessions to be restarted.

Example:

This example shows how to associate the route policy named RP_INTERNET with a BGP neighbor. This route policy must be previously created.

```
(config)# router bgp 101
(config-bgp-101)# neighbor 1.1.10.2
(config-neighbor-1.1.10.2)# route-policy RP_INTERNET
(config-neighbor-1.1.10.2)# commit
```

Impacts and precautions

If there is no route refresh capability support any update on the route policy configuration that is associated with a BGP neighbor will cause its BGP session to be restarted.

Hardware restrictions

N/A

router bgp neighbor route-reflector

Description

Configures the BGP route-reflector option.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **route-reflector** *option*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

route-reflector *option*

Description:	Configure the route reflector options
Value:	client non-client.
Default Value:	non-client.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure route-reflector after entering in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# route-reflector client
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor timers hold-time

Description

Configure the hold time interval for the session with the neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **timers hold-time** *time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

timers hold-time *time*

Description:	Specifies the hold time interval to use when negotiating a connection with the neighbor.
Value:	3-65535. (0 for infinite hold time)
Default Value:	180.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI. The hold time interval must be greater than or equal to the keepalive interval. Indeed, it is recommended that the hold time is 3 times the interval at which keepalive messages are sent. A zeroed value means an infinite time. If the hold time interval is set to zero, the keepalive interval must be set to zero as well.

Example:

This example shows how to configure the BGP neighbor hold time interval in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1 remote-as 66000
(config-neighbor-50.50.50.1)# timers hold-time 90
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor timers keepalive

Description

Configure the keepalive interval for the session with the neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **timers keepalive** *time*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

timers keepalive *time*

Description:	Specifies the keepalive interval to use when negotiating a connection with the neighbor.
Value:	0-21845.
Default Value:	60.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI. The keepalive interval must be lower than or equal to the hold-time interval. Indeed, it is recommended that the hold time is 3 times the interval at which keepalive messages are sent. A zeroed value for keepalive timer disables the sending of keepalive messages. In this case, the hold-time interval must be set to zero as well.

The router automatically adjusts the effective keepalive timer based on the configured values, according to the following formula:

$$\text{keepalive} = \text{negotiated hold-time} / \text{truncate} (\text{configured hold-time} / \text{configured keepalive})$$

As example, if the configured and negotiated hold-time are both 150 and keepalive is configured to 60:

$$\text{keepalive} = 150 / \text{truncate} (150 / 60)$$

keepalive = 150 / 2

keepalive = 75

Example:

This example shows how to configure the BGP neighbor keepalive interval in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1 remote-as 66000
(config-neighbor-50.50.50.1)# timers keepalive 30
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp neighbor update-source-address

Description

Configures the BGP neighbor source address to be used during the session establishment.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **neighbor** *address* **update-source-address** *address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

update-source-address *address*

Description: Specifies the BGP neighbor source address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the BGP neighbor IPv4 source address in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 50.50.50.1
(config-neighbor-50.50.50.1)# update-source-address 100.100.100.1
(config-neighbor-50.50.50.1)# commit
Commit complete.
```

This example shows how to configure the BGP neighbor IPv6 source address in the neighbor command tree.

```
(config)# router bgp 65000 neighbor 2222::2
(config-neighbor-2222::2)# update-source-address 2002::1
(config-neighbor-2222::2)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp network address-family ipv4

Description

Inserts a network present locally in the routing table into BGP domain and advertises it to the neighbor, when that network exactly matches a given prefix.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number network address-family ipv4 address a.b.c.d/x
```

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

network address-family ipv4

Description: Specifies that the network prefix entry is from IPv4 address family.

Value: N/A

Default Value: N/A

address *a.b.c.d/x*

Description: Defines the network that must be matched in order to be inserted into BGP domain.

Value: Must be a valid IPv4 prefix/mask.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to create a list of 2 network prefixes to be redistributed into BGP domain.

```
(config)# router bgp 65000
(config-bgp-65000)# network address-family ipv4 address 40.40.40.240/28
(config-network/ipv4)# exit
(config-bgp-65000)# network address-family ipv4 address 80.80.128.0/17
(config-network/ipv4)# commit
```

Impacts and precautions

The network inserted into BGP domain will have its path attribute origin set as IGP. The network will be advertised to the neighbors only if it is already present in the routing table. That means, there must be a route learned using local or connected networks, static routes, or a dynamic IGP such as OSPF.

Hardware restrictions

N/A

router bgp network address-family ipv6

Description

Inserts a network present locally in the routing table into BGP domain and advertises it to the neighbor, when that network exactly matches a given prefix.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **network address-family ipv6 address** *x:x:x:x::x/y*

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

network address-family ipv6

Description: Specifies that the network prefix entry is from IPv6 address family.

Value: N/A

Default Value: N/A

address *x:x:x:x::x/y*

Description: Defines the network that must be matched in order to be inserted into BGP domain.

Value: Must be a valid IPv6 prefix/mask.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to create a list of 2 network prefixes to be redistributed into BGP domain.

```
(config)# router bgp 65000
(config-bgp-65000)# network address-family ipv6 address 1111::1/128
(config-network/ipv6)# exit
(config-bgp-65000)# network address-family ipv6 address 2222::2/128
(config-network/ipv6)# commit
```

Impacts and precautions

The network inserted into BGP domain will have its path attribute origin set as IGP. The network will be advertised to the neighbors only if it is already present in the routing table. That means, there must be a route learned using local or connected networks, static routes, or a dynamic IGP such as OSPF.

Hardware restrictions

N/A

router bgp prefix-list

Description

Prefix list configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **prefix-list** *name* **seq** *seq-number* [**permit** | **deny**] **address-family** *ipv4 unicast* [**address** *prefix*] [**le** *prefix-len*] [**ge** *prefix-len*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

prefix-list *name*

Description: Creates a prefix list with the given *name*.

Value: N/A

Default Value: N/A

seq *seq-number*

Description: Apply the sequence number to the prefix list entry.

Value: 1-4294967295.

Default Value: N/A

permit

Description: In case of match the route is allowed to be redistributed. The **permit** keyword is the default option.

Value: N/A

Default Value: permit.

deny

Description: In case of match the route is rejected and no further processing is performed.

Value: N/A

Default Value: permit.

address-family *ipv4 unicast*

Description: Unicast IPv4 address family configuration.

Value: N/A

Default Value: N/A

address *prefix*

Description: A unicast IPv4 prefix in A.B.C.D/length format.

Value: a.b.c.d/x.

Default Value: 0.0.0.0/0.

le *prefix-len*

Description: The maximum prefix length to match.

Value: 1-32.

Default Value: N/A

ge *prefix-len*

Description: The minimum prefix length to match.

Value: 1-32.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
2.2	Added the optional parameters deny and permit.
3.0	Changes on the behavior when a prefix list and a route policy are associated with a neighbor.
4.6	This Command was deprecated. From this version on, the prefix list is configured in the config level. For further information please see Prefix List command.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a prefix list that permits the network address 50.50.50.0/24.

```
(config)# router bgp 101
(config-bgp-101)# prefix-list TEST
(config-prefix-list-TEST)# seq 10
(config-seq-10)# address-family ipv4 unicast
(config-unicast)# address 50.50.50.0/24
(config-unicast)# commit
Commit complete.
```

This example shows how to configure a prefix list with a permitted prefix range from

subnetwork 60.60.60.0/25 to network 60.60.60.0/24.

```
(config)# router bgp 101
(config-bgp-101)# prefix-list TEST_RANGE
(config-prefix-list-TEST_RANGE)# seq 20
(config-seq-20)# address-family ipv4 unicast
(config-unicast)# address 60.60.60.0/24 ge 24 le 25
(config-unicast)# commit
Commit complete.
```

This example shows how to configure a prefix list that denies the network address 60.60.60.0/24 but allows the others.

```
(config)# router bgp 101
(config-bgp-101)# prefix-list TEST_DENY
(config-prefix-list-TEST_DENY)# seq 20
(config-seq-20)# deny
(config-seq-20)# address-family ipv4 unicast
(config-unicast)# address 60.60.60.0/24
(config-unicast)# exit
(config-seq-20)# exit
(config-prefix-list-TEST_DENY)# seq 30
(config-seq-30)# address-family ipv4 unicast
(config-unicast)# address 0.0.0.0/0 ge 1 le 32
(config-unicast)# commit
Commit complete.
```

Impacts and precautions

When the prefix list is associated with a route map the permit or deny configuration of the prefix list entry is ignored.

In case of prefix list directly associated with a BGP neighbor and no permit matches are found, all routes will be denied. Therefore, it is necessary to add an additional sequence with a clause to permit the other routes by setting a matching all address (0.0.0.0/0 ge 1 le 32).

Notice that when there is a route policy importing a route map associated with a neighbor the prefix list for import directly associated with it will be ignored. The same precedence applies to the case when both are set for export.

If there is no route refresh capability support any update on the prefix list configuration that is associated with a BGP neighbor will cause its BGP session to be restarted.

Updates on prefix-lists associated with a neighbor or with a route map will trigger either route-refresh or update messages. Route-refresh messages request to the neighbor the sending of all its prefixes. Differently from a route-refresh message the sending of update messages is an optimization because only the prefixes not included on the previous BGP update will be advertised.

Hardware restrictions

N/A

router bgp redistribute

Description

Redistributes routes into the domain of this BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number redistribute {connected | static | ospf} address-family {ipv4 | ipv6}
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

redistribute connected

Description: Redistributes connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute ospf

Description: Redistributes ospf routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

address-family ipv4

Description: Redistributes only routes from IPv4 address family.

Value: N/A

Default Value: N/A

address-family ipv6

Description: Redistributes only routes from IPv6 address family.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

2.0	This command was introduced.
-----	------------------------------

4.0	Added support for IPv6.
-----	-------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a redistribution of all IPv4 static routes.

```
# router bgp 65000 redistribute static address-family ipv4
(config-redistribute-static/ipv4)# commit
```

This example shows how to configure a redistribution of all IPv4 connected routes.

```
# router bgp 65000 redistribute connected address-family ipv4
(config-redistribute-connected/ipv4)# commit
```

This example shows how to configure a redistribution of all IPv4 ospf routes.

```
# router bgp 65000 redistribute ospf address-family ipv4
(config-redistribute-ospf/ipv4)# commit
```

This example shows how to configure a redistribution of all IPv6 static routes.

```
# router bgp 65000 redistribute static address-family ipv6
(config-redistribute-static/ipv6)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp redistribute administrative-status

Description

Configures the desired administrative status of a redistribution rule.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number redistribute {connected | static | ospf} address-family {ipv4 | ipv6} administrative-status status
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

redistribute connected

Description: Redistributes connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute ospf

Description: Redistributes ospf routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

address-family ipv4

Description: Redistributes only routes from IPv4 address family.

Value: N/A

Default Value: N/A

address-family ipv6

Description: Redistributes only routes from IPv6 address family.

Value: N/A

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the BGP router redistribution.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to disable IPv4 static routes redistribution.

```
# router bgp 65000 redistribute static address-family ipv4
(config-redistribute-static/ipv4)# administrative-status down
(config-redistribute-static/ipv4)# commit
```

This example shows how to disable IPv6 static routes redistribution.

```
# router bgp 65000 redistribute static address-family ipv6
(config-redistribute-static/ipv6)# administrative-status down
(config-redistribute-static/ipv6)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp redistribute match-address address-family ipv4

Description

Redistributes only the routes that match the specified address into the domain of this BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **redistribute** {**connected** | **static**} **address-family ipv4 match-address** *a.b.c.d/x*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

redistribute connected

Description: Redistributes connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

address-family ipv4

Description: Redistributes only routes from IPv4 address family.

Value: N/A

Default Value: N/A

match-address *a.b.c.d/x*

Description: Redistributes specific routes that match the supplied prefix/mask filter into the domain of this BGP router.

Value: Must be a valid IPv4 prefix/mask.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a route redistribution which matches a single IPv4 address prefix.

```
# router bgp 65000 redistribute static address-family ipv4
(config-redistribute-static/ipv4)# match-address 10.1.0.0/24
(config-redistribute-static/ipv4)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp redistribute match-address address-family ipv6

Description

Redistributes only the routes that match the specified address into the domain of this BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **redistribute** {**connected** | **static**} **address-family ipv6 match-address** *x:x:x:x::x/y*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

redistribute connected

Description: Redistributes connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

address-family ipv6

Description:	Redistributes only routes from IPv6 address family.
Value:	N/A
Default Value:	N/A

match-address *x:x:x:x::x/y*

Description:	Redistributes specific routes that match the supplied prefix/mask filter into the domain of this BGP router.
Value:	Must be a valid IPv6 prefix/mask.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a route redistribution which matches a single IPv6 address prefix.

```
# router bgp 65000 redistribute static address-family ipv6
(config-redistribute-static/ipv6)# match-address 2001::1/128
(config-redistribute-static/ipv6)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp route-map

Description

Route map configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **route-map** *rmap-name* { *seq-number* | * } **action** { **permit** | **deny** } { **match-ip** *nlri* **prefix-list** *prfx-name* | **match-as-path** *as-path* | **match-med** *med* | **match-origin** *origin* | **set-local-preference** *value* | **set-med** *med* | **set-origin** *origin* | **set-prepend-local-as** *num-times* | **continue** *seq-number* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

route-map *rmap-name*

Description: Creates a route map with the given *rmap-name*.

Value: N/A

Default Value: N/A

seq-number

Description: Applies the sequence number to the route map entry.

Value: 1-4294967295.

Default Value: N/A

*

Description: A reference for all route map sequences. This option allows edition or deletion of all route map sequences simultaneously.

Value: N/A

Default Value: N/A

action

Description: When **action permit** is used in case of match of any criteria the route is allowed to be redistributed and the set of actions is performed. When **action deny** is used in case of match of any criteria the route is rejected and no further processing is performed.

Value: permit - deny.

Default Value: permit.

match-ip nlri prefix-list *prfx-name*

Description: Matches IP addresses present on BGP NLRI based on an existent prefix list named as *prfx-name*.

Value: Name of a prefix list.

Default Value: N/A

match-as-path *as-path*

Description: Regular expression to match BGP AS paths (write regex using POSIX extended standard ensuring the use of double quote in order to avoid problems with special characters)

Value: string (length 1 - 127).

Default Value: N/A

match-med *med*

Description: Matches BGP Multi Exit Discriminator (MED).

Value: 0-4294967295.

Default Value: N/A

match-origin *origin*

Description: Matches BGP origin.

Value: egp, igp or incomplete.

Default Value: N/A

set-local-preference *value*

Description: Sets the BGP local preference path attribute.

Value: 0-2147483647.

Default Value: N/A

set-med *med*

Description: Sets the BGP Multi Exit Discriminator (MED).

Value: 0-4294967295.

Default Value: 0.

set-origin *origin*

Description: Sets the BGP origin.

Value: egp, igp or incomplete.

Default Value: N/A

set-prepend-local-as *num-times*

Description: Prepends the AS number to the AS path the number of times specified by *num-times*.

Value: 1-254.

Default Value: N/A

continue *seq-number*

Description: Continues the route map on a different sequence number. The sequence number must exist and be higher than the current one. The continue parameter can only be used with permit sequences of route map.

Value: 1-4294967295.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
2.2	Added match-as-path option. Added range mode to edit or delete all route map sequences.
4.6	Added action parameter to configure permit or deny actions.

Usage Guidelines

This command can be executed directly via CLI.

The route map must be associated with a route policy in order to be applied to a neighbor. The route refresh capability in router BGP is required to avoid BGP sessions to be restarted.

Example:

This example shows how to configure a route map with matching for a prefix list and setting of local preference.

```
(config)# router bgp 101
(config-bgp-101)# route-map RMAP 10
(config-route-map-RMAP/10)# match-ip nlri prefix-list PRX_LIST
(config-route-map-RMAP/10)# set-local-preference 200
(config-route-map-RMAP/10)# commit
```

This example shows how to configure all sequences of a route map simultaneously to perform a deny action.

```
(config)# router bgp 101
(config-bgp-101)# route-map RMAP 10
(config-route-map-RMAP/10)# exit
(config-bgp-101)# route-map RMAP 20
(config-route-map-RMAP/20)# exit
(config-bgp-101)# route-map RMAP *
(config-route-map-RMAP/*)# action deny
(config-route-map-RMAP/*)# commit
```

This example shows how to delete the entire route map.

```
(config)# router bgp 101
(config-bgp-101)# route-map RMAP 10
(config-route-map-RMAP/10)# exit
(config-bgp-101)# route-map RMAP 20
(config-route-map-RMAP/20)# exit
(config-bgp-101)# no route-map RMAP *
(config-bgp-101)# commit
```

Some examples of regular expressions to be used in match-as-path parameter:

Second AS number should be 300 or 400

```
(config-route-map-RMAP/10)# match-as-path "(.300|400)" or "(.300)|(.400)"
```

Specific sequence (all three values should appear in this exact order)

```
(config-route-map-RMAP/10)# match-as-path "333.100.444"
```

Path must contain AS 400 or AS 200

```
(config-route-map-RMAP/10)# match-as-path "400|200"
```

Path must start with 333 and finish with 300

```
(config-route-map-RMAP/10)# match-as-path "^333.300$"
```

Path must not end with 333

```
(config-route-map-RMAP/10)# match-as-path "[^3]33$"
```

Path must not start with 333

```
(config-route-map-RMAP/10)# match-as-path "^[^3]33"
```

Path does not contain 333 (see impacts and precautions for more details about deny rules)

```
(config-route-map-RMAP/10)# match-as-path "(333)"
(config-route-map-RMAP/10)# action deny
(config-route-map-RMAP/10)# exit
(config-bgp-101)# route-map RMAP 20
(config-route-map-RMAP/20)# commit
```

Impacts and precautions

When a route map is not specified, routes are automatically permitted by default. However, if a route map is created but no matching clauses are found, all routes will be denied. In this case it is necessary to add an additional sequence without any clause in order to permit all other routes.

If there is no route refresh capability support any update on the route map configuration

that is associated with a BGP neighbor will cause its BGP session to be restarted.

Updates on route map associated with a neighbor through a route policy will trigger either route-refresh or update messages. Route-refresh messages request to the neighbor the sending of all its prefixes. Differently from a route-refresh message the sending of update messages is an optimization because only the prefixes not included on the previous BGP update will be advertised.

Hardware restrictions

N/A

router bgp route-map match-community

Description

Match community configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **route-map** *rmap-name* { *seq-number* | * } **match-community** *communities*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System (AS) number.

Value: 1-4294967295.

Default Value: N/A

route-map *rmap-name*

Description: Creates a route map with the given *rmap-name*.

Value: N/A

Default Value: N/A

seq-number

Description: Applies the sequence number to the route map entry.

Value: 1-4294967295.

Default Value: N/A

*

Description: A reference for all route map sequences. This option allows edition or deletion of all route map sequences simultaneously.

Value: N/A

Default Value: N/A

match-community *communities*

Description: Sets the regular expression for matching communities.

Value: String (length 1 - 127).

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a match for communities.

```
(config)# router bgp 100
(config-bgp-100)# route-map RMAP 10
(config-route-map-RMAP/10)# match-community 200:123
(config-route-map-RMAP/10)# route-map RMAP 11
```

```
(config-route-map-RMAP/11)# match-community "[65535:65281|65535:65282]"
(config-route-map-RMAP/11)# route-map RMAP 12
(config-route-map-RMAP/12)# match-community "65535:6528.*"
(config-route-map-RMAP/12)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp route-map set-community

Description

Set community configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number route-map rmap-name { seq-number | * } set-community {  
community | internet | local-AS | no-advertise | no-export }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System (AS) number.

Value: 1-4294967295.

Default Value: N/A

route-map *rmap-name*

Description: Creates a route map with the given *rmap-name*.

Value: N/A

Default Value: N/A

seq-number

Description: Applies the sequence number to the route map entry.

Value: 1-4294967295.

Default Value: N/A

*

Description: A reference for all route map sequences. This option allows edition or deletion of all route map sequences simultaneously.

Value: N/A

Default Value: N/A

set-community { *community* | **internet** | **local-AS** | **no-advertise** | **no-export** }

Description: Sets the community attribute.

Value: Well-known community or specific community in AS:nn format.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a community for prefixes.

```
(config)# router bgp 100
(config-bgp-100)# route-map RMAP 10
(config-route-map-RMAP/10)# set-community 100:123
(config-route-map-RMAP/10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp route-map set-community-action

Description

Set action to be applied to route communities

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number route-map rmap-name { seq-number | * } set-community-action { none | remove-all | remove-all-and-set | remove-specific | set-specific }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System (AS) number.

Value: 1-4294967295.

Default Value: N/A

route-map *rmap-name*

Description: Creates a route map with the given *rmap-name*.

Value: N/A

Default Value: N/A

seq-number

Description: Applies the sequence number to the route map entry.

Value: 1-4294967295.

Default Value: N/A

*

Description: A reference for all route map sequences. This option allows edition or deletion of all route map sequences simultaneously.

Value: N/A

Default Value: N/A

set-community-action { none | remove-all | remove-all-and-set | remove-specific | set-specific }

Description: Possible actions to be applied to route communities. Actions **remove-all-and-set**, **remove-specific** and **set-specific** must have set-community attribute configured. Action **none** has the same effect as **no set-community-action**.

Value: none | remove-all | remove-all-and-set | remove-specific | set-specific

Default Value: none.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a community action for prefixes.

```
(config)# router bgp 100
(config-bgp-100)# route-map RMAP 10
(config-route-map-RMAP/10)# set-community 100:123
(config-route-map-RMAP/10)# set-community-action remove-all-and-set
(config-route-map-RMAP/10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp route-policy

Description

Route policy configuration.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number route-policy rp-name [ import-route-map rmap-name ] [ export-route-map rmap-name ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

route-policy *rp-name*

Description: Creates a route-policy named *rp-name*.

Value: String

Default Value: N/A

import-route-map *rmap-name*

Description: Specifies the route map that will be used for route imports.

Value: String

Default Value: N/A

export-route-map *rmap-name*

Description:	Specifies the route map that will be used for route exports.
Value:	String
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
4.6	Added <i>action</i> parameter to configure permit or deny actions in the command route-map.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how create a policy to export a Route Map.

```
(config-bgp-101)# route-map rm-route50 10
(config-route-map-rm-route50/10)# action permit
(config-bgp-101)# route-policy rp-route50
(config-route-policy-rp-route50)# export-route-map rm-route50
(config-route-policy-rp-route50)# commit
Commit complete.
(config-route-policy-rp-route50)#
```


Impacts and precautions

If there is no route refresh capability support any update on the route policy configuration that is associated with a BGP neighbor will cause its BGP session to be restarted.

Updates on route policy associated with a neighbor will trigger either route-refresh or update messages. Route-refresh messages request to the neighbor the sending of all its prefixes. Differently from a route-refresh message the sending of update messages is an optimization because only the prefixes not included on the previous BGP update will be advertised.

Hardware restrictions

N/A

router bgp router-id

Description

Configures the router identifier of a BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number router-id id
```

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

router-id *id*

Description: Specifies the Router BGP identifier expressed in IPv4 address format. The value 0.0.0.0 and addresses in range 224.0.0.0 - 247.255.255.255 cannot be used as *id*.

Value: a.b.c.d.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the router-id of a BGP router.

```
(config)# router bgp 65000 router-id 1.1.1.1
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf

Description

Associates a VRF with router BGP.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

The VRF must be previously created.

Example:

This example shows how to associate a VRF with the router BGP.

```
(config)# router bgp 65000 vrf example
(config-vrf-example)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf address-family

Description

Enables the router BGP address family support per VRF.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **address-family** { **ipv4** | **ipv6** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.
Value: 1-4294967295.
Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.
Value: Name of an existent VRF.
Default Value: N/A

address-family { **ipv4** | **ipv6** }

Description: Selects the address family (AFI).
Value: **ipv4** or **ipv6**. IPv4 or IPv6 address family.
Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast.** IPv4 or IPv6 unicast routes.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

The disabling of a router BGP address family support is only possible if it is not configured in any BGP neighbor. Thus, the removal of all BGP neighbors address family configuration is required before disabling the address family on the router BGP.

Example:

This example shows how to enable the router BGP IPv4 unicast address family support.

```
(config)# router bgp 65000 vrf red
(config-bgp-vrf)# address-family ipv4 unicast
(config-bgp-vrf-address-family-ipv4/unicast)# commit
Commit complete.
```

Impacts and precautions

Changes on the address family will impact the router BGP capabilities. It also causes a flap in the established BGP sessions.

Hardware restrictions

N/A

router bgp vrf address-family network

Description

Inserts a network present locally in the routing table into BGP VRF domain and advertises it to the neighbor, when that network exactly matches a given prefix.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number vrf vrf-name address-family { ipv4 | ipv6 } unicast network
ip-prefix
```

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.
Value: 1-4294967295.
Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.
Value: Name of an existent VRF.
Default Value: N/A

address-family { **ipv4** | **ipv6** }

Description: Selects the address family (AFI).
Value: **ipv4** or **ipv6**. IPv4 or IPv6 address family.
Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast.** IPv4 or IPv6 unicast routes.

Default Value: N/A

network *ip-prefix*

Description: Defines the network that must be matched in order to be inserted into BGP domain.

Value: Must be a valid IPv4 or IPv6 prefix/mask.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

4.6	This command was introduced.
-----	------------------------------

6.2	Added support for IPv6.
-----	-------------------------

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to create a list of 2 network prefixes to be redistributed into

BGP domain in a VRF.

```
(config)# router bgp 65000
(config-bgp-65000)# vrf red
(config-bgp-vrf-red)# address-family ipv4 unicast
(config-bgp-vrf-address-family-ipv4/unicast)# network 40.40.40.240/28
(config-network-40.40.40.240/28)# top
(config)# router bgp 65000 vrf red address-family ipv4 unicast network 80.80.128.0/17
(config-network-80.80.128.0/17)# commit
```

Impacts and precautions

The network inserted into BGP domain will have its path attribute origin set as IGP. The network will be advertised to the neighbors only if it is already present in the VRF routing table. That means, there must be a route learned using local or connected networks or static routes.

Hardware restrictions

N/A

router bgp vrf address-family redistribute match-address

Description

Redistributes only the routes from VRF that match the specified address into the domain of this BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **address-family** { **ipv4** | **ipv6** } **unicast redistribute** { **connected** | **static** } **match-address** *ip-prefix*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

address-family { **ipv4** | **ipv6** }

Description:	Selects the address family (AFI).
Value:	ipv4 or ipv6 . IPv4 or IPv6 address family.
Default Value:	N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast.** IPv4 or IPv6 unicast routes.

Default Value: N/A

redistribute connected

Description: Redistributes VRF connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes VRF static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

match-address *ip-prefix*

Description: Redistributes specific routes that match the supplied prefix/mask filter into the domain of this BGP router.

Value: Must be a valid IPv4 or IPv6 prefix/mask.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure redistribution of IPv4 connected routes from VRF *example* which matches a single IPv4 address prefix.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-connected)# match-address 10.1.0.0/24
(config-bgp-vrf-address-family-redirect-connected)# commit
```

This example shows how to configure redistribution of IPv4 static routes from VRF *example* which matches a single IPv4 address prefix.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute static
(config-bgp-vrf-address-family-redirect-static)# match-address 10.1.0.0/24
(config-bgp-vrf-address-family-redirect-static)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf address-family { ipv4 | ipv6 } unicast redistribute

Description

Redistributes routes from the VRF into the domain of this BGP router.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **address-family** { **ipv4** | **ipv6** } **unicast redistribute** {**connected** | **ospf** | **static**}

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

address-family { **ipv4** | **ipv6** } **unicast**

Description: Redistributes unicast routes from IPv4 and/or IPv6 address family. Dual stack can be enabled.

Value: N/A

Default Value: N/A

redistribute connected

Description: Redistributes VRF connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute ospf

Description: Redistributes VRF OSPF routes into the domain of this BGP router. OSPF is onnly valid for IPv4 address-families.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes VRF static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Release	Modification
5.0	Support for redistribute OSPF.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure a redistribution of all IPv4 connected routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-connected)# commit
```

This example shows how to configure a redistribution of all IPv6 connected routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv6 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-connected)# commit
```

This example shows how to configure a redistribution of all OSPF routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute ospf
(config-bgp-vrf-address-family-redirect-ospf)# commit
```

This example shows how to configure a redistribution of all IPv4 static routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute static
(config-bgp-vrf-address-family-redirect-static)# commit
```

This example shows how to configure a redistribution of dual stack connected routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute connected
# router bgp 65000 vrf example address-family ipv6 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-connected)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf address-family { ipv4 | ipv6 } unicast redistribute administrative-status

Description

Configures the administrative status of a redistribution rule.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **address-family** { **ipv4|ipv6** } **unicast redistribute** {**connected** | **static** } **administrative-status** { **up** | **down** }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

address-family { **ipv4** | **ipv6** } **unicast**

Description: Redistributes only unicast routes from IPv4/IPv6 address family.

Value: N/A

Default Value: N/A

redistribute connected

Description: Redistributes VRF connected routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes VRF static routes into the domain of this BGP router.

Value: N/A

Default Value: N/A

administrative-status { up | down }

Description: Activates (up) or deactivates (down) the BGP router redistribution.

Value: **up** or **down**.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to deactivate the redistribution of IPv4 connected routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-static)# administrative-status down
(config-bgp-vrf-address-family-redirect-static)# commit
```

This example shows how to deactivate the redistribution of IPv4 static routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv4 unicast redistribute static
(config-bgp-vrf-address-family-redirect-static)# administrative-status down
(config-bgp-vrf-address-family-redirect-static)# commit
```

This example shows how to deactivate the redistribution of IPv6 connected routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv6 unicast redistribute connected
(config-bgp-vrf-address-family-redirect-static)# administrative-status down
(config-bgp-vrf-address-family-redirect-static)# commit
```

This example shows how to deactivate the redistribution of IPv6 static routes from VRF *example*.

```
# router bgp 65000 vrf example address-family ipv6 unicast redistribute static
(config-bgp-vrf-address-family-redirect-static)# administrative-status down
(config-bgp-vrf-address-family-redirect-static)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor

Description

Configures a neighbor for a BGP VRF router.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure a neighbor for a BGP VRF router.

```
(config)# router bgp 65000
(config-bgp-65000)# vrf red
(config-bgp-vrf-red)# neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor address-family

Description

Enables the BGP VRF neighbor address family support and enters in mode configuration.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **address-family** { **ipv4** | **ipv6** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

address-family { **ipv4** | **ipv6** }

Description: Selects the address family (AFI).

Value: **ipv4** or **ipv6**. IPv4 or IPv6 address family.

Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast**. IPv4 or IPv6 unicast routes.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

The enabling of a BGP VRF neighbor address family support is only possible if it is already configured in router BGP VRF.

Example:

This example shows how to enable the IPv4 unicast address family support for a BGP VRF neighbor.

```
(config)# router bgp 65000 vrf red
(config-bgp-vrf-red)# neighbor 1.1.10.2
(config-bgp-vrf-neighbor-1.1.10.2)# remote-as 65000
(config-bgp-vrf-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# commit
```

Impacts and precautions

Changes on the address family will impact the BGP neighbor capabilities. It also causes a flap in the established BGP neighbor session.

Hardware restrictions

N/A

router bgp vrf neighbor address-family allow-as-in

Description

When receiving routes from the respective neighbor, this option allows the installation of routes with local Autonomous System(AS) number present in AS path.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
router bgp as-number vrf vrf-name neighbor address address-family { ipv4 | ipv6 } unicast allow-as-in number-of-occurrences
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

address-family { ipv4 | ipv6 }

Description: Selects the address family (AFI).

Value: **ipv4** or **ipv6**. IPv4 or IPv6 address family.

Default Value: N/A

unicast

Description: Selects the subsequent address family (SAFI).

Value: **unicast**. IPv4 or IPv6 unicast routes.

Default Value: N/A

allow-as-in *number-of-occurrences*

Description: Specifies the maximum number of local AS number occurrences in AS path.

Value: 0-10.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

The enabling of a BGP VRF neighbor address family support is only possible if it is already configured in router BGP VRF.

Example:

This example shows how to configure **allow-as-in** to accept routes with up to five local AS occurrences in AS path.

```
(config)# router bgp 65000 vrf red
(config-bgp-vrf-red)# neighbor 1.1.10.2
(config-bgp-vrf-neighbor-1.1.10.2)# remote-as 65001
(config-bgp-vrf-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# allow-as-in 5
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor address-family as-override

Description

When advertising routes to the respective neighbor, this option replaces the remote Autonomous System(AS) number occurrences in AS path by the local AS number.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **address-family** { **ipv4** | **ipv6** } **unicast as-override**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

address-family { ipv4 | ipv6 }

- Description:** Selects the address family (AFI).
- Value:** **ipv4** or **ipv6**. IPv4 or IPv6 address family.
- Default Value:** N/A

unicast

- Description:** Selects the subsequent address family (SAFI).
- Value:** **unicast**. IPv4 or IPv6 unicast routes.
- Default Value:** N/A

as-override

- Description:** Option to replace the remote AS number by the local AS number in AS path.
- Value:** N/A
- Default Value:** N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

The enabling of a BGP VRF neighbor address family support is only possible if it is already configured in router BGP VRF.

Example:

This example shows how to configure **as-override** for a BGP VRF neighbor.

```
(config)# router bgp 65000 vrf red
(config-bgp-vrf-red)# neighbor 1.1.10.2
(config-bgp-vrf-neighbor-1.1.10.2)# remote-as 65001
(config-bgp-vrf-neighbor-1.1.10.2)# address-family ipv4 unicast
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# as-override
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor address-family prefix-list

Description

Associates a prefix list with a BGP neighbor in a VRF for export or import based on the address family.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **address-family** **ipv4 unicast** [**export-prefix-list** *prfx-name*] [**import-prefix-list** *prfx-name*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP neighbor address in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

address-family ipv4 unicast

Description: Enters in the BGP neighbor address family mode configuration.

Value: **ipv4 unicast.** IPv4 unicast address family.

Default Value: N/A

export-prefix-list *prfx-name*

Description: Specifies the prefix list for export to be directly associated with the BGP neighbor. Use the **no** form to remove this parameter.

Value: Name of a prefix list.

Default Value: N/A

import-prefix-list *prfx-name*

Description: Specifies the prefix list for import to be directly associated with the BGP neighbor. Use the **no** form to remove this parameter.

Value: Name of a prefix list.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

The VRF must be previously created.

The prefix-list must exist.

This command is only supported in IPv4 address family mode configuration.

Example:

This example shows how to associate the prefix list for export named PRXE with a BGP neighbor. This prefix list must be previously created.

```
(config)# router bgp 65000
(config-bgp-65000)# vrf red
(config-bgp-vrf-red)# neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# address-family ipv4 unicast
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# export-prefix-list PRXE
```

This example shows how to associate the prefix list for import named PRXI with a BGP neighbor. This prefix list must be previously created.

```
(config)# router bgp 65000
(config-bgp-65000)# vrf red
(config-bgp-vrf-red)# neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# address-family ipv4 unicast
(config-bgp-vrf-neighbor-address-family-ipv4/unicast)# import-prefix-list PRXI
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor administrative-status

Description

Configures the desired administrative status of a BGP VRF neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

administrative-status *status*

Description:	Activate (up) or deactivate (down) the BGP VRF neighbor.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure the administrative status for a BGP VRF neighbor.

```
(config)# router bgp 65000 vrf red neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# remote-as 65001
(config-bgp-vrf-neighbor-50.50.50.1)# administrative-status down
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor next-hop-self

Description

Configures the BGP VRF neighbor to use its own address as next hop in the advertised routes.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **next-hop-self**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

next-hop-self

Description:	Enables the neighbor option to use itself as next-hop.
Value:	N/A
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure the BGP VRF neighbor to use its own address as next hop in the advertised routes.

```
(config)# router bgp 65000 vrf red neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# next-hop-self
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor password

Description

Configures the BGP VRF neighbor password to be used in the Message Digest 5 (MD5) algorithm for TCP authentication.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **password** *pwd*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description: Specifies the Router BGP Autonomous System(AS) number.

Value: 1-4294967295.

Default Value: N/A

vrf *vrf-name*

Description: Specifies a VRF name.

Value: Name of an existent VRF.

Default Value: N/A

neighbor *address*

Description: Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

password *pwd*

Description:	Specifies the BGP neighbor case-sensitive password to be use in the TCP connection authentication.
Value:	string (length 2 - 80).
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

The same password must be applied for both BGP peers.

Example:

This example shows how to configure the BGP VRF neighbor password using a plain text. This password is shown encrypted after the commit.

```
(config)# router bgp 65000 vrf green neighbor 50.50.50.1 remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# password pwdTest
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

This example shows how to configure the BGP VRF neighbor password using an encrypted password.

```
(config)# router bgp 65000 vrf green neighbor 50.50.50.1 remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# password "hls:2922743918:337ZpL=Z"
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

This example shows how to configure the BGP VRF neighbor password using special characters (i.e: " " , "?" , "!" , ";"). Please note that it is necessary to use double quotation marks in this case.

```
(config)# router bgp 65000 vrf green neighbor 50.50.50.1 remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# password "pwd?test:2"
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

Impacts and precautions

Password must be enclosed in double quotation marks if special characters were used (i.e: " " , "?" , "!" , ";").

Note that in an established BGP session if password is configured or changed the session will be restarted.

Hardware restrictions

N/A

router bgp vrf neighbor remote-as

Description

Configures the BGP VRF neighbor remote Autonomous System(AS) number.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **remote-as** *as-number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

remote-as *as-number*

Description:	Specifies the BGP VRF neighbor remote Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to configure a remote Autonomous System (AS) number for a VRF neighbor.

```
(config)# router bgp 65000 vrf red neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# remote-as 65000
(config-bgp-vrf-neighbor-50.50.50.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf neighbor update-source-address

Description

Configures the BGP VRF neighbor source address to be used during the session establishment.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **neighbor** *address* **update-source-address** *address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

neighbor *address*

Description:	Specifies the BGP VRF neighbor address in IPv4 or IPv6 address format.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

update-source-address *address*

Description: Specifies the BGP neighbor source address in IPv4 or IPv6 address format.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
6.2	Added support for IPv6.

Usage Guidelines

The VRF must be previously created.

Example:

This example show how to configure the source address for a BGP VRF neighbor in the neighbor command tree.

```
(config)# router bgp 65000 vrf red neighbor 50.50.50.1
(config-bgp-vrf-neighbor-50.50.50.1)# update-source-address 100.100.100.1
(config-bgp-vrf-neighbor-50.50.50.1)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router bgp vrf router-id

Description

Configures the router identifier of a BGP router per VRF.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router bgp *as-number* **vrf** *vrf-name* **router-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

as-number

Description:	Specifies the Router BGP Autonomous System(AS) number.
Value:	1-4294967295.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies a VRF name.
Value:	Name of an existent VRF.
Default Value:	N/A

router-id *id*

Description:	Specifies the Router BGP identifier expressed in IPv4 address format. The value 0.0.0.0 and addresses in range 224.0.0.0 - 247.255.255.255 cannot be used as <i>id</i> .
Value:	a.b.c.d.
Default Value:	global bgp router-id

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.

Usage Guidelines

The VRF must be previously created.

When the router-id for the BGP router in the VRF is not configured, the global BGP router-id is used.

Example:

This example shows how to configure the router-id for the BGP router in the VRF red.

```
(config)# router bgp 65000 vrf red router-id 1.1.1.1
(config-bgp-65000)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip bgp

Description

Shows summarized information about the BGP routing processes.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show ip bgp [vrf name] summary
```

Parameters

vrf name

Description: Specifies a VRF name (only in supported platforms).

Value: Name of an existent VRF.

Default Value: N/A

Output Terms

Output	Description
VRF Name	Indicates the VRF name for the current BGP instance.
BGP router identifier	Indicates the router identifier of BGP.
local AS number	Local Autonomous System(AS) number.
Admin Status	Indicates the administrative status of BGP.
iBGP routes in	The total number of IBGP routes received.

Output	Description
eBGP routes in	The total number of EBGP routes received.
Eligible routes	The number of prefixes received that are eligible to become active.
Ineligible routes	The number of prefixes received that are not eligible to become active.
Active routes	The number of active routes.
Advertised routes	The number of advertised prefixes currently associated with any neighbor.
Neighbor	The IP address of the neighbor.
V	BGP version.
AS	The remote Autonomous System(AS) number.
MsgRcvd	The total number of messages received from the neighbor.
MsgSent	The total number of messages transmitted to the neighbor.
Up/Down	How long the neighbor is in the established state or since the last time it was established. When zeroed, the session were never established. See the usage guidelines of this command for information about time counter format.
State/PfxRcd	The BGP neighbor state while the session is not established or the number of prefixes received from the neighbor if the session is already established.
Default	
N/A	

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.
4.6	Added VRF support.

Usage Guidelines

The time counter format is showed using only three units progressively:

- hh:mm:ss - example: 23:59:59
- XX**d**aysYY**h**oursZZ**m**in - example: 06d23h59m
- XX**w**eeksYY**d**aysZZ**h**ours - example: 04w01d23h
- XX**m**onthsYY**w**eeksZZ**d**ays - example: 11m04w01d
- XX**y**earsYY**m**onthsZZ**w**eeks - example: 99y11m04w

Example:

This example shows summarized information about BGP routers on global VRF.

```
# show ip bgp
BGP router identifier 1.1.10.1, local AS number 101, Admin Status: up
ipv4 unicast statistics:
  iBGP routes in      : 1      eBGP routes in      : 0      Eligible routes      : 0
  Ineligible routes    : 1      Active routes       : 0      Advertised routes    : 0
ipv6 unicast statistics:
```

```

iBGP routes in      : 5    eBGP routes in      : 0    Eligible routes   : 3
Ineligible routes   : 2    Active routes      : 3    Advertised routes : 0

Neighbor    V    AS    MsgRcvd    MsgSent    Up/Down    State/PfxRcd
-----
1.1.1.1      4    101    165        157        00:24:41        1
1111::1      4    101    169        157        00:24:18        5

```

This example shows summarized information about all BGP routers on VRFs.

```

# show ip bgp vrf all summary
VRF: global
=====
BGP router identifier 1.1.10.1, local AS number 101, Admin Status: up

ipv4 unicast statistics:
iBGP routes in      : 1    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 1    Active routes      : 0    Advertised routes : 0

vpngv4 unicast statistics:
iBGP routes in      : 0    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 0    Active routes      : 0    Advertised routes : 0

ipv6 unicast statistics:
iBGP routes in      : 5    eBGP routes in      : 0    Eligible routes   : 3
Ineligible routes   : 2    Active routes      : 3    Advertised routes : 0

Neighbor    V    AS    MsgRcvd    MsgSent    Up/Down    State/PfxRcd
-----
1.1.1.1      4    101    165        157        00:24:41        1
1111::1      4    101    169        157        00:24:18        5

VRF: GREEN
=====
BGP router identifier 1.1.10.1, local AS number 101, Admin Status: up

ipv4 unicast statistics:
iBGP routes in      : 1    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 1    Active routes      : 0    Advertised routes : 0

Neighbor    V    AS    MsgRcvd    MsgSent    Up/Down    State/PfxRcd
-----
2.2.2.2      4    101    165        157        00:00:00        idle

```

This example shows summarized information about a specific VRF.

```

# show ip bgp vrf GREEN summary
VRF: GREEN
=====
BGP router identifier 1.1.10.1, local AS number 101, Admin Status: up

ipv4 unicast statistics:
iBGP routes in      : 1    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 1    Active routes      : 0    Advertised routes : 0

vpngv4 unicast statistics:
iBGP routes in      : 0    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 0    Active routes      : 0    Advertised routes : 0

ipv6 unicast statistics:
iBGP routes in      : 0    eBGP routes in      : 0    Eligible routes   : 0
Ineligible routes   : 0    Active routes      : 0    Advertised routes : 0

Neighbor    V    AS    MsgRcvd    MsgSent    Up/Down    State/PfxRcd
-----
2.2.2.2      4    101    165        157        00:00:00        idle

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip bgp community

Description

Shows information about communities received from neighbors and included in the BGP routing table.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show ip bgp community [ attribute { community | internet | local-AS | no-advertise | no-export } | network ip-address ]*
```

Parameters

community

Description: Shows information about all received communities.

Value: N/A

Default Value: N/A

attribute *community* | **internet** | **local-AS** | **no-advertise** | **no-export**

Description: Specifies the community attribute to be searched for.

Value: Well-known community or specific community in AS:nn format.

Default Value: N/A

network *ip-address*

Description: Specifies the network to filter displayed information.

Value: Must be a valid IPv4 or IPv6 network.

Default Value: N/A

Output Terms

Output	Description
Status Code	The status of the prefix entry. This information is displayed prior to the Network column. The legend of status codes is displayed at the beginning of each report.
Network	The network address.
Next Hop	Indicates the IP address for forwarding traffic to destination network.
Metric	Indicates the route metric.
LocPrf	Indicates the route local preference value. The default value is 100.
Community	Indicates the route communities attribute.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command to list all communities.

```
# show ip bgp community
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal; S Stale;
-----
Network          Next Hop      Metric  LocPrf  Community
-----
*>i 40.40.40.0/24 200.200.200.4 0        100     no-export
*>i 30.30.30.0/24 200.200.200.3 0        100     no-advertise
*>i 20.20.20.0/24 200.200.200.2 0        100     local-AS
*>i 10.10.10.0/24 200.200.200.1 0        100     internet 200:200
*> 21.21.21.0/24 0.0.0.0       0        100     100:100 200:200 300:300
*> 22.22.22.0/24 0.0.0.0       0        100     100:100 200:200 300:30000
```

This example shows how to use this command to filter a specific community.

```
# show ip bgp community attribute 100:100
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal; S Stale;
-----
Network          Next Hop      Metric  LocPrf  Community
-----
*> 21.21.21.0/24 0.0.0.0       0        100     100:100 200:200 300:300
*> 22.22.22.0/24 0.0.0.0       0        100     100:100 200:200 300:30000
```

This example shows how to use this command to filter a specific network.

```
# show ip bgp community network 10.10.10.0/24
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal; S Stale;
-----
Network          Next Hop      Metric  LocPrf  Community
-----
*>i 10.10.10.0/24 200.200.200.1 0        100     internet 200:200
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip bgp neighbor

Description

Shows information about the BGP neighbors.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show ip bgp [ vrf name ] neighbor [ ip-address | summary | brief | detail | extensive ]
```

Parameters

vrf name

Description: Specifies a VRF name (only in supported platforms)

Value: Name of an existent VRF.

Default Value: N/A

ip-address

Description: Filters the command output by the remote IP address.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

summary

Description: Shows summarized information about BGP neighbors.

Value: N/A

Default Value: N/A

brief

Description: Shows brief information about BGP neighbors.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the BGP neighbors.

Value: N/A

Default Value: N/A

extensive

Description: Shows extensive information about the BGP neighbors.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Remote address	The neighbor IP address.
Port	Indicates the remote and local TCP ports used in this connection.
Local address	The local IP address of BGP session.
Admin	Administrative status of the neighbor.
BGP state	The negotiation stage of BGP session.
Local AS	Local Autonomous System(AS) number.
BGP Version	BGP Protocol Version.
Remote AS	Autonomous System(AS) number of the neighbor.

Output	Description
Last received Update message	Elapsed time since the last BGP Update message was received from the neighbor. If no Update messages were received, this value remains zeroed. See the usage guidelines of this command for information about time counter format.
Last received message	Elapsed time since the last BGP message was received from the neighbor. If no BGP messages were received, this value remains zeroed. See the usage guidelines of this command for information about time counter format.
Up/Down time	How long the neighbor is in the established state or since the last time it was established. When zeroed, the session was never established. See the usage guidelines of this command for information about time counter format.
Neighbor ID	BGP neighbor router identifier.
Hold time	Time interval in seconds for the hold timer established with the neighbor.
Keepalive	Time interval in seconds for the keepalive timer established with the neighbor.
Neighbor capabilities	Capabilities exchanged with the neighbor. Capabilities neither advertised nor received are omitted from the list.
Address family IPv4 Unicast	Address family IPv4 Unicast capability was advertised and/or received.
Address family IPv6 Unicast	Address family IPv6 Unicast capability was advertised and/or received.
Four Bytes AS Number	Four Bytes AS Number capability was advertised and/or received.

Output	Description
Graceful Restart	Graceful Restart capability was advertised and/or received.
ORF	Outbound Route Filters capability was advertised and/or received.
ORF Cisco	Outbound Route Filters Cisco capability was advertised and/or received.
Route Refresh	Route Refresh capability was advertised and/or received.
Route Refresh Cisco	Route Refresh Cisco capability was advertised and/or received.
Message counters	Number of BGP messages sent or received for each type of message.
Type	<p>Type of BGP message:</p> <ul style="list-style-type: none"> • Open: used to establish a BGP session; • Notification: used to notify an error condition and close a BGP session; • Update: exchange network reachability information; • Keepalive: exchange between peers to keep a BGP session established; • Route refresh: used to request BGP route updates from BGP neighbor or to send outbound route updates to a BGP neighbor; • Total: the number of all BGP message types exchanged with the neighbor.
Sent	The number of sent messages of each BGP message type.
Received	The number of received messages of each BGP message type.

Output	Description
Connect retries	The number of connection retry attempts of this peer.
BGP transitions established	The total number of times the state transitioned into established state for this neighbor.
Last BGP state	The BGP neighbor previous state.
Last BGP event	The last BGP event which was used to transition the BGP state.
Selected local address	The local address used by the transport connection for the peering session.
Selected local port	The local port used by the transport connection for the peering session.
Selected remote port	The remote port used by the transport connection for the peering session.
Peer prefix counters	The number of prefixes exchanged with the peer classified according to the performed action.
Received	The total number of prefixes received from this peer.
Sent	The number of prefixes ready to be sent.
Accepted	The number of accepted prefixes.
Advertised	The number of advertised prefixes.
Rejected	The number of rejected prefixes.
Active	The number of active prefixes.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.
4.6	Added VRF support.

Usage Guidelines

The time counter format is showed using only three units progressively:

- hh:mm:ss - example: 23:59:59
- XX**d**aysYY**h**oursZZ**m**in - example: 06d23h59m
- XX**w**eeksYY**d**aysZZ**h**ours - example: 04w01d23h
- XX**m**onthsYY**w**eeksZZ**d**ays - example: 11m04w01d
- XX**y**earsYY**m**onthsZZ**w**eeks - example: 99y11m04w

When the command does not provide any VRF filter, only the information about the BGP in the *global* VRF will be displayed.

Example:

This example shows how to use the `show ip bgp neighbor brief` command.
Please note that for sessions not established the Port value is zero.

```
# show ip bgp neighbor brief
```

Remote address	Port	Local address	Port	Admin	BGP state
150.150.150.2	0	199.199.199.1	0	up	active
100.100.100.1	48078	200.200.200.1	179	up	established
200.200.200.3	0	200.200.200.2	0	up	active
1111::1	179	2222::2	39015	up	established

To show just the entry with Remote IP address 100.100.100.1, the following command must be used:

```
# show ip bgp neighbor 100.100.100.1 brief
```

Remote address	Port	Local address	Port	Admin	BGP state
100.100.100.1	48078	200.200.200.1	179	up	established

To order neighbor entries by the Remote address column, the following command must be used:

```
# show ip bgp neighbor brief | sort-by remote-addr-type
```

Remote address	Port	Local address	Port	Admin	BGP state
100.100.100.1	48078	200.200.200.1	179	up	established
150.150.150.2	0	199.199.199.1	0	down	idle
200.200.200.3	0	200.200.200.2	0	up	active

This example shows how to use the `show ip bgp neighbor detail` command.

```
# show ip bgp neighbor detail
Local AS: 300;
  Local address: 8.8.8.2; Admin: enable; BGP state: established;
  BGP Version: 4; Remote address: 8.8.8.1; Remote AS: 200;
  Last received Update message 00:00:12
  Last received message: 00:00:10
  Up/Down time: 00:04:01;
  Neighbor ID: 200.200.200.1;
  Hold time: 180 secs;
  Keepalive: 60 secs;

Neighbor capabilities:
  Address family IPv4 Unicast: advertised and received
  Address family IPv6 Unicast: advertised
  Four Bytes AS Number: advertised and received
  Route Refresh: advertised and received
  Route Refresh Cisco: advertised and received

Message counters:
  Type      Sent      Received
  ---      -
  Open      1          1
  Notification 0          0
  Update    1          1
  Keepalive 1          1
```

```

Route refresh 0          0
Total          3          3

Connect retries: 2; BGP transitions established: 1;
Last BGP state: Established; Last BGP event: received-keepalive;

Selected local address: 8.8.8.2;
Selected local port: 179; Selected remote port: 51304;

Local AS: 300;
Local address: 2222::2; Admin: enable; BGP state: established;
BGP Version: 4; Remote address: 1111::1; Remote AS: 200;
Last received update message: 00:55:01;
Last received message: 00:00:41;
Up/Down time: 01:01:16;
Neighbor ID: 1.1.1.1;
Hold time: 180 secs;
Keepalive: 60 secs;

Neighbor capabilities:
  Address family IPv4 Unicast: advertised
  Address family IPv6 Unicast: advertised and received
  Four Bytes AS Number: advertised and received
  Route Refresh: advertised and received
  Route Refresh Cisco: advertised and received

Message counters:
  Type          Sent          Received
  ---          -
  Open          2            2
  Notification  0            1
  Update        0            11
  Keepalive     197          197
  Route refresh 0            0
  Total         199          211

Connect retries: 2; BGP transitions established: 2;
Last BGP state: Established; Last BGP event: received-keepalive;

Selected local address: 2222::2;
Selected local port: 39015; Selected remote port: 179;

```

This example shows how to use the `show ip bgp neighbor extensive` command.

```

# show ip bgp neighbor extensive
Local AS: 300;
Local address: 8.8.8.2; Admin: enable; BGP state: established;
BGP Version: 4; Remote address: 8.8.8.1; Remote AS: 200;
Last received Update message 01d02h03m
Last received message: 00:00:25
Up/Down time: 04w01d03h;
Neighbor ID: 200.200.200.1;
Hold time: 180 secs;
Keepalive: 60 secs;

Neighbor capabilities:
  Address family IPv4 Unicast: advertised and received
  Address family IPv6 Unicast: advertised
  Four Bytes AS Number: advertised and received
  Route Refresh: advertised and received
  Route Refresh Cisco: advertised and received

Message counters:
  Type          Sent          Received
  ---          -
  Open          1            1
  Notification  0            0
  Update        1            1
  Keepalive     3154          3154
  Route refresh 0            0
  Total         3156          3156

```

```

Connect retries: 2; BGP transitions established: 1;
Last BGP state: Established; Last BGP event: received-keepalive;

Selected local address: 8.8.8.2;
Selected local port: 179; Selected remote port: 51304;

Peer prefix counters:
  ipv4 unicast:
    Received: 1          Sent: 1
    Accepted: 1          Advertised: 1
    Rejected: 0         Active: 0

Local AS: 300;
Local address: 2222::2; Admin: enable; BGP state: established;
BGP Version: 4; Remote address: 1111::1; Remote AS: 200;
Last received update message: 01:00:18;
Last received message: 00:00:53;
Up/Down time: 01:06:33;
Neighbor ID: 1.1.1.1;
Hold time: 180 secs;
Keepalive: 60 secs;

Neighbor capabilities:
  Address family IPv4 Unicast: advertised
  Address family IPv6 Unicast: advertised and received
  Four Bytes AS Number: advertised and received
  Route Refresh: advertised and received
  Route Refresh Cisco: advertised and received

Message counters:
  Type      Sent      Received
  ----      -
  Open      2          2
  Notification 0          1
  Update    0          11
  Keepalive 203         203
  Route refresh 0          0
  Total     205         217

Connect retries: 2; BGP transitions established: 2;
Last BGP state: Established; Last BGP event: received-keepalive;

Selected local address: 2222::2;
Selected local port: 39015; Selected remote port: 179;

Peer prefix counters:
  ipv4 unicast:
    Received: 0          Sent: 0
    Accepted: 0          Advertised: 0
    Rejected: 0         Active: 0

Peer prefix counters:
  ipv6 unicast:
    Received: 5          Sent: 0
    Accepted: 3          Advertised: 0
    Rejected: 2         Active: 3

```

This command shows brief information about neighbors from the given VRF (*red*, in the example).

```

#show ip bgp vrf red neighbor brief
Remote address      Port  Local address  Port  Admin  BGP State
-----
172.30.20.2         179   172.30.20.1    43647 up    established

```

This command shows just summary information about neighbors from all VRFs.

```
#show ip bgp vrf all neighbor summary
```

```

VRF: global
=====
Neighbor          V  AS    MsgRcvd  MsgSent  Up/Down  State/PfxRcd
-----
10.10.10.1         4  300    2109     4918     00:00:15      0
a:f0ca:bebe:cafe::1 4  400    1760     2019     14:38:07      4
cafe:c0ca:caca::1  4  300     0         0         00:00:00  idle
VRF: black
=====
Neighbor          V  AS    MsgRcvd  MsgSent  Up/Down  State/PfxRcd
-----
40.40.40.1         4  900    1777     2042     14:46:50      0
VRF: red, route-distinguisher 255.255.255.255:99
=====
Neighbor          V  AS    MsgRcvd  MsgSent  Up/Down  State/PfxRcd
-----
172.30.20.2        4  200     671     1013     14:39:14     11

#show ip bgp vrf red neighbor summary
Neighbor          V  AS    MsgRcvd  MsgSent  Up/Down  State/PfxRcd
-----
172.30.20.2        4  200     34         36     00:14:59     10

```

Impacts and precautions

For *sessions not established* the Local/Remote Port value will display zero and Local Address will display "0.0.0.0".

Hardware restrictions

N/A

show ip bgp prefixes

Description

Shows information about prefixes received from neighbors and included in the BGP routing table.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show ip bgp [vrf name] prefixes [destination prefix]
```

Parameters

vrf *name*

Description: Specifies a VRF name (only in supported platforms)

Value: Name of an existent VRF.

Default Value: N/A

destination *prefix*

Description: Specifies a destination prefix to be searched for. The search result will include prefixes that matches networks with the same prefix length or longer.

Value: Must be a valid IPv4 or IPv6 prefix.

Default Value: N/A

Output Terms

Output	Description
VRF Name	Indicates the VRF name for the current BGP instance.

Output	Description
Status Code	The status of the prefix entry. This information is displayed prior to the Network column. The legend of status codes is displayed at the beginning of each report.
Origin codes	The origin of the prefix entry. This information is displayed right after the Path column. The legend of origin codes is displayed at the beginning of each report.
Network	The network address.
Next Hop	Indicates the IP address for forwarding traffic to destination network.
Metric	Indicates the route metric.
LocPrf	Indicates the route local preference value. The default value is 100.
Weight	Indicates the route local degree of preference. A lower weight value is preferred.
Learned from	Indicates the IP address from where this entry was learned from.
Path	Indicates the AS path through which the destination network was learned.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
4.0	Added support for IPv6.
4.6	<ul style="list-style-type: none"> Added VRF support. Added destination filter.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command to list prefixes learned on VRF Global. Please note the different status code for entries "221.10.0.19/19" since one was selected as best path due to higher local preference.

```
# show ip bgp prefixes
```

```
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
```

```
Origin codes: i - IGP; e - EGP; ? - incomplete;
```

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	221.10.0.0/19	172.16.78.1	0	200	0	172.16.78.1	65001 ?
*>	221.10.0.0/20	172.16.78.1	0	100	0	172.16.78.1	65001 ?
*	221.10.0.0/19	172.16.78.3	0	100	0	172.16.78.3	65001 ?
*>	221.10.16.0/20	172.16.78.3	0	100	0	172.16.78.3	65001 ?
*>i	2001::/64	2002::3	0	100	0	1111::1	i
*>i	2002::/64	1111::1	0	100	0	1111::1	i
* i	5050::/64	8009::2	0	100	0	1111::1	i
*>i	8009::/64	1111::1	0	100	0	1111::1	i

To show just the network 221.10.16.0/20 entry, use the following destination filter:

```
# show ip bgp prefixes destination 221.10.16.0/20
```

Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
Origin codes: i - IGP; e - EGP; ? - incomplete;

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	221.10.16.0/20	172.16.78.3	0	100	0	172.16.78.3	65001 ?

Similarly, to search for all networks that start with 221.10.X.X, this filter could be used:

```
# show ip bgp prefixes destination 221.10.0.0/16
```

Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
Origin codes: i - IGP; e - EGP; ? - incomplete;

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	221.10.0.0/19	172.16.78.1	0	200	0	172.16.78.1	65001 ?
*>	221.10.0.0/20	172.16.78.1	0	100	0	172.16.78.1	65001 ?
*	221.10.0.0/19	172.16.78.3	0	100	0	172.16.78.3	65001 ?
*>	221.10.16.0/20	172.16.78.3	0	100	0	172.16.78.3	65001 ?

This example shows how to use this command to list prefixes learned on all VRFs including VRF global.

```
# show ip bgp vrf all prefixes
```

VRF: global

=====

Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
Origin codes: i - IGP; e - EGP; ? - incomplete;

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	2.1.0.0/19	7.6.8.1	0	200	0	7.6.8.1	500 ?
*>	2.1.0.0/20	7.6.8.1	0	100	0	7.6.8.1	500 ?
*	2.1.0.0/19	7.6.8.3	0	100	0	7.6.8.3	500 ?
*>	2.1.6.0/20	7.6.8.3	0	100	0	7.6.8.3	500 ?
*>i	2001::/64	2002::3	0	100	0	1111::1	i
*>i	2002::/64	1111::1	0	100	0	1111::1	i
* i	5050::/64	8009::2	0	100	0	1111::1	i
*>i	8009::/64	1111::1	0	100	0	1111::1	i

VRF: red

=====

Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
Origin codes: i - IGP; e - EGP; ? - incomplete;

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	2.2.1.0/20	7.6.8.2	0	100	0	7.6.8.2	200 ?

To filter a specific VRF, the following command must be used:

```
# show ip bgp vrf red prefixes
```

Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
Origin codes: i - IGP; e - EGP; ? - incomplete;

	Network	Next Hop	Metric	LocPrf	Weight	Learned from	Path
*>	2.2.1.0/20	7.6.8.2	0	100	0	7.6.8.2	200 ?

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip bgp vpnv4 labels

Description

Shows information about incoming and outgoing BGP labels for each prefix on a Virtual Private Network IPv4 (VPNv4).

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618, DM4050, DM4250.

Syntax

```
show ip bgp [vrf name] vpnv4 labels
```

Parameters

vrf *name*

Description: Specifies a VRF name (only in supported platforms)

Value: Name of an existent VRF.

Default Value: N/A

vpnv4 labels

Description: Shows the incoming and outgoing labels for each prefix on a VPNv4.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
VRF Name	Indicates the VRF name for the current BGP instance.

Output	Description
Status codes	The status of the prefix entry. This information is displayed prior to the Network column. The legend of status codes is displayed at the beginning of each report.
RD	Route Distinguisher of the VPNv4 prefix.
Network	The network address.
Next Hop	Indicates the IP address for forwarding traffic to destination network.
In Label	Indicates the incoming label.
Out Label	Indicates the outgoing label.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.6	This command was introduced.

Usage Guidelines

This command can be used to show information about the prefixes and respective incoming and outgoing labels on a VPNv4.

Example:

This example shows how to use this command to display all prefixes and the respective labels related to VRF global.

```
# show ip bgp vpnv4 labels
```

```
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
```

RD	Network	Next Hop	In Label	Out Label
*> 100:1	50.50.50.0/24	200.200.200.1	17	--
*> 100:1	50.50.51.0/28	200.200.200.1	17	--
*> 100:1	50.50.52.0/31	200.200.200.1	17	--
*>i 100:1	150.150.150.0/24	200.200.200.2	--	17
*>i 100:1	150.150.151.0/28	200.200.200.2	--	17
*>i 100:1	150.150.152.0/31	200.200.200.2	--	17
*> 100:2	90.90.90.0/24	200.200.200.1	16	--
*>i 100:2	190.190.190.0/24	200.200.200.2	--	16
*>i 101:1	6.6.6.0/24	200.200.200.3	--	16
*>i 101:1	160.160.160.0/24	200.200.200.3	--	16
*>i 1.2.3.4:1	9.9.9.0/24	200.200.200.3	--	17
*>i 1.2.3.4:1	195.195.195.0/24	200.200.200.3	--	17
*>i 90000:5	2.2.2.0/24	200.200.200.3	--	18

To show the VPNv4 information for all VRFs the following command can be used:

```
# show ip bgp vrf all vpnv4 labels
```

```
VRF: green, route-distinguisher 100:1
```

```
=====
```

```
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
```

RD	Network	Next Hop	In Label	Out Label
*> 100:1	50.50.50.0/24	200.200.200.1	17	--
*> 100:1	50.50.51.0/28	200.200.200.1	17	--
*> 100:1	50.50.52.0/31	200.200.200.1	17	--
*>i 100:1	150.150.150.0/24	200.200.200.2	--	17
*>i 100:1	150.150.151.0/28	200.200.200.2	--	17
*>i 100:1	150.150.152.0/31	200.200.200.2	--	17
*>i 101:1	6.6.6.0/24	200.200.200.3	--	16
*>i 101:1	160.160.160.0/24	200.200.200.3	--	16

```
VRF: red, route-distinguisher 100:2
```

```
=====
```

```
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
```

RD	Network	Next Hop	In Label	Out Label
*> 100:2	90.90.90.0/24	200.200.200.1	16	--


```
*>i 100:2 190.190.190.0/24 200.200.200.2 -- 16
```

To show the VPNv4 information for a specific VRF the following command can be used:

```
# show ip bgp vrf red vpnv4 labels
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;

      RD      Network      Next Hop      In      Out
-----
*> 100:2  90.90.90.0/24    200.200.200.1  16      --
*>i 100:2  190.190.190.0/24 200.200.200.2  --      16
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip bgp vpnv6 labels

Description

Shows information about incoming and outgoing BGP labels for each prefix on a Virtual Private Network IPv6 (VPNv6).

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618, DM4050, DM4250.

Syntax

```
show ip bgp [vrf name] vpnv6 labels
```

Parameters

vrf *name*

Description: Specifies a VRF name (only in supported platforms)

Value: Name of an existent VRF.

Default Value: N/A

vpnv6 labels

Description: Shows the incoming and outgoing labels for each prefix on a VPNv6.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
VRF Name	Indicates the VRF name for the current BGP instance.

Output	Description
Status codes	The status of the prefix entry. This information is displayed prior to the Network column. The legend of status codes is displayed at the beginning of each report.
RD	Route Distinguisher of the VPNv6 prefix.
Network	The network address.
Next Hop	Indicates the IP address for forwarding traffic to destination network.
In Label	Indicates the incoming label.
Out Label	Indicates the outgoing label.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

This command can be used to show information about the prefixes and respective incoming and outgoing labels on a VPNv6.

Example:

This example shows how to use this command to display all prefixes and the respective labels related to VRF global.

```
# show ip bgp vpnv6 labels
Status codes: s suppressed; d damped; h history; * valid; > best; i - internal;
S Stale;
```

	RD	Network	Next Hop	In Label	Out Label
*>	60000:740	2001:db8:101::/64	::ffff:1.1.1.1	16	--
*>	60000:740	2001:db8:201::/64	::ffff:1.1.1.1	16	--
*>i	60000:750	2001:db8:102::/64	::ffff:4.4.4.1	--	16
*>i	60000:750	2001:db8:202::/64	::ffff:4.4.4.1	--	16

To show the VPNv6 information for all VRFs the following command can be used:

```
# show ip bgp vrf all vpnv6 labels
```

To show the VPNv6 information for a specific VRF the following command can be used:

```
# show ip bgp vrf red vpnv6 labels
```

Impacts and precautions

N/A

Hardware restrictions

N/A

OSPF

This topic describes the commands related to management of OSPF topologies such as commands to configure the OSPF parameters or to inspect the protocol status.

clear ospf

Description

Clears OSPF information about neighbors, processes or statistics.

Supported Platforms

This command is supported in all platforms.

Syntax

clear ospf neighbor [**ip** *neighbor-ip*][**process-id** *process-id*]

clear ospf process *process-id*

clear ospf statistics interface

Parameters

neighbor

Description: Clears OSPF neighbor information.

Value: N/A

Default Value: N/A

neighbor ip *neighbor-ip*

Description: Clears only neighbor information for the specified OSPF neighbor.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

neighbor process-id *process-id*

Description: Clears only neighbor information for the specified OSPF process ID.

Value: 1-65535.

Default Value: N/A

process *process-id*

Description: Clears OSPF information for the specified OSPF process ID.

Value: 1-65535.

Default Value: N/A

statistics interface

Description: Clears OSPF interface statistics.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to clear OSPF information.

```
# clear ospf process 1
# clear ospf neighbor
# clear ospf neighbor ip 10.10.10.0
# clear ospf neighbor ip 10.10.10.0 process-id 1
# clear ospf statistics interface
```

Impacts and precautions

The command “clear ospf process” will restart all OSPF adjacencies from the specified router instance. The command “clear ospf neighbor” will restart all OSPF adjacencies if neighbor address was not specified.

Hardware restrictions

N/A

router ospf

Description

Configures an OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router. For platforms with VRF restrictions, only the VRF 'global' is available.
Value:	string.
Default Value:	global

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.
5.0	The command was modified to support OSPF routers in VRFs.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure an OSPF router.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# commit
```

This example shows how to configure an OSPF router in VRF *green*.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 10 vrf green
(config-ospf-10-vrf-green)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf administrative-status

Description

Configures the administrative status of an OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

administrative-status *status*

Description: Activates (up) or deactivates (down) the OSPF router.
Value: up | down.
Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# administrative-status down
(config-ospf-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area

Description

Configures the area of a router OSPF.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area-id

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	1-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf area.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 5
(config-area-5)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area administrative-status

Description

Configures the administrative status of an OSPF area.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

administrative-status *status*

Description:	Activates (up) or deactivates (down) the OSPF area.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 5 administrative-status down
(config-area-5)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface

Description

Enables the OSPF protocol on an specified L3 or loopback interface.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

area-id

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value: 0-4294967295. 0.0.0.0-255.255.255.255.
Default Value: 0.

interface-name

Description:	Specifies L3 and loopback interfaces for the OSPF router. The L3 and loopback interfaces must be created before the commit.
Value:	Any L3 and loopback interfaces.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf interface.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 5 interface l3-vlan1
(config-interface-l3-vlan1)# exit
(config-area-0)# interface loopback-1
(config-interface-loopback-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface administrative-status

Description

Configures the administrative status of an OSPF area interface.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: L3 interface.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the L3 interface.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 administrative-status down
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface authentication

Description

Configures the authentication type for an OSPF interface. Only one type of authentication may be configured.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **authentication** { **md5** | **none** | **simple-password** } [**authentication-key-id** *key-id*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: N/A

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: L3 interface.

Default Value: N/A

authentication { md5 | none | simple-password }

Description: Specifies the type of authentication to be used.

Value: **md5**, **none** or **simple-password**.

Default Value: **none**.

authentication md5 authentication-key-id *key-id*

Description: Specifies a key ID for MD5 authentication. This parameter is only available for the MD5 authentication type.

Value: 0-255.

Default Value: 0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the available authentication types.

```
# config terminal
Entering configuration mode terminal
(config-ospf-area-intf-l3-if1)# authentication md5 authentication-key-id 1
(config)# commit
(config-ospf-area-intf-l3-if1)# authentication none
(config)# commit
(config-ospf-area-intf-l3-if1)# authentication simple-password
(config)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface authentication-key

Description

Configures the authentication key for an OSPF interface. This command is only available after an authentication type of MD5 or simple password has been configured.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **authentication-key** *key*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.

Value: 1-65535.

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.

Value: string.

Default Value: global

area *area-id*

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: N/A

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: L3 interface.

Default Value: N/A

authentication-key *key*

Description: Specifies the authentication key to be used.

Value: String containing from 2 to 8 characters for simple password authentication, or from 2 to 16 characters for MD5 authentication.

Default Value: Empty string.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure MD5 authentication.

```
# config terminal
Entering configuration mode terminal
(config-ospf-area-intf-l3-if1)# authentication md5 authentication-key-id 1
(config-ospf-area-intf-l3-if1)# authentication-key abcde
(config)# commit
```

This example shows how to configure simple password authentication.

```
(config-ospf-area-intf-l3-if1)# authentication simple-password
(config-ospf-area-intf-l3-if1)# authentication-key abcde
(config)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface bfd session-type

Description

Configures the BFD session type for an L3 interface in OSPF router.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **bfd session-type** *type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.

Value: 1-65535.

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.

Value: string.

Default Value: global

area *area-id*

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

bfd session-type *type*

Description: Configures BFD session-type for this OSPF interface. The *none* type means BFD is disabled for this OSPF interface. The *desired* type means BFD is enabled right after the OSPF session establishment and will be used to monitor the session. In case of session type mismatch between the two endpoints, the OSPF may be run on this interface ignoring BFD state.

Value: desired | none

Default Value: none

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release

Modification

5.2

This command was introduced

Usage Guidelines

Commands to configure the BFD session type.

When the BFD session type is configured as desired, the timers min-tx-interval and min-rx-interval have both the value of 100ms and the multiplier has a fixed value of 3.

Example:

This example shows how to configure BFD session type.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100
(config-ospf-area-intf-l3-vlan100-bfd)# session-type desired
(config-ospf-area-intf-l3-vlan100-bfd)# commit
(config-ospf-area-intf-l3-vlan100-bfd)# session-type none
(config-ospf-area-intf-l3-vlan100-bfd)# commit
```

Impacts and precautions

When the session type is changed from desired to none, the OSPF session may flap.

Hardware restrictions

N/A

router ospf area interface cost

Description

Explicitly sets the OSPF routing cost of a L3 interface.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **cost** *cost*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

cost *cost*

Description: Explicitly sets the OSPF routing cost of a L3 interface.

Value: 1-65535

Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the cost.

Example:

This example shows how to configure the cost.

```
# config terminal
Entering configuration mode terminal
```

```
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface 13-vlan100 cost 2
(config-ospf-area-intf-13-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface dead-interval

Description

Configures how long the OSPF process will wait before declaring a neighbor down if it stops receiving Hello packets.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **dead-interval** {*seconds* | **minimal fast-hello-multiplier** *multiplier*}

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.

Value: 1-65535.

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.

Value: string.

Default Value: global

area *area-id*

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

dead-interval *seconds*

Description: Interval after which a neighbor is declared down. If configured to 1 second, the configured Hello interval will be ignored and the Fast Hello multiplier will be used instead.

Value: 1-65535.

Default Value: 40.

dead-interval minimal fast-hello-multiplier *multiplier*

Description: Number of Hello packets to be sent per second when dead-interval is configured to 1 second (Fast Hellos).

Value: 3-20.

Default Value: 5.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the dead-interval.

Example:

This example shows how to configure the dead interval.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0 interface l3-vlan100
(config-ospf-area-intf-l3-vlan100)# dead-interval 50
(config-ospf-area-intf-l3-vlan100)# commit
(config-ospf-area-intf-l3-vlan100)# dead-interval 1
(config-ospf-area-intf-l3-vlan100)# dead-interval minimal fast-hello-
multiplier 3
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

A mismatch in the OSPF dead-intervals between neighbors will not permit the adjacency to be established or cause it to goes down.

Hardware restrictions

N/A

router ospf area interface hello-interval

Description

Configures the interval in which Hello packets will be sent.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **hello-interval** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

hello-interval *seconds*

Description: Sets the interval in which a Hello packet will be sent.

Value: 1-65535.

Default Value: 10.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the hello-interval.

Example:

This example shows how to configure the Hello interval.


```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 hello-interval 20
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

A mismatch in the OSPF hello-intervals between neighbors will not permit the adjacency to be established or cause it to go down.

Hardware restrictions

N/A

router ospf area interface mtu-ignore

Description

Disables OSPF Maximum Transmission Unit (MTU) mismatch detection on received Database Description (DBD) packets.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **mtu-ignore**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.

Value: 1-65535.

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.

Value: string.

Default Value: global

area *area-id*

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

mtu-ignore

Description: Sets the interface to ignore the MTU mismatch detection on received DBD packets.

Value: N/A

Default Value: N/A

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the mtu-ignore.

Example:

This example shows how to configure the mtu-ignore.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 mtu-ignore
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface network-type

Description

Configures the network type of an OSPF L3 interface.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *l3-interface-name* **network-type** *type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	N/A

interface l3-interface-name

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

network-type type

Description: Defines the network type to be used for this interface. For broadcast, the interface must be connected to a broadcast network. For point-to-point, the connection is between a single source and a single destination.

Value: broadcast | point-to-point.

Default Value: broadcast.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History**Release****Modification**

2.0

This command was introduced

Usage Guidelines

Commands to configure the network-type.

Example:

This example shows how to configure the network-type.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 network-type point-to-point
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface passive

Description

Configures an OSPF interface as passive. Passive interfaces neither establish adjacencies nor send OSPF updates, but is still advertised as part of the OSPF routing domain.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *interface-name* **passive**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface *interface-name*

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

passive

Description: Defines the interface as passive.

Value: N/A

Default Value: N/A

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the passive interface.

Example:

This example shows how to configure the interface as passive.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 passive
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area interface router-priority

Description

Configures the router priority of an OSPF L3 interface.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **interface** *l3-interface-name* **router-priority** *priority*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	N/A

interface l3-interface-name

Description: Specifies L3 interface for the OSPF router. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

router-priority priority

Description: Defines the router priority value, which determines the designated router for the specific network.

Value: 0-255.

Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the router-priority.

Example:

This example shows how to configure the router-priority.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 router-priority 120
(config-ospf-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area nssa

Description

Configures an OSPF area as NSSA (Not-So-Stubby Area).

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **nssa** [**no-summary** | **suppress-external**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	N/A

nssa

Description: Defines the OSPF area as NSSA. It is not possible to define the backbone area (area-id 0 or 0.0.0.0) or a stub area as NSSA.

Value: N/A

Default Value: N/A

no-summary

Description: Defines the OSPF area as a totally NSSA. It prevents an Area Border Router (ABR) from sending summary LSAs into the NSSA.

Value: N/A

Default Value: N/A

suppress-external

Description: When the NSSA ABR is also an ASBR, prevents it from originating Type-7 LSAs into the NSSA for redistributed external routes.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History**Release****Modification**

2.0

This command was introduced

Usage Guidelines

Commands to configure an area as NSSA.

Example:

This example shows how to configure an area as NSSA.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 1 nssa
(config-nssa)# no-summary
(config-nssa)# suppress-external
(config-nssa)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area range

Description

Summarizes routes matching IP address/mask at an area border.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **range** *ip mask* [**advertise** | **not-advertise**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

area *area-id*

Description:	Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	N/A

range *ip mask*

Description: Specifies the IP address and mask portion of the range. All inter-area network addresses that match the specified area range are summarized.

Value: N/A

Default Value: N/A

ip

Description: IP address to match.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

mask

Description: Netmask to match.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

advertise

Description: Advertises the address range.

Value: N/A

Default Value: N/A

not-advertise

Description: Does not advertise the range.

Value: N/A

Default Value: N/A

Default

advertise.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to summarize a route matching address/mask.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 0 range 172.16.0.1 255.255.255.0
(config-area-0)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf area stub

Description

Configures an OSPF area as a stub area.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **area** *area-id* **stub** [**no-summary**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

area *area-id*

Description: Specifies the OSPF router area identifier. It may be specified in decimal or in dot-decimal notation.
Value: 0-4294967295. 0.0.0.0-255.255.255.255.
Default Value: N/A

stub

Description: Defines the OSPF router area as stub area. It is not possible to define the backbone area (area-id 0 or 0.0.0.0) as a stub area.

Value: N/A

Default Value: N/A

no-summary

Description: Defines the OSPF area as a totally stub area. It prevents an Area Border Router (ABR) from sending summary LSAs into the stub area.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

2.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure an area as stub area.

Example:

This example shows how to configure an area as stub area.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# area 1 stub
(config-stub)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf export-prefix-list

Description

Configures the prefix-list to filter prefixes advertisement from route table into OSPF domain.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **export-prefix-list** *prefix-list-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

export-prefix-list *prefix-list-name*

Description: Specifies the prefix-list to be exported.
Value: Name of a prefix list.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to associate the prefix-list named PRX_LIST_EXPORT for export with an OSPF router. This prefix-list must be previously created.

```
(config)# router ospf 1
(config-ospf-1-vrf-global)# export-prefix-list PRX_LIST_EXPORT
(config-ospf-1-vrf-global)# commit
```

Impacts and precautions

This command only works on the prefixes redistributed by the ASBR into OSPF.

Hardware restrictions

N/A

router ospf import-prefix-list

Description

Configures the prefix-list to filter the installation of incoming OSPF prefixes on route table.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **import-prefix-list** *prefix-list-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

import-prefix-list *prefix-list-name*

Description: Specifies the prefix-list to be imported.
Value: Name of a prefix-list.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to associate the prefix-list for import named PRX_LIST_IMPORT with an OSPF router. This prefix-list must be previously created.

```
(config)# router ospf 1
(config-ospf-1-vrf-global)# import-prefix-list PRX_LIST_IMPORT
(config-ospf-1-vrf-global)# commit
```

Impacts and precautions

Note that once a prefix-list is associated to the OSPF router all other prefixes are denied, i.e., they are not installed on HW. But, even if not installed to HW, it does not affect network topology: prefixes are added to OSPF database and are still forwarded to other neighbors.

Hardware restrictions

N/A

router ospf maximum paths

Description

Configures the maximum number of equal-cost multi-paths (ECMP) for each OSPF router process.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **maximum paths** *number-of-paths*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

maximum paths *number-of-paths*

Description: Specifies the maximum number of paths with equal cost.
Value: 1-16.
Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the maximum number of paths of a router ospf.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# maximum paths 4
(config-ospf-1-vrf-global)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf mpls-te router-id

Description

Configure the MPLS Traffic Engineering (TE) routing protocol parameters.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospf mpls-te router-id *interface*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls-te router-id *interface*

Description: Specifies a loopback interface whose IP address will be used as MPLS TE router identifier.

Value: Any loopback interface redistributed by the OSPF router.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI. This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a router ospf mpls-te router-id.

```
# config terminal
Entering configuration mode terminal
(config)# interface loopback 0
(config-loopback-0)# ipv4 address 200.200.200.1/32
(config-loopback-0)# top
(config)# router ospf 1
(config-ospf-1-vrf-global)# mpls-te router-id loopback-0
(config-ospf-1-vrf-global)# area 0 interface loopback-0
(config-area-0)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf redistribute

Description

Redistributes external routes into the domain of this OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **redistribute** {**bgp** [**metric** *metric-value*] | **connected** | **static**} [**match-address** *a.b.c.d/x*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.
Value: 1-65535.
Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value: string.
Default Value: global

redistribute bgp

Description: Redistributes BGP routes into the domain of this OSPF router.
Value: N/A
Default Value: N/A

redistribute connected

Description: Redistributes connected routes into the domain of this OSPF router.

Value: N/A

Default Value: N/A

redistribute static

Description: Redistributes static routes into the domain of this OSPF router.

Value: N/A

Default Value: N/A

match-address *a.b.c.d/x*

Description: Redistributes specific routes, that match the supplied prefix/mask filter, into the domain of this OSPF router.

Value: Must be a valid IPv4 prefix/mask.

Default Value: N/A

metric

Description: Allows to set the metric that will be carried from BGP process to OSPF process. The default metric value is 1.

Value: 1-16777214.

Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the route redistribution.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# redistribute connected
(config-redistribute-connected)# exit
(config-ospf-1-vrf-global)# redistribute static
(config-redistribute-static)# exit
(config-ospf-1-vrf-global)# redistribute connected match-address 192.168.0.0/24
(config-redistribute-connected)# exit
(config-ospf-1-vrf-global)# redistribute static match-address 10.1.0.0/24
(config-redistribute-static)# commit
```

Example:

This example shows how to configure a metric for the redistributed routes from BGP. It allows managing the metric selection criteria in the OSPF database.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# redistribute bgp
(config-redistribute-connected)# metric 1000
(config-redistribute-connected)# exit
(config-ospf-1-vrf-global)# commit
```

Impacts and precautions

Redistributed routes always use metric-type 2 and the metric value is the original value of the external route.

Hardware restrictions

N/A

router ospf router-id

Description

Configures the router identifier of an OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **router-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

router-id *id*

Description:	Specifies the OSPF router identifier expressed in IPv4 address.
Value:	a.b.c.d.
Default Value:	0.0.0.0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the router-id of a router ospf.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# router-id 1.1.1.1
(config-ospf-1-vrf-global)# commit
```

Impacts and precautions

Changing the OSPF router-id will restart the OSPF router process.

Hardware restrictions

N/A

router ospf timers lsa-arrival

Description

Configures the minimum interval in which the same link-state advertisement (LSA) from OSPF neighbors is accepted by a router OSPF.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **timers lsa-arrival** *delay*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

lsa-arrival *delay*

Description:	Specifies the minimum delay between accepting the same LSA in milliseconds.
Value:	0-600000.
Default Value:	100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
4.9	The default value of parameter lsa-arrival has been changed to 100ms.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf timers lsa-arrival.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# timers lsa-arrival 5000
(config-timers)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf timers throttle lsa-originate

Description

Configures the rate-limiting for link-state advertisement (LSA) generation of a OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

router ospf *process-id* [**vrf** *vrf-name*] **timers throttle lsa-originate** **hold-interval** *interval* | **max-interval** *interval* | **start-interval** *interval*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the OSPF router process identifier.

Value: 1-65535.

Default Value: N/A

vrf *vrf-name*

Description: Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.

Value: string.

Default Value: global

hold-interval *interval*

Description: Specifies the minimum delay between originating the same LSA in milliseconds.

Value: 0-600000.

Default Value: 500.

max-interval *interval*

Description: Specifies the maximum delay between originating the same LSA in milliseconds.

Value: 0-600000.

Default Value: 5000.

start-interval *interval*

Description: Specifies the start delay to generate the first LSA occurrence in milliseconds.

Value: 0-600000.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
4.9	The default values of parameters hold-interval , max-interval and start-interval have been changed.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf timers throttle lsa-originate.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# timers throttle
(config-throttle)# lsa-originate hold-interval 1000
(config-throttle)# lsa-originate max-interval 10000
(config-throttle)# lsa-originate start-interval 500
(config-throttle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospf timers throttle spf

Description

Configures the scheduling for Shortest Path First (SPF) calculations of a OSPF router.

Supported Platforms

This command is supported in all platforms.

Syntax

```
router ospf process-id [vrf vrf-name] timers throttle spf hold-interval interval |  
max-interval interval | start-interval interval
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the OSPF router process identifier.
Value:	1-65535.
Default Value:	N/A

vrf *vrf-name*

Description:	Specifies the name of the VRF this router will be associated with. The VRF 'global' is implied if no parameter is specified. It is not possible to associate the VRF 'mgmt' with an OSPF router.
Value:	string.
Default Value:	global

hold-interval *interval*

Description:	Specifies the minimum wait time between SPF calculations in milliseconds.
Value:	0-600000.
Default Value:	500.

max-interval *interval*

Description: Specifies the maximum wait time for SPF calculation in milliseconds.

Value: 0-600000.

Default Value: 5000.

start-interval *interval*

Description: Specifies the delay between receiving a change to start SPF calculation in milliseconds.

Value: 0-600000.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf timers throttle spf.

```
# config terminal
Entering configuration mode terminal
(config)# router ospf 1
(config-ospf-1-vrf-global)# timers throttle
(config-throttle)# spf hold-interval 1000
(config-throttle)# spf max-interval 10000
(config-throttle)# spf start-interval 500
(config-throttle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip ospf

Description

Shows information about the OSPF routing processes.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip ospf [{brief | detail | extensive}] [process-id]
```

Parameters

brief

Description:	Shows summarized information about the routing OSPF processes.
Value:	N/A
Default Value:	N/A

detail

Description:	Shows detailed information about the routing OSPF processes.
Value:	N/A
Default Value:	N/A

extensive

Description:	Shows extensive information about the routing OSPF processes.
Value:	N/A
Default Value:	N/A

process-id

Description:	Shows only information about the specified OSPF process.
Value:	1-65535.
Default Value:	N/A

Output Terms

Output	Description
<code>Router-ID</code>	Indicates the router identifier of the OSPF routing process.
<code>Version</code>	Indicates the OSPF protocol version.
<code>Admin</code>	Indicates the administrative status of the OSPF routing process.
<code>Op-status</code>	Indicates the operational status of the OSPF routing process.
<code>Routing-process</code>	Indicates the process identifier of the OSPF routing process.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show ip ospf

Router-ID      Version Admin Op-status Routing-process
-----
1.1.1.1        2      up    up        1

# show ip ospf brief

Router-ID      Version Admin Op-status Routing-process
-----
1.1.1.1        2      up    up        1

# show ip ospf detail

Routing-process: 1;
  Version: 2; Router-ID: 1.1.1.1; Current router-ID: 1.1.1.1;
  Area border router: no; Autonomous system border router: enable;
  Support type-of-service routing: no;
  Support opaque LSA: yes;

  Type-5, external LSA:                                0; Checksum sum: 0x00000000
  Type-11, AS opaque LSA:                              0; Checksum sum: 0x00000000
  New originated LSA:                                  231;
  New instances LSA:                                   230;
  LSA with checksum pending:                           0;

  Number pending updates:                              0;
  Number merged updates:                               0;

  Hitless restart status:                             none;
  Remaining hitless restart interval:                  none;
  Last hitless restart result:                         none;

# show ip ospf extensive

Routing-process: 1;
  Version: 2; Router-ID: 1.1.1.1; Current router-ID: 1.1.1.1;
  Area border router: no; Autonomous system border router: enable;
  Support type-of-service routing: no;
  Support opaque LSA: yes;

  Type-5, external LSA:                                0; Checksum sum: 0x00000000
  Type-11, AS opaque LSA:                              0; Checksum sum: 0x00000000
  New originated LSA:                                  231;
  New instances LSA:                                   230;
  LSA with checksum pending:                           0;

  Number pending updates:                              0;
  Number merged updates:                               0;

  Hitless restart status:                             none;
  Remaining hitless restart interval:                  none;
  Last hitless restart result:                         none;

Number of areas in this router: 1;
  Normal areas: 1; Stub areas: 0; NSSA areas: 0;
  Number transit capable areas: 0;

Area 0; Op-state: up;
  Number of interfaces: 1; Authentication: no;
  Transit capable: no
  Number of reachable area border routers: 0;
  Number of reachable autonomous system border routers: 2;
  Number of times SPF algorithm executed: 3;
  NSAA translation state: disabled; NSSA state changes: n/a;
```


LSA Type	Count	Checksum sum
-----	-----	-----
Total LSA	2	0x0000F02A
Type-1, router	2	0x0000F02A
Type-2, network	0	0x00000000
Type-3, summary	0	0x00000000
Type-4, ASBR	0	0x00000000
Type-7, NSSA	0	0x00000000
Type-10, area opaque	0	0x00000000

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip ospf database

Description

Shows a set of information related to the OSPF database.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show ip ospf [process-id [area-id]] database [opaque-area | asbr | network | router  
| summary] [adv-router adv-router-id | self-originate] [link-state-id] [brief | detail]
```

```
show ip ospf database external [{brief | detail} [process-id {type-5 | type-11}  
[link-state-id [adv-router-id]]]
```

Parameters

process-id

Description: Specifies the Router OSPF process identifier.

Value: 1-65535.

Default Value: N/A

area-id

Description: Specifies the Router OSPF area identifier. May be specified in decimal or in dot-decimal notation.

Value: 0-4294967295 | 0.0.0.0-255.255.255.255.

Default Value: N/A

link-state-id

Description: Shows only information identified by the specified Link State ID.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

brief

Description:	Shows resumed information about the OSPF database.
Value:	N/A
Default Value:	N/A

detail

Description:	Shows detailed information about the OSPF database.
Value:	N/A
Default Value:	N/A

adv-router *adv-router-id*

Description:	Shows only information about LSAs advertized by the specified router.
Value:	0.0.0.0-255.255.255.255.
Default Value:	N/A

opaque-area

Description:	Shows information about opaque area link states.
Value:	N/A
Default Value:	N/A

asbr

Description:	Shows only information about Autonomous System Boundary Router(ASBR) LSAs.
Value:	N/A
Default Value:	N/A

external

Description:	Shows only information about external LSAs.
Value:	N/A
Default Value:	N/A

network

Description:	Shows only information about network LSAs.
Value:	N/A
Default Value:	N/A

router

Description: Shows only information about router LSAs.

Value: N/A

Default Value: N/A

self-originate

Description: Shows only information about self-originated LSAs (from the local router).

Value: N/A

Default Value: N/A

summary

Description: Shows only information about summary LSAs.

Value: N/A

Default Value: N/A

type-5

Description: Shows only information about Type-5 external LSAs.

Value: N/A

Default Value: N/A

type-11

Description: Shows only information about Type-11 external LSAs.

Value: N/A

Default Value: N/A

Output Terms**Output****Description**

ADV router Indicates the advertising router.

Advertising router Indicates the advertising router.

Output	Description
Advertisement	Indicates the LSA in the hex format.
Advertisement length	Indicates the length in bytes of the LSA.
Age	Indicates the link state age.
Area	Indicates the OSPF area ID.
Bits	Indicates the bits values of the “Options” field.
Checksum	Indicates the link state checksum.
Links	Indicate the number of active links.
Link data	Indicates the router interface address.
Link ID	Indicates the link ID.
Link state ID	Indicates the link state ID.
Link type	Indicates the link type.
OSPF Router with id	Indicates the Router ID.
Options	Indicates the optional capabilities.
Process ID	Indicates the OSPF process ID.
Sequence	Indicates the link state sequence.

Output	Description
Sequence number	Indicates the link state sequence.
TOS	Indicates the type of service.
Type	Indicates the link type.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
4.0	The extensive parameter was removed.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use this command.

```
# show ip ospf database brief
OSPF Router with ID (121.121.121.1) Process ID (1)

Area 0.0.0.0;
Link type      Link ID      ADV router    Age (secs) Sequence    Checksum
-----
1 - router     120.120.120.1  120.120.120.1 1000        0x80000002 0x000051F1
1 - router     121.121.121.1  121.121.121.1  999         0x80000002 0x00004FEE

# show ip ospf database detail
OSPF Router with ID (121.121.121.1) Process ID (1)

Area 0.0.0.0; Link type: router;
Link state ID: 120.120.120.1; Advertising router: 120.120.120.1;
Age: 1595 secs; Sequence number: 0x80000002; Checksum: 0x000051F1
Advertisement length: 60 (first 58 chars displayed)
Advertisement: 0x0001020178787801787878018000000251f1003c0200000379797901ac
Options: E
Bits: E
Links: 3
Router links:
  1. Link ID: 121.121.121.1; Link data: 172.16.0.2; Type: 1;
    Num. of TOS: 0; TOS metric: 1
  2. Link ID: 172.16.0.0; Link data: 255.255.255.0; Type: 3;
    Num. of TOS: 0; TOS metric: 1
  3. Link ID: 100.100.100.1; Link data: 255.255.255.255; Type: 3;
    Num. of TOS: 0; TOS metric: 1

Link state ID: 121.121.121.1; Advertising router: 121.121.121.1;
Age: 1595 secs; Sequence number: 0x80000002; Checksum: 0x00004FEE
Advertisement length: 60 (first 58 chars displayed)
Advertisement: 0x000102017979790179797901800000024fee003c0200000378787801ac
Options: E
Bits: E
Links: 3
Router links:
  1. Link ID: 120.120.120.1; Link data: 172.16.0.1; Type: 1;
    Num. of TOS: 0; TOS metric: 1
  2. Link ID: 172.16.0.0; Link data: 255.255.255.0; Type: 3;
    Num. of TOS: 0; TOS metric: 1
  3. Link ID: 101.101.101.1; Link data: 255.255.255.255; Type: 3;
    Num. of TOS: 0; TOS metric: 1

# show ip ospf database external
Link Type      Link ID      ADV Router    Age (secs) Sequence    Checksum
-----
5 - external   10.10.10.0   2.2.2.2       254         0x80000009 0x00002D77
5 - external   20.20.20.0   2.2.2.2       414         0x80000006 0x0000C3C6

# show ip ospf database external detail
Link type: type-5, external; Link ID: 10.10.10.0;
Advertising router: 2.2.2.2;
Age: 364 secs; Sequence number: 0x80000009; Checksum: 0x00002D77;
Advertisement: 0x000102050a0a0a00020202800000092d770024fffffffff8000000000;
Forwarding Address: 0.0.0.0; Metric Type: 2; Metric: 0;

Link type: type-5, external; Link ID: 20.20.20.0;
Advertising router: 2.2.2.2;
Age: 524 secs; Sequence number: 0x80000006; Checksum: 0x0000C3C6;
Advertisement: 0x000102051414140002020280000006c3c60024ffffffffffe8000000000;
Forwarding Address: 0.0.0.0; Metric Type: 2; Metric: 0;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip ospf interface

Description

Shows information about the OSPF interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

show ip ospf interface

show ip ospf interface brief [*interface-ip* [*process-id*]]

show ip ospf interface detail [*interface-ip* [*process-id*]]

show ip ospf interface statistics [*interface-ip* [*process-id*]]

Parameters

brief

Description: Shows resummed information about the OSPF interfaces.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the OSPF interfaces.

Value: N/A

Default Value: N/A

statistics

Description: Shows various statistics about the OSPF interfaces.

Value: N/A

Default Value: N/A

*interface-ip***Description:** Shows only information about the specified OSPF interface.**Value:** 0.0.0.0-255.255.255.255.**Default Value:** N/A*process-id***Description:** Shows only information about the specified OSPF process.**Value:** 1-65535.**Default Value:** N/A**Output Terms**

Output	Description
Interface-name	Indicates the name of the OSPF interface.
Area	Indicates the area ID of the OSPF interface.
Interface-address	Indicates the IP address of the OSPF interface.
If-state	Indicates the state of the OSPF interface.
area-mismatch	Indicates the number of OSPF packet header 'area mismatch' errors detected on each interface.
authentication	Indicates the number of OSPF packet header authentication errors detected on each interface.
auth-failure	Indicates the number of OSPF packets received on each interface that were dropped because of authentication failure.
auth-mismatch	Indicates the number of OSPF packets received on each interface that were dropped because of a bad authentication type.
bad-lsa-len	Indicates the number of OSPF LS Update packets received on each interface that were discarded because of a bad LSA length.

Output	Description
bad-packet	Indicates the number of OSPF packets received on each interface that have been dropped for a reason which does not have a more specific type defined.
bad-source	Indicate the number of OSPF packet header 'bad source' errors detected on each interface.
checksum	Indicates the number of OSPF packet header checksum errors detected on each interface.
dead-mismatch	Indicates the number of OSPF Hello packets received on each interface that were dropped because of a bad Router Dead Interval.
duplicate-id	Indicates the number of OSPF packet header 'duplicate id' errors detected on each interface.
hello	Indicates the number of OSPF packet header 'Hello' errors detected on each interface.
hello-mismatch	Indicates the number of OSPF Hello packets received on each interface that were dropped because of a bad Hello Interval.
length	Indicates the number of OSPF packet header length errors detected on each interface.
lsa-bad-checksum	Indicates the number of OSPF LSAs received on each interface that were ignored because of a bad LSA checksum value.
lsa-bad-data	Indicates the number of OSPF LSAs received on each interface that were ignored because of a bad LSA data.
lsa-bad-len	Indicates the number of OSPF LSAs received on each interface that were ignored because of a bad LSA length.

Output	Description
<code>lsa-bad-type</code>	Indicates the number of OSPF LSAs received on each interface that were ignored because of a bad LSA type.
<code>mtu-mismatch</code>	Indicates the number of OSPF packet header 'MTU mismatch' errors detected on each interface.
<code>nbr-ignored</code>	Indicates the number of OSPF packet header 'neighbor ignored' errors detected on each interface.
<code>options-mismatch</code>	Indicates the number of OSPF Hello packets received on each interface that were dropped because of bad Optional Capabilities.
<code>packet-local-addr</code>	Indicates the number of OSPF Hello packets received on each interface that were dropped because they appear to come from the local router.
<code>resource-err</code>	Indicates the number of OSPF packet header resource errors detected on each interface.
<code>rx-db-des-byte</code>	Indicates the number of bytes received in OSPF Database Description packets on each interface.
<code>rx-db-description</code>	Indicates the number of OSPF Database Description packets received on each interface.
<code>rx-hello</code>	Indicates the number of OSPF Hello packets received on each interface.
<code>rx-hello-byte</code>	Indicates the number of bytes received in OSPF Hello packets on each interface.
<code>rx-invalid</code>	Indicates the number of OSPF packets with an invalid type field received on each interface.

Output	Description
rx-invalid-byte	Indicates the number of bytes received in OSPF packets with an invalid type field on each interface.
rx-ls-ack	Indicates the number of OSPF LS Acknowledgement packets received on each interface.
rx-ls-ack-byte	Indicates the number of bytes received in OSPF LS Acknowledgement packets on each interface.
rx-ls-req	Indicates the number of OSPF LS Request packets received on each interface.
rx-ls-req-byte	Indicates the number of bytes received in OSPF LS Request packets on each interface.
rx-ls-upd	Indicates the number of OSPF LS Update packets received on each interface.
rx-ls-upd-byte	Indicates the number of bytes received in OSPF LS Update packets on each interface.
self-originated	Indicates the number of OSPF packet header 'self-originated' errors detected on each interface.
tx-db-des	Indicates the number of OSPF Database Description packets sent on each interface.
tx-db-des-byte	Indicates the number of bytes sent in OSPF Database Description packets on each interface.
tx-failed	Indicates the number of packets that OSPF could not send on each interface.
tx-failed-byte	Indicates the number of bytes sent in packets that OSPF could not send on each interface.

Output	Description
tx-hello	Indicates the number of OSPF Hello packets sent on each interface.
tx-hello-byte	Indicates the number of bytes sent in OSPF Hello packets on each interface.
tx-ls-ack	Indicates the number of OSPF LS Acknowledgement packets sent on each interface.
tx-ls-ack-byte	Indicates the number of bytes sent in OSPF LS Acknowledgement packets on each interface.
tx-ls-req	Indicates the number of OSPF LS Request packets sent on each interface.
tx-ls-req-byte	Indicates the number of bytes sent in OSPF LS Request packets on each interface.
tx-ls-upd	Indicates the number of OSPF LS Update packets sent on each interface.
tx-ls-upd-byte	Indicates the number of bytes sent in OSPF LS Update packets on each interface.
version	Indicates the number of OSPF packet header version errors detected on each interface.
wrong-protocol	Indicates the number of OSPF packet header 'wrong protocol' errors detected on each interface.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
2.2	The statistics parameter was updated.
4.6	The State output was renamed to If-state.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show ip ospf interface
Codes for operation state (If-state):
  BDR - backup designated router; DR - designated router;
  ODR - other designated router; P2P - point-to-point;
  DWN - down; LBK - loopback; WTG - waiting
Interface-name  Area          Interface-address  If-State
-----
vlan100        0.0.0.0       10.10.10.1       P2P
# show ip ospf interface brief
Codes for operation state (If-state):
  BDR - backup designated router; DR - designated router;
  ODR - other designated router; P2P - point-to-point;
  DWN - down; LBK - loopback; WTG - waiting
Interface-name  Area          Interface-address  If-state
-----
vlan100        0.0.0.0       10.10.10.1       P2P
# show ip ospf interface detail
Interface-name: vlan100; Interface ID: 201326692;
```

```

Admin state: enabled; MTU: 1500;
Operational status: up; OSPF interface state: point-to-point;
Link IP address: 10.10.10.1; Mask: 255.255.255.254;
Area: 0.0.0.0; Router ID: 1.1.1.1; Network type: point-to-point;
Process ID: 1; Instance ID: n/a; Cost: 1; Priority: 1;
Designated router: none; Backup designated router: none;
Number of OSPF interface state changes or error: 104;
LSA count: 0; Checksum: 0x00000000;
Timer intervals configured:
  Hello: 10 secs; Dead: 40 secs;
  Transit delay: 1 sec; Retransmit: 5 secs;

# show ip ospf interface statistics
ip ospf interface statistics 10.10.10.1 1
rx-invalid                0
rx-invalid-byte           0
rx-hello                  1279973
rx-hello-byte             87038156
rx-db-description         10
rx-db-des-byte            700
rx-ls-req                 5
rx-ls-req-byte            280
rx-ls-upd                 388
rx-ls-upd-byte            37188
rx-ls-ack                 388
rx-ls-ack-byte            24832
tx-failed                 0
tx-failed-byte            0
tx-hello                  1280018
tx-hello-byte             87041200
tx-db-des                 13
tx-db-des-byte            856
tx-ls-req                 5
tx-ls-req-byte            280
tx-ls-upd                 388
tx-ls-upd-byte            37188
tx-ls-ack                 388
tx-ls-ack-byte            24832
length                    0
checksum                  0
version                   0
bad-source                 0
area-mismatch              0
self-originated            0
duplicate-id               0
hello                      103
mtu-mismatch               0
nbr-ignored                0
authentication             0
wrong-protocol              0
resource-err                0
bad-lsa-len                0
lsa-bad-type               0
lsa-bad-len                0
lsa-bad-data               0
lsa-bad-checksum           0
auth-mismatch              0
auth-failure               0
hello-mismatch             102
dead-mismatch               1
options-mismatch            0
packet-local-addr          0
bad-packet                 0

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ip ospf neighbor

Description

Shows information about the OSPF neighbors.

Supported Platforms

This command is supported in all platforms.

Syntax

show ip ospf neighbor

show ip ospf neighbor brief [*Router-ID* [*process-id*]]

show ip ospf neighbor detail [*Router-ID* [*process-id*]]

Parameters

brief

Description: Shows resummed information about the OSPF neighbors.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the OSPF neighbors.

Value: N/A

Default Value: N/A

Router-ID

Description: Shows only information about the specified OSPF neighbor.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

process-id

Description: Shows only information about the specified OSPF process.

Value: 1-65535.

Default Value: N/A

Output Terms

Output	Description
Neighbor-ID	Indicates the router ID value of the OSPF neighbor router-ID.
Pri	Indicates the priority value of the OSPF neighbor.
State	Indicates the adjacency state with the OSPF neighbor.
If-state	Indicates the interface state of the OSPF neighbor.
Interface-address	Indicates the interface address of the OSPF neighbor.
Interface-name	Indicates the interface name of the OSPF neighbor.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.0	This command was introduced.
4.6	The interface state output was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show ip ospf neighbor

State codes: atmtpt - attempt; exchg - exchange; exst - exchange start;
              load - loading; 2-way - two-way;
Neighbor interface state codes:
  BDR - backup designated router; DR - designated router;
  ODR - other designated router; P2P - point-to-point;

Neighbor-ID      Pri State If-state Interface-address Interface-name
-----
2.2.2.2          1  full BDR      10.10.10.0        vlan100

# show ip ospf neighbor brief

State codes: atmtpt - attempt; exchg - exchange; exst - exchange start;
              load - loading; 2-way - two-way;
Neighbor interface state codes:
  BDR - backup designated router; DR - designated router;
  ODR - other designated router; P2P - point-to-point;

Neighbor-ID      Pri State If-State Interface-address Interface-name
-----
2.2.2.2          1  full BDR      10.10.10.0        vlan100

# show ip ospf neighbor detail

Neighbor-ID: 2.2.2.2; Interface-address: 10.10.10.0;
Area: 0.0.0.0; Interface-name: vlan100;
Relationship state with neighbor: full; Oper status: up;
Neighbor interface state: backup designated router;
Neighbor priority: 1; Options: 0x42; Re-transmission queue length: 0;
Number of neighbor relationship state changes or error: 6;
Permanence: dynamic; Hello suppressed: no; Requested LSAs: 0;
Dead timer due in: 00:00:37 (hrs:mins:secs);
Hitless restart status: not helping;
Remaining hitless restart interval: none;
Hitless restart result: none;

# show ip ospf neighbor detail 10.10.10.0

Neighbor-ID: 2.2.2.2; Interface-address: 10.10.10.0;
Area: 0.0.0.0; Interface-name: vlan100;
Relationship state with neighbor: full; Oper status: up;
Neighbor interface state: backup designated router;
Neighbor priority: 1; Options: 0x42; Re-transmission queue length: 0;
Number of neighbor relationship state changes or error: 6;
Permanence: dynamic; Hello suppressed: no; Requested LSAs: 0;
Dead timer due in: 00:00:31 (hrs:mins:secs);
Hitless restart status: not helping;
Remaining hitless restart interval: none;
```

```
Hitless restart result: none;
# show ip ospf neighbor detail 10.10.10.0 1
Neighbor-ID: 2.2.2.2; Interface-address: 10.10.10.0;
Area: 0.0.0.0; Interface-name: vlan100;
Relationship state with neighbor: full; Oper status: up;
Neighbor interface state: backup designated router;
Neighbor priority: 1; Options: 0x42; Re-transmission queue length: 0;
Number of neighbor relationship state changes or error: 6;
Permanence: dynamic; Hello suppressed: no; Requested LSAs: 0;
Dead timer due in: 00:00:36 (hrs:mins:secs);
Hitless restart status: not helping;
Remaining hitless restart interval: none;
Hitless restart result: none;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

OSPFV3

This topic describes the commands related to management of OSPFv3 topologies such as commands to configure the OSPFv3 parameters or to inspect the protocol status.

clear ospfv3

Description

Clears OSPFv3 information.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

clear ospfv3 process *process-id*

Parameters

process *process-id*

Description: Clears OSPFv3 information for the specified OSPFv3 process ID.

Value: 1-65535.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to clear OSPFv3 process.

```
# clear ospfv3 process 1
```

Impacts and precautions

This command will restart all OSPFv3 adjacencies from the specified router instance.

Hardware restrictions

N/A

router ospfv3

Description

Configures an OSPFv3 router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure an OSPFv3 router.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1
(config-ospfv3-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 administrative-status

Description

Configures the administrative status of an OSPFv3 router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the OSPFv3 router.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config
Entering configuration mode terminal
(config)# router ospfv3 1 administrative-status down
(config-ospfv3-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area

Description

Configures the area of a router OSPFv3.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

area-id

Description:	Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.
Value:	1-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospfv3 area.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 5
(config-area-5)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area administrative-status

Description

Configures the administrative status of an OSPFv3 area.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

area *area-id*

Description:	Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

administrative-status *status*

Description:	Activates (up) or deactivates (down) the OSPFv3 area.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config
Entering configuration mode terminal
(config)# router ospfv3 1 area 0 administrative-status down
(config-area-0)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface

Description

Enables the OSPFv3 protocol on an specified L3 or loopback interface.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

area-id

Description:	Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface-name

Description:	Specifies L3 and loopback interfaces for the Router OSPFv3. The L3 and loopback interfaces must be created before the commit.
Value:	Any L3 and loopback interfaces.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospfv3 interface.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 5 interface l3-vlan1
(config-interface-l3-vlan1)# top
(config)# router ospfv3 1 area 5 interface loopback-1
(config-interface-loopback-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface administrative-status

Description

Configures the administrative status of an OSPFv3 area interface.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.

Value: L3 interface.

Default Value: N/A

administrative-status *status*

- Description:** Activates (up) or deactivates (down) the L3 interface.
- Value:** up | down.
- Default Value:** up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status.

```
# config
Entering configuration mode terminal
(config)# router ospfv3 1 area 0
(config-area-0)# interface l3-vlan100 administrative-status down
(config-ospfv3-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface cost

Description

Explicitly sets the OSPFv3 routing cost of an L3 interface.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **cost** *cost*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.
Value: 1-65535.
Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.
Value: 0-4294967295. 0.0.0.0-255.255.255.255.
Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.
Value: Any L3 interface.
Default Value: N/A

cost *cost*

Description:	Explicitly sets the OSPFv3 routing cost of an L3 interface.
Value:	1-65535
Default Value:	1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the cost.

Example:

This example shows how to configure the cost.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 cost 2
(config-ospfv3-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface dead-interval

Description

Configures how long the OSPFv3 process will wait before declaring a neighbor down if it stops receiving Hello packets.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **dead-interval** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

dead-interval *seconds*

Description: Interval after which a neighbor is declared down.

Value: 2-65535.

Default Value: 40.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the dead-interval.

Example:

This example shows how to configure the dead interval.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0 interface l3-vlan100
(config-interface-l3-vlan100)# dead-interval 50
(config-interface-l3-vlan100)# commit
```

Impacts and precautions

A mismatch in the OSPFv3 dead-intervals between neighbors will not permit the adjacency to be established or cause it to go down.

Hardware restrictions

N/A

router ospfv3 area interface hello-interval

Description

Configures the interval in which Hello packets will be sent.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **hello-interval** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

hello-interval *seconds*

Description: Sets the interval in which a Hello packet will be sent.

Value: 1-65535.

Default Value: 10.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the hello-interval.

Example:

This example shows how to configure the Hello interval.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 hello-interval 20
(config-interface-l3-vlan100)# commit
```

Impacts and precautions

A mismatch in the OSPFv3 hello-intervals between neighbors will not permit the adjacency to be established or cause it to go down.

Hardware restrictions

N/A

router ospfv3 area interface mtu-ignore

Description

Disables OSPFv3 Maximum Transmission Unit (MTU) mismatch detection on received Database Description (DBD) packets.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **mtu-ignore**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: 0.

interface *interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

mtu-ignore

Description: Sets the interface to ignore the MTU mismatch detection on received DBD packets.

Value: N/A

Default Value: N/A

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the mtu-ignore.

Example:

This example shows how to configure the mtu-ignore.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 mtu-ignore
(config-ospfv3-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface network-type

Description

Configures the network type of an OSPFv3 L3 interface.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *l3-interface-name* **network-type** *type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. It may be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: N/A

interface *l3-interface-name*

Description: Specifies L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.

Value: any L3 interface.

Default Value: N/A

network-type *type*

Description: Defines the network type to be used for this interface. For point-to-point, the connection is between a single source and a single destination.

Value: point-to-point.

Default Value: point-to-point.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Commands to configure the network-type.

Example:

This example shows how to configure the network-type.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 network-type point-to-point
(config-ospfv3-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area interface passive

Description

Configures an OSPFv3 interface as passive.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **interface** *interface-name* **passive**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

area *area-id*

Description:	Specifies the Router OSPFv3 area identifier. It may be specified in decimal or in dot-decimal notation.
Value:	0-4294967295. 0.0.0.0-255.255.255.255.
Default Value:	0.

interface *interface-name*

Description:	Specifies an L3 interface for the Router OSPFv3. The L3 interface must be created before the commit.
Value:	Any L3 interface.
Default Value:	N/A

passive

Description:	Sets the interface as passive.
Value:	N/A
Default Value:	N/A

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

Passive interfaces neither establish adjacencies nor send OSPFv3 updates, but it is still advertised as part of the OSPFv3 routing domain. Commands to configure the passive interface.

Example:

This example shows how to configure the interface as passive.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 area 0.0.0.0
(config-area-0.0.0.0)# interface l3-vlan100 passive
(config-ospfv3-area-intf-l3-vlan100)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 area range

Description

Summarizes routes matching IPv6 address/prefix length at an area border.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **area** *area-id* **range** *x:x:x:x::x/y* [**advertise** | **not-advertise**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area *area-id*

Description: Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.

Value: 0-4294967295. 0.0.0.0-255.255.255.255.

Default Value: N/A

range *x:x:x:x::x/y*

Description: Specifies the IPv6 network portion of the range. All inter-area network addresses that match the specified area range are summarized.

Value: Must be a valid IPv6 network address and prefix length.

Default Value: N/A

advertise

Description: Advertises the address range.

Value: N/A

Default Value: N/A

not-advertise

Description: Does not advertise the range.

Value: N/A

Default Value: N/A

Default

advertise.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced
-----	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to summarize a route matching address/prefix length.

```
# config
```



```
Entering configuration mode terminal
(config)# router ospfv3 1 area 0 range 2001:db8::/64
(config-range-2001:db8::/64)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 maximum paths

Description

Configures the maximum number of equal-cost multi-paths (ECMP) for the OSPFv3 router process.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **maximum paths** *number-of-paths*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

maximum paths *number-of-paths*

Description: Specifies the maximum number of paths with equal cost.

Value: 1-16.

Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the maximum number of paths of a router ospfv3.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1
(config-ospfv3-1)# maximum paths 4
(config-ospfv3-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 redistribute

Description

Redistributes external routes into the domain of this OSPFv3 router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **redistribute** {*connected* | *static*} [**match-address** *x:x:x:x::x/x*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

redistribute *connected*

Description: Redistributes connected routes into the domain of this OSPFv3 router.

Value: N/A

Default Value: N/A

redistribute *static*

Description: Redistributes static routes into the domain of this OSPFv3 router.

Value: N/A

Default Value: N/A

match-address *x:x:x:x::x/x*

Description:	Redistributes specific routes, that match the supplied prefix/mask filter, into the domain of this OSPFv3 router.
Value:	Must be a valid IPv6 prefix/mask.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the route redistribution.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 redistribute connected
(config-redistribute-connected)# top
(config)# router ospfv3 1 redistribute static
(config-redistribute-static)# top
(config)# router ospfv3 1 redistribute connected match-address 2001:db8::/64
(config-redistribute-connected)# top
(config)# router ospfv3 1 redistribute static match-address 2001:db8::/64
(config-redistribute-static)# commit
```

Impacts and precautions

Redistributed routes always use metric-type 2 and the metric value is the original value of the external route.

Hardware restrictions

N/A

router ospfv3 router-id

Description

Configures the router identifier of an OSPFv3 router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **router-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

router-id *id*

Description:	Specifies the Router OSPFv3 identifier expressed in IPv4 address.
Value:	a.b.c.d.
Default Value:	0.0.0.0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the router-id of a router ospfv3.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1 router-id 1.1.1.1
(config-ospfv3-1)# commit
```

Impacts and precautions

Changing the OSPFv3 router-id will restart the OSPFv3 router process.

Hardware restrictions

N/A

router ospfv3 timers lsa-arrival

Description

Configures the minimum interval in which the same link-state advertisement (LSA) from OSPFv3 neighbors is accepted by a router OSPFv3.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **timers lsa-arrival** *milliseconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

lsa-arrival

Description: Specifies the minimum delay between accepting the same LSA in milliseconds.

Value: 0-600000.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
4.9	The default value of parameter lsa-arrival has been changed to 100ms.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospfv3 timers lsa-arrival.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1
(config-ospfv3-1)# timers lsa-arrival 5000
(config-timers)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 timers throttle lsa-originate

Description

Configures the rate-limiting for link-state advertisement (LSA) generation of a router OSPFv3.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **timers throttle lsa-originate hold-interval** *milliseconds* | **max-interval** *milliseconds* | **start-interval** *milliseconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

hold-interval

Description:	Specifies the minimum delay between originating the same LSA in milliseconds.
Value:	0-600000.
Default Value:	500.

max-interval

Description:	Specifies the maximum delay between originating the same LSA in milliseconds.
Value:	0-600000.

Default Value: 5000.

start-interval

Description: Specifies the start delay to generate the first LSA occurrence in milliseconds.

Value: 0-600000.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
4.9	The default values of parameters hold-interval , max-interval and start-interval have been changed.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospf timers throttle lsa-originate.

```
# config terminal
Entering configuration mode terminal
```

```
(config)# router ospfv3 1
(config-ospfv3-1)# timers throttle
(config-throttle)# lsa-originate hold-interval 1000
(config-throttle)# lsa-originate max-interval 10000
(config-throttle)# lsa-originate start-interval 500
(config-throttle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router ospfv3 timers throttle spf

Description

Configures the scheduling for Shortest Path First (SPF) calculations of a router OSPFv3.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router ospfv3 *process-id* **timers throttle spf** **hold-interval** *milliseconds* | **max-interval** *milliseconds* | **start-interval** *milliseconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description:	Specifies the Router OSPFv3 process identifier.
Value:	1-65535.
Default Value:	N/A

hold-interval

Description:	Specifies the minimum wait time between SPF calculations in milliseconds.
Value:	0-600000.
Default Value:	500.

max-interval

Description:	Specifies the maximum wait time for SPF calculation in milliseconds.
Value:	0-600000.
Default Value:	5000.

start-interval

Description: Specifies the delay between receiving a change to start SPF calculation in milliseconds.

Value: 0-600000.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a router ospfv3 timers throttle spf.

```
# config terminal
Entering configuration mode terminal
(config)# router ospfv3 1
(config-ospfv3-1)# timers throttle
(config-throttle)# spf hold-interval 1000
(config-throttle)# spf max-interval 10000
(config-throttle)# spf start-interval 500
(config-throttle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ipv6 ospf

Description

Shows information about the OSPFv3 routing processes.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
show ipv6 ospf [brief process-id]
```

Parameters

brief

Description: Shows summarized information about the routing OSPFv3 processes.

Value: N/A

Default Value: N/A

process-id

Description: Shows only information about the specified OSPFv3 process.

Value: 1-65535.

Default Value: N/A

Output Terms

Output	Description
Router-ID	Indicates the router identifier of the OSPFv3 routing process.
Version	Indicates the OSPFv3 protocol version.

Output	Description
<code>Admin</code>	Indicates the administrative status of the OSPFv3 routing process.
<code>Op-status</code>	Indicates the operational status of the OSPFv3 routing process.
<code>Routing-process</code>	Indicates the process identifier of the OSPFv3 routing process.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show ipv6 ospf
Router-ID      Version Admin Op-status Routing-process
-----
```

```
1.1.1.1      3      up    up      1
# show ipv6 ospf brief
Router-ID----- Version Admin Op-status Routing-process
1.1.1.1      3      up    up      1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ipv6 ospf database

Description

Shows a set of information related to the OSPFv3 database.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

show ipv6 ospf [*process-id* [*area-id*]] **database** [**inter-area-prefix** | **inter-area-router** | **intra-area-prefix** | **router**] [**adv-router** *adv-router-id* | **self-originate**] [*link-state-id*] [**brief** | **detail**]

show ipv6 ospf database external [{**brief** | **detail**} [*process-id*]]

show ipv6 ospf database link [{**brief** | **detail**} [*process-id*]]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

process-id

Description: Specifies the Router OSPFv3 process identifier.

Value: 1-65535.

Default Value: N/A

area-id

Description: Specifies the Router OSPFv3 area identifier. May be specified in decimal or in dot-decimal notation.

Value: 0-4294967295 | 0.0.0.0-255.255.255.255.

Default Value: N/A

inter-area-prefix

Description: Shows only information about inter-area prefix LSAs.

Value: N/A

Default Value: N/A

inter-area-router

Description: Shows only information about inter-area router LSAs.

Value: N/A

Default Value: N/A

intra-area-prefix

Description: Shows only information about intra-area prefix LSAs.

Value: N/A

Default Value: N/A

router

Description: Shows only information about router LSAs.

Value: N/A

Default Value: N/A

adv-router *adv-router-id*

Description: Shows only information about LSAs advertised by the specified router.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

self-originate

Description: Shows only information about self-originated LSAs (from the local router).

Value: N/A

Default Value: N/A

link-state-id

Description: Shows only information identified by the specified Link State ID.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

brief

Description: Shows resumed information about the OSPFv3 database.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the OSPFv3 database.

Value: N/A

Default Value: N/A

external

Description: Shows only information about external LSAs.

Value: N/A

Default Value: N/A

link

Description: Shows only information about link LSAs.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Address prefix	Indicates the IPv6 address prefix.
Age	Indicates the link state age.
ADV router	Indicates the advertising router.
Advertisement	Indicates in the hex format the LSA.
Advertisement length	Indicates the length in bytes of the LSA.

Output	Description
Advertising router	Indicates the advertising router.
Area	Indicates the OSPFv3 area ID.
Bits	Indicates the bits that represent various router roles within the OSPFv3 domain.
Checksum	Indicates the link state checksum.
Destination Router-ID	Indicates the router-ID of the destination router.
Forwarding Address	Indicates the forwarding address.
Interface-ID	Indicates the local interface ID.
Interface index	Indicates the local interface index.
Interface IP address	Indicates the interface IPv6 address.
Link ID	Indicates the link ID.
Link-local Interface Address	Indicates the originating router's link-local interface address.
Link state ID	Indicates the link state ID.
Link type	Indicates the link type.
Metric	Indicates the link metric.

Output	Description
Neighbor interface-ID	Indicates the remote neighbor interface ID.
Neighbor router-ID	Indicates the router-ID from the neighbor router.
Number of interfaces	Indicates the number of OSPFv3 interfaces on the router.
Number of prefixes	Indicates the number of prefixes present into the LSA.
Options	Indicates the optional capabilities.
OSPFv3 Router with ID	Indicates the Router-ID.
Prefix options	Indicates the prefix optional capabilities.
Process ID	Indicates the OSPFv3 process ID.
Referenced advertising router	Indicates the originating router-ID.
Referenced LS ID	Indicates the link state ID.
Referenced LS Type	Indicates the type of LSA to which these prefixes are associated with.
Router priority	Indicates the router priority.
Sequence	Indicates the link state sequence.

Output	Description
--------	-------------

Sequence number	Indicates the link state sequence number.
-----------------	---

Type	Indicates the link type.
------	--------------------------

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

These commands can be executed directly via CLI.

Example:

These examples show how to use show commands for OSPFv3 database information.

```
# show ipv6 ospf database brief
Codes: IA - inter area, iA - intra area,
       net - network,    prf - prefix, rtr - router, TE - traffic-engineering
OSPF Router with ID (1.1.1.3) Process ID (1)
Area 0.0.0.1;
```

```

Link type      Link ID      ADV router      Age (secs) Sequence      Checksum
-----
0x2001-router 0.0.0.0      1.1.1.2         547          0x8000000B 0x0000015D
0x2001-router 0.0.0.0      1.1.1.3         546          0x80000002 0x0000F374
0x2003-IA prf 0.0.0.1  1.1.1.2         460          0x80000008 0x0000B26E
0x2004-IA rtr 0.0.0.1  1.1.1.2         446          0x80000008 0x00001401
0x2009-ia prf 0.0.0.1  1.1.1.2         547          0x8000000F 0x00008DD0
0x2009-ia prf 0.0.0.1  1.1.1.3         546          0x80000002 0x00008B79

# show ipv6 ospf database detail

OSPF Router with ID (1.1.1.2) Process ID (1)

Area 0.0.0.0; Link type: router;
  Link state ID: 0.0.0.0; Advertising router: 1.1.1.1;
  Age: 747 secs; Sequence number: 0x8000028B; Checksum: 0x00005A4D
  Advertisement length: 40 (first 58 chars displayed)
  Advertisement: 0x0001200100000000010101018000028b5a4d002802000013010000010c
  Options: R, E, V6
  Bits: E
  Number of interfaces: 1
  Interfaces:
    1. Interface-ID: 201326692; Neighbor interface-ID: 201326692;
      Neighbor router-ID: 1.1.1.2; Type: 1; Metric: 1

  Link state ID: 0.0.0.0; Advertising router: 1.1.1.2;
  Age: 752 secs; Sequence number: 0x800000C3; Checksum: 0x0000D699
  Advertisement length: 40 (first 58 chars displayed)
  Advertisement: 0x000120010000000001010102800000c3d699002803000013010000010c
  Options: R, E, V6
  Bits: E, B
  Number of interfaces: 1
  Interfaces:
    1. Interface-ID: 201326692; Neighbor interface-ID: 201326692;
      Neighbor router-ID: 1.1.1.1; Type: 1; Metric: 1

Area 0.0.0.0; Link type: inter-area-prefix;
  Link state ID: 0.0.0.1; Advertising router: 1.1.1.2;
  Age: 752 secs; Sequence number: 0x800000BD; Checksum: 0x0000C344
  Advertisement length: 36 (first 58 chars displayed)
  Advertisement: 0x000120030000000101010102800000bdc3440024000000014000000020
  Address prefix: 2005:600::/64; Metric: 1; Prefix Options: None

  Link state ID: 0.0.0.36; Advertising router: 1.1.1.2;
  Age: 1690 secs; Sequence number: 0x80000003; Checksum: 0x0000ABF6
  Advertisement length: 36 (first 58 chars displayed)
  Advertisement: 0x00012003000000240101010280000003abf60024000000024000000020
  Address prefix: 2005:200::/64; Metric: 2; Prefix Options: None

  Link state ID: 0.0.0.37; Advertising router: 1.1.1.2;
  Age: 1690 secs; Sequence number: 0x80000003; Checksum: 0x00003655
  Advertisement length: 40 (first 58 chars displayed)
  Advertisement: 0x0001200300000025010101028000000336550028000000025000000020
  Address prefix: 2005:202::/80; Metric: 2; Prefix Options: None

Area 0.0.0.0; Link type: inter-area-router;
  Link state ID: 0.0.0.18; Advertising router: 1.1.1.2;
  Age: 1690 secs; Sequence number: 0x80000003; Checksum: 0x00008F77
  Advertisement length: 32 (first 58 chars displayed)
  Advertisement: 0x000120040000001201010102800000038f770020000000130000000101
  Destination router ID: 1.1.1.3; Metric: 1; Options: R, E, V6

Area 0.0.0.0; Link type: intra-area-prefix;
  Link state ID: 0.0.0.1; Advertising router: 1.1.1.2;
  Age: 752 secs; Sequence number: 0x800000C3; Checksum: 0x0000A24
  Advertisement length: 52 (first 58 chars displayed)
  Advertisement: 0x000120090000000101010102800000c30a240034000120010000000001
  Referenced LS type: router
  Referenced LS ID: 0.0.0.0
  Referenced advertising router: 1.1.1.2
  Number of prefixes: 1
  Prefixes:
    1. Address prefix: 2005:555::1/128; Metric: 0; Prefix Options: LA

# show ipv6 ospf database external brief

Link Type      Link ID      ADV Router      Age (secs) Sequence      Checksum
-----

```

```

-----
0x4005-AS-ext 0.0.0.1          200.200.200.1  11          0x80000001  0x00001F33

# show ipv6 ospf database external detail

Link type: AS-external; Link ID: 0.0.0.1;
Advertising router: 200.200.200.1;
Age: 77 secs; Sequence number: 0x80000001; Checksum: 0x00001F33;
Advertisement: 0x0001400500000001c8c8c801800000011f33;
  Address Prefix: 2001:100::/64; Forwarding Address: n/a;
  Metric: 0; Metric Type: 1; Prefix Options: None;

# show ipv6 ospf database link

Link ID          ADV Router          Age (secs) Sequence          Checksum
-----
12.0.0.100      200.200.200.1      74          0x80000001      0x0000FB0C
0.0.0.100       200.200.200.2      72          0x80000001      0x00003D44

# show ipv6 ospf database link detail 1

Link type: link; Link ID: 12.0.0.200;
Advertising router: 1.1.1.2; Area ID: 0.0.0.1;
Interface IP address: n/a; Interface index: 201326792;
Age: 1328 secs; Sequence number: 0x8000000B; Checksum: 0x0000E377;
Advertisement length: 128; (first 58 chars displayed..)
Advertisement: 0x053000080c0000c8010101028000000be37701bc01000013fe80000000;
  Router priority: 1
  Options: R, E, V6
  Link-local Interface Address: fe80::801:9ff:fec5:100
  Number of prefixes: 20
  Prefixes:
    1. Address prefix: 2005:919::3/128; Prefix Options: LA
    2. Address prefix: 2005:918::3/128; Prefix Options: LA
    3. Address prefix: 2005:917::3/128; Prefix Options: LA
    4. Address prefix: 2005:916::3/128; Prefix Options: LA
    5. Address prefix: 2005:915::3/128; Prefix Options: LA
    6. Address prefix: 2005:914::3/128; Prefix Options: LA
    7. Address prefix: 2005:913::3/128; Prefix Options: LA
    8. Address prefix: 2005:912::3/128; Prefix Options: LA
    9. Address prefix: 2005:911::7/128; Prefix Options: LA
    10. Address prefix: 2005:810::7/128; Prefix Options: LA
    11. Address prefix: 2005:809::7/128; Prefix Options: LA
    12. Address prefix: 2005:808::7/128; Prefix Options: LA
    13. Address prefix: 2005:707::7/128; Prefix Options: LA
    14. Address prefix: 2005:706::2/128; Prefix Options: LA
    15. Address prefix: 2005:705::2/128; Prefix Options: LA
    16. Address prefix: 2005:604::2/128; Prefix Options: LA
    (First 16 prefixes displayed)

Link type: link; Link ID: 12.0.0.200;
Advertising router: 1.1.1.3; Area ID: 0.0.0.1;
Interface IP address: n/a; Interface index: 201326792;
Age: 62 secs; Sequence number: 0x80000001; Checksum: 0x0000A79C;
Advertisement length: 128; (first 58 chars displayed..)
Advertisement: 0x003d00080c0000c80101010380000001a79c005401000013fe80000000;
  Router priority: 1
  Options: R, E, V6
  Link-local Interface Address: fe80::801:9ff:fe00:100
  Number of prefixes: 2
  Prefixes:
    1. Address prefix: 2005:202::5/128; Prefix Options: LA
    2. Address prefix: 2005:200::1/128; Prefix Options: LA

```

Impacts and precautions

Only first 16 prefixes are displayed in database link show.

The full prefixes list can be viewed in the intra-area LSAs using the `show ipv6 ospf database detail` command.

Hardware restrictions

N/A

show ipv6 ospf neighbor

Description

Shows information about the OSPFv3 neighbors.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

show ipv6 ospf neighbor

show ipv6 ospf neighbor brief [*Router-ID*]

show ipv6 ospf neighbor detail [*Router-ID*]

Parameters

brief

Description: Shows resummed information about the OSPFv3 neighbors.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the OSPFv3 neighbors.

Value: N/A

Default Value: N/A

Router-ID

Description: Shows only information about the specified OSPFv3 neighbor.

Value: 0.0.0.0-255.255.255.255.

Default Value: N/A

Output Terms

Output	Description
Neighbor-ID	Indicates the router ID value of the OSPFv3 neighbor router-ID.
Pri	Indicates the priority value of the OSPFv3 neighbor.
State	Indicates the adjacency state with the OSPFv3 neighbor.
Interface-address	Indicates the interface address of the OSPFv3 neighbor.
Interface-name	Indicates the interface name of the OSPFv3 neighbor.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show ipv6 ospf neighbor

State codes: atmpt - attempt; exchg - exchange; exst - exchange start;
              load - loading; 2-way - two-way;

Neighbor-ID   Pri  State  Interface-address      Interface-name
-----
10.10.10.2    1    full  fe80::204:dfff:fe5c:1089  vlan100

# show ipv6 ospf neighbor brief

State codes: atmpt - attempt; exchg - exchange; exst - exchange start;
              load - loading; 2-way - two-way;

Neighbor-ID   Pri  State  Interface-address      Interface-name
-----
10.10.10.2    1    full  fe80::204:dfff:fe5c:1089  vlan100

# show ipv6 ospf neighbor detail

Neighbor-ID: 10.10.10.2; Interface-address: fe80::204:dfff:fe5c:1089;
Area: 0.0.0.0; Interface-name: vlan100;
Relationship state with neighbor: full; Oper status: up;
Neighbor priority: 1; Options: 0x13; Re-transmission queue length: 0;
Number of neighbor relationship state changes or error: 6;
Hello suppressed: no; Requested LSAs: 0;
Dead timer due in: 00:00:35 (hrs:mins:secs);
Hitless restart status: not helping;
Remaining hitless restart interval: none;
Hitless restart result: none;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

VRRP

This topic describes the commands related to management of VRRP topologies such as commands to configure the VRRP parameters or to inspect the protocol status.

router vrrp

Description

Configures a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a VRRP router.

```
(config)# router vrrp
(config-vrrp)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface

Description

Configures VRRP on a L3 interface.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Currently it is supported up to 32 protected L3 interfaces. i.e 32 instances of VRRP.

Example:

This example shows how to configure VRRP in a L3 interface.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family

Description

Configures VRRP for an address family.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*}

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure VRRP for an address family.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id

Description

Configures the virtual router identifier for a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure VR-ID for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id address

Description

Configures a virtual address for a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** { *ipv4* | *ipv6* } **vr-id** *id* **address** { *a.b.c.d* | *x:x:x:x::x* | **link-local** { *auto-configuration* | *x:x:x:x::x* } }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family { *ipv4* | *ipv6* }

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

address { *a.b.c.d* | *x:x:x:x::x* }

Description: Specifies an IPv4 or IPv6 address to be a virtual address for this VRRP router.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

address link-local { *auto-configuration* | *x:x:x:x::x* }

Description: Configures automatically the virtual IPv6 64-bit Extended Unique Identifier link-local address obtained through VRRP MAC address or specifies an IPv6 link-local address to be a virtual address for this VRRP router.

Value: x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Configuring the virtual IPv6 link-local address is mandatory to enable VRRP with IPv6

address family, and this command will be available only for this address family.

Examples:

This example shows how to configure virtual IPv4 address for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# address 10.10.10.1
(config-vrrp-if-address-family-10)# commit
```

This example shows how to configure virtual IPv6 link-local address and virtual IPv6 address for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan101
(config-vrrp-if)# address-family ipv6
(config-vrrp-if-address-family)# vr-id 11
(config-vrrp-if-address-family-11)# address link-local auto-configuration
(config-vrrp-if-address-family-11)# address 2001:db8::1
(config-vrrp-if-address-family-11)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id administrative-status

Description

Configures the desired administrative status of a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

administrative-status *status*

Description: Activate (up) or deactivate (down) the VRRP router.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# administrative-status down
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id advertisement-interval

Description

Configures the advertisement interval for a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **advertisement-interval** *interval*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

advertisement-interval *interval*

Description: Specifies a maximum advertisement interval value between advertisement messages, in seconds, sent by this VRRP router.

Value: 1-40.

Default Value: 1.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the advertisement interval for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# advertisement-interval 40
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

Low maximum advertisement interval will generate messages at a high rate and may affect bandwidth throughput.

Hardware restrictions

N/A

router vrrp interface address-family vr-id authentication

Description

Configures the authentication of a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **authentication simple-text** *password*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

authentication simple-text *password*

Description: Specify a simple text password authentication for the VRRP router.

Value: Simple text password.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the simple text password authentication for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# authentication simple-text test123
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id preempt

Description

Configures the preemption for a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **preempt** *preempt*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

preempt *preempt*

Description: Controls whether a higher-priority Backup router preempts a lower-priority Master router.

Value: true | false.

Default Value: true.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the preemption for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# preempt false
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id priority

Description

Configures the priority for a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **priority** *priority*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

priority *priority*

Description: Specifies a priority value to be advertised by this VRRP router during Master election.

Value: 1-254.

Default Value: 100.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Priority value of 255 will be automatically assigned to the VRRP router address owner.

Example:

This example shows how to configure the priority for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# priority 150
(config-vrrp-if-address-family-10)# commit
```


Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id track

Description

Configures the track interface of a VRRP router.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **track** {**interface** *l3-interface-name* | **decrement** *decrement-priority*}

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

track decrement *decrement-priority*

Description: Specifies the value to decrement priority by when all tracked interfaces are operationally down.

Value: 1-253.

Default Value: 50.

track interface I3-*interface-name*

Description: Specifies L3 interfaces to track their operational state.

Value: Any L3 interface.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

3.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Track feature only acts decrementing priority if VRRP router is not the address owner.

Priority will be decremented only if all tracked L3 interfaces are operationally down.

Example:

This example shows how to configure the track interface and decrement for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# track decrement 60
(config-vrrp-if-address-family-10)# track interface l3-uplink1
(config-vrrp-if-address-family-10)# track interface l3-uplink2
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

router vrrp interface address-family vr-id version

Description

Configures the VRRP router protocol version.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

router vrrp interface *l3-interface-name* **address-family** {*ipv4* | *ipv6*} **vr-id** *id* **version** *vrrp-version*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description: Specifies an L3 interface in which VRRP will be enabled. The L3 interface must be created before the commit.

Value: Any L3 interface.

Default Value: N/A

address-family {*ipv4* | *ipv6*}

Description: Specifies the address family for which VRRP will be enabled on this interface.

Value: IPv4 or IPv6.

Default Value: N/A

vr-id *id*

Description: Specifies the virtual router identifier.

Value: 1-255.

Default Value: N/A

version *vrrp-version*

Description:	Specifies the virtual router protocol version.
Value:	v2 v3.
Default Value:	v3.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This this command will be available only for IPv4 address family.

Examples:

This example shows how to configure protocol version for a VRRP router.

```
(config)# router vrrp
(config-vrrp)# interface l3-vlan100
(config-vrrp-if)# address-family ipv4
(config-vrrp-if-address-family)# vr-id 10
(config-vrrp-if-address-family-10)# version v2
(config-vrrp-if-address-family-10)# commit
```

Impacts and precautions

Changing the VRRP router protocol version will restart the VRRP router process.

Hardware restrictions

N/A

PBR

This topic describes the commands related to management of PBR topologies such as commands to configure the PBR parameters or to inspect the protocol status.

router pbr

Description

Create policy-based rules that are applied before the normal layer 3 routing. Also allows enforcing the L3 routing as a rule exception.

Supported Platforms

This command is not supported in the following platforms: DM4360, DM4370, DM4611, DM4612, DM4618.

Syntax

```
router pbr id [ priority { rule_priority } description { description_string } match { source ipv4-address ipv4/mask } match { destination ipv4-address ipv4/mask } match { interface interface-name ... } action { I3-routing | next-hop ipv4 } ]
```

Parameters

id

Description: The PBR rule id. Up to 64 rules can be configured.

Value: 1-64

Default Value: N/A

priority *rule_priority*

Description: The PBR rule priority. Lower values have higher priority. Must be unique between all PBR rules. Priority is a mandatory configuration.

Value: 0-255

Default Value: N/A

description *description_string*

Description: The PBR rule description. A user field to help identify the rule meaning. Enclose the content in double quotes for multi word description.

Value: string up to 32 characters.

Default Value: N/A

match source ipv4-address *ipv4/mask*

Description: A PBR rule match for source IPv4 host or subnet address. Any packet with source IP (or masked range) that matches with the configured one will be forwarded by the PBR rule. For a single IP match, the mask can be omitted. At least one match type (source, destination or interface) must be provided.

Value: A.B.C.D[/mask] IPv4 host or subnet address

Default Value: N/A

match destination ipv4-address *ipv4/mask*

Description: A PBR rule match for destination IPv4 host or subnet address. Any packet with destination IP (or range) that matches with the configured one will be forwarded by the PBR rule. For a single IP match, the mask can be omitted. At least one match type (source, destination or interface) must be provided.

Value: A.B.C.D[/mask] IPv4 host or subnet address

Default Value: N/A

match interface *interface-name ...*

Description: A PBR rule match for input interface names. Any packet that enters the switch through any of the named interfaces will be forwarded by the PBR rule. Several interfaces can be configured in the rule. At least one match type (source, destination or interface) must be provided.

Value: *interface-type-chassis/slot/port* - The interface name.
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, gpon**

Default Value: N/A

action l3-routing

Description: A PBR rule action that overrides another PBR rule, by enforcing the use of the L3-routing. This can be used to add an exception to a much broader rule. This kind of exception must have a higher priority than the rule it is meant to override. Only one action type (l3-routing, next-hop) must be provided.

Value: none

Default Value: N/A

action next-hop *ipv4*

Description: A PBR rule action that forwards all matched traffic to an specific host. Only one action type (l3-routing, next-hop) must be provided.

Value: A.B.C.D IPv4 host

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History**Release****Modification**

5.10

This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a PBR rule for:

- “Client X”
- With priority 10
- For packets that enter through interfaces gigabit-ethernet-1/1/1 and 1/1/2
- Coming from IPs 10.0.0.1 to 10.0.0.254
- That will be forwarded to 172.22.16.10

```
(config)# router pbr 1
(config-pbr-1)# priority 10
(config-pbr-1)# description "Client X"
(config-pbr-1)# match interface gigabit-ethernet-1/1/1 gigabit-ethernet-1/1/2
(config-pbr-1)# match source ipv4-address 10.0.0.0/24
(config-pbr-1)# action next-hop 172.22.16.10
(config-pbr-1)# commit
```

Example:

This example adds an exception to the role 1:

- “Client X”
- With priority 5
- For packets that enter through interfaces gigabit-ethernet-1/1/1 and 1/1/2
- Coming from IP 10.0.0.15
- That will be forwarded by L3 routing

```
(config)# router pbr 2
(config-pbr-2)# priority 5
(config-pbr-2)# description "Client X3 exception"
(config-pbr-2)# match interface gigabit-ethernet-1/1/1 gigabit-ethernet-1/1/2
(config-pbr-2)# match source ipv4-address 10.0.0.15
(config-pbr-2)# action l3-routing
(config-pbr-2)# commit
```

Example:

This example adds another rule, now with destination match:

- “Client Z”
- With priority 20
- For packets that enter through any interface
- Destinated to IP 172.20.100.100
- That will be forwarded to 172.20.0.1

```
(config)# router pbr 3
(config-pbr-3)# priority 20
(config-pbr-3)# description "Client Z"
(config-pbr-3)# match destination ipv4-address 172.20.100.100
(config-pbr-3)# action next-hop 172.20.0.1
(config-pbr-3)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show router pbr

Description

Display information about Policy-based routes status and configuration. When omitted the *rule-id*, the show displays all configured rules status.

Supported Platforms

This command is not supported in the following platforms: DM4360, DM4370, DM4611, DM4612, DM4618.

Syntax

```
show router pbr [ rule-id ]
```

Parameters

rule-id

Description: The rule id whose status is desired to show.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
ID	The PBR rule Id.
Priority	The Priority of the rule. Lower values are applied first.
Match Source IP	The Source IP that should match (in the packets) to the rule be enforced.
Match Destination IP	The Destination IP that should match (in the packets) to the rule be enforced.

Output	Description
Match Interface	The Inbound interface(s) that should match (in the packets) to the rule be enforced.
Action Next-hop	<p>The action that will be applied to the packet:</p> <ul style="list-style-type: none"> -Redirect to a configured IP address; -Proceed with I3-routing.
Hardware Status	<p>Informes if the rule is installed and effective in the hardware:</p> <ul style="list-style-type: none"> -Pending: The configured next-hop is not available or the rule pends installation; -Installing: The rule is being installed and will be available soon; -Installed: The rule is installed and will be enforced on any matched packet.
Description	The rule description as configured by the user.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.12	This command was introduced.

Usage Guidelines

Given the equipment has a PBR configuration. A show will present:

```
# show router pbr
```

ID	Priority	Match Source IP	Match Dest. IP	Match Interface	Action Next-Hop	Hardware Status	Description
1	1	-	3.3.3.3/24	gigabit-ethernet-1/1/1 hundred-gigabit-ethernet-1/1/1	1.1.1.1	installing	-
2	40	2.2.2.1	-	gigabit-ethernet-1/1/3	2.2.1.1	installed	Client X
3	10	1.1.1.1	-	-	l3-routing	pending	IPTV
4	5	2.2.2.2	-	-	l3-routing	pending	-

#

</code> <newline>

When the rule id is specified:

```
# show router pbr 1
```

ID	Priority	Match Source IP	Match Dest. IP	Match Interface	Action Next-Hop	Hardware Status	Description
1	1	-	3.3.3.3/24	gigabit-ethernet-1/1/1 hundred-gigabit-ethernet-1/1/1	1.1.1.1	installing	-

#

Impacts and precautions

None

Hardware restrictions

None

VRF

This topic describes the commands related to management of VRF topologies such as commands to configure the VRF parameters or to inspect the protocol status.

vrf

Description

Creates a VRF.

Supported Platforms

This command is supported in all platforms.

Syntax

vrf *vrf-name* [**description** *vrf-description*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF. Only accepts alphanumeric characters, '_' and '-'.

Value: string (length 1 - 32).

Default Value: N/A

description *vrf-description*

Description: Specifies the description of the VRF. It may point out a more meaningful text about its purpose.

Value: string (length 1 - 32).

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
4.4	The description parameter was introduced.

Usage Guidelines

Use the **vrf** command to create a new virtual routing forwarding instance for the system. There are two VRFs already created, *global* is the default VRF and *mgmt* is a VRF dedicated to out-of-band management interface. Neither of them can be changed or deleted.

Example:

This example shows how to configure a new VRF named “green” for the system.

```
(config)# vrf green
(config)# commit
Commit complete.
```

Impacts and precautions

The overall number of available VRFs includes both the system’s reserved *global* and *mgmt*. The word *all* is reserved for VRF filter purposes, thus no VRF named *all* can be created.

Hardware restrictions

The following platforms support only the system VRFs *global* and *mgmt*:

- DM4050
- DM4610
- DM4611
- DM4612
- DM4615
- DM4618

vrf address-family ipv4 unicast

Description

Creates an address-family associated with VRF.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

vrf *vrf-name* **address-family** { **ipv4** } **unicast**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF. Only accepts alphanumeric characters, '_' and '-'.

Value: string (length 1 - 32).

Default Value: N/A

address-family { **ipv4** }

Description: Selects the address family identifier (AFI).

Value: **ipv4**. IPv4 address family.

Default Value: N/A

unicast

Description: Selects the subsequent address family identifier (SAFI).

Value: **unicast**. IPv4 unicast routes.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.2	This command was introduced.
7.0	This command was removed.

Usage Guidelines

This command can be executed directly via CLI.

This example shows how to configure an address-family ipv4 unicast in the VRF.

```
(config)# vrf green address-family ipv4 unicast
(config-address-family-ipv4/unicast)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

vrf rd

Description

Creates a route distinguisher.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

```
vrf vrf-name rd { ASN:nn | IPv4:nn }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF. Only accepts alphanumeric characters, '_' and '-'.

Value: string (length 1 - 32).

Default Value: N/A

```
rd { ASN:nn | IPv4:nn }
```

Description: Specifies the VRF route distinguisher.

Value: ASN:nn or IPv4:nn format.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.2	This command was introduced.
-----	------------------------------

Usage Guidelines

Use the **rd** command in order to associate a route distinguisher with a VRF.

Example:

This example shows how to configure a new route distinguisher in ASN:nn format.

```
(config)# vrf green rd 65000:1000
(config-vrf-green)# commit
```

This example shows how to configure a new route distinguisher in IPv4:nn format.

```
(config)# vrf green rd 10.20.2.3:1000
(config-vrf-green)# commit
```

Impacts and precautions

Route distinguisher must be unique in the system. The VRFs *global* and *mgmt* do not support route distinguisher configuration.

Hardware restrictions

N/A

vrf route-target

Description

Configures a route target to be exported or imported.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4610, DM4611, DM4612, DM4615, DM4618.

Syntax

vrf *vrf-name* **route-target** { **export** | **import** } *route-target-number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf-name

Description: Specifies the name of the VRF. Only accepts alphanumeric characters, '_' and '-'.

Value: string (length 1 - 32).

Default Value: N/A

route-target export

Description: Selects the route target to be exported from this VRF.

Value: N/A

Default Value: N/A

route-target import

Description: Selects the route target to be imported to this VRF.

Value: N/A

Default Value: N/A

route-target-number

Description:	Specifies the route target.
Value:	ASN:nn or IPv4:nn format.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.2	This command was introduced.
7.0	The address-family option was removed.

Usage Guidelines

A route distinguisher must be previously associated with this VRF.

This example shows how to configure a route target in ASN:nn format to be exported.

```
((config-vrf-red))# route-target export 1:2
(config-route-target-export/1:2)# commit
```

This example shows how to configure a route target in ASN:nn format to be imported.

```
((config-vrf-red))# route-target import 1:4
(config-route-target-import/1:4)# commit
```


Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 7: MPLS

This chapter describes the commands related to management of MPLS topologies in the DmOS CLI. MPLS features are available under specific license control. Please contact the Technical Support for further information.

INFRA

This topic describes the commands related to management of basic MPLS infrastructure such as commands to configure MPLS generic behavior parameters.

show mpls forwarding-table

Description

Show list of MPLS entries installed on data plane.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

show mpls forwarding-table [**prefix-or-tnl-name** *ipv4-prefix or tunnel-name* | **action** *action* | **in-label** *label* | **in-protocol** *protocol* | **out-label** *label* | **out-protocol** *protocol* | **outgoing-interface** *I3-interface* | **status** *status*]

Parameters

prefix-or-tnl-name *ipv4-prefix or tunnel name*

Description: Use IP prefix or tunnel name to filter the output.

Value: a.b.c.d/x | string

Default Value: N/A

action *action*

Description: Use Action to filter the output.

Value: none | fwd | psh | pop | php | swp

Default Value: N/A

in-label *label*

Description: Use In Label to filter the output.

Value: label value

Default Value: N/A

in-protocol *protocol*

Description: Use In Protocol to filter the output.

Value: ldp | rsvp | unk | –

Default Value: N/A

out-label *label*

Description: Use Out Label to filter the output.

Value: label value

Default Value: N/A

out-protocol *protocol*

Description: Use Out Protocol to filter the output.

Value: ldp | rsvp | unk | –

Default Value: N/A

outgoing-interface *l3-interface*

Description: Use Outgoing-Interface to filter the output.

Value: l3-vlan id

Default Value: N/A

status *status*

Description: Use Status to filter the output.

Value: active | pending | stale

Default Value: N/A

Output Terms

Output	Description
Prefix or Tunnel-Name	Display the LSP prefix or Tunnel-Name associated with MPLS entry.
Action	<p>Display the MPLS action performed on data plane by the entry.</p> <ul style="list-style-type: none"> • none: no action associated with entry • fwd: originated MPLS tunnel with Implicit Null Label. • psh: originated MPLS tunnel pushing the outgoing label. • pop: remove incoming label to forward the packet. • php: swap the incoming label to Implicit Null label. • swp: swap incoming label to outgoing label.
In Label	Display the incoming label associated with entry.
In Proto	<p>Display the incoming protocol which distributes the incoming label.</p> <ul style="list-style-type: none"> • ldp: LDP distributed the label. • rsvp: RSVP distributed the label. • unk: an unknown protocol has distributed the label.
Out Label	Display the outgoing label associated with entry.
Out Proto	<p>Display the outgoing protocol which distributes the outgoing label.</p> <ul style="list-style-type: none"> • ldp: LDP distributed the label. • rsvp: RSVP distributed the label. • unk: an unknown protocol has distributed the label.
Out interface	Display the outgoing vlan interface for the MPLS traffic associated with entry.

Output	Description
Status	<p>Display the MPLS outgoing vlan interface for the MPLS traffic associated with entry.</p> <ul style="list-style-type: none">• Active: indicates entry is active.• Pending: indicates entry has installation pending due neighbor resolution.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.0	This command was introduced.
5.4	Traffic engineering (TE) info was added.

Usage Guidelines

To simply show the list of MPLS entries installed on data plane the following command can be used:

Example:

```
# show mpls forwarding-table
```

It is possible to filter the results by Prefix or Tunnel-Name, Action, In Label, In Protocol, Out Label, Out Protocol, Out interface and Status.

Filter by Prefix:

Example:

```
# show mpls forwarding-table prefix-or-tnl-name 200.200.200.1/32
```

Filter by Tunnel Name:

Example:

```
# show mpls forwarding-table prefix-or-tnl-name tunnel-te-1000
```

Filter by Action:

Example:

```
# show mpls forwarding-table action swp
```

Filter by In Label:

Example:

```
# show mpls forwarding-table in-label 16
```

Filter by In Protocol:

Example:

```
# show mpls forwarding-table in-protocol ldp
```

Filter by Out Label:

Example:

```
# show mpls forwarding-table out-label ImpNull
```

Filter by Out Protocol:

Example:

```
# show mpls forwarding-table out-protocol ldp
```

Filter by Out Interface:

Example:

```
# show mpls forwarding-table outgoing-interface 13-vlan 100
```

Filter by Status:

Example:

```
# show mpls forwarding-table status active
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls traffic-eng tunnel-te brief

Description

Show all RSVP-TE tunnel instances information present.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

```
show mpls traffic-eng tunnel-te brief [ backup backup | destination dest | id id | in-label label | in-vlan vlan | instance instance | name name | out-label label | out-vlan vlan | status status ]
```

Parameters

backup *backup*

Description: Use backup information to filter the output.

Value: available | in-use | none

Default Value: N/A

destination *dest*

Description: Use tunnel destination IPV4 address to filter the output.

Value: a.b.c.d/x | string

Default Value: N/A

id *id*

Description: Use tunnel id to filter the output.

Value: tunnel id value

Default Value: N/A

in-label *label*

Description: Use In Label to filter the output.

Value: label value

Default Value: N/A

in-vlan *vlan*

Description: Use incoming VLAN to filter the output.

Value: vlan value

Default Value: N/A

instance *instance*

Description: Use tunnel instance to filter the output.

Value: tunnel instance value

Default Value: N/A

name *name*

Description: Use tunnel name to filter the output.

Value: tunnel name value

Default Value: N/A

out-label *label*

Description: Use Out Label to filter the output.

Value: label value

Default Value: N/A

out-vlan *vlan*

Description: Use outgoing VLAN to filter the output.

Value: vlan value

Default Value: N/A

status *status*

Description: Use tunnel status to filter the output.

Value: up | down | testing | unknown | dormant | not-present | lower-layer-down

Default Value: N/A

Output Terms

Output	Description
ID	Display the Tunnel identifier associated with tunnel interface entry.
Name	Display the Tunnel-Name associated with tunnel interface entry.
Destination	Display the IPV4 address associated with tunnel interface entry.
Instance	Display the tunnel instance associated with tunnel interface entry.
In Label	Display the incoming label associated with entry.
In vlan	Display the incoming VLAN associated with entry.
Out Label	Display the outgoing label associated with entry.
Out vlan	Display the outgoing VLAN associated with entry.
Backup	<p>Display status of the backup instance associated with the tunnel interface.</p> <ul style="list-style-type: none">• available: Backup is current available.• in-use: Backup is current in use.• none: Backup is not available.

Output	Description
Status	Display the tunnel instance status. <ul style="list-style-type: none">• up: The tunnel instance is ready to pass packets.• down: The tunnel instance is not ready to pass packets.• testing: The tunnel instance is in some test mode.• unknown: The tunnel instance status cannot be determined.
	<ul style="list-style-type: none">• dormant: The tunnel instance has some missing components.• not-present: The tunnel instance has some missing components.• lower-layer-down: The tunnel instance is down due to the state of lower-layer interfaces.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.8	This command was updated to receive the <i>brief</i> tag.
5.4	This command was introduced.

Usage Guidelines

Use the command to show the list of tunnel instances:

Example:

```
# show mpls traffic-eng tunnel-te brief
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

It is possible to filter the results by ID, Name, Destination, Instance, In label, In VLAN, Out label, Out VLAN, Backup, and Status.

Filter by ID:

Example:

```
# show mpls traffic-eng tunnel-te brief id 2
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up

Filter by Name:

Example:

```
# show mpls traffic-eng tunnel-te brief name TUNNEL-TE-2
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up

Filter by Destination:

Example:

```
# show mpls traffic-eng tunnel-te brief destination 120.120.120.1
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up

Filter by Instance:

Example:

```
# show mpls traffic-eng tunnel-te brief instance 2
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Filter by In Label:**Example:**

```
# show mpls traffic-eng tunnel-te brief in-label 20
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Filter by In VLAN:**Example:**

```
# show mpls traffic-eng tunnel-te brief in-vlan 150
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up

Filter by Out Label:**Example:**

```
# show mpls traffic-eng tunnel-te brief out-label ImpNull
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Filter by Out VLAN:**Example:**

```
# show mpls traffic-eng tunnel-te brief out-vlan 150
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Filter by Backup:**Example:**

```
# show mpls traffic-eng tunnel-te brief backup none
```

ID	Name	Destination	Inst	In label	In vlan	Out label	Out vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Filter by Status:**Example:**

```
# show mpls traffic-eng tunnel-te brief status up
```

```
In      In      Out      Out
```

ID	Name	Destination	Inst	label	vlan	label	vlan	Backup	Status
2	TUNNEL-TE-2	120.120.120.1	2	19	150	ImpNull	151	none	up
3	TUNNEL-TE-3	100.100.100.1	2	20	151	ImpNull	150	none	up

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls traffic-eng tunnel-te id | name

Description

Show detailed RSVP-TE tunnel information for a single instance (by name or id).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

```
show mpls traffic-eng tunnel-te { id id | name name }
```

Parameters

id *id*

Description: The tunnel id.
Value: tunnel id value
Default Value: N/A

name *name*

Description: The tunnel name.
Value: tunnel name value
Default Value: N/A

Output Terms

Output	Description
Id	Display the Tunnel identifier associated with tunnel interface entry.
Name	Display the Tunnel-Name associated with tunnel interface entry.

Output	Description
Active Instance	Display the tunnel instance that is currently active.
Src	Display the IPV4 address associated with tunnel interface entry.
Dst	Display the IPV4 address associated with tunnel interface destination.
Status	Display the status of the active tunnel instance. Contains the Admin, Oper, Role and Dir information.
Admin	Admin status of the active instance.
Oper	Operation status of the active instance.
Role	The role of this node in the LSP.
Dir	The direction of the active instance tunnel.
Path option	Describes all the paths defined for the tunnel.
Path-option attribute	Display the index of the path.
type	Display the type of the path. <ul style="list-style-type: none"> Currently only <i>dynamic</i> is supported
path status	Display the status of the path: <ul style="list-style-type: none"> active: The path is active. holding: The path is in hold state.
instance	Display the instance associated with the path.

Output	Description
Affinity	Display the configuration of the path affinity.
profile	Display the name of the affinity profile associated with the path.
Incl.Any	Affinity attribute values to be any included.
Incl.All	Affinity attribute values to be all included.
Excl.Any	Affinity attribute values to be any excluded.
Tunnel LSP: Inlabel	Display the Inlabel of the tunnel path.
Tunnel LSP: Outlabel	Display the Outlabel of the tunnel path.
Path Info for active instance	Display the path trace of the active instance

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

5.8	This command was introduced.
-----	------------------------------

Usage Guidelines

Use the command to show the detailed information of a tunnel (by id):

Example:

```
# show mpls traffic-eng tunnel-te id 1
Id: 1 Name: R1-R4 [Active instance 2]
Src: 192.168.1.1 Dst: 192.168.1.4
Status:
  Admin: up      Oper: up      Role: head      Dir: out

Path option:
  Path-option attribute: PATH_1 , type: dynamic (holding, instance 1)
  Affinity (blue):      0x1 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: --

  Path-option attribute: PATH_2 , type: dynamic (active, instance 2)
  Affinity (red):       0x2 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: ImpNull

Path Info for active instance:
  1: 192.168.14.4
```

Use the command to show the detailed information of a tunnel (by name):

Example:

```
# show mpls traffic-eng tunnel-te name R1-R4
Id: 1 Name: R1-R4 [Active instance 2]
Src: 192.168.1.1 Dst: 192.168.1.4
Status:
  Admin: up      Oper: up      Role: head      Dir: out

Path option:
  Path-option attribute: PATH_1 , type: dynamic (holding, instance 1)
  Affinity (blue):      0x1 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: --

  Path-option attribute: PATH_2 , type: dynamic (active, instance 2)
  Affinity (red):       0x2 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: ImpNull

Path Info for active instance:
  1: 192.168.14.4
```

In case of all paths being down, no Path Info is shown:

Example:

```
# show mpls traffic-eng tunnel-te name R1-R4
```

```

Id: 1 Name: R1-R4 [Active instance 2]
Src: 192.168.1.1 Dst: 192.168.1.4
Status:
  Admin: up      Oper: up      Role: head      Dir: out

Path option:
  Path-option attribute: PATH_1 , type: dynamic (holding, instance 1)
  Affinity (blue):      0x1 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: --

  Path-option attribute: PATH_2 , type: dynamic (active, instance 2)
  Affinity (red):       0x2 [Incl.Any] 0x0 [Incl.All] 0x0 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: ImpNull

Tunnel is down - no path info available

```

For unnamed tunnels (they receive a default name but can't be queried by name) use the show by id:

Example:

```

# show mpls traffic-eng tunnel-te id 2
Id: 2 Name: tunnel-te-2 [Active instance 10]
Src: 192.168.1.1 Dst: 1.1.1.1
Status:
  Admin: up      Oper: down      Role: head      Dir: out

Path option:
  Path-option attribute: PATH_1 , type: dynamic (holding, instance 10)
  Affinity (green):      0x0 [Incl.Any] 0x0 [Incl.All] 0x3 [Excl.Any]
  Tunnel LSP: Inlabel: -- , Outlabel: --

Tunnel is down - no path info available

```

Impacts and precautions

N/A

Hardware restrictions

N/A

L2VPN

clear mpls l2vpn counters vpls

Description

Clears the Virtual Private LAN Services (VPLS) counters.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
clear mpls l2vpn counters vpls-group [name | vpn-name name ]
```

Parameters

vpls-group *name*

Description: Use Group name to filter the output.
Value: vpls-group name
Default Value: N/A

vpn-name *name*

Description: Use VPN name to filter the output.
Value: vpn-name name
Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.4	This command was introduced.
4.9	This command was modified.

Usage Guidelines

To clear the VPLS counters values the following command can be used:

Example:

```
# clear mpls l2vpn counters vpls-group Group1 vpn-name Vpn1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

clear mpls l2vpn counters vpws

Description

Clears the Virtual Private Wire Services (VPWS) counters.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
clear mpls l2vpn counters vpws-group [name | vpn-name name ]
```

Parameters

vpls-group *name*

Description: Use Group name to filter the output.

Value: vpls-group name

Default Value: N/A

vpn-name *name*

Description: Use VPN name to filter the output.

Value: vpn-name name

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.
4.9	This command was modified.

Usage Guidelines

To clear the VPWS counters values the following command can be used:

Example:

```
# clear mpls l2vpn counters vpws-group Group1 vpn-name Vpn1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

clear mpls l2vpn mac-address vpls

Description

Clears the L2VPN VPLS macs.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
clear mpls l2vpn mac-address vpls-group [name | vpn-name name ]
```

Parameters

vpls-group *name*

Description: Use Group name to filter the output.

Value: vpls-group name

Default Value: N/A

vpn-name *name*

Description: Use VPN name to filter the output.

Value: vpn-name name

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.4	This command was introduced.
4.9	This command was modified.

Usage Guidelines

To clear the L2VPN VPLS mac-address values the following commands can be used:

Example:

```
# clear mpls l2vpn mac-address vpls-group Group1 vpn-name Vpn1
# clear mpls l2vpn mac-address vpls-group Group1
# clear mpls l2vpn mac-address vpls-group
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn logging pw-status

Description

Enables logs to monitor the status of the MPLS L2VPN Pseudowires.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn logging pw-status

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable the MPLS L2VPN Pseudowire status log.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# logging pw-status
(config-l2vpn)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group

Description

The Group ID field is a textual string arbitrary value that is assigned to a group of Virtual Private LAN Services (VPLS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

text

Description:	A textual string assigned to a group of VPLS.
Value:	String - maximum 32 characters.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the l2vpn vpls-group.

```
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn

Description

A textual string to uniquely identify a Virtual Private LAN Services (VPLS) that supports Layer 2 VPN technology and provides multi-point Layer 2 connectivity for customers.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn administrative-status

Description

Configures the desired administrative status on a Virtual Private LAN Services (VPLS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Virtual Private LAN Services (VPLS).
Value: up | down.
Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# administrative-status down
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain

Description

Specifies a virtual bridge that connects the multiple access circuits together.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

bridge-domain

Description: A virtual bridge representation.
Value: N/A
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn bridge-domain.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain access-interface

Description

Specifies the access interfaces to be attached inside a Virtual Private LAN Services (VPLS) bridge-domain.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain access-interface** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

access-interface *id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
4.9	Support for 100-gigabit Ethernet was added.
5.4	Support for service-port was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the bridge-domain access interfaces.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/2
(config-vpn-Seattle-bd)# commit
```

To use a service-port as an access interface, the service-port must be configured without any translate rule, bridge domain mtu must be set to 2000 or less and transparent-lan-service must be enabled.

```
# config
(config)# service-port 1 gpon 1/1/1 onu 1 gem 1
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# bridge-mtu 2000
(config-vpn-Seattle-bd)# transparent-lan-service
(config-vpn-Seattle-bd)# access-interface service-port-1
(config-access-port-service-port-1)# commit
```

Impacts and precautions

Vlan-mapping rules do not have effect over vpn access ports because the latter takes precedence over the former.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain access-interface administrative-status

Description

Configures the desired administrative status on a Virtual Private LAN Services (VPLS) access interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain access-interface** *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

access-interface *id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Virtual Private LAN Services (VPLS) access interface.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
4.9	Support for 100-gigabit Ethernet was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn bridge-domain access-interface administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-access-interface-gigabit-ethernet-1/1/1)# administrative-status down
(config-access-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain access-interface encapsulation dot1q

Description

Configures the encapsulation of customer VLANs (C-VLANs) on a Virtual Private LAN Services (VPLS) access interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain access-interface** *id* **encapsulation dot1q** *values*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

access-interface *id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id.

Default Value: N/A

encapsulation dot1q *values*

Description: dot1q vlan (C-VLAN) or ranges of dot1q vlans (C-VLANs) to be encapsulated.

Value: 1 - 4094

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.10	This command was introduced. Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further in-

formation.

Example:

This example shows how to configure the vpn bridge-domain access-interface encapsulation dot1q.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# qinq
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation dot1q 5,10-15,20
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain access-interface encapsulation untagged

Description

Enable the encapsulation of untagged frames.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain access-interface** *id* **encapsulation untagged**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

access-interface *id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id.

Default Value: N/A

encapsulation untagged

Description: Enable the untagged mode on the encapsulation of customer VLANs (C-VLANs).

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.12	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn bridge-domain access-interface encapsulation untagged.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle)# qinq
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation untagged
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain administrative-status

Description

Configures the desired administrative status on a Virtual Private LAN Services (VPLS) bridge-domain.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

administrative-status *status*

Description:	Activates (up) or deactivates (down) the Virtual Private LAN Services (VPLS) bridge-domain.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the bridge-domain administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# administrative-status down
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain bridge-mtu

Description

Specifies the explicit Maximum Transmission Unit(MTU) of the Virtual Private LAN Services(VPLS) bridge-domain.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain bridge-mtu** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

bridge-mtu *value*

Description: Specifies the VPLS bridge-domain MTU.

Value: 64 - 9198.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the bridge-mtu value that explicitly specifies the MTU value used by the VPLS.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# bridge-mtu 64
(config-vpn-Seattle-bd)# commit
```

Impacts and precautions

Make sure to set an appropriate MTU to account for all the encapsulation overhead that will take place on your MPLS backbone to avoid packet drop. When the MTU is not explicitly configured by this command the value set on this VPLS is the lowest MTU value of the attached physical access interfaces.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain dot1q

Description

Configures the Virtual Private LAN Services (VPLS) bridge-domain to match a specific 802.1Q VLAN packets (VLAN-based).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain dot1q** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

bridge-domain

Description: A virtual bridge representation.
Value: N/A
Default Value: N/A

dot1q *id*

Description: Dot1q VLAN Id to be matched on bridge-domain for this VPN.

Value: 1 - 4094
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

To configure a VLAN-based VPLS bridge-domain, perform this task on the provider edge routers:

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# dot1q 23
(config-vpn-Seattle-bd)# commit
```


Impacts and precautions

A VPLS bridge-domain and a Layer 2 bridge-domain that have the same Dot1Q identifier cannot share interfaces.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain mac-limit

Description

Configures the maximum limit of MAC addresses that can be learned on a Virtual Private LAN Services (VPLS) bridge-domain.

Supported Platforms

This command is supported only in the following platforms: DM4170, DM4360, DM4370, DM4610, DM4615.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain mac-limit** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

mac-limit *value*

Description:	Specifies the VPLS bridge-domain mac-limit.
Value:	1 - 32767.
Default Value:	1024.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the bridge-domain mac-limit

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# mac-limit 4096
(config-vpn-Seattle)# commit
```

Impacts and precautions

Although mac-limit configuration is per VPN, MAC address table is common for all of them in hardware. Therefore, according to the mac-limit value, one or a few VPNs can already consume all the MAC address table entries.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain qinq

Description

Enable Selective Encapsulation QinQ mode for VPLS. This mode allows the configuration of multiple VLANs in the **access-interface encapsulation** command in order to set up a Selective Encapsulation VPN. This mode requires the **vfi pw-type** to be **vlan** and contain the service-delimiting VLAN which will be stacked up top into the frame along with the ingressed access VLANs.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain qinq**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

qinq

Description:	Enable Selective Encapsulation QinQ mode for VPLS.
Value:	N/A
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.10	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a Selective Encapsulation VPN QinQ mode.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# qinq
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation dot1q 5,10-15,20
```

```
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn bridge-domain transparent-lan-service

Description

Enable the Transparent LAN Service (TLS) mode on a Virtual Private LAN Services (VPLS) bridge-domain.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **bridge-domain transparent-lan-service**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

bridge-domain

Description: A virtual bridge representation.

Value: N/A

Default Value: N/A

transparent-lan-service

Description:	Enable the Transparent LAN Service (TLS) mode on a VPLS bridge-domain.
Value:	N/A
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable the bridge-domain transparent-lan-service:

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# bridge-domain
(config-vpn-Seattle-bd)# transparent-lan-service
(config-vpn-Seattle-bd)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn description

Description

Specifies a textual string containing information about the Virtual Private LAN Services (VPLS) entity.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **description** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

description *text*

Description: A textual string containing information about the VPLS entity.

Value: String - maximum 32 characters

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn description.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# description Text
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi

Description

Specifies a Virtual Forwarding Instance (VFI) that connects multiples neighbors together.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.
Value: N/A
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi administrative-status

Description

Configures the desired administrative status on a Virtual Forwarding Instance (VFI).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi** **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.
Value: N/A
Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Virtual Forwarding Instance.

Value: up | down.
Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# administrative-status down
(config-vfi)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor

Description

Specifies the IPv4 address to uniquely identify a Virtual Private LAN Services (VPLS) neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description:	Specifies the VPLS neighbor identifier expressed in IPv4 address format.
Value:	a.b.c.d.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi neighbor.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor administrative-status

Description

Configures the desired administrative status on a Virtual Private LAN Services (VPLS) neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description: Specifies the VPLS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Virtual Private LAN Services (VPLS) neighbor.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi neighbor administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# administrative-status down
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor pw-id

Description

Specifies the pseudo-wire (PW) ID, a non-zero identifier that distinguishes between two MPLS peers from the others. To connect two attachment circuits through a PW, you need to associate each one with the same PW ID. This configuration is mandatory for neighbor enabling.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **pw-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description:	Specifies the VPLS neighbor identifier expressed in IPv4 address format.
Value:	a.b.c.d.
Default Value:	N/A

pw-id *id*

Description:	Specifies the VPLS pseudo-wire numerical identifier.
Value:	1-4294967294.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi neighbor pw-id.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-id 222
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor pw-load-balance

Description

Specifies mechanisms to load-balance the traffic over the Virtual Private LAN Services(VPLS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **pw-load-balance**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.
Value: N/A
Default Value: N/A

neighbor *id*

Description: Specifies the VPLS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

pw-load-balance

Description: Specifies the VPLS load-balance mechanisms.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a load-balance mechanism over VPLS traffic.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
```

```
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-load-balance
(config-pw-load-balance)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor pw-load-balance flow-label

Description

Specifies the Flow-Aware Transport(FAT) that provides the capability to identify individual flows within a VPLS. This provides the routers the ability to use these flows to load-balance traffic.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **pw-load-balance flow-label** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description:	Specifies the VPLS neighbor identifier expressed in IPv4 address format.
Value:	a.b.c.d.
Default Value:	N/A

pw-load-balance

Description:	Specifies the VPLS load-balance mechanisms.
Value:	N/A
Default Value:	N/A

flow-label *value*

Description:	Specifies the VPLS Flow-Aware Transport.
Value:	both receive transmit.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the VPLS Flow-Aware Transport.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-load-balance
(config-pw-load-balance)# flow-label both
(config-pw-load-balance)# commit
```

Impacts and precautions

Make sure that both edges on the VPN have a consistently FAT configuration.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor pw-mtu

Description

Specifies the explicitly signalization of the Maximum Transmission Unit(MTU) on the Virtual Private LAN Services(VPLS) neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **pw-mtu** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description: Specifies the VPLS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

pw-mtu *value*

Description: Specifies the VPLS neighbor signalization MTU.

Value: 64 - 9198.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi neighbor pw-mtu value that explicitly specifies the MTU value used on the VPLS neighbor signalization.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-mtu 64
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

The pw-mtu configuration is used by the signalization process, signaling purpose only. For packet dropping, check the access interface MTU.

When the pw-mtu is not explicitly configured by this command the MTU value signaled by this VPLS is the same as the access interface MTU value.

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor split-horizon

Description

Control the pseudowire (PW) split-horizon group to prevents/allows packets received from a PW from being forwarded into another PW. This technique is important for creating loop-free paths in a full-meshed network.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **split-horizon** *command*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.

Value: String - maximum 32 characters.

Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.

Value: N/A

Default Value: N/A

neighbor *id*

Description: Specifies the VPLS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

split-horizon *command*

Description: Control the VPLS pseudowire split-horizon group.

Value: enable | disable.

Default Value: enable.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi neighbor split-horizon.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vfi)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# split-horizon disable
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi neighbor tunnel-interface

Description

Specifies the MPLS Traffic Engineering (TE) Tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi neighbor** *id* **tunnel-interface** *interface*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.
Value: N/A
Default Value: N/A

neighbor *id*

Description: Specifies the VPLS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

tunnel-interface *interface-name*

Description: Specifies the (TE) Traffic Engineering tunnel interface.

Value: tunnel-te-<tunnel ID>.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure vpn tunnel interface.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
```

```
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# vfi
(config-vpn-Seattle)# neighbor 40.40.40.40
(config-neighbor-40.40.40.40)# tunnel-interface tunnel-te-1000
(config-neighbor-40.40.40.40)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpls-group vpn vfi pw-type

Description

Specifies the Virtual Forwarding Instance (VFI) encapsulation mode.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpls-group *text* **vpn** *text* **vfi** **pw-type** *type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpls-group *text*

Description: A textual string to represent a VPLS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPLS entity.
Value: String - maximum 32 characters.
Default Value: N/A

vfi

Description: A Virtual Forwarding Instance representation.
Value: N/A
Default Value: N/A

pw-type *type*

Description: Specifies the VPLS VFI pseudo-wire encapsulation type.
Value: ethernet | vlan | vlan id.

Default Value: ethernet.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn vfi pw-type ethernet. In this mode, all Ethernet frames received on the attachment circuit will be transmitted on a single PW. This service corresponds to PW type 0x0005 “Ethernet”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# pw-type ethernet
(config-vpn-Seattle)# commit
```

This example shows how to configure the vpn vfi pw-type vlan. This mode uses access dot1q id as a service-delimiting tag to map input Ethernet frames to respective PWs and

corresponds to PW type 0x0004 “Ethernet Tagged Mode”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# pw-type vlan
(config-vpn-Seattle)# commit
```

This example shows how to configure the vpn neighbor pw-type vlan with a explicit VLAN Id. This mode uses a explicit service-delimiting tag to map input Ethernet frames to respective PWs and corresponds to PW type 0x0004 “Ethernet Tagged Mode”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpls-group Washington
(config-vpls-group-Washington)# vpn Seattle
(config-vpn-Seattle)# pw-type vlan 22
(config-vpn-Seattle)# commit
```

Impacts and precautions

The pw-type must be selected in such a way that it matches both ends of the VPLS neighbors.

Hardware restrictions

N/A

mpls l2vpn vpws-group

Description

The Group ID field is a textual string arbitrary value that is assigned to a group of pseudo-wire (PW).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

text

Description:	A textual string assigned to a group of pseudo-wire (PW).
Value:	String - maximum 32 characters.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the l2vpn vpws-group.

```
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn

Description

A textual string to uniquely identify a Virtual Private Wire Services (VPWS). A VPWS connection deploys a Layer 2 service over MPLS to build a point-to-point topology connection attaching end customer sites in a VPN.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# commit
```

Impacts and precautions

Service-port cannot be used as VPN uplink.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface

Description

Specifies the access interface for a Virtual Private Wire Services (VPWS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

access-interface *id*

Description: Access interface configuration.
Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
3.0	Support for 40-gigabit Ethernet and LAG was added.
4.8	Support for service-port was added.
4.9	Support for 100-gigabit Ethernet was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn access interface.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
```

```
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

To use a service-port as an access interface, the service-port must be configured without any translate rule and mtu must be set to 2000 or less.

```
# config
(config)#service-port 1 gpon 1/1/1 onu 1 gem 1
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# access-interface service-port-1
(config-access-port-service-port-1)# mtu 2000
(config-access-port-service-port-1)# commit
```

Impacts and precautions

Vlan-mapping rules do not have effect over vpn access ports because the latter takes precedence over the former.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface administrative-status

Description

Configures the desired administrative status on an access interface for a Virtual Private Wire Services (VPWS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

access-interface *id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Access Interface.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.
3.0	Support for 40-gigabit Ethernet and LAG was added.
4.8	Support for service-port was added.
4.9	Support for 100-gigabit Ethernet was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn access-interface administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# administrative-status down
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface dot1q

Description

Enables the Virtual Private Wire Services (VPWS) access interface to match specific 802.1Q VLAN packets (VLAN-based).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *intf-id* **dot1q** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

access-interface *intf-id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

dot1q *id*

Description: Dot1q VLAN Id to be matched on access interface for this VPN.

Value: 1 - 4094

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.
3.0	Support for 40-gigabit Ethernet and LAG was added.
4.8	Support for service-port was added.
4.9	Support for 100-gigabit Ethernet was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further in-

formation.

Example:

To configure a VLAN-based VPWS, perform this task on the provider edge routers:

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# dot1q 23
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface encapsulation dot1q

Description

Configures the encapsulation of multiple customer VLANs (C-VLANs) on a Virtual Private Wire Services (VPWS) access interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *intf-id* **encapsulation dot1q** *values*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

access-interface *intf-id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

encapsulation dot1q *values*

Description: dot1q vlan (C-VLAN) or ranges of dot1q vlans (C-VLANs) to be encapsulated.

Value: 1 - 4094

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.12	This command was introduced.
------	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn access-interface encapsulation dot1q.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
```

```
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# qinq
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation dot1q 5,10-15,20
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface encapsulation untagged

Description

Enable the encapsulation of untagged frames.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *intf-id* **encapsulation untagged**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

access-interface *intf-id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id.

Default Value: N/A

encapsulation untagged

Description: Enable the untagged mode on the encapsulation of customer VLANs (C-VLANs).

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

6.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn access-interface encapsulation untagged.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
```

```
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# qinq
(config-vpn-Seattle-bd)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation untagged
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn access-interface mtu

Description

Specifies the explicit Maximum Transmission Unit(MTU) of the Virtual Private Wire Services(VPWS) access interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **access-interface** *intf-id* **mtu** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

access-interface *intf-id*

Description: Access interface configuration.

Value: gigabit-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | hundred-gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

mtu value

Description: Specifies the explicit MTU used by the VPWS access interface.

Value: 64 - 9198.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.
4.8	Support for service-port was added.
4.9	Support for 100-gigabit Ethernet was added.
5.10	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

To configure an explicit access interface MTU on a VPWS, perform this task on the provider edge routers:

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# mtu 64
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

Make sure to set an appropriate MTU to account for all the encapsulation overhead that will take place on your MPLS backbone to avoid packet drop. When the mtu is not explicitly configured by this command the mtu value set on this VPWS is the same one set on the access interface. For a service-port access interface, mtu must be set to 2000 or less.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn administrative-status

Description

Configures the desired administrative status on a Virtual Private Wire Services (VPWS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the Virtual Private Wire Services (VPWS).
Value: up | down.
Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# administrative-status down
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn backup-neighbor

Description

Virtual Private Wire Services (VPWS) backup neighbor configuration.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **backup-neighbor** *id* [**pw-load-balance flow-label** *value* | **pw-id** *id* | **administrative-status** *status*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

backup-neighbor *id*

Description: Specifies the VPWS backup neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d

Default Value: N/A

pw-load-balance

Description: Specifies mechanisms to load-balance the traffic over the Virtual Private Wire Services (VPWS).

Value: N/A

Default Value: N/A

flow-label *value*

Description: Specifies the Flow-Aware Transport (FAT) that provides the capability to identify individual flows within a VPWS. This provides the routers the ability to use these flows to load-balance traffic.

Value: *both | receive | transmit*

Default Value: None

pw-id *id*

Description: Specifies the VPWS pseudo-wire numerical identifier. This configuration is mandatory for neighbor enabling.

Value: 1-4294967294

Default Value: N/A

administrative-status *status*

Description: Specifies the desired administrative status on a Virtual Private Wire Services (VPWS) backup neighbor.

Value: *up | down*

Default Value: up

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the VPN backup neighbor.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# backup-neighbor 30.30.30.30
(config-backup-neighbor-30.30.30.30)# pw-id 100
(config-backup-neighbor-30.30.30.30)# administrative-status up
(config-backup-neighbor-30.30.30.30)# pw-load-balance flow-label both
(config-pw-load-balance)# commit
```

Impacts and precautions

Both **pw-type** and **pw-mtu** configuration from the main neighbor are shared with the backup neighbor.

Make sure that both edges on the VPN have a consistent FAT configuration.

If the main neighbor is up, it will be the active PW for this VPN. If a failure is detected in the main PW, it will switchover to the backup PW. When failure from the main PW is recovered, there will be a 30 seconds guard-time before restoring the main as the active PW. If a new failure is detected in the main PW within the guard time, it will remain in the backup PW. If a failure is detected in the backup PW while the main PW is up, it will immediately switch back to the main PW.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn description

Description

Specifies a textual string containing information about the VPWS entity.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **description** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

description *text*

Description: A textual string containing information about the VPWS entity.
Value: String - maximum 32 characters
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn description.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# description Text
(config-vpn-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor

Description

Specifies the IPv4 address to uniquely identify a Virtual Private Wire Services (VPWS) neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn neighbor.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor administrative-status

Description

Configures the desired administrative status on a Virtual Private Wire Services (VPWS) neighbor.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

administrative-status *status*

Description:	Activates (up) or deactivates (down) the Virtual Private Wire Services (VPWS) neighbor.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn neighbor administrative-status.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Name
(config-vpws-group-Washington)# vpn Name
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# administrative-status down
(config-neighbor-30.30.30.30)# commit
```


Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor pw-id

Description

Specifies the pseudo-wire (PW) ID, a non-zero identifier that distinguishes between two MPLS peers from the others. To connect two attachment circuits through a PW, you need to associate each one with the same PW ID. This configuration is mandatory for neighbor enabling.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **pw-id** *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

pw-id *id*

Description:	Specifies the VPWS pseudo-wire numerical identifier.
Value:	1-4294967294.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn neighbor pw-id.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-id 222
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor pw-load-balance

Description

Specifies mechanisms to load-balance the traffic over the Virtual Private Wire Services(VPWS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **pw-load-balance**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.
Value: a.b.c.d.
Default Value: N/A

pw-load-balance

Description: Specifies the VPWS load-balance mechanisms.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a load-balance mechanism over VPWS traffic.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-load-balance
(config-pw-load-balance)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor pw-load-balance flow-label

Description

Specifies the Flow-Aware Transport(FAT) that provides the capability to identify individual flows within a VPWS. This provides the routers the ability to use these flows to load-balance traffic.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **pw-load-balance flow-label** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

pw-load-balance

Description: Specifies the VPWS load-balance mechanisms.

Value: N/A

Default Value: N/A

flow-label *value*

Description: Specifies the VPWS Flow-Aware Transport.

Value: both | receive | transmit.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the VPWS Flow-Aware Transport.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-load-balance
(config-pw-load-balance)# flow-label both
(config-pw-load-balance)# commit
```

Impacts and precautions

Make sure that both edges on the VPN have a consistently FAT configuration.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor pw-mtu

Description

Specifies the explicitly signalization of the Maximum Transmission Unit(MTU) on the Virtual Private Wire Services(VPWS).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **pw-mtu** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.

Value: a.b.c.d.

Default Value: N/A

pw-mtu *value*

Description:	Specifies the VPWS signalization MTU.
Value:	64 - 9198.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn neighbor pw-mtu value that explicitly specifies the MTU value used on the VPWS signalization.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-mtu 64
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

Make sure to set an appropriate MTU to account for all the encapsulation overhead that will take place on your MPLS backbone to avoid packet drop. When the pw mtu is not explicitly configured by this command the mtu value signaled by this VPWS is the same as the access interface mtu value.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor pw-type

Description

Specifies the Virtual Private Wire Services(VPWS) encapsulation mode.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **pw-type** *type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.
Value: a.b.c.d.
Default Value: N/A

pw-type *type*

Description: Specifies the VPWS neighbor pseudo-wire encapsulation type.

Value: ethernet | vlan | vlan id.
Default Value: ethernet.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the vpn neighbor pw-type ethernet. In this mode, all Ethernet frames received on the attachment circuit will be transmitted on a single PW. This service corresponds to PW type 0x0005 “Ethernet”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-type ethernet
(config-neighbor-30.30.30.30)# commit
```

This example shows how to configure the vpn neighbor pw-type vlan. This mode uses access dot1q id as a service-delimiting tag to map input Ethernet frames to respective PWs and corresponds to PW type 0x0004 “Ethernet Tagged Mode”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-type vlan
(config-neighbor-30.30.30.30)# commit
```

This example shows how to configure the vpn neighbor pw-type vlan with a explicit VLAN Id. This mode uses a explicit service-delimiting tag to map input Ethernet frames to respective PWs and corresponds to PW type 0x0004 “Ethernet Tagged Mode”.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 30.30.30.30
(config-neighbor-30.30.30.30)# pw-type vlan 22
(config-neighbor-30.30.30.30)# commit
```

Impacts and precautions

The pw-type must be selected in such a way that it matches both ends of the VPWS.

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn neighbor tunnel-interface

Description

Specifies the MPLS Traffic Engineering (TE) Tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **neighbor** *id* **tunnel-interface** *interface*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.
Value: String - maximum 32 characters.
Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.
Value: String - maximum 32 characters.
Default Value: N/A

neighbor *id*

Description: Specifies the VPWS neighbor identifier expressed in IPv4 address format.
Value: a.b.c.d.
Default Value: N/A

tunnel-interface *interface-name*

Description: Specifies the (TE) Traffic Engineering tunnel interface.

Value: tunnel-te-<tunnel ID>.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure vpn tunnel interface.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# neighbor 40.40.40.40
(config-neighbor-40.40.40.40)# tunnel-interface tunnel-te-1000
(config-neighbor-40.40.40.40)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls l2vpn vpws-group vpn qinq

Description

Enable Selective Encapsulation QinQ mode for VPWS. This mode allows the configuration of multiple VLANs in the **access-interface encapsulation** command in order to set up a Selective Encapsulation VPN. This mode requires the **neighbor pw-type** to be **vlan** and contain the service-delimiting VLAN which will be stacked up top into the frame along with the ingressed access VLANs.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls l2vpn vpws-group *text* **vpn** *text* **qinq**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls l2vpn vpws-group *text*

Description: A textual string to represent a VPWS group.

Value: String - maximum 32 characters.

Default Value: N/A

vpn *text*

Description: A textual string to represent a VPWS entity.

Value: String - maximum 32 characters.

Default Value: N/A

qinq

Description: Enable Selective Encapsulation QinQ mode for VPWS.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.12	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a Selective Encapsulation VPN QinQ mode.

```
# config
(config)# mpls l2vpn
(config-l2vpn)# vpws-group Washington
(config-vpws-group-Washington)# vpn Seattle
(config-vpn-Seattle)# qinq
(config-vpn-Seattle)# access-interface gigabit-ethernet-1/1/1
(config-access-port-gigabit-ethernet-1/1/1)# encapsulation dot1q 5,10-15,20
(config-access-port-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls l2vpn counters

Description

Displays the L2VPN counters values since the last clear mpls l2vpn counters command.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls l2vpn counters [ vpws-group name | vpls-group name ] [ vpn-name name ] [ access-interface name ]
```

Parameters

vpws-group *name*

Description: Use Group name to filter the Virtual Private Wire Services (VPWS) groups.

Value: group name

Default Value: N/A

vpls-group *name*

Description: Use Group name to filter the Virtual Private LAN Services (VPLS) groups.

Value: group name

Default Value: N/A

vpn-name *name*

Description: Use VPN name to filter the output.

Value: vpn name

Default Value: N/A

access-interface *name*

Description: Use access interface name to filter the output.

Value: access interface name

Default Value: N/A

Output Terms

Output	Description
VPWS-Group	Display the VPWS group name associated with entry.
VPLS-Group	Display the VPLS group name associated with entry.
VPN-Name	Display the VPN name associated with entry.
State	Display the MPLS VPN status associated with entry. <ul style="list-style-type: none"> • created: indicates entry is created in hardware. • pending: indicates entry has installation pending. • failed: indicates a failed installation in hardware.
Segment-1	Display the access interface id associated with entry.
State	Display the MPLS access status associated with entry. <ul style="list-style-type: none"> • created: indicates entry is created in hardware. • pending: indicates entry has installation pending. • failed: indicates a failed installation in hardware.
Received	Display the number of packets received in the L2VPN access interface.
Sent	Display the number of packets sent by the L2VPN access interface.
Segment-2	Display the neighbor id associated with entry.
Pw-ID	Display the PW id associated with entry.

Output	Description
Received	Display the number of packets received in the L2VPN uplink interface.
Sent	Display the number of packets sent by the L2VPN uplink interface.
State	Display the MPLS uplink status associated with entry. <ul style="list-style-type: none">• created: indicates entry is created in hardware.• pending: indicates entry has installation pending due neighbor resolution.• failed: indicates a failed installation in hardware.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	The VPWS filter was introduced.
5.6	The access-interface filter was introduced for vpls.

Usage Guidelines

To displays the L2VPN counters values since the last `clear mpls l2vpn counters` command the following command can be used:

Example:

It is possible to filter the results by VPWS Group and VPN Name.

```
# show mpls l2vpn counters vpws-group California vpn-name LA
VPLS-Group: California, VPN-Name: LA, State: created
Segment-1: gigabit-ethernet-1/1/3, State: created
Statistics:
  Packets: Received: 42, Sent: 42
Segment-2: 20.20.20.20, Pw-ID: 3, State: created
Statistics:
  Packets: Received: 42, Sent: 42
```

Also, for VPLS vpns it is possible to filter the results by access interface.

```
# show mpls l2vpn counters vpls-group Texas vpn-name Houston access-interface service-port-1
VPLS-Group: Texas, VPN-Name: Houston, State: created
Segment-1: bridge-domain, Status: up
  service-port-1, State: created
Statistics:
  Packets: Received: 42, Sent: 42
Segment-2: Virtual Forwarding Instance, Status: up
  200.200.200.2, Pw-ID: 101, State: created
Statistics:
  Packets: Received: 42, Sent: 42

# show mpls l2vpn counters vpls-group Texas vpn-name Houston access-interface gigabit-ethernet-1/1/5
VPLS-Group: Texas, VPN-Name: Houston, State: created
Segment-1: bridge-domain, Status: up
  gigabit-ethernet-1/1/5, State: created
Statistics:
  Packets: Received: 42, Sent: 42
Segment-2: Virtual Forwarding Instance, Status: up
  200.200.200.2, Pw-ID: 101, State: created
Statistics:
  Packets: Received: 42, Sent: 42
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls l2vpn hardware

Description

Show list of L2VPN entries installed on data plane.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls l2vpn hardware [ vpws-group name | vpn-name name | vpn-state state | seg1-id gigabit/ten-gigabit-ethernet | seg1-state state | seg2-id ipv4-prefix | local-label label | remote-label label | seg2-state state | pw-id id | pw-type type ]
```

Parameters

vpws-group *name*

Description: Use Group name to filter the output.

Value: group name

Default Value: N/A

vpn-name *name*

Description: Use VPN name to filter the output.

Value: vpn name

Default Value: N/A

vpn-state *state*

Description: Use VPN state to filter the output.

Value: created | pending | failed

Default Value: N/A

seg1-id *gigabit-ethernet*

Description: Use Segment 1 ID to filter the output.

Value: gigabit/ten-gigabit-ethernet

Default Value: N/A

seg1-state *state*

Description: Use Segment 1 State to filter the output.

Value: created | pending | failed

Default Value: N/A

seg2-id *ipv4-prefix*

Description: Use Segment 2 ID to filter the output.

Value: a.b.c.d

Default Value: N/A

local-label *label*

Description: Use Segment 2 Local Label to filter the output.

Value: local label

Default Value: N/A

remote-label *label*

Description: Use Segment 2 Remote Label to filter the output.

Value: remote label

Default Value: N/A

seg2-state *state*

Description: Use Segment 2 State to filter the output.

Value: created | pending | failed

Default Value: N/A

pw-id *id*

Description: Use PW ID to filter the output.

Value: pw id

Default Value: N/A

pw-type *type*

Description: Use PW type to filter the output.

Value: ethernet | vlan | vlan XXX

Default Value: N/A

Output Terms

Output	Description
VPWS-Group	Display the VPWS group name associated with entry.
VPN-Name	Display the VPN name associated with entry.
State	Display the MPLS VPN status associated with entry. <ul style="list-style-type: none"> • created: indicates entry is created in hardware. • pending: indicates entry has installation pending. • failed: indicates a failed installation in hardware.
Segment-1	Display the access interface id associated with entry.
State	Display the MPLS access status associated with entry. <ul style="list-style-type: none"> • created: indicates entry is created in hardware. • pending: indicates entry has installation pending. • failed: indicates a failed installation in hardware.
Segment-2	Display the neighbor id associated with entry.
Pw-ID	Display the PW id associated with entry.
Pw-Type	Display the PW type associated with entry.
Local Label	Display the local label associated with entry.
Remote Label	Display the remote label associated with entry.

Output	Description
State	<p>Display the MPLS uplink status associated with entry.</p> <ul style="list-style-type: none">• created: indicates entry is created in hardware.• pending: indicates entry has installation pending due neighbor resolution.• failed: indicates a failed installation in hardware.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.
2.4	Added new pw-type parameter.

Usage Guidelines

To simply show the list of MPLS L2VPN installed on data plane the following command can be used:

Example:

```
# show mpls l2vpn hardware
```

It is possible to filter the results by VPWS Group, VPN Name, VPN State, Segment-1 Id, Access State, Segment-2 Id, Pw-ID, Local Label, Remote Label and Neighbor State.

Filter by VPWS Group:

Example:

```
# show mpls l2vpn hardware vpws-group NAME
```

Filter by VPN Name:

Example:

```
# show mpls l2vpn hardware vpn-name NAME
```

Filter by VPN State:

Example:

```
# show mpls l2vpn hardware vpn-state created
```

Filter by Segment-1 Id:

Example:

```
# show mpls l2vpn hardware seg1-id gigabit-ethernet-1/1.1/1
```

Filter by Access State:

Example:

```
# show mpls l2vpn hardware seg1-state created
```

Filter by Segment-2 Id:

Example:

```
# show mpls l2vpn hardware seg2-id 2.2.2.2
```

Filter by Pw-ID:

Example:

```
# show mpls l2vpn hardware pw-id 55
```

Filter by Pw-Type:

Example:

```
# show mpls l2vpn hardware pw-type vlan 100
```

Filter by Local Label:

Example:

```
# show mpls l2vpn hardware local-label 11
```

Filter by Remote Label:

Example:

```
# show mpls l2vpn hardware remote-label 12
```

Filter by Neighbor State:

Example:

```
# show mpls l2vpn hardware seg2-state created
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls l2vpn vpls-group

Description

Shows list of L2VPN (VPLS) entries present on control plane.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls l2vpn vpls-group [ brief | detail ] [ vpls-group name | vpn-name name ]
```

Parameters

brief

Description: Shows resumed information about the L2VPN (VPLS) control plane.

Value: N/A

Default Value: N/A

detail

Description: Shows detailed information about the L2VPN (VPLS) control plane.

Value: N/A

Default Value: N/A

vpls-group *name*

Description: Uses Group name to filter the output.

Value: group name

Default Value: N/A

vpn-name *name*

Description: Uses VPN name to filter the output.

Value: vpn name

Default Value: N/A

Output Terms

Output	Description
Pw-ID	Displays the PW id associated with that entry.
Segment-1	Displays the access interface id associated with that entry.
Segment-2	Displays the neighbor id associated with that entry.
Segment-1 State	<p>Displays the MPLS access interface status associated with that entry.</p> <ul style="list-style-type: none"> up: The interface is ready to pass packets. down: The interface is admin down and deprogrammed.
Segment-2 State	<p>Displays the MPLS pseudowire status associated with that entry.</p> <ul style="list-style-type: none"> up: The PW is ready to pass packets. down: The PW is admin down and deprogrammed. dormant: The PW is not in a condition to pass packets. It is waiting for signaling to complete. lowerLayerDown: One or more of the lower-layer interfaces is not in OperStatus 'up' state. failed: The PW is admin up but has failed to go operationally Up. It is not ready to pass packets because of a local or remote failure.
Status	Displays the MPLS VPN status associated with that entry.
Transparent-LAN-Service	Displays the VPLS bridge-domain TLS mode i.e. disabled or enabled.
Bridge-MTU	Displays the VPLS bridge-domain MTU.

Output	Description
Dot1q	Displays the VPLS bridge-domain Dot1q VLAN Id that is set for the VPN's bridge-domain.
Encapsulation Dot1q	Displays the set of C-VLANs that are encapsulated on the VPLS access interface.
Last state change time	Displays the last time that PW operational state has changed.
MAC Learning	Displays the MAC Learning status. It is always enabled.
MAC aging time	Displays the MAC aging time. This parameter is configured globally, see mac-address-table aging-time command configuration for more details.
MAC Limit	Displays the VPN MAC limit. It can be configured.
MPLS VC labels	Displays the exchanged labels information for VPLS service.
Pw-type	Displays the VFI pseudowire encapsulation type.
Remote access interface state	Displays the neighbor access interface operational state.
Split-horizon	Displays the split-horizon forwarding mode.
Tunnel interface	Displays the tunnel interface name.
Up Time	Displays the total time that the PW has been Up and running.
VPLS-Group	Displays the VPLS group name associated with that entry.

Output	Description
VPN-Name	Displays the VPN name associated with that entry.
Flow-label receive	<p>Displays the Flow-Aware Transport(FAT) status for received flows.</p> <ul style="list-style-type: none"> • true: The local configuration has flow label reception capability enabled and the remote configuration has the flow label transmission capability enabled. • false: The local configuration doesn't have flow label reception capability enabled or the remote configuration doesn't have the flow label transmission capability enabled.
Flow-label transmit	<p>Displays the Flow-Aware Transport(FAT) status for transmitted flows.</p> <ul style="list-style-type: none"> • true: The local configuration has flow label transmission capability enabled and the remote configuration has the flow label reception capability enabled. • false: The local configuration doesn't have flow label transmission capability enabled or the remote configuration doesn't have the flow label reception capability enabled.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To simply show the list of MPLS L2VPN present on control plane the following command can be used:

Example:

```
# show mpls l2vpn vpls-group brief
```

VPLS-Group	VPN-Name	Status	Segment-1	State	Segment-2	Pw-ID	Sta
California	LA	up	gigabit-ethernet-1/1/19.1000	up	-	-	-
			ten-gigabit-ethernet-1/1/1.1000	up	-	-	-
			ten-gigabit-ethernet-1/1/2.1000	up	-	-	-
			-	-	200.200.2.2	147852	up
			-	-	200.200.2.3	1478524	up
	SD	down	-	-	200.200.2.45	14785256	dor
			gigabit-ethernet-1/1/12	down	-	-	-
			-	-	200.200.200.2	1234	dow
	SF	up	-	-	200.200.200.3	1234567989	fai
			ten-gigabit-ethernet-1/1/1.1519	up	-	-	-
			ten-gigabit-ethernet-1/1/2.1519	up	-	-	-
			ten-gigabit-ethernet-1/1/3.1519	up	-	-	-
	SJ	up	ten-gigabit-ethernet-1/1/4.1519	up	-	-	-
			-	-	200.200.200.2	19664	dor
			-	-	200.200.200.2	987652412	up
			-	-	200.200.200.22	987652412	up
Illinois	Chicago	up	-	-	200.200.200.221	987652412	low
			gigabit-ethernet-1/1/20	down	-	-	-
			gigabit-ethernet-1/1/22	up	-	-	-
			gigabit-ethernet-1/1/23	up	-	-	-
			gigabit-ethernet-1/1/24	up	-	-	-
			-	-	200.200.20.20	20	up
			-	-	200.200.200.123	123	up

It is possible to filter the results by VPLS Group or VPN Name.

Filter by VPLS Group:

Example:

```
# show mpls l2vpn vpls-group brief vpls-group Illinois
```

VPLS-Group	VPN-Name	Status	Segment-1	State	Segment-2	Pw-ID	Sta
Illinois	Chicago	up	gigabit-ethernet-1/1/20	up	-	-	-
			gigabit-ethernet-1/1/22	up	-	-	-
			gigabit-ethernet-1/1/23	up	-	-	-
			gigabit-ethernet-1/1/24	up	-	-	-
			-	-	200.200.20.20	20	dow
			-	-	200.200.200.123	123	dow

To simply show the detailed list of MPLS L2VPN present on control plane the following command can be used:

It is possible to filter the results by VPLS Group or VPN Name.

Example:

```
# show mpls l2vpn vpls-group detail
VPLS-Group: Texas; VPN-Name: Dallas; Admin status: up;

Bridge-Domain: Admin status: up; Oper state: up;

  MAC learning: enabled
  MAC aging time: 339 s, Type: inactivity
  MAC limit: 1024, Action: drop

  Transparent-LAN-Service: enabled
  Bridge-MTU: 4000
  Dot1q: 72

AC:  forty-gigabit-ethernet-1/1/1.72; Admin status: up; Oper state: up;
    MTU: 4000;
    Encapsulation Dot1q: 150-300,untagged;
AC:  forty-gigabit-ethernet-1/1/2.72; Admin status: up; Oper state: up;
    MTU: 4000;
    Encapsulation Dot1q: 10,50-100,120;
AC:  forty-gigabit-ethernet-1/1/3.72; Admin status: up; Oper state: up;
    MTU: 4000;
    Encapsulation Dot1q: untagged;
AC:  lag-1.72; Admin status: up; Oper state: up;
    Encapsulation Dot1q: 15,20,30;
    MTU: 4000;

VFI: Admin status: up; Oper state: up;
  Pw-type: vlan 71;
  Signalling protocol: ldp;

PW:  Neighbor address: 200.200.200.3; Admin status: up; Oper state: up;
    Up time:  0 days 0 hours 0 minutes 24 seconds;
    Last state change time: Wed Sep 12 13:13:44 2018;
    Pw-ID: 72; Pw-MTU: 4000; Tunnel interface: tunnel-te-100;
    FAT: Flow-label receive: true; Flow-label transmit: false;
    Split-horizon: enabled;
    Remote access interface state: up;
    MPLS VC labels: Local: 27; Remote: 17;
    MTU: Local: 4000; Remote: 4000;

PW:  Neighbor address: 200.200.200.4; Admin status: up; Oper state: up;
    Up time:  0 days 0 hours 0 minutes 24 seconds;
    Last state change time: Wed Sep 12 13:13:44 2018;
    Pw-ID: 71; Pw-MTU: 4000; Tunnel interface: tunnel-te-200;
    FAT: Flow-label receive: true; Flow-label transmit: false;
    Split-horizon: enabled;
    Remote access interface state: up;
    MPLS VC labels: Local: 34; Remote: 17;
    MTU: Local: 4000; Remote: 4000;

VPLS-Group: Texas; VPN-Name: Houston; Admin status: up;

Bridge-Domain: Admin status: up; Oper state: down;

  MAC learning: enabled
  MAC aging time: 339 s, Type: inactivity
  MAC limit: 1024, Action: drop

  Bridge-MTU: 1555
```

```
Dot1q: 92
AC: forty-gigabit-ethernet-1/1/1.92; Admin status: down; Oper state: down;
    MTU: 1555;
AC: forty-gigabit-ethernet-1/1/2.92; Admin status: up; Oper state: up;
    MTU: 1555;
AC: lag-1.92; Admin status: up; Oper state: up;
    MTU: 1555;

VFI: Admin status: up; Oper state: up;
    Pw-type: vlan 4000;
    Signalling protocol: ldp;

PW: Neighbor address: 200.200.200.2; Admin status: up; Oper state: up;
    Up time: 0 days 0 hours 0 minutes 24 seconds;
    Last state change time: Wed Sep 12 13:13:44 2018;
    Pw-ID: 92; Pw-MTU: 1555; Tunnel interface: ldp;
    FAT: Flow-label receive: true; Flow-label transmit: false;
    Split-horizon: enabled;
    Remote access interface state: up;
    MPLS VC labels: Local: 18; Remote: 18;
    MTU: Local: 1555; Remote: 1555;

PW: Neighbor address: 200.200.200.4; Admin status: up; Oper state: up;
    Up time: 0 days 0 hours 0 minutes 24 seconds;
    Last state change time: Wed Sep 12 13:13:44 2018;
    Pw-ID: 91; Pw-MTU: 1999; Tunnel interface: ldp;
    FAT: Flow-label receive: false; Flow-label transmit: true;
    Split-horizon: enabled;
    Remote access interface state: up;
    MPLS VC labels: Local: 33; Remote: 16;
    MTU: Local: 1999; Remote: 1999;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls l2vpn vpws-group

Description

Shows list of L2VPN entries present on control plane.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls l2vpn vpws-group [ group-name | vpn-name name | group-name vpn-name name ] [ brief | detail ]
```

Parameters

brief

Description: Shows resumed information about the L2VPN control plane.

Value: N/A

Default Value: N/A

group-name

Description: Uses Group name to filter the output.

Value: group name

Default Value: N/A

vpn-name *name*

Description: Uses VPN name to filter the output.

Value: vpn name

Default Value: N/A

detail

Description: Shows detailed information about the L2VPN control plane.

Value: N/A

Default Value: N/A

*group-name***Description:** Uses Group name to filter the output.**Value:** group name**Default Value:** N/A**vpn-name** *name***Description:** Uses VPN name to filter the output.**Value:** vpn name**Default Value:** N/A**Output Terms**

Output	Description
VPWS-Group	Display the VPWS group name associated with entry.
VPN-Name	Display the VPN name associated with entry.
Oper State	Display the MPLS VPN status associated with entry.
Segment-1	Display the access interface id associated with entry.
Oper State	Display the MPLS access status associated with entry. <ul style="list-style-type: none"> • up: The interface is ready to pass packets. • down: The interface is admin down and deprogrammed.
Segment-2	Display the neighbor id associated with entry.
Pw-ID	Display the PW id associated with entry.

Output	Description
	<p>Display the MPLS uplink status associated with entry.</p> <ul style="list-style-type: none"> • up: The PW is ready to pass packets. • down: The PW is admin down and deprogrammed. • dormant: The PW is not in a condition to pass packets. It is waiting for signaling to complete.
Oper State	<ul style="list-style-type: none"> • lowerLayerDown: One or more of the lower-layer interfaces is not in OperStatus 'up' state. • failed: The PW is admin up but has failed to go operationally Up. It is not ready to pass packets because of a local or remote failure.
	<p>Display the Role associated with entry. Empty if the PW does not have backup neighbor configured.</p> <ul style="list-style-type: none"> • main: The PW is the main neighbor associated with entry. • backup: The PW is the backup neighbor associated with entry.
Redundancy Role	
	<p>Display the status associated with entry. Empty if the PW does not have backup neighbor configured.</p> <ul style="list-style-type: none"> • active: The PW is active and ready to pass packets. • standby: The PW is standby and could be ready to pass packets if the other neighbor is down.
Redundancy State	

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.
6.0	Backup PW state was introduced. Update show brief to display the VPN operational state instead of administrative status.

Usage Guidelines

To simply show the list of MPLS L2VPN present on control plane the following command can be used:

Example:

```
# show mpls l2vpn vpws-group brief
```

VPWS-Group	VPN-Name	Oper State	Segment-1	Oper State	Segment-2	Pw-ID	Oper State	Redundancy Role	Redundancy State
California	Eureka	up	gigabit-ethernet-1/1/1	up	172.0.10.120	12503	up	main	active
					172.0.10.150	22500	up	backup	standby
Illinois	Fresno	up	gigabit-ethernet-1/1/2	up	172.0.10.160	99222	up	-	-
	Chicago	up	gigabit-ethernet-1/1/3	up	172.0.10.177	12123	up	-	-

It is possible to filter the results by VPWS Group and VPN Name.

Filter by VPWS Group:

Example:

```
# show mpls l2vpn vpws-group Illinois brief
VPWS-Group: Illinois;
```

VPN-Name	Oper State	Segment-1	Oper State	Segment-2	Pw-ID	Oper State	Redundancy Role	Redundancy State
Fresno	up	gigabit-ethernet-1/1/2	up	172.0.10.160	99222	up	-	-
Chicago	up	gigabit-ethernet-1/1/3	up	172.0.10.177	12123	up	-	-

Filter by VPWS Group and VPN Name:

Example:

```
# show mpls l2vpn vpws-group Illinois vpn-name Chicago brief
  VPN-Name: Chicago; Oper state: up;

  AC: gigabit-ethernet-1/1/3; Oper state: up;

  PW: Neighbor address: 172.0.10.177; Oper state: up;
      Pw-ID: 12123; Redundancy: Role: n/a; Local state: n/a
```

To simply show the detailed list of MPLS L2VPN present on control plane the following command can be used:

Example:

```
# show mpls l2vpn vpws-group detail
VPWS-Group: California;

  VPN-Name: Eureka; Admin Status: up; Oper state: up;

    AC: gigabit-ethernet-1/1/1; Admin Status: up; Oper state: up;
        Encapsulation Dot1q: 10,20,30-50

    PW: Neighbor address: 172.0.10.120; Admin Status: up; Oper state: up;
        Up time: 0 day(s) 0 hour(s) 1 minute(s) 30 second(s);
        Last state change time: Thu Sep 21 15:24:17 2017;
        Pw-ID: 12503; Pw-type: vlan 2017; Tunnel interface: ldp;
        FAT: Flow-label receive: true; Flow-label transmit: false;
        Remote access interface state: up;
        MPLS VC labels: Local: 37; Remote: 57;
        MTU: Local: 1500; Remote: 1500;
        Signaling protocol: ldp;
        Redundancy: Role: main; Local active: none; Remote state: active;

    PW: Neighbor address: 172.0.10.150; Admin Status: up; Oper state: dormant;
        Up time: 0 day(s) 0 hour(s) 0 minute(s) 0 second(s);
        Last state change time: Thu Sep 21 15:24:17 2017;
        Pw-ID: 22500; Pw-type: vlan 2017; Tunnel interface: ldp;
        FAT: Flow-label receive: true; Flow-label transmit: false;
        Remote access interface state: up;
        MPLS VC labels: Local: 14; Remote: 18;
        MTU: Local: 1500; Remote: 1500;
        Signaling protocol: ldp;
        Redundancy: Role: backup; Local state: standby; Remote state: active;

  VPN-Name: Fresno; Admin Status: up; Oper state: up;

    AC: gigabit-ethernet-1/1/2; Admin Status: up; Oper state: up;
        Encapsulation Dot1q: 10,20,30-50,untagged

    PW: Neighbor address: 172.0.10.160; Admin Status: up; Oper state: up;
        Up time: 0 day(s) 0 hour(s) 1 minute(s) 28 second(s);
        Last state change time: Thu Sep 21 15:24:20 2017;
        Pw-ID: 99222; Pw-type: vlan 2017; Tunnel interface: tunnel-te-200;
        FAT: Flow-label receive: true; Flow-label transmit: false;
        Remote access interface state: up;
        MPLS VC labels: Local: 40; Remote: 60;
        MTU: Local: 1500; Remote: 1500;
        Signaling protocol: ldp;
        Redundancy: Role: n/a; Local state: n/a; Remote state: n/a;

  VPN-Name: Sacramento; Admin Status: up; Oper state: up;

    AC: gigabit-ethernet-1/1/2; Admin Status: up; Oper state: up;
        Encapsulation Dot1q: none

    PW: Neighbor address: 172.0.10.160; Admin Status: up; Oper state: up;
        Up time: 0 day(s) 0 hour(s) 2 minute(s) 38 second(s);
        Last state change time: Thu Sep 21 15:24:20 2017;
        Pw-ID: 3314; Pw-type: vlan 2017; Tunnel interface: tunnel-te-300;
        FAT: Flow-label receive: true; Flow-label transmit: false;
        Remote access interface state: up;
```

```

MPLS VC labels: Local: 40; Remote: 60;
MTU: Local: 1500; Remote: 1500;
Signaling protocol: ldp;
Redundancy: Role: n/a; Local state: n/a; Remote state: n/a;

VPWS-Group: Illinois;

VPN-Name: Chicago; Admin Status: up; Oper state: up;

AC: gigabit-ethernet-1/1/3; Admin Status: up; Oper state: up;
Encapsulation Dot1q: untagged

PW: Neighbor address: 172.0.10.177; Admin Status: up; Oper state: up;
Up time: 0 day(s) 0 hour(s) 1 minute(s) 15 second(s);
Last state change time: Thu Sep 21 15:24:18 2017;
Pw-ID: 12123; Pw-type: vlan 2017; Tunnel interface: ldp;
FAT: Flow-label receive: true; Flow-label transmit: false;
Remote access interface state: up;
MPLS VC labels: Local: 22; Remote: 21;
MTU: Local: 1500; Remote: 1500;
Signaling protocol: ldp;
Redundancy: Role: n/a; Local state: n/a; Remote state: n/a;

```

It is possible to filter the results by VPWS Group and VPN Name.

Filter by VPWS Group:

Example:

```

# show mpls l2vpn vpws-group Illinois detail

VPWS-Group: Illinois;

VPN-Name: Chicago; Admin Status: up; Oper state: up;

AC: gigabit-ethernet-1/1/3; Admin Status: up; Oper state: up;
Encapsulation Dot1q: untagged

PW: Neighbor address: 172.0.10.177; Admin Status: up; Oper state: up;
Up time: 0 day(s) 0 hour(s) 1 minute(s) 15 second(s);
Last state change time: Thu Sep 21 15:24:18 2017;
Pw-ID: 3; Pw-type: vlan 2017; Tunnel interface: ldp;
FAT: Flow-label receive: true; Flow-label transmit: false;
Remote access interface state: up;
MPLS VC labels: Local: 22; Remote: 21;
MTU: Local: 1500; Remote: 1500;
Signaling protocol: ldp;
Redundancy: Role: n/a; Local state: n/a; Remote state: n/a;

```

Filter by VPWS Group and VPN Name:

Example:

```

# show mpls l2vpn vpws-group Illinois vpn-name Chicago

VPN-Name: Chicago; Admin Status: up; Oper state: up;

AC: gigabit-ethernet-1/1/3; Admin Status: up; Oper state: up;
Encapsulation Dot1q: untagged

PW: Neighbor address: 172.0.10.177; Admin Status: up; Oper state: up;
Up time: 0 day(s) 0 hour(s) 1 minute(s) 15 second(s);
Last state change time: Thu Sep 21 15:24:18 2017;
Pw-ID: 3; Pw-type: vlan 2017; Tunnel interface: ldp;
FAT: Flow-label receive: true; Flow-label transmit: false;
Remote access interface state: up;
MPLS VC labels: Local: 22; Remote: 21;
MTU: Local: 1500; Remote: 1500;
Signaling protocol: ldp;

```

Redundancy: Role: n/a; Local state: n/a; Remote state: n/a;

Impacts and precautions

N/A

Hardware restrictions

N/A

L3VPN

show mpls l3vpn

Description

Shows information regarding L3VPN prefixes.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls l3vpn { vpn4 | vpn6 } vrf vrf-name brief
```

Parameters

vrf *vrf-name*

Description: VRF used to filter the output.

Value: Name of VRF or all VRFs.

Default Value: N/A

Output Terms

Output	Description
VRF-name	Display the VRF in which the L3VPN entry exists.
Prefix	Display the prefix associated with the L3VPN entry.
Next-hop	Display the next-hop associated with the L3VPN entry.

Output	Description
Action	<p>Display the MPLS action performed on data plane by the L3VPN entry.</p> <ul style="list-style-type: none"> • none: no action associated with entry. • psh: tunnel incoming traffic by pushing the outgoing label to the packets. • pop: remove incoming label to forward the packet.
In Label	Display the incoming label associated with the L3VPN entry.
Out Label	Display the outgoing label associated with the L3VPN entry.
Out Interface	Display the outgoing interface for the MPLS traffic associated with the L3VPN entry. The outgoing interface could be an access VRF or the uplink tunnel.
Status	<p>Display the status of this rule entry.</p> <ul style="list-style-type: none"> • Active: indicates entry is active. • Pending: indicates entry has installation pending due to neighbor resolution. • Unused: indicates entry is not in used to forward traffic.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.6	This command was introduced.
6.0	The <i>vpn6</i> parameter was added.

Usage Guidelines

To simply show MPLS L3VPN information, the following command can be used:

Example:

```
# show mpls l3vpn vpnv4 vrf all brief
```

VRF-name	Prefix	Next-hop	Action	In Label	Out Label	Out Interface	Status
VRF_GREEN	--	--	pop	16	--	VRF_GREEN	active
VRF_GREEN	1.1.1.0/24	200.200.200.2/32	psh	--	17	tunnel-ldp	active
VRF_GREEN	2.1.1.0/24	200.200.200.2/32	psh	--	17	tunnel-ldp	active
VRF_RED	--	--	pop	17	--	VRF_RED	active
VRF_RED	1.1.1.0/24	200.200.200.2/32	psh	--	16	tunnel-ldp	active
VRF_RED	2.1.1.0/24	200.200.200.2/32	psh	--	16	tunnel-ldp	active

```
DM4270# show mpls l3vpn vpnv6 vrf all brief
```

VRF-name	Prefix	Next-hop	Action	In Label	Out Label	Out Interface	Status
VRF_GREEN	2001:1::/64	::ffff:4.4.4.1	psh	--	16	tunnel-ldp	active
VRF_GREEN	2001:2::/64	::ffff:4.4.4.1	psh	--	16	tunnel-ldp	active

It is possible to filter the output by VRF.

Filter by VRF:

Example:

```
# show mpls l3vpn vpnv4 vrf VRF_RED brief
```

Impacts and precautions

N/A

Hardware restrictions

N/A

RSVP

interface tunnel-te

Description

Configure MPLS Traffic Engineering Tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure an MPLS Traffic Engineering Tunnel interface.

```
# config
(config)# interface tunnel-te 1
```

Impacts and precautions

The tunnel interface destination parameter is mandatory.

Hardware restrictions

N/A

interface tunnel-te administrative-status

Description

Configure MPLS Traffic Engineering Tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

administrative-status *status*

Description: Activates (up) or deactivates (down) the tunnel interface.

Value: up | down.

Default Value: up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to set the tunnel interface administrative-status.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# administrative-status up
(config-tunnel-te-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te description

Description

Specifies a textual string containing information about the tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **description** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

description *text*

Description: A textual description of the tunnel interface.

Value: String - maximum 64 characters. Any character is supported.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to add a tunnel interface description.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# description Text
(config-tunnel-te-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te destination

Description

Specifies the IPv4 address destination of the tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **destination** *addr*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

destination *addr*

Description: Tunnel destination IPv4 address.

Value: a.b.c.d.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a tunnel interface destination.

```
# config
(config)# interface tunnel-te 2
(config-tunnel-te-1)# destination 1.1.1.1
(config-tunnel-te-1)# commit
```

Impacts and precautions

The tunnel interface destination address is mandatory.

Hardware restrictions

N/A

interface tunnel-te name

Description

Specifies a textual string to identify the tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **name** *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

name *text*

Description: A textual string to represent a tunnel interface.

Value: String - maximum 32 characters. Characters supported are 'a-z', 'A-Z', '0-9', '_' and '-'.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to add a tunnel interface name.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# name tunnell
(config-tunnel-te-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te path-option

Description

A tunnel interface can have six path options associated with different priorities. The path option with a lower priority value is tried first. If this path is unavailable in the CSPF database, the next path option with lower priority value is tried.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **path-option** *prio*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

path-option *prio*

Description: Priority for the path option.

Value: 1-255.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure a tunnel interface path-option priority.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# path-option 1
(config-tunnel-te-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te path-option

Description

Enable or disable a specific path option.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **path-option** *prio* [*enable* | *disable*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

path-option *prio*

Description: Priority for the path option.

Value: 1-255.

Default Value: N/A

status

Description: Enables or disables the path option.

Value: enable | disable.

Default Value: enable.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to disable and enable a specific tunnel interface path-option.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# path-option 1 disable
(config-tunnel-te-1)# commit
(config-tunnel-te-1)# path-option 1 enable
(config-tunnel-te-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te path-option dynamic attribute-set

Description

Set of attributes that are associated with the dynamic path-option. The CSPF uses these attributes information on the tunnel ingress to determine whether the path can be established for a specific destination or not.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **path-option** *prio* **dynamic attribute-set** *attribute*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

path-option *prio*

Description: Priority for the path option.

Value: 1-255.

Default Value: N/A

dynamic attribute-set *attribute*

Description: Specifies the attributes that are associated with a dynamic path-option. The attribute-set must be created in the mpls traffic-eng configuration.

Value: Any attribute-set created in the mpls traffic-eng configuration.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to associated an attribute-set in a dynamic path-option.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# path-option 1 dynamic attribute-set Set1
(config-tunnel-te-1)# commit
```

It is not possible to configure both dynamic and explicit path within the same path-option, nor the same tunnel interface.

Impacts and precautions

N/A

Hardware restrictions

N/A

interface tunnel-te path-option explicit name

Description

Set of nodes that are associated with the explicit path-option.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

interface tunnel-te *id* **path-option** *prio* **explicit name** *explicit-path*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface tunnel-te *id*

Description: Specifies the identifier of the tunnel interface.

Value: 1-65535.

Default Value: N/A

path-option *prio*

Description: Priority for the path option.

Value: 1-255.

Default Value: N/A

explicit name *explicit-path*

Description: Specifies the path that is associated with an explicit path-option. The explicit-path must be created in the mpls traffic-eng configuration.

Value: Any explicit-path created in the mpls traffic-eng configuration.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

7.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to associated an explicit-path in a path-option.

```
# config
(config)# interface tunnel-te 1
(config-tunnel-te-1)# path-option 1 explicit name Seattle
(config-tunnel-te-1)# commit
```

It is not possible to configure both dynamic and explicit path within the same path-option, nor the same tunnel interface.

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls rsvp

Description

Enable Resource Reservation Protocol (RSVP) that provides traffic management capabilities.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls rsvp

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls rsvp

Description: Enable Resource Reservation Protocol.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the RSVP.

```
# config
(config)# mpls rsvp
(config-rsvp)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls rsvp interface

Description

Enable Resource Reservation Protocol (RSVP) capabilities in a specific interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls rsvp interface *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls rsvp

Description:	Enable Resource Reservation Protocol.
Value:	N/A
Default Value:	N/A

interface *interface-name*

Description:	Enable RSVP capabilities in an L3 interface. The L3 interface must be created.
Value:	any L3 interface.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable RSVP capabilities in an L3 interface.

```
# config
(config)# mpls rsvp
(config-rsvp)# interface l3-vlan1
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng

Description

Enable MPLS traffic engineering that ensures Quality of Service (QoS) for data transmission.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable MPLS traffic engineering.

```
# config
(config)# mpls traffic-eng
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng attribute-set

Description

Set of attributes to be used by MPLS traffic engineering.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng attribute-set

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set

Description: Enable MPLS traffic engineering attributes.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure MPLS traffic engineering attributes.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng attribute-set path-option

Description

Configure an MPLS traffic engineering (MPLS-TE) dynamic path to be associated with a tunnel interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng attribute-set path-option *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set

Description: Enable MPLS traffic engineering attributes.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set path-option *text*

Description: A textual string to represent a path-option.

Value: String - maximum 32 characters. Characters supported are 'a-z', 'A-Z', '0-9', '_' and '-'.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option attribute-set.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# path-option Seattle
(config-path-option-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng attribute-set path-option affinity-flags exclude-any

Description

Affinity flags attribute configured to define a path option. The path will be valid if any link to a destination does not have any affinity-flag bits in the CSPF calculation base.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng attribute-set path-option *text* **affinity-flags exclude-any** *flag*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set

Description: Enable MPLS traffic engineering attributes.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set path-option *text*

Description: A textual string to represent a path-option.

Value: String - maximum 64 characters.

Default Value: N/A

mpls traffic-eng attribute-set path-option *text* **affinity-flags exclude-any** *flag*

Description:	Affinity attribute values to be any excluded.
Value:	Hexadecimal in lower-case - 0x0-0xffffffff
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option attribute-set to exclude any affinity-flag bits.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# path-option Seattle
(config-path-option-Seattle)# affinity-flags exclude-any 0xa
(config-path-option-Seattle)# commit
```

Impacts and precautions

A path can have different affinity statements associated at the same time.

Hardware restrictions

N/A

mpls traffic-eng attribute-set path-option affinity-flags include-all

Description

Affinity flags attribute configured to define a path option. The path will be valid if each link to a destination has the same affinity-flag bits in the CSPF calculation base.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng attribute-set path-option *text* **affinity-flags include-all** *flag*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set

Description: Enable MPLS traffic engineering attributes.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set path-option *text*

Description: A textual string to represent a path-option.

Value: String - maximum 64 characters.

Default Value: N/A

mpls traffic-eng attribute-set path-option *text* **affinity-flags include-all** *flag*

Description:	Affinity attribute values to be all included.
Value:	Hexadecimal in lower-case - 0x0-0xffffffff
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option attribute-set to include all affinity-flag bits.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# path-option Seattle
(config-path-option-Seattle)# affinity-flags include-all 0xa
(config-path-option-Seattle)# commit
```

Impacts and precautions

A path can have different affinity statements associated at the same time.

Hardware restrictions

N/A

mpls traffic-eng attribute-set path-option affinity-flags include-any

Description

Affinity flags attribute configured to define a path option. The path will be valid if all links to a destination have at least one affinity-flag bit in the CSPF calculation base.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng attribute-set path-option *text* **affinity-flags include-any** *flag*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set

Description: Enable MPLS traffic engineering attributes.

Value: N/A

Default Value: N/A

mpls traffic-eng attribute-set path-option *text*

Description: A textual string to represent a path-option.

Value: String - maximum 64 characters.

Default Value: N/A

mpls traffic-eng attribute-set path-option *text* **affinity-flags include-any** *flag*

Description:	Affinity attribute values to be any included.
Value:	Hexadecimal in lower-case - 0x0-0xffffffff
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option attribute-set to include any affinity-flag bits.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# path-option Seattle
(config-path-option-Seattle)# affinity-flags include-any 0xa
(config-path-option-Seattle)# commit
```

Impacts and precautions

A path can have different affinity statements associated at the same time.

Hardware restrictions

N/A

mpls traffic-eng explicit-path

Description

Configure an MPLS traffic engineering (MPLS-TE) explicit path to be associated with a tunnel interface. It consists of a series of nodes through which the MPLS-TE tunnel will be established.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng explicit-path *text*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng explicit-path *text*

Description: A textual string to represent a explicit-path.

Value: String - maximum 48 characters. Characters supported are 'a-z', 'A-Z', '0-9', '_' and '-'.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option explicit-path.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# explicit-path Seattle
(config-explicit-path-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng explicit-path hop

Description

Configure a node in an explicit path with its attributes, including the IP address and hop type.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng explicit-path *text* **hop** *id* **ipv4 next-address** *addr* *hop-type*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

mpls traffic-eng explicit-path *text*

Description: A textual string to represent a explicit-path.

Value: String - maximum 48 characters. Characters supported are 'a-z', 'A-Z', '0-9', '_' and '-'.

Default Value: N/A

mpls traffic-eng explicit-path *text* **hop** *id*

Description: Index of a node on the explicit-path.

Value: 1-65535.

Default Value: N/A

mpls traffic-eng explicit-path *text* **hop** *id* **ipv4 next-address** *addr*

Description: The IPv4 address of a node on the explicit-path. It must be unique in current **explicit-path**.

Value: a.b.c.d.

Default Value: N/A

mpls traffic-eng explicit-path *text* **hop** *id* **ipv4 next-address** *addr* *hop-type*

Description: The connection to a node on the explicit-path. A strict hop is directly connected to its next hop, while for loose hop, other nodes may exist between them.

Value: loose | strict.

Default Value: strict.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

7.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the path option explicit-path to include a series of hops.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# explicit-path Seattle
(config-explicit-path-Seattle)# hop 42 ipv4 next-address 1.2.3.4 strict
(config-explicit-path-Seattle)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng interface

Description

Enable MPLS traffic engineering capabilities in a specific interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng interface *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

interface *interface-name*

Description: Enable MPLS traffic engineering capabilities in a specific L3 interface. The L3 interface must be created.

Value: any L3 interface.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable MPLS traffic engineering capabilities in an L3 interface.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# interface l3-vlan1
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls traffic-eng interface affinity-flags

Description

Enable affinity-flag bits in a specific L3 interface. The IGP advertises the affinity-flag to devices in the same IGP area. Then the CSPF on the ingress uses this information to determine whether a link can be used to establish an RSVP-TE path or not.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250, DM4615, DM4610, DM4611, DM4612.

Syntax

mpls traffic-eng interface *interface-name* **affinity-flags** *flag*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mpls traffic-eng

Description: Enable MPLS traffic engineering.

Value: N/A

Default Value: N/A

interface *interface-name*

Description: Enable MPLS traffic engineering capabilities in a specific L3 interface. The L3 interface must be created.

Value: any L3 interface.

Default Value: N/A

affinity-flags *flag*

Description: Affinity-flag value to be used by a specific L3 interface.

Value: Hexadecimal in lower-case - 0x0-0xffffffff

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable MPLS traffic engineering capabilities in an L3 interface.

```
# config
(config)# mpls traffic-eng
(config-traffic-eng)# attribute-set
(config-attribute-set)# interface l3-vlan1
(config-interface-l3-vlan1)# affinity-flags 0xa
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

LDP

This topic describes the commands related to management of Label Distribution Protocol such as commands to configure LDP parameters or to inspect the protocol status.

mpls ldp lsr-id

Description

Configures a LSR-ID that uniquely identifies the label switch router (LSR) within the network and enables MPLS LDP in the device. This configuration is mandatory to enable LDP in the device.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router.

Value: Any loopback interface.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the LDP lsr id.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# commit
```

Impacts and precautions

The loopback interface to be used as an LDP LSR identifier must be previously created. In addition, it must be configured with an IPv4 address and a /32 netmask.

Hardware restrictions

N/A

mpls ldp lsr-id interface

Description

Enables LDP basic discovery on the specified interface.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **interface** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router. The loopback interface must be created.

Value: Any loopback interface.

Default Value: N/A

interface-name

Description: Specifies the L3 interfaces for LDP basic discovery. The L3 interfaces must be created.

Value: any L3 interface.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable LDP basic discovery on the interface.

```
# config
(config)# mpls ldp lsr-id loopback-1 interface l3-vlan1
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

The l3 interface to be used for LDP basic discovery must be previously created. In addition, it must be configured with an IPv4 address.

Hardware restrictions

N/A

mpls ldp lsr-id interface hello-holdtime

Description

Configures the Hello hold timer for this LDP Basic Discovery.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **interface** *interface-name* **hello-holdtime** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description:	Specifies a loopback interface for the label switching router. The loopback interface must be created.
Value:	Any loopback interface.
Default Value:	N/A

interface-name

Description:	Specifies the L3 interfaces for LDP basic discovery. The L3 interfaces must be created.
Value:	any L3 interface.
Default Value:	N/A

hello-holdtime

Description:	Hello hold timer for the LDP Basic Discovery.
Value:	1-65535.
Default Value:	15.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the LDP interface Hello holdtime.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# interface l3-vlan1
(config-interface-l3-vlan1)# hello-holdtime 20
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls ldp lsr-id interface keep-alive-holdtime

Description

Configures the Keep alive hold timer for this LDP Basic Discovery.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **interface** *interface-name* **keep-alive-holdtime** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router. The loopback interface must be created.

Value: Any loopback interface.

Default Value: N/A

interface-name

Description: Specifies the L3 interfaces for LDP basic discovery. The L3 interfaces must be created.

Value: any L3 interface.

Default Value: N/A

keep-alive-holdtime

Description: Keep alive hold timer for the LDP Basic Discovery.

Value: 1-65535.

Default Value: 40.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the LDP interface Keep alive holdtime.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# interface l3-vlan1
(config-interface-l3-vlan1)# keep-alive-holdtime 50
(config-interface-l3-vlan1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls ldp lsr-id neighbor targeted

Description

Enables LDP extended discovery with the specified internetwork layer address.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **neighbor targeted** *address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router. The loopback interface must be created.

Value: Any loopback interface.

Default Value: N/A

address

Description: The internetwork layer address used for the extended discovery.

Value: any IPv4 address.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

2.2	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to enable LDP extended discovery with the specified inter-network layer address.

```
# config
(config)# mpls ldp lsr-id loopback-1 neighbor targeted 9.9.9.9
(config-neighbor-9.9.9.9)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls ldp lsr-id neighbor targeted hello-holdtime

Description

Configures the Hello hold timer for this LDP Extended Discovery.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **neighbor targeted** *address* **hello-holdtime** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description:	Specifies a loopback interface for the label switching router. The loopback interface must be created.
Value:	Any loopback interface.
Default Value:	N/A

address

Description:	The value of the internetwork layer address used for the Extended Discovery.
Value:	any IPv4 address.
Default Value:	N/A

hello-holdtime

Description:	Hello hold timer for the LDP Extended Discovery.
Value:	1-65535.
Default Value:	45.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the Hello holdtime.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# neighbor targeted 9.9.9.9
(config-neighbor-9.9.9.9)# hello-holdtime 20
(config-neighbor-9.9.9.9)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls ldp lsr-id neighbor targeted keep-alive-holdtime

Description

Configures the Keep alive hold timer for this LDP Extended Discovery.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **neighbor targeted** *address* **keep-alive-holdtime** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router. The loopback interface must be created.

Value: Any loopback interface.

Default Value: N/A

address

Description: The value of the internetwork layer address used for the Extended Discovery.

Value: any IPv4 address.

Default Value: N/A

keep-alive-holdtime

Description: Keep alive hold timer for the LDP Extended Discovery.

Value: 1-65535.

Default Value: 40.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the Keep alive holdtime.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# neighbor targeted 9.9.9.9
(config-neighbor-9.9.9.9)# keep-alive-holdtime 50
(config-neighbor-9.9.9.9)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

mpls ldp lsr-id neighbor targeted password

Description

Configures the neighbor to use Message-Digest algorithm 5 (MD5) authentication on the TCP connection between LDP peers.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

mpls ldp lsr-id *loopback-name* **neighbor targeted** *address* **password** *pwd*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

loopback-name

Description: Specifies a loopback interface for the label switching router. The loopback interface must be created.

Value: Any loopback interface.

Default Value: N/A

address

Description: The value of the internetwork layer address used for the Extended Discovery.

Value: any IPv4 address.

Default Value: N/A

password *pwd*

Description: Specifies the LDP neighbor case-sensitive password to be used between the TCP peer connection.

Value: string (length 2 - 80).

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
2.4	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.
This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to configure the LDP password.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# neighbor targeted 9.9.9.9
(config-neighbor-9.9.9.9)# password pwdTest
(config-neighbor-9.9.9.9)# commit
```

This example shows the configuration of a neighbor password using an already encrypted password.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# neighbor targeted 9.9.9.9
(config-neighbor-50.50.50.1)# password "hls:2922743918:337ZpL=z"
(config-neighbor-50.50.50.1)# commit
```

This example shows the configuration of a neighbor password using special characters (i.e: " " , "?" , "!" , ";"). Please note that it is necessary to use double quotation marks in this case.

```
# config
(config)# mpls ldp lsr-id loopback-1
(config-lsr-id-loopback-1)# neighbor targeted 9.9.9.9
(config-neighbor-50.50.50.1)# password "pwd?test:2"
(config-neighbor-50.50.50.1)# commit
```

Impacts and precautions

Password must be enclosed in double quotation marks if special characters were used (i.e: " " , "?" , "!" , ";"). Note that in an established LDP session if password is configured or changed the session will be restarted.

Hardware restrictions

N/A

show mpls ldp database

Description

This command shows a list of all labels present in LDP database, including non-selected labels, marked with NS, which are not installed. (not used to forward packets).

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show mpls ldp database [ ** prefix ** ]
```

Parameters

prefix *ipv4-prefix*

Description: Use Network Prefix to filter the output.

Value: a.b.c.d/x

Default Value: N/A.

Output Terms

Output	Description
Network Prefix	Indicates a specific FEC present on MPLS LDP database.
Upstream LSR-ID	ID of an upstream LSR to which a label for this FEC was distributed via a MPLS LDP label mapping message.
Label	Indicates the label distributed to the upstream LSR.
DownStream LSR-ID	ID of a downstream LSR from which a label was received for this FEC via a MPLS LDP label mapping message.

Output	Description
Label	Indicates the downstream label distributed by the downstream LSR.
State	Indicates the state of a specific FEC. Entries marked with NS are not installed (not used to forward packets).

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.
2.4	This command was updated.

Usage Guidelines

Every label mapping received from a peer LSR is retained regardless of whether the LSR is the active next hop for the advertised mapping or not. Only the label received from the current next hop will be installed. This command can be executed directly via CLI. This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to use this command.

```
# show mpls ldp database
```

State codes: A - active, NS - not selected

Network Prefix	UpStream LSR-ID	Label	DownStream LSR-ID	Label	State
1.1.1.1/32	4.4.4.4	19	--	--	A
1.1.1.1/32	5.5.5.5	19	--	--	A
1.1.1.1/32	8.8.8.8	19	--	--	A
2.2.2.2/32	4.4.4.4	17	--	--	A
2.2.2.2/32	5.5.5.5	17	--	--	A
2.2.2.2/32	8.8.8.8	17	--	--	A
1.1.1.1/32	--	--	2.2.2.2	179	A
1.1.1.1/32	--	--	4.4.4.4	133	NS
1.1.1.1/32	--	--	5.5.5.5	26	NS
2.2.2.2/32	--	--	2.2.2.2	3	A
2.2.2.2/32	--	--	4.4.4.4	38	NS
2.2.2.2/32	--	--	5.5.5.5	85	NS

```
# show mpls ldp database 1.1.1.1/32
```

State codes: A - active, NS - not selected

Network Prefix	UpStream LSR-ID	Label	DownStream LSR-ID	Label	State
1.1.1.1/32	4.4.4.4	19	--	--	A
1.1.1.1/32	5.5.5.5	19	--	--	A
1.1.1.1/32	8.8.8.8	19	--	--	A
1.1.1.1/32	--	--	2.2.2.2	179	A
1.1.1.1/32	--	--	4.4.4.4	133	NS
1.1.1.1/32	--	--	5.5.5.5	26	NS

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls ldp neighbor

Description

Shows either summarized or detailed information about LDP sessions.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

show mpls ldp neighbor [brief | detail]

Parameters

brief

Description: Shows summarized information about the MPLS LDP sessions.

Value: N/A

Default Value: N/A

detail

Description: The full output of this command displays general status information about the established LDP sessions (status, role, up-time, remaining keepalive hold time, etc.), negotiated session timer values, and the addresses advertised by the neighbors through LDP Address Messages.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Neighbor	Indicates the Peer-ID value of the MPLS LDP neighbor.

Output	Description
LDP-ID	Indicates the label space value of the MPLS LDP neighbor.
State	Indicates the adjacency state with the MPLS LDP neighbor.
Nbr type	Indicates the operation type <targeted/linked> of the MPLS LDP session.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to use this command.

```
# show mpls ldp neighbor
```

Neighbor LDP-ID	State	Nbr type
20.20.20.20:0	Operational	linked/targeted
30.30.30.30:0	Operational	targeted

```
Local LDP-ID: 222.222.222.222:0; Peer LDP-ID: 20.20.20.20:0;
  Last change: 00:00:00; State: operational; Role: active;
  Max ldp pdu: 1440; Protocol version: 1;
  Local configured KeepAlive (KA) hold time: 40s;
  Peer's advertised KA hold time: 40s;
  Negotiated KeepAlive (KA) hold time: 40s;
  Negotiated time between KA messages: 7s;
  KA hold time remaining for this session: 00:00:39s;
  Remote addresses:
    1.1.1.2
    4.4.4.2
    20.20.20.20
```

```
Adjacency: 20.20.20.20:0; - Basic Discovery Mechanism
  Adjacency discovery hello hold time: 15s;
  Local discovery hello hold time: 15s;
  Negotiated discovery hello hold time: 15s;
  Remaining hello hold time: 14s;
```

```
Adjacency: 20.20.20.20:0; - Extended Discovery Mechanism
  Adjacency discovery hello hold time: 45s;
  Local discovery hello hold time: 45s;
  Negotiated discovery hello hold time: 45s;
  Remaining hello hold time: 39s;
```

```
Local LDP-ID: 222.222.222.222:0; Peer LDP-ID: 30.30.30.30:0;
  Last change: 00:00:00; State: operational; Role: active;
  Max ldp pdu: 1440; Protocol version: 1;
  Local configured KeepAlive (KA) hold time: 40s;
  Peer's advertised KA hold time: 40s;
  Negotiated KeepAlive (KA) hold time: 40s;
  Negotiated time between KA messages: 7s;
  KA hold time remaining for this session: 00:00:39s;
  Remote addresses:
    30.30.30.30
    4.4.4.1
```

```
Adjacency: 30.30.30.30:0; - Extended Discovery Mechanism
  Adjacency discovery hello hold time: 45s;
  Local discovery hello hold time: 45s;
  Negotiated discovery hello hold time: 45s;
  Remaining hello hold time: 44s;
```

```
# show mpls ldp neighbor brief
```

Neighbor LDP-ID	State	Nbr type
20.20.20.20:0	Operational	linked/targeted
30.30.30.30:0	Operational	targeted

```
# show mpls ldp neighbor detail
```

```
Local LDP-ID: 222.222.222.222:0; Peer LDP-ID: 20.20.20.20:0;
  Last change: 00:00:00; State: operational; Role: active;
  Max ldp pdu: 1440; Protocol version: 1;
  Local configured KeepAlive (KA) hold time: 40s;
  Peer's advertised KA hold time: 40s;
  Negotiated KeepAlive (KA) hold time: 40s;
  Negotiated time between KA messages: 7s;
  KA hold time remaining for this session: 00:00:39s;
  Remote addresses:
    1.1.1.2
    4.4.4.2
    20.20.20.20
```

```
Adjacency: 20.20.20.20:0; - Basic Discovery Mechanism
  Adjacency discovery hello hold time: 15s;
```



```
Local discovery hello hold time: 15s;
Negotiated discovery hello hold time: 15s;
Remaining hello hold time: 14s;

Adjacency: 20.20.20.20:0; - Extended Discovery Mechanism
Adjacency discovery hello hold time: 45s;
Local discovery hello hold time: 45s;
Negotiated discovery hello hold time: 45s;
Remaining hello hold time: 39s;

Local LDP-ID: 222.222.222.222:0; Peer LDP-ID: 30.30.30.30:0;
Last change: 00:00:00; State: operational; Role: active;
Max ldp pdu: 1440; Protocol version: 1;
Local configured KeepAlive (KA) hold time: 40s;
Peer's advertised KA hold time: 40s;
Negotiated KeepAlive (KA) hold time: 40s;
Negotiated time between KA messages: 7s;
KA hold time remaining for this session: 00:00:39s;
Remote addresses:
 30.30.30.30
 4.4.4.1

Adjacency: 30.30.30.30:0; - Extended Discovery Mechanism
Adjacency discovery hello hold time: 45s;
Local discovery hello hold time: 45s;
Negotiated discovery hello hold time: 45s;
Remaining hello hold time: 44s;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show mpls ldp parameters

Description

Shows information about the current control-plane configuration state of several LDP parameters.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

show mpls ldp parameters [brief]

Parameters

brief

Description:	Shows resumed information about the current LDP control-plane configuration.
Value:	N/A
Default Value:	N/A

Output Terms

Output	Description
<code>LSR_ID</code>	Indicates the local Label Switch Router ID.
<code>Protocol version</code>	Indicates the version of the MPLS LDP protocol.
<code>Allocation mode</code>	Indicates the advertising FEC-label bindings mode.
<code>Encapsulation mode</code>	Indicates the MPLS LDP encapsulation mode.

Output	Description
Distribution mode	Indicates the label distribution mode.
Retention mode	Indicates the label retention mode.
Local addresses	Indicates the local LDP-enabled interfaces (the IP addresses that are advertised by this router to its neighbors through LDP Address Message).

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
2.2	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

This command requires a license to be used. Please contact the support for further information.

Example:

This example shows how to use this command.

```
# show mpls ldp parameters

LSR_ID: 222.222.222.222;
  Protocol version: 1;
  Allocation mode: Ordered;
  Encapsulation mode: PHP implicit-null;
  Distribution mode: Unsolicited;
  Retention mode: Liberal;

Local addresses:
  222.222.222.222
  1.1.1.1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 8: MULTICAST

This chapter describes the commands related to management of Multicast protocols in the DmOS CLI.

IGMP SNOOPING

This topic describes the CLI commands related to the IGMP snooping functionality. The IGMP snooping feature allows a network switch to listen to the IGMP protocol messages exchanged between routers and hosts, with the purpose of identifying which host ports are interested on a specific multicast traffic, and sending that traffic only to those ports.

clear multicast igmp snooping statistics

Description

Resets IGMP snooping statistics.

Supported Platforms

This command is supported in all platforms.

Syntax

```
clear multicast igmp snooping statistics { instance [instance-id] | interface [interface-name][instance instance-id] }
```

Parameters

instance

Description: Resets the statistics of the IGMP snooping instance.

Value: N/A

Default Value: N/A

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface

Description: Resets the IGMP snooping statistics of an interface. All interfaces will be affected if an interface is not defined.

Value: N/A

Default Value: N/A

interface-name

Description: Name of the interface that will have its statistics cleared.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

instance *instance-id*

Description: IGMP snooping instance ID where the interface is configured.

Value: 1-8.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.4	Command syntax was modified.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

These examples show how to use this command.

```
# clear multicast igmp snooping statistics instance 1
# clear multicast igmp snooping statistics interface gigabit-ethernet 1/1/1 instance 1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping

Description

Configures an IGMP snooping instance.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description:	IGMP snooping instance ID.
Value:	1-8.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.10	This command was introduced.
------	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping administrative-status

Description

Configures the desired administrative status on an IGMP snooping instance.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **administrative-status** { **up** | **down** }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

administrative-status

Description: Configures the administrative status.

Value: N/A

Default Value: N/A

up

Description: Activates (up) the IGMP snooping instance.

Value: N/A

Default Value: N/A

down

Description: Deactivates (down) the IGMP snooping instance.

Value: N/A

Default Value: N/A

Default

up.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.10	This command was introduced
------	-----------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# config terminal
Entering configuration mode terminal
(config)# multicast igmp snooping 1 administrative-status down
(config-igmp-snooping-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping bridge-domain

Description

Configures a bridge domain on an IGMP snooping instance.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **bridge-domain id** *bridge-domain-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.
Value: 1-8.
Default Value: N/A

bridge-domain id *bridge-domain-id*

Description: Configures the bridge domain.
Value: N/A
Default Value: N/A

id *bridge-domain-id*

Description: Bridge domain ID to be configured on the IGMP snooping instance.
Value: 1-4093.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1 bridge-domain id 1000
(config-igmp-snooping-1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface

Description

Configures an interface on an IGMP snooping instance.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.
Value: 1-8.
Default Value: N/A

interface *interface-name*

Description: Interface to be configured on the IGMP snooping instance.
Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.
Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1 interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface administrative-status

Description

Configures the desired administrative status on an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **administrative-status**
{ **up** | **down** }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

administrative-status

Description: Configures the administrative status on the interface.

Value: N/A

Default Value: N/A

up

Description: Activates (up) the interface.

Value: N/A

Default Value: N/A

down

Description: Deactivates (down) the interface.

Value: N/A

Default Value: N/A

Default

up.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# administrative-status down
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface group-limit

Description

Configures the maximum number of multicast groups allowed on an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **group-limit** *limit*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.
Value: 1-8.
Default Value: N/A

interface *interface-name*

Description: Interface name.
Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.
Default Value: N/A

group-limit *limit*

Description: Maximum number of groups allowed on the interface. 0 (zero) means unlimited.
Value: 0-3000.
Default Value: N/A

Default

0.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# group-limit 100
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface ignore

Description

Configures which version of the IGMP packets should be ignored on an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **ignore** { **igmp-v1** | **igmp-v2** }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

ignore

Description: Configures which version of the IGMP packets should be ignored.

Value: N/A

Default Value: N/A

igmp-v1

Description: Configures the interface to ignore IGMPv1 packets.

Value: N/A

Default Value: N/A

igmp-v2

Description: Configures the interface to ignore IGMPv2 packets.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.

Release	Modification
---------	--------------

5.0	Support for 25-gigabit Ethernet was added.
-----	--

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1 ignore igmp-v1
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface immediate-leave

Description

Configures the immediate leave on an interface. In immediate leave mode, the group membership on an interface is immediately deleted right after receiving an IGMP Leave message i.e. any group-specific or group-and-source queries is not sent before deleting the entry.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **immediate-leave**

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

immediate-leave

Description: Enable the immediate leave on the interface.

Value: N/A

Default Value: N/A

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.12	This command was introduced.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# immediate-leave
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface last-member-query

Description

Configures the interval of time in seconds between the group-specific query messages on an interface. The group-specific-query messages have their Max Response time set to the value of the last member query interval. If no Reports are received after the response time of the last query expires, the group is removed.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **last-member-query interval** *seconds*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

last-member-query

Description: Configures the last-member-query.

Value: N/A

Default Value: N/A

interval *seconds*

Description: Interval of time to be configured on the interface.

Value: 1-25.

Default Value: N/A

Default

1.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# last-member-query interval 2
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface maximum response time

Description

Configures the maximum response time on an interface. It specifies the maximum allowed time which the host interface is expected to reply to an IGMP General Query message. In addition, it is applied along with other timers to modify the group membership interval ($robustness-variable \times query-interval + max-response-time$).

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **max-response-time** *seconds*

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

max-response-time *seconds*

Description: The maximum response time to be configured on the interface.

Value: 1-25.

Default Value: N/A

Default

10.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.12	This command was introduced.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# max-response-time 15
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface mrouter

Description

Configures an interface as a multicast router interface, host interface, or capable of being either of them. An interface can learn if it is a router interface by detecting the reception of Query messages.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **mrouter** { **always** | **learn-queries** | **never** }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id.

Default Value: N/A

mrouter

Description: Configures the mrouter option of the interface.

Value: N/A

Default Value: N/A

always

Description: Configures the interface to be a multicast router interface.

Value: N/A

Default Value: N/A

learn-queries

Description: Configures the interface to learn via the detection of Query messages.

Value: N/A

Default Value: N/A

never

Description: Configures the interface to be a host interface.

Value: N/A

Default Value: N/A

Default

learn-queries.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# mrouter always
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface query interval

Description

Configures the query interval on an interface. It specifies the frequency at which the IGMP General Query messages are sent from an interface. In addition, it is applied along with other timers to modify the group membership interval ($robustness-variable \times query-interval + max-response-time$).

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **query-interval** *seconds*

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

query-interval *seconds*

Description: The query interval to be configured on the interface.

Value: 125-3600.

Default Value: N/A

Default

125.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.12	This command was introduced.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# query-interval 300
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```


Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface robustness-variable

Description

Configures the value of robustness-variable which allows tuning for the expected packet loss on a subnetwork. The robustness-variable modifies certain IGMP message intervals for IGMPv2 and IGMPv3. By increasing its value, the packet loss tolerance is increased, but the leave latency in the subnetwork is also increased.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **robustness-variable** *variable*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

robustness-variable *variable*

Description: Value of robustness-variable to be configured on the interface.

Value: N/A

Default Value: N/A

Default

2.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# robustness-variable 5
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

multicast igmp snooping interface version

Description

Configures the IGMP version on an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

multicast igmp snooping *instance-id* **interface** *interface-name* **version** *version*

Parameters

instance-id

Description: IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface *interface-name*

Description: Interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

version *version*

Description: IGMP version to be configured on the interface.

Value: 1-3.

Default Value: N/A

Default

3.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
(config)# multicast igmp snooping 1
(config-igmp-snooping-1)# interface gigabit-ethernet-1/1/1
(config-igmp-interface-gigabit-ethernet-1/1/1)# version 2
(config-igmp-interface-gigabit-ethernet-1/1/1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show multicast igmp snooping

Description

Shows information about IGMP snooping instances.

Supported Platforms

This command is supported in all platforms.

Syntax

show multicast igmp snooping *instance-id*

Parameters

instance-id

Description:	Shows information about the specified IGMP snooping instance ID.
Value:	1-8.
Default Value:	N/A

Output Terms

Output	Description
IGMP Snooping Instance	Indicates the IGMP snooping instance.
Bridge Domain	Indicates the bridge domain type and its ID.
Administrative State	Indicates the administrative state of the IGMP snooping instance (enable/disable).
Operational state	Indicates the operational state of the IGMP snooping instance (Up/Down).

Output	Description
Interface	Shows IGMP snooping information related to a specific network interface.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show multicast igmp snooping 1
IGMP Snooping Instance: 1;
Bridge Domain: vlan; ID: 2000;
  Administrative State: enable;
  Operational state: Up;
Interface: gigabit-ethernet-1/1/9;
  Query Interval (Configured Value): 125 seconds;
  Query Interval (Value In Use): 125 seconds;
  Query Maximum Response Time (Configured Value): 10 seconds;
```

```

Query Maximum Response Time (Value In Use): 10 seconds;
Groups Limit: 0;
Sources Limit: 0;
Robustness (Configured Value): 2;
Robustness (Value In Use): 2;
Last Member Query Interval (Configured Value): 1 seconds;
Last Member Query Interval (Value In Use): 1 seconds;
Drop IGMPv1 packets: false;
Drop IGMPv2 packets: false;
Immediate Leave: false;
Query Before Immediate Leave: false;

Interface: gigabit-ethernet-1/1/10;
Query Interval (Configured Value): 125 seconds;
Query Interval (Value In Use): 125 seconds;
Query Maximum Response Time (Configured Value): 10 seconds;
Query Maximum Response Time (Value In Use): 10 seconds;
Groups Limit: 0;
Sources Limit: 0;
Robustness (Configured Value): 2;
Robustness (Value In Use): 2;
Last Member Query Interval (Configured Value): 1 seconds;
Last Member Query Interval (Value In Use): 1 seconds;
Drop IGMPv1 packets: false;
Drop IGMPv2 packets: false;
Immediate Leave: false;
Query Before Immediate Leave: false;

Interface: service-port-201;
Query Interval (Configured Value): 125 seconds;
Query Interval (Value In Use): 125 seconds;
Query Maximum Response Time (Configured Value): 10 seconds;
Query Maximum Response Time (Value In Use): 10 seconds;
Groups Limit: 0;
Sources Limit: 0;
Robustness (Configured Value): 2;
Robustness (Value In Use): 2;
Last Member Query Interval (Configured Value): 1 seconds;
Last Member Query Interval (Value In Use): 1 seconds;
Drop IGMPv1 packets: false;
Drop IGMPv2 packets: false;
Immediate Leave: false;
Query Before Immediate Leave: false;

Interface: service-port-202;
Query Interval (Configured Value): 125 seconds;
Query Interval (Value In Use): 125 seconds;
Query Maximum Response Time (Configured Value): 10 seconds;
Query Maximum Response Time (Value In Use): 10 seconds;
Groups Limit: 0;
Sources Limit: 0;
Robustness (Configured Value): 2;
Robustness (Value In Use): 2;
Last Member Query Interval (Configured Value): 1 seconds;
Last Member Query Interval (Value In Use): 1 seconds;
Drop IGMPv1 packets: false;
Drop IGMPv2 packets: false;
Immediate Leave: false;
Query Before Immediate Leave: false;

```

Impacts and precautions

N/A

Hardware restrictions

N/A

show multicast igmp snooping groups

Description

Shows information about IGMP snooping groups.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show multicast igmp snooping groups [{brief | detail | extensive} [instance-id]  
[ipv4-address] [interface-name]
```

Parameters

brief

Description:	Shows a summary of the active multicast group memberships.
Value:	N/A
Default Value:	N/A

detail

Description:	Shows detailed information about the active multicast group memberships.
Value:	N/A
Default Value:	N/A

extensive

Description:	Shows detailed information about the active multicast group memberships, and the IGMP snooping instance.
Value:	N/A
Default Value:	N/A

instance-id

Description:	Shows information about the specified IGMP snooping instance ID.
---------------------	--

Value: 1-8.

Default Value: N/A

ipv4-address

Description: Filters the command output by the multicast group IP address.

Value: a.b.c.d.

Default Value: N/A

interface-name

Description: Filters the command output by the provided network interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

Output Terms

Output	Description
ID	Indicates the IGMP snooping instance ID.
Group address	Indicates the multicast group membership address.
Source address	Indicates the specific source address.
Interface	Indicates the network interface where the multicast group membership is active.
Uptime	Indicates the amount of time (in seconds) that the multicast group membership is active.
Expires	Indicates the amount of time (in seconds) for the multicast group membership to become inactive, if no other IGMP report messages is received on the interface.

Output	Description
Last Reporter	Indicates the IP address of the last host to report that multicast group membership.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.0	Source address field was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show multicast igmp snooping groups
```

ID	Group-address	Source-address	Interface	Uptime	Expires	Last-reporter
1	226.2.2.2	172.16.0.1	service-port-201	99	160	100.2.2.103

```

IGMP Snooping Instance: 1;
Group address: 226.2.2.2;
Source address: 172.16.0.1;
Interface: service-port-201;
Version: V3;
Last reporter: 100.2.2.103;
Exclude state expire: 00:00:00;
Uptime: 00:01:40; Expires: 00:02:39;

IGMP Snooping Instance: 1;
Bridge Domain:vlan; ID: 2000;
Group address: 226.2.2.2;
Source address: 172.16.0.1;
Filter mode: Include;
Membership type: dynamic;
Interface: service-port-201;
Version: V3;
Last reporter: 100.2.2.103;
Exclude state expire: 00:00:00;
Uptime: 00:01:40; Expires: 00:02:39;
Host timer: V1: 00:00:00; V2: 00:02:39;
Source filter mode: Include;

# show multicast igmp snooping groups brief
```

ID	Group-address	Source-address	Interface	Uptime	Expires	Last-reporter
1	226.2.2.2	172.16.0.1	service-port-201	99	160	100.2.2.103

```

# show multicast igmp snooping groups detail

IGMP Snooping Instance: 1;
Group address: 226.2.2.2;
Source address: 172.16.0.1;
Interface: service-port-201;
Version: V3;
Last reporter: 100.2.2.103;
Exclude state expire: 00:00:00;
Uptime: 00:01:40; Expires: 00:02:39;

# show multicast igmp snooping groups extensive

IGMP Snooping Instance: 1;
Bridge Domain:vlan; ID: 2000;
Group address: 226.2.2.2;
Source address: 172.16.0.1;
Filter mode: Include;
Membership type: dynamic;
Interface: service-port-201;
Version: V3;
Last reporter: 100.2.2.103;
Exclude state expire: 00:00:00;
Uptime: 00:01:40; Expires: 00:02:39;
Host timer: V1: 00:00:00; V2: 00:02:39;
Source filter mode: Include;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show multicast igmp snooping mrouter

Description

Shows which interfaces are multicast router interfaces, host interfaces, or capable of being either of them.

Supported Platforms

This command is supported in all platforms.

Syntax

show multicast igmp snooping mrouter [*instance-id* [*interface-name*]]

Parameters

instance-id

Description: Filters output by the provided IGMP snooping instance ID.

Value: 1-8.

Default Value: N/A

interface-name

Description: Filters the command output by the provided network interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

Output Terms

Output	Description
ID	Indicates the IGMP snooping instance ID.
VLAN	Indicates the VLAN ID.
Interface	Indicates the network interface.
MRouter	Indicates whether the interface is statically configured as a multicast router interface (yes), host interface (no), or capable of being either of them (learn-queries).
Learned	Indicates whether the interface is a multicast router interface (yes) or host interface (no). This field is only valid for the interfaces that are configured in the learn-queries mode.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.

Release	Modification
---------	--------------

3.0	Support for 40-gigabit Ethernet was added.
-----	--

4.6	Support for 100-gigabit Ethernet was added.
-----	---

5.0	Support for 25-gigabit Ethernet was added.
-----	--

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show multicast igmp snooping mrouter 1
```

ID	VLAN	Interface	MRouter	Learned
--	----	-----	-----	-----
1	2000	gigabit-ethernet-1/1/9	yes	-
1	2000	gigabit-ethernet-1/1/10	learn-queries	no
1	2000	service-port-201	no	-
1	2000	service-port-202	no	-

```
# show multicast igmp snooping mrouter 1 gigabit-ethernet-1/1/9
```

ID	VLAN	Interface	MRouter	Learned
--	----	-----	-----	-----
1	2000	gigabit-ethernet-1/1/9	yes	-

Impacts and precautions

N/A

Hardware restrictions

N/A

show multicast igmp snooping port

Description

Shows IGMP snooping interface information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show multicast igmp snooping port [{brief | detail | extensive} [instance-id]  
[interface-name]
```

Parameters

brief

Description:	Shows a summary of the IGMP snooping interface information.
Value:	N/A
Default Value:	N/A

detail

Description:	Shows detailed information about the IGMP snooping interfaces.
Value:	N/A
Default Value:	N/A

extensive

Description:	Shows detailed information about the IGMP snooping interfaces, and the IGMP activity as well.
Value:	N/A
Default Value:	N/A

instance-id

Description:	Filters the command output by the provided IGMP snooping instance ID.
---------------------	---

Value: 1-8.

Default Value: N/A

interface-name

Description: Filters the command output by the provided network interface name.

Value: hundred-gigabit-ethernet-chassis/slot/port | forty-gigabit-ethernet-chassis/slot/port | twenty-five-g-ethernet-chassis/slot/port | ten-gigabit-ethernet-chassis/slot/port | gigabit-ethernet-chassis/slot/port | lag-id | service-port-id.

Default Value: N/A

Output Terms

Output	Description
ID	Indicates the IGMP snooping instance ID.
Interface	Indicates the network interface.
Ad	Indicates the administrative status of the interface.
Op	Indicates the operational status of the interface.
Ver	Indicates the configured IGMP version on the interface.
Joins	Indicates the number of IGMP report messages received by the interface.
General Queries	Indicates the number of IGMP general query messages sent by the interface.
Specific Queries	Indicates the number of IGMP specific query messages sent by the interface.

Output	Description
Invalid Msgs	Indicates the number of invalid IGMP messages received by the interface.
Total	Indicates the total amount of IGMP messages exchanged by the interface.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.10	This command was introduced.
1.12	Support for LAG was added.
3.0	Support for 40-gigabit Ethernet was added.
4.6	Support for 100-gigabit Ethernet was added.
5.0	Support for 25-gigabit Ethernet was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show multicast igmp snooping port brief 1 service-port-202
```

ID	Interface	Ad Op	Ver	Joins	Queries (sent)		Msgs (recv)	
					General	Specific	Invalid	Total
1	service-port-202	en up	3	8	2	10	0	13

```
# show multicast igmp snooping port detail 1 service-port-202
IGMP Snooping Instance: 1;
Interface: service-port-202;
Administrative state: enable;
Operational state: up;
IGMP version: 3;
IGMP query interval: 125 seconds;
IGMP querier timeout: 0 seconds;
IGMP querier last changed: 0 seconds;
IGMP querier robustness: 2;
IGMP max query response time is 10 seconds;
Last member query count: 2;
Startup query interval: 31 seconds;
Startup query count: 2;
Last member query response interval: 1 seconds;

# show multicast igmp snooping port extensive 1 service-port-202
IGMP Snooping Instance: 1;
Bridge Domain: vlan; ID: 2000;
Interface: service-port-202;
Administrative state: enable;
Operational state: up;
IGMP version: 3;
IGMP query interval: 125 seconds;
IGMP querier timeout: 0 seconds;
IGMP querier last changed: 0 seconds;
IGMP querier robustness: 2;
IGMP max query response time is 10 seconds;
Last member query count: 2;
Startup query interval: 31 seconds;
Startup query count: 2;
Last member query response interval: 1 seconds;
IGMP activity:
  Joins: 8; Failed joins: 0;
  Counters last reset: 13559 seconds;
  Peak groups: 1;
  Sent:
    General queries sent: 2;
    Specific queries sent: 10;
  Received:
    Wrong version queries: 0;
    Invalid messages: 0;
    IGMP v1 messages: 0;
    IGMP v2 messages: 13;
    IGMP v3 messages: 0;
    Total messages: 13;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show multicast igmp snooping statistics

Description

Shows IGMP snooping statistics.

Supported Platforms

This command is supported in all platforms.

Syntax

show multicast igmp snooping statistics [*instance-id*]

Parameters

instance-id

Description:	Filters the command output by the provided IGMP snooping instance ID.
Value:	1-8.
Default Value:	N/A

Output Terms

Output	Description
IGMP Snooping	Indicates the IGMP snooping instance ID.
Bridge Domain	Displays bridge domain information.
IGMP messages	Indicates the number of each IGMP message type sent and received by the IGMP snooping instance.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

1.10	This command was introduced.
------	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to use this command.

```
# show multicast igmp snooping statistics 1
IGMP Snooping: 1;
Bridge Domain: vlan; ID: 2000;
IGMP messages:
  Valid:
    Received queries: 0;
    Received reports: 12;
    Received leaves: 9;
    Total: 21;
  Filtered:
    Received queries: 7;
    Received reports: 0;
    Exceeded limit: 0;
    Groups & sources: 0;
    Link local: 0;
    Other: 0;
    Total: 7;
  Bad:
    Checksum: 0;
    Router alert: 0;
    Other: 0;
    Total: 0;
  Other:
    Sent queries: 26;
    Snooping queries: 0;
```

Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 9: QUALITY OF SERVICE

This chapter describes the commands related to management of QoS in the DmOS CLI.

QOS POLICER

This topic describes the commands related to Policer and Meter such as commands to configure CIR and PIR or to inspect bandwidth rates.

qos policer hierarchical

Description

Create hierarchical policer instance.

Supported Platforms

This command is supported only in the following platforms: DM4050, DM4250, DM4360, DM4370, DM4610, DM4611, DM4612, DM4615.

Syntax

qos policer hierarchical *id* **profile** *profile-name* [**instance** *instance-id*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

qos policer hierarchical *id*

Description: User defined hierarchical policer instance ID.

Value: 1 - 512

Default Value: N/A

profile *profile-name*

Description: Profile of the hierarchical policer instance.

Value: String with up to 48 characters: letters, numbers, '_', and '-'.

Default Value: N/A

qos policer instance *instance-id*

Description: User defined first level policer instance ID.

Value: 1 - 1280

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

6.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Hierarchical policer instances can be created to police lower level policer instances which are attached to it.

Examples:

The following example creates a hierarchical policer instance, that will operate according to profile foo and attach to it two previously created lower level instances.

```
#config
Entering configuration mode terminal
(config)# qos policer hierarchical 1 profile foo
(policer-hierarchical-1)# instance 1
(policer-hierarchical-1)# instance 2
(policer-hierarchical-1)# top
(config)# commit
Commit complete.
```

(config) #

Impacts and precautions

N/A

Hardware restrictions

N/A

qos policer instance

Description

Create a policer instance and apply it to a network traffic.

Supported Platforms

This command is supported in all platforms.

Syntax

qos policer instance *instance-id* { **interface** *interface-name* } **profile** *profile-name* [**vlan** *vlan-id*] [**pcp** *pcp*] [**inner-vlan** *vlan-id*] [**name** *instance-name*] [**counters** { *enabled* | *disabled* }]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

qos policer instance *instance-id*

Description: User defined policer instance ID.

Value: 1 - 1280

Default Value: N/A

interface *interface-name*

Description: Interface the policer instance refers to. Multiple interfaces may be specified, and the policer bandwidth will be shared in this case.

Value: *interface-type-chassis/slot/port* | *lag-id*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, gpon.

Default Value: N/A

profile *profile-name*

Description: Name of the policer profile created with **qos policer profile**.

Value: String with a maximum of 48 characters. It only accepts alphanumeric characters and '_', '+', and '-'.

Default Value: N/A

vlan *vlan-id*

Description: Apply this policer to a list or to a specific outer VLAN ID.

Value: 1 - 4094

Default Value: N/A

pcp *pcp*

Description: Apply this policer to a list or to a specific outer Priority 802.1p.

Value: 0 - 7

Default Value: N/A

inner-vlan *vlan-id*

Description: Apply this policer to a list or to a specific inner VLAN ID. The inner VLAN is the second VLAN Tag after ingress VLAN manipulations (QinQ/Vlan Translations). It is applicable only to double tagged packets.

Value: 1 - 4094

Default Value: N/A

inner-pcp *pcp*

Description: Apply this policer to a list or to a specific inner Priority 802.1p. The inner Priority 802.1p is the PCP in the second VLAN Tag after ingress VLAN manipulations (QinQ/Vlan Translations). It is applicable only to double tagged packets.

Value: 0 - 7

Default Value: N/A

dscp *dscp*

Description: Apply this policer only to a specific IPv4/IPv6 DSCP value. This parameter is only valid for *ingress* policers.

Value: 0 - 63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef

Default Value: N/A

name *instance-name*

Description: Configure a name for the policer instance.

Value: String with a maximum of 48 characters. It only accepts alphanumeric characters and '_', '+', and '-'.

Default Value: N/A

counters

Description: Configure counters for the policer instance.

Value: { enabled | disabled }

Default Value: disabled

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
4.6	Added support for GPON interfaces and added support for filtering the traffic by inner-VLAN and inner-pcp.
4.7	Added support for filtering the traffic by DSCP value.
5.0	Added support for 25G interfaces.

Release	Modification
5.2	Added support for policer instance counters.
5.4	Support multiple VLAN ID in the policer instance.
5.6	Support multiple PCPs in the policer instance.
5.12	Increase maximum number of policers to 1280. DM4770 supports up to 768 ingress and up to 512 egress policers. DM4270 supports up to 512 or 768 ingress and up to 256 or 512 egress policers according to model.

Usage Guidelines

Policer instances can be created to police shared bandwidth or exclusive bandwidth. Interfaces entered in the same policer instance parameter are treated as shared bandwidth.

Examples:

The following example creates one policer instance to police shared bandwidth between two interfaces.

```
#config
Entering configuration mode terminal
(config)# qos policer instance 1
(policer-instance-1)# interface lag-1
(policer-instance-1)# interface ten-gigabit-ethernet-1/5/2
(policer-instance-1)# profile profile1
(policer-instance-1)# vlan 100-102,110
(policer-instance-1)# counters enabled
(policer-instance-1)# top
(config)# commit
Commit complete.
(config)#
```

The following example creates two policer instances to police the same interfaces but as exclusive bandwidths instead of shared.

```
#config
Entering configuration mode terminal
(config)# qos policer instance 1
(policer-instance-1)# interface lag-1
(policer-instance-1)# profile profile1
(policer-instance-1)# pcp 1
(policer-instance-1)# top
(config)# qos policer instance 2
(policer-instance-2)# interface ten-gigabit-ethernet-1/5/2
(policer-instance-2)# profile profile1
(policer-instance-2)# pcp 1-3
```

```
(policer-instance-2)# counters enabled
(policer-instance-1)# top
(config)# commit
Commit complete.
(config)#
```

Impacts and precautions

The priority of a Policer instance is determined by its matching filters. For example, an instance with matching filter by PCP has higher priority than an instance with matching filter by VLAN.

From higher to lower, the priority order is: inner-PCP, PCP, DSCP, inner-VLAN, VLAN.

Instances with multiple matching filters will follow the same priority order. E.g.: The instance with matching filters VLAN 100, PCP 5 and inner-VLAN 500 has higher priority than the instance with matching filter VLAN 100 and inner-VLAN 500. A packet with VLAN 100, PCP 5 and inner-VLAN 500 will be accounted by the first Policer instance, while a packet with VLAN 100, PCP 0 and inner-VLAN 500 will be accounted by the second Policer.

Hardware restrictions

On DM4050, the Policer matching filters do not consider the possible packet modifications due to ACLs rules.

On DM4270, DM4770 and DM4380 series: it is not possible to classify the packets by VLAN when applying an Egress Policer in an interface which is an untagged member of that VLAN.

On DM4770 series: policer instances cannot contain different speed interfaces.

qos policer profile

Description

Create and configure a policer profile for ingress and egress Ethernet traffic policing.

Supported Platforms

This command is supported in all platforms.

Syntax

```
qos policer profile profile-name
mode { flow | srtcm | trtcm | trtcmds }
parameters { cir committed-rate cbs committed-burst eir excess-rate ebs excess-burst
pir peak-rate pbs peak-burst }
{ actions { green | yellow | red } { drop | set-dscp dscp | set-pcp pcp } }
stage { ingress | egress }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

qos policer profile *profile-name*

Description: User defined policer profile name.

Value: String with a maximum of 48 characters. It only accepts alphanumeric characters and '_', '+', and '-'.

Default Value: N/A

mode

Description: Policer configuration mode.

Value:

- **flow:** Single-rate two-color marker mode (flow mode)
- **srtcm:** Single-rate three-color marker mode (RFC 2697)

- **trtcm**: Two-rate three-color marker mode (RFC 2698)
- **trtcmds**: Differentiated Service two-rate three-color marker mode (RFC 4115)

Default Value: flow

cir *committed-rate*

Description: Committed information rate (kbits/s)

Value: 0 - 100,000,000

Default Value: N/A

cbs *committed-burst*

Description: Committed burst size (bytes)

Value: 0 - 268,435,456

Default Value: N/A

eir *excess-rate*

Description: Excess information rate (kbits/s)

Note: this parameter is only available in policer mode **trtcmds**.

Value: 0 - 100,000,000

Default Value: N/A

ebs *excess-burst*

Description: Excess burst size (bytes)

Note: this parameter is only available in policer modes **trtcmds** and **srtcm**.

Value: 0 - 268,435,456

Default Value: N/A

pir *peak-rate*

Description: Peak information rate (kbits/s)

Note: this parameter is only available in policer mode **trtcm**.

Value: 0 - 100,000,000

Default Value: N/A

pbs *peak-burst*

Description:	Peak burst size (bytes) Note: this parameter is only available in policer mode trtcm .
Value:	0 - 268,435,456
Default Value:	N/A

stage

Description:	Interface traffic stage.
Value:	<ul style="list-style-type: none"> • ingress: apply policing to incoming traffic. • egress: apply policing to outgoing traffic.
Default Value:	N/A

actions green

Description:	Actions for green-marked packets.
Value:	<ul style="list-style-type: none"> • drop: Drop packet • set-dscp dscp: Set new value for DSCP (RFC 2474) field • set-pcp pcp: Set new value for PCP (802.1p) field
Default Value:	N/A

actions yellow

Description:	<p>Actions for yellow-marked packets.</p> <p>When the action for green-marked packets is drop, the actions yellow must be drop as well.</p> <p>Note: not configurable in flow mode as there are no yellow-marked packets on this mode.</p>
Value:	<ul style="list-style-type: none"> • drop: Drop packet • set-dscp dscp: Set new value for DSCP (RFC 2474) field • set-pcp pcp: Set new value for PCP (802.1p) field
Default Value:	N/A

actions red

Description: Actions for red-marked packets.
When the action for green-marked or yellow-marked packets is **drop**, the **actions red** must be **drop** as well.

Value:

- **drop:** Drop packet
- **set-dscp** *dscp*: Set new value for DSCP (RFC 2474) field
- **set-pcp** *pcp*: Set new value for PCP (802.1p) field

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.4	This command was introduced.
4.7	Added support for configuring action set-dscp with RFC2474 classes.

Usage Guidelines

Example:

The following example demonstrates how to create a policer profile. This policer will make red-marked packets be dropped at ingress stage.

```
#config
Entering configuration mode terminal
(config)# qos policer profile poll
(policer-profile-poll)# mode flow
(policer-profile-poll)# stage ingress
(policer-profile-poll)# parameters cbs 100000
(policer-profile-poll)# parameters cir 1000000
(policer-profile-poll)# actions red drop
(policer-profile-poll)# top
(config)# commit
Commit complete.
(config)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show qos policer

Description

Displays statistics counters for policer instances.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show qos policer [brief] [detail]
```

Parameters

brief

Description: This parameter displays summary information about each policer: instance ID, hierarchical ID, profile name, policer mode, policer stage, CIR, EIR, PIR, interface index, interface name and policer counters (forwarded bytes and dropped bytes). When no parameter is given the show command displays the same content of **brief** parameter.

Value: N/A

Default Value: N/A

detail

Description: Includes all data presented by **brief**, and includes extra data about hierarchical policers: CIR, EIR, PIR, and policer counters (forwarded bytes and dropped bytes).

Value: N/A

Default Value: N/A

hierarchical

Description: This parameter displays only the information related to hierarchical policers.

Value: N/A

Default Value: N/A**Output Terms**

Output	Description
INSTANCE ID	Policer instance id.
HIERARCHICAL ID	Hierarchical policer ID.
PROFILE	Configured profile for a policer instance, either a regular or hierarchical policer.
MODE	Mode of operation for a policer instance, either a regular or hierarchical policer.
STAGE	Stage of policer (ingress or egress).
CIR	Committed information rate in kbits/s.
EIR	Excess information rate in kbits/s.
PIR	Peak information rate in kbits/s.
FORWARDED	Number of forwarded bytes for a given policer instance.
DROPPED	Number of dropped bytes for a given policer instance.
IF-INDEX	Index of the interface configured with a policer instance.
IF-NAME	Name of the interface configured with a policer instance.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.2	This command was introduced.
6.0	Added support for hierarchical policer.

Usage Guidelines

Given the equipment has two policer profiles named foo and bar configured with the flow mode, the command could result in the following output:

```
# show qos policer
```

INSTANCE ID	HIERARCHICAL ID	PROFILE	MODE	STAGE	CIR	EIR	PIR	FORWARDED	DROPPED	IFINDEX	INTERFACE
1	1	foo	flow	ingress	10000	-	-	1000	100	51412993	gigabit-e
2	1	foo	flow	ingress	10000	-	-	2000	200	51412994	gigabit-e
3	2	foo	flow	ingress	10000	-	-	3000	300	51412995	gigabit-e

Note: When a counter is disabled or unsupported it is displayed as '--'

HIERARCHICAL ID	PROFILE	MODE	STAGE	CIR	INSTANCE ID	PROFILE
1	bar	flow	ingress	20000	1	foo
					2	foo
2	bar	flow	ingress	20000	3	foo

Now let's see the **detail** information:

```
# show qos policer detail
```

INSTANCE ID	HIERARCHICAL ID	PROFILE	MODE	STAGE	CIR	EIR	PIR	FORWARDED	DROPPED	IFINDEX	INTERFACE
1	1	foo	flow	ingress	10000	-	-	1000	100	51412993	gigabit-e
2	1	foo	flow	ingress	10000	-	-	2000	200	51412994	gigabit-e
3	2	foo	flow	ingress	10000	-	-	3000	300	51412995	gigabit-e

Note: When a counter is disabled or unsupported it is displayed as '--'

HIERARCHICAL ID	PROFILE	MODE	STAGE	CIR	INSTANCE ID	PROFILE	CIR	EIR	PIR	FORWARDED	DROPPED
1	bar	flow	ingress	20000	1	foo	10000	-	-	1000	100
					2	foo	10000	-	-	2000	200

```
2          bar      flow ingress 20000 3          foo      10000 -      -      3000      300
```

Impacts and precautions

The values presented by this command are accumulated since the last time the operator issued a clear command.

Hardware restrictions

On DM461x, the dropped counters on the egress stage are not supported.

show qos policer resources

Description

Displays information about the use of policer resources.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show qos policer resources
```

Parameters

N/A

Output Terms

Output	Description
<code>qos policer total ingress resources</code>	Total ingress policer resources.
<code>qos policer used ingress resources</code>	Used ingress policer resources.
<code>qos policer free ingress resources</code>	Free ingress policer resources.
<code>qos policer total egress resources</code>	Total egress policer resources.
<code>qos policer used egress resources</code>	Used egress policer resources.

Output	Description
<code>qos policer free egress resources</code>	Free egress policer resources.
<code>INSTANCE ID</code>	Policer instance id.
<code>HIERARCHICAL ID</code>	Hierarchical policer ID.
<code>PROFILE</code>	Configured profile for a policer instance, either a regular or hierarchical policer.
<code>STAGE</code>	Stage of policer (ingress or egress).
<code>RESOURCES</code>	Number of resources used by this policer instance, either a regular or hierarchical policer.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.4	This command was introduced.

Release	Modification
---------	--------------

6.0	Added support for hierarchical policer.
-----	---

Usage Guidelines

Given the equipment has four policer instances and one hierarchical policer containing one of these instances, this command would result in the following output:

```
# show qos policer resources
STAGE      TOTAL  USED  FREE
-----
ingress    256    22   234
egress     128    76    52

INSTANCE   HIERARCHICAL
ID          ID          PROFILE  STAGE  RESOURCES
-----
1           1           foo      ingress 1
2           -           foo      ingress 20
3           -           bar      egress  12
4           -           bar      egress  64

HIERARCHICAL  PROFILE  STAGE  RESOURCES  INSTANCE
ID            ID            ID            ID            ID
-----
1            foo      ingress  1            1            foo
```

Impacts and precautions

N/A

Hardware restrictions

N/A

QOS PACKET SCHEDULER AND EGRESS SHAPERS

This topic describes the commands related to QoS Packet Scheduler such as commands to configure Strict Priority or Early Discard at individual queues, and commands to set rate limits at egress interfaces.

qos interface scheduler-profile

Description

Set a QoS Scheduler Profile into an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

qos interface *interface-identification* [**scheduler-profile** {*profile-name*}]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-identification

Description: Identifies the interface to be configured.

Value: *interface-type-chassis/slot/port*
Where *interface-type* can assume **gigabit-ethernet**, **ten-gigabit-ethernet**, **forty-gigabit-ethernet** or **gpon**.

Default Value: N/A

scheduler-profile *profile-name*

Description: The profile name to be set in specified interface. It MUST assume one of the previous created profiles.

Value: String

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.
3.0	Added support for 40G interfaces.

Usage Guidelines

This command associates a QoS Scheduler Profile to a specific interface. To set a QoS Scheduler Profile to an interface you have to first create the QoS Scheduler Profile:

```
DMOS(config)# qos scheduler-profile testXYZ
DMOS(config-qos-scheduler-profile-testXYZ)# mode wfq
DMOS(config-qos-scheduler-profile-testXYZ)# queue 0 weight 5
DMOS(config-qos-sch-prof-queue-0)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 1 weight 5
DMOS(config-qos-sch-prof-queue-1)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 2 weight 5
DMOS(config-qos-sch-prof-queue-2)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 3 weight 5
DMOS(config-qos-sch-prof-queue-3)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 4 weight 5
DMOS(config-qos-sch-prof-queue-4)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 5 weight 5
DMOS(config-qos-sch-prof-queue-5)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 6 weight 70
DMOS(config-qos-sch-prof-queue-6)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 7 weight SP
DMOS(config-qos-sch-prof-queue-7)# top
DMOS(config)# commit
Commit complete.
DMOS(config)#
```

Now let's associate the created profile to an interface:

```
DMOS(config)# qos interface gigabit-ethernet 1/1/1 scheduler-profile testXYZ
DMOS(config-qos-interface-gigabit-ethernet 1/1/1)#
```

After that let's check the config and commit it:

```
DMOS(config-qos-interface-gigabit-ethernet 1/1/1)# top
DMOS(config)# show full-configuration
qos interface gigabit-ethernet 1/1/1
  scheduler-profile testXYZ
!
qos scheduler-profile testXYZ
  mode wfq
  queue 0
    weight 5
  !
  queue 1
    weight 5
  !
  queue 2
    weight 5
  !
  queue 3
    weight 5
  !
  queue 4
    weight 5
  !
  queue 5
    weight 5
  !
  queue 6
    weight 70
  !
  queue 7
    weight SP
  !
!
DMOS(config)# commit
Commit complete.
DMOS(config)#
```

Impacts and precautions

Using SP for a queue's weight could cause starvation for other queues.

Hardware restrictions

None

qos scheduler-profile

Description

Configure a QoS Scheduler profile to be applied on interfaces.

Supported Platforms

This command is supported in all platforms.

Syntax

qos scheduler-profile *profile-name* [**mode** {**wfq**} | **queue** *queue-index* [**weight** *weight-value*]]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

profile-name

Description: The QoS Scheduler profile identifier. This value is used to distinguish the various profiles. It's possible to create up to 500 different profiles.

Value: String

Default Value: N/A

mode

Description: Define the QoS Scheduling mode.

Value: *wfq* (Weighted Fair Queue)

Default Value: N/A

queue

Description: Perform configuration of a specific scheduler queue.

Value: 0-7

Default Value: N/A

weight

Description:	Weight of an specific queue related to the pre-selected scheduling mode. It can assume a numeric percent bandwidth value or the Strict Priority (SP) tag.
Value:	1-100 SP
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.

Usage Guidelines

This command is used to define a QoS Scheduler Profile. After it's done, it's necessary to associate the profile to an interface in order to the QoS profile take effect over the outgoing traffic of the interface.

Each profile can have only one scheduling mode at a time. Once the mode is set it enables the queues' creation and configuration. Each mode must have all its queues created and configured with a weight. The weight represents the percentage of available bandwidth, and the sum of the weights must be 100.

The current supported scheduling mode is WFQ (Weighted Fair Queue), which balances the egress traffic according to the weights set in its queues. The scheduling is based on bytes.

To configure a QoS Scheduler Profile the first thing to do is to create the profile:

```
DM4610(config)# qos scheduler-profile testXYZ
DM4610(config-profile-testXYZ)#
```

Now let's configure the scheduling mode:

```
DM4610(config-profile-testXYZ)# mode wfq
DM4610(config-profile-testXYZ)#
```

Then it's necessary to configure all queues:

```
DMOS(config)# qos scheduler-profile testXYZ
DMOS(config-qos-scheduler-profile-testXYZ)# mode wfq
DMOS(config-qos-scheduler-profile-testXYZ)# queue 0 weight 5
DMOS(config-qos-sch-prof-queue-0)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 1 weight 5
DMOS(config-qos-sch-prof-queue-1)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 2 weight 5
DMOS(config-qos-sch-prof-queue-2)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 3 weight 5
DMOS(config-qos-sch-prof-queue-3)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 4 weight 5
DMOS(config-qos-sch-prof-queue-4)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 5 weight 5
DMOS(config-qos-sch-prof-queue-5)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 6 weight 70
DMOS(config-qos-sch-prof-queue-6)# exit
DMOS(config-qos-scheduler-profile-testXYZ)# queue 7 weight SP
DMOS(config-qos-sch-prof-queue-7)# exit
DMOS(config-qos-scheduler-profile-testXYZ)#
```

Now let's check the configuration and commit it:

```
DMOS(config-qos-scheduler-profile-testXYZ)# top
DMOS(config)# show full-configuration
qos scheduler-profile testXYZ
  mode wfq
  queue 0
    weight 5
  !
  queue 1
    weight 5
  !
  queue 2
    weight 5
  !
  queue 3
    weight 5
  !
  queue 4
    weight 5
  !
  queue 5
    weight 5
  !
  queue 6
    weight 70
  !
  queue 7
    weight SP
  !
DMOS(config)# commit
Commit complete.
DMOS(config)#
```

Impacts and precautions

Using SP for a queue's weight could cause starvation for other queues.

To remove a profile it's necessary to remove all interfaces assignments to the referred profile.

So in the following scenario to remove myProfile1 we have to:

```
DMOS(config)# show full-configuration
qos interface gigabit-ethernet 1/1/1
  scheduler-profile myProfile1
!
qos interface gigabit-ethernet 1/1/2
  scheduler-profile myProfile2
!
qos scheduler-profile myProfile1
  mode wfq
  (...)
!
qos scheduler-profile myProfile2
  mode wfq
  (...)
!
DMOS(config)# qos interface gigabit-ethernet 1/1/1
DMOS(config-qos-interface-gigabit-ethernet 1/1/1)# no scheduler-profile
DMOS(config-qos-interface-gigabit-ethernet 1/1/1)# top
DMOS(config)# no qos scheduler-profile myProfile1
DMOS(config)# commit
Commit complete.
DMOS(config)#
```

Hardware restrictions

N/A

rate-limit

Description

Limits the traffic of an interface according to a configurable bandwidth and burst.

Supported Platforms

This command is supported in all platforms.

Syntax

rate-limit { **egress** | **ingress** } **bandwidth** *value* **burst** *value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

egress

Description:	Configure rate-limit parameters to egress traffic.
Value:	N/A
Default Value:	N/A

ingress

Description:	Configure rate-limit parameters to ingress traffic.
Value:	N/A
Default Value:	N/A

bandwidth *value*

Description:	Bandwidth, in kbps, to limit the traffic.
Value:	100-1000000000
Default Value:	N/A

burst *value*

Description:	Accepted burst rate in kbytes.
Value:	2-2000

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.12	This command was introduced.
2.0	Added rate-limit mode ingress.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
5.1	Added support for 25G interfaces.
7.0	Removed support for 25G, 40G and 100G interfaces.

Usage Guidelines

This command is located inside **qos** node. So, to configure a rate limit into an interface follow these steps:

Access the interface in **qos** node.


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

Now access the rate limit configuration informing the traffic flow to be limited. Suppose **egress** traffic:

```
DmOS(config-qos-interface-gigabit-ethernet-1/1/1)# rate-limit egress
DmOS(config-rate-limit-egress)#
```

Now configure the **bandwidth** and **burst** to limit the interface. Both parameters are required. At the end of configuration, commit it:

```
DmOS(config-rate-limit-egress)# bandwidth 64000
DmOS(config-rate-limit-egress)# burst 1024
DmOS(config-rate-limit-egress)# commit
Commit complete.
DmOS(config-rate-limit-egress)#
```

Impacts and precautions

N/A

Hardware restrictions

- ingress rate-limit is not supported on DM4270, DM4770 and DM4380 series.

STORM CONTROL

This topic describes the commands related to Storm Control such as commands to configure multicast, broadcast and unknown unicast(DLF) rate limits.

switchport interface storm-control

Description

Configure Storm Control protection to an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

switchport interface *interface-identification* [**storm-control** { **broadcast** *percent* | **multicast** *percent* | **unicast** *percent* }*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-identification

Description: Identifies the ingress interface to be configured.

Value: *interface-type-chassis/slot/port*
Where *interface-type* can assume **gigabit-ethernet**, **ten-gigabit-ethernet**, **twenty-five-g-ethernet**, **forty-gigabit-ethernet**, **hundred-gigabit-ethernet** or **lag**.

Default Value: N/A

broadcast *percent*

Description: Specifies a rate-limit on an ingress interface for broadcast packets as a percentage of the interface's nominal speed in steps of 0.01.

Value: 0.01-100.00

Default Value: N/A

multicast *percent*

Description: Specifies a rate-limit on an ingress interface for unknown multicast packets as a percentage of the interface's nominal speed in steps of 0.01.

Value: 0.01-100.00

Default Value: N/A

unicast *percent*

Description: Specifies a rate-limit on an ingress interface for unknown unicast (DLF) packets as a percentage of the interface's nominal speed in steps of 0.01.

Value: 0.01-100.00

Default Value: N/A

Default

Disabled

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.1	This command was introduced.
-----	------------------------------

3.0	Added support for 40G and LAG interfaces.
-----	---

Release	Modification
4.6	Added support for 100G interfaces.
5.1	Added support for 25G interfaces.

Usage Guidelines

The following commands enable storm-control for ingress traffic on interface *gigabit-ethernet-1/1/1*, with rate-limit of 0.5% of interface's nominal speed for broadcast packets, 10% for unknown multicast packets and 1% for unknown unicast (DLF) packets:

```
DMOS(config)# switchport interface gigabit-ethernet-1/1/1
DMOS(config-switchport-gigabit-ethernet-1/1/1)# storm-control
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# broadcast 0.5
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# multicast 10
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# unicast 1
```

Check the configuration and commit it so it is applied:

```
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# top
DMOS(config)# show configuration this switchport interface gigabit-ethernet-1/1/1 storm-control
switchport
interface gigabit-ethernet-1/1/1
storm-control
broadcast 0.5
multicast 10.0
unicast 1.0
!
!
!
DMOS(config)# commit
Commit complete.
DMOS(config)#
```

Precede the command with *no* to disable Storm Control. The following commands disable Storm Control multicast for interface *gigabit-ethernet-1/1/1*, and then disable all types of Storm Control for the same interface:

```
DMOS(config)# switchport interface gigabit-ethernet-1/1/1
DMOS(config-switchport-gigabit-ethernet-1/1/1)# storm-control
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# no multicast
DMOS(config-switchport-gigabit-ethernet-1/1/1-storm-ctrl)# exit
DMOS(config-switchport-gigabit-ethernet-1/1/1)# commit
Commit complete.
DMOS(config-switchport-gigabit-ethernet-1/1/1)# no storm-control
DMOS(config-switchport-gigabit-ethernet-1/1/1)# commit
Commit complete.
```

Impacts and precautions

Enabling Storm Control may result in unexpected lost of packets. You can use the command: **show interface interface-identification statistics** to verify possible dropped

packets.

Hardware restrictions

N/A

CHAPTER 10: ACCESS LISTS

This chapter describes the commands related to management of ACLs in the DmOS CLI.

BASIC ACLS

This topic describes the commands related to management of ACLs such as commands to configure match criteria or actions.

access-list acl-profile

Description

This command is used to create or enter an Access List Profile. The profile can contain multiple ACL entries used to specify match and action criteria. ACL profiles have priorities among them. An ACL profile must have at least one ACL entry configured. For a profile to take effect, it needs to be applied to an interface. L2 profiles always have priority over L3 profiles.

Supported Platforms

This command is supported in all platforms.

Syntax

acl-profile *stage type name* **priority** *priority*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

stage

Description:	The ACL profile stage. <i>ingress</i> stage ACLs will affect traffic entering the configured interfaces. <i>cpu</i> stage ACLs will affect traffic entering the CPU.
Value:	{ingress cpu}

Default Value: N/A

type

Description: The ACL profile type.

Value: {I2 | I3}

Default Value: N/A

name

Description: The ACL profile name.

Value: Text

Default Value: N/A

priority

Description: The ACL profile priority, being 0 the highest priority. L2 profiles can have priorities from 0 to 255 and L3 profiles can have priorities from 256 to 511.

Value: 0-511

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.1	This command was introduced.
-----	------------------------------

5.0	Added new stage <i>cpu</i> .
-----	------------------------------

Usage Guidelines

Creating a L2 Access List Profile at ingress stage with name *my_acl_profile* and priority 0:

```
(config)# access-list
(config-acl)# acl-profile ingress l2 my_acl_profile
(config-acl-profile-l2-my_acl_profile)# priority 0
```

Adding an entry to the profile:

```
(config-acl-profile-l2-my_acl_profile)# access-list-entry 0 action deny
(config-access-list-entry-0)# match vlan 10
```

Apply the profile to an interface so the profile can take effect:

```
(config)# access-list interface gigabit-ethernet-1/1/1 ingress my_acl_profile
```

Impacts and precautions

ACL Rules created with L2 profiles will match only pure Ethernet headers. If the Ethernet header is encapsulated over any protocol, the rule will not apply.

ACL Rules created with L3 profiles will match only L3 packets encapsulated over Ethernet header (i.e. if the L3 packet is encapsulated over PPPoE, or other non Ethernet L2 header, the match will not apply).

Hardware restrictions

N/A

access-list interface

Description

This command is used to attach a given ACL profile to an interface.

Supported Platforms

This command is supported in all platforms.

Syntax

interface *interface-name stage profile-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface-name

Description:	The interface identification.
Value:	<i>interface-type-chassis/slot/port</i> Examples of <i>interface-type</i> : gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet, gpon, cpu-port.
Default Value:	N/A

stage

Description:	The ACL profile stage. <i>ingress</i> stage ACLs will affect traffic entering the configured interfaces.
Value:	ingress
Default Value:	N/A

profile-name

Description:	The ACL profile name.
Value:	Text

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.1	This command was introduced.
3.0	Added support for 40G interfaces.
4.6	Added support for 100G interfaces.
5.0	Added support for 25G interfaces.

Usage Guidelines

Given a profile named *l2-ingress-acl*, the following sequence of commands will apply it on port *gigabit-ethernet-1/1/1*:

```
(config)# access-list
(config-acl)# interface gigabit-ethernet-1/1/1 ingress l2-ingress-acl
(config-acl)# commit
```

You can apply the same profile to several interfaces. You can also apply more than one profile to the same interface.

Impacts and precautions

Every device has a different amount of ACL resources to be used. The resources are consumed when the profile is applied to an interface. Please refer to the hardware restriction section for more information about how they operate on each hardware.

Hardware restrictions

The maximum number of ACL rules will depend on the amount of entries applied to all interfaces. DM4610 supports up to 256 entries per profile type (L2 or L3) applied to all interfaces. For instance, when a L2 profile with 128 entries is applied to two interfaces, no new L2 rules will be allowed to be applied.

access-list protection

Description

This command is used to apply a given ACL profile to the traffic with CPU destination. It is aimed to allow the user to protect the CPU from malicious traffic data.

Supported Platforms

This command is supported in all platforms.

Syntax

protection *stage profile-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

stage

Description:	The ACL profile stage. <i>cpu</i> stage ACLs will affect traffic entering the CPU.
Value:	cpu
Default Value:	N/A

profile-name

Description:	The ACL profile name.
Value:	Text
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

To protect the CPU, it is recommended to create an access-list with a White List that blocks all the access to a certain TCP/UDP Destination-Port, and accept connection only from trusted sources: **Example:**

```
#config
Entering configuration mode terminal
(config)# access-list
(config-acl)# acl-profile cpu l3 whitelist
(config-acl-profile-l3-whitelist)# priority 0
(config-acl-profile-l3-whitelist)# access-list-entry 0 action permit
(config-access-list-entry-0)# match source-ipv4-address 10.10.0.1
(config-access-list-entry-0)# exit
(config-acl-profile-l3-whitelist)# access-list-entry 1 action permit
(config-access-list-entry-0)# match source-ipv4-address 10.10.1.0/24
(config-access-list-entry-0)# exit
(config-acl-profile-l3-whitelist)# access-list-entry 100 action deny
(config-access-list-entry-0)# match destination-port ssh
(config-access-list-entry-0)# top
(config)# access-list
(config-acl)# protection cpu whitelist
(config-acl)# commit
```

Impacts and precautions

Every device has a different amount of ACL resources to be used. The resources on *cpu* stage are consumed when the profile is applied as a protection profile.

Hardware restrictions

N/A

access-list-entry

Description

Manages Access List Entries at an Access List Profile. Access list entries must contain at least one match and one action.

Supported Platforms

This command is supported in all platforms.

Syntax

access-list-entry *entry-id*

access-list-entry *entry-id* [**match source-mac-address** *mac-address* [**match source-mac-address-mask** *mac-address-mask*]] [**match destination-mac-address** *mac-address* [**match destination-mac-address-mask** *mac-address-mask*]] [**match ethertype** *ether-type*] [**match pcnp** *pcnp*] [**match vlan** *vid*] [**match inner-pcnp** *pcnp*] [**match inner-vlan** *vid*] [**match dscp** *dscp* | **match tos** *tos*] [**match source-ipv4-address** *ipv4-address*] [**match destination-ipv4-address** *ipv4-address*] [**match ip-protocol** *ip-protocol*] [**match destination-port** *destination-port*] [**match source-port** *source-port*] [**match ttl** *ttl*]

access-list-entry *entry-id* **action** {**deny** | **permit** | **redirect** | **copy pcnp** | **set pcnp** *pcnp* | **set inner-pcnp** *pcnp* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

entry-id

Description: The ACL entry identifier. This value will be used as the relative priority among other ACL entries from the same ACL profile, being 0 the highest priority.

Value: 0-255

Default Value: N/A

match source-mac-address *mac-address*

Description: The source MAC address of a match.

Available at stages: *ingress*.

Available at types: *L2*.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

match source-mac-address-mask *mac-address-mask*

Description: A wildcard mask for the source MAC address of a match. This mask is sometimes referred to as an inverse mask because a 1 and 0 mean the opposite of what they mean in a subnet (network) mask. Only bits corresponding to “0” are considered from MAC. Bits with “1” are ignored.

This match is only available if a match for a source MAC address has been configured.

Available at stages: *ingress*.

Available at types: *L2*.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

match destination-mac-address *mac-address*

Description: The destination MAC address of a match.

Available at stages: *ingress*.

Available at types: *L2*.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

match destination-mac-address-mask *mac-address-mask*

Description: A wildcard mask for the destination MAC address of a match. This mask is sometimes referred to as an inverse mask because a 1 and 0 mean the opposite of what they mean in a subnet (network) mask. Only bits corresponding to “0” are considered from MAC. Bits with “1” are ignored.

This match is only available if a match for a destination MAC address has been configured.

Available at stages: *ingress*.

Available at types: *L2*.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

match ethertype *ethertype*

Description: The Ethernet type code for a match.

Available at stages: *ingress, cpu*.

Available at types: *L2* (on *ingress* stage), *L3* (on *cpu* stage).

Value: 0x0000-0xffff | arp | bpdu | ipv4 | ipv6 | mpls | mpls-mcast |
pppoed | pppoes | snmp

Default Value: N/A

match pcp *pcp*

Description: Outer priority 802.1p for a match.

Available at stages: *ingress*.

Available at types: *L2, L3*.

Value: 0-7

Default Value: N/A

match vlan *vid*

Description: Outer VLAN ID for a match.

Available at stages: *ingress, cpu*.

Available at types: *L2, L3*.

Value: 1-4094

Default Value: N/A

match inner-pcp *pcp*

Description: Inner priority 802.1p for a match.

The inner Priority 802.1p is the PCP in the second VLAN Tag after ingress VLAN manipulations (QinQ/Vlan Translations). It is applicable only to double tagged packets.

Available at stages: *ingress*.

Available at types: *L2, L3*.

Value: 0-7

Default Value: N/A

match inner-vlan *vid*

Description: Inner VLAN ID for a match.
The inner VLAN is the second VLAN Tag after ingress VLAN manipulations (QinQ/Vlan Translations). It is applicable only to double tagged packets.

Available at stages: *ingress*.

Available at types: *L2, L3*.

Value: 1-4094

Default Value: N/A

match dscp *dscp*

Description: The Differentiated Services Code Point code for a match.
Remark: DSCP match can not be configured with ToS match in the same entry.

Available at stages: *ingress*.

Available at types: *L3*.

Value: 0-63 | 0 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef

Default Value: N/A

match tos *tos*

Description: The IPv4 Type of Service or IPv6 Traffic Class for a match.
Remark: ToS match can not be configured with DSCP match in the same entry.

Available at stages: *ingress*.

Available at types: *L3*.

Value: 0-255

Default Value: N/A

match source-ipv4-address *ipv4-address*

Description: The source IPv4 address and an optional mask of a match.

Available at stages: *ingress, cpu*.

Available at types: *L3*.

Value: [a.b.c.d | a.b.c.d/x]

Default Value: N/A

match destination-ipv4-address *ipv4-address*

Description: The destination IPv4 address and an optional mask of a match.

Available at stages: *ingress, cpu*.

Available at types: *L3*.

Value: [a.b.c.d | a.b.c.d/x]

Default Value: N/A

match ip-protocol *ip-protocol*

Description: The IPv4 or IPv6 protocol field of a match.

Available at stages: *ingress, cpu*.

Available at types: *L3*.

Value: 0-255 | icmp | igmp | ipv6-icmp | tcp | udp

Default Value: N/A

match destination-port *destination-port*

Description: TCP/UDP destination port number of a match.

Available at stages: *ingress, cpu*.

Available at types: *L3*.

Value: 0-65535 | bgp | dns | ftpdata | ftpcontrol | http | https | ntp | smb | snmp | snmptrap | ssh | telnet | whois

Default Value: N/A

match source-port *source-port*

Description: TCP/UDP source port number of a match.

Available at stages: *cpu*.

Available at types: *L3*.

Value: 0-65535 | bgp | dns | ftpdata | ftpcontrol | http | https | ntp | smb | snmp | snmptrap | ssh | telnet | whois

Default Value: N/A

match ttl *ttl*

Description: IPv4 TTL or IPv6 Hop Limit field.

Available at stages: *cpu*.

Available at types: *L3*.

Value: 0-255

Default Value: N/A

action deny

Description: Action to deny, i.e. drop any packets matching the filter.

Available at stages: *ingress, cpu*.

Available at types: *L2, L3*.

Value: N/A

Default Value: N/A

action permit

Description: Action to permit, i.e. allow any packets that was blocked by a deny rule.

Available at stages: *ingress, cpu*.

Available at types: *L2, L3*.

Value: N/A

Default Value: N/A

action redirect

Description: Action to redirect, i.e. redirect any packets matching the filter to an specific queue.

Available at stages: *cpu*.

Available at types: *L3*.

Value: N/A

Default Value: N/A

action copy pcp

Description: Action to copy the PCP field value from inner VLAN tag of the frame to the outer VLAN tag.

Available at stages: *ingress*.

Available at types: *L2, L3*.

This action can not be configured if already exists action set *pcp*.

Value: N/A

Default Value: N/A

action set pcp pcp

Description: Action to set or replace the PCP field value of the frame with parameter set in action.
This action also schedules the packet to a QoS scheduling queue. Please refer to the QoS chapters for more information about the QoS features.

Available at stages: *ingress*.

Available at types: *L2, L3*.

This action can not be configured if already exists action *copy pcp*.

Value: 0-7

Default Value: N/A

action set inner-pcp pcp

Description: Action to set or replace the PCP field value of the inner VLAN tag in frame with parameter set in action.

Available at stages: *ingress*.

Available at types: *L2, L3*.

This action is not available for DM4050 and DM4250 series.

Value: 0-7

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.
1.1	Removed actions <i>set DSCP</i> and <i>set queue</i> . Added action <i>permit</i> . Removed match <i>interface</i> .
3.0	Added new L3 matches: <i>ip-protocol</i> and <i>destination-port</i> .
4.4	Added new L3 matches: <i>vlan</i> and <i>pcp</i> .
4.6	Added new L3 match: <i>tos</i>
4.7	Added new L2 and L3 matches: <i>inner-vlan</i> and <i>inner-pcp</i> .
4.8	Added action <i>set inner-pcp</i> on ingress ACLs.

Release	Modification
5.0	Added new stage <i>cpu</i> , and matches <i>source-port</i> and <i>ttl</i>
5.6	Added action <i>copy pcp</i> on ingress ACLs.
7.0	Added action <i>redirect</i> on cpu ACLs.

Usage Guidelines

As ACL entries must be in an ACL profile, it is necessary first to create an Access List Profile. The profile needs a stage, type, priority and name. In this case the stage is *ingress*, the type is *L2*, the name is *l2-ingress-acl* and the priority *0*:

```
(config)# access-list acl-profile ingress l2 l2-ingress-acl
(config-acl-profile-l2-l2-ingress-acl)# priority 0
```

The ACL entry must be created with its *id* as well:

```
(config-acl-profile-l2-l2-ingress-acl)# access-list-entry 2
(config-access-list-entry-2)#
```

Then it is possible to add matches and actions, for instance, to deny all ingress traffic with *VLAN tag 10*:

```
(config-access-list-entry-2)# match vlan 10
(config-access-list-entry-2)# action deny
```

It is possible to augment this entry with more matches of type *L2*. For instance, adding a match to the source MAC address with a mask will start blocking only traffic from that VLAN with the specified set of MAC addresses.

```
(config-access-list-entry-2)#
  match source-mac-address 00:00:00:00:00:ad
  match source-mac-address-mask ff:ff:ff:ff:ff:00
```

In this case, the match specifies all MAC addresses that ends with the *ad* octet.

In the end, you must apply the profile created to an *interface* for the entry to take effect.

```
(config)# access-list
(config-acl)# interface gigabit-ethernet-1/1/1 ingress l2-ingress-acl
(config-acl)# commit
```

After the commit, all packets arriving on interface *gigabit-ethernet-1/1/1* with a VLAN tag of *10* and source MAC address ending in *ad* will be dropped.

Impacts and precautions

None

Hardware restrictions

DM4050 and DM4250 series do not support *action set inner-pcp*.

show acl-resources

Description

This command is used to display the ACL resources status.

Supported Platforms

This command is supported in all platforms.

Syntax

show acl-resources [brief | detail | extensive]

show acl-resources [interface [*interface-name*]] [detail | extensive]

Parameters

brief

Description:	This parameter displays a summary information split into two big groups: L2 ACL resources and L3 ACL resources.
Value:	N/A
Default Value:	None

detail

Description:	This parameter displays detailed ACL resources information about the profiles and general ACL interfaces resources information.
Value:	N/A
Default Value:	None

extensive

Description:	This parameter displays detailed ACL resources information about the profiles and the interface information discriminating the resources spent by each profile in each interface.
Value:	N/A
Default Value:	None

interface

Description: This parameter displays only ACL resources information related to interfaces.

Value: N/A

Default Value: None

interface-name

Description: This parameter displays resources information of a specific interface.

Value: N/A

Default Value: None

Output Terms

Output	Description
<code>Total entries</code>	Total number of entries available on hardware.
<code>Used entries</code>	Number of hardware resources spent.
<code>Free entries</code>	Number of unused resources.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

2.0	This command was introduced.
-----	------------------------------

5.0	Added new stage <i>cpu</i> .
-----	------------------------------

Usage Guidelines

Given the equipment has a total of 256 entries for ingress L2 ACLs, 256 entries for ingress L3 ACLs and 256 entries for CPU L3 ACLs, and the following configuration is applied:

```
DmOS# show running-config
access-list
 interface gigabit-ethernet-1/1/1
 ingress testL2
 !
 interface gigabit-ethernet-1/1/2
 ingress testL2 testL3-OneEntry
 !
 interface gigabit-ethernet-1/1/3
 ingress testL2 testL3-OneEntry testL3-ZeroEntries
 !
acl-profile ingress 12 testL2
 priority 0
 access-list-entry 0
 action permit
 !
 access-list-entry 1
 action permit
 !
 !
acl-profile ingress 13 testL3-OneEntry
 priority 256
 access-list-entry 0
 action permit
 !
 !
acl-profile ingress 13 testL3-ZeroEntries
 priority 257
 !
 !
acl-profile cpu 13 cpuL3
 priority 1
 access-list-entry 0
 action permit
 !
 access-list-entry 1
 action permit
 !
 access-list-entry 2
 action permit
 !
 !
```

To display just a summary of resources use **show acl-resources brief**:

```
DmOS# show acl-resources brief

Total ingress L2 entries: 256
Used ingress L2 entries:   6
Free ingress L2 entries:  250
```

```

Total ingress L3 entries: 256
Used ingress L3 entries:  2
Free ingress L3 entries: 254

Total CPU L3 entries:    256
Used CPU L3 entries:    3
Free CPU L3 entries:    253

```

Note that the *testL3-ZeroEntries* does not count towards **Used L3 entries** just because it does not have any entry inside it.

To display a detailed information of resources use **show acl-resources detail**. This command will display the amount of used entries by profile, summing all interfaces that use that profile, and the amount of used entries per interface summing all profiles that the interface uses:

```
DmOS# show acl-resources detail
```

ACL Ingress L2 Profile	Used entries
testL2	6
TOTAL	6

ACL Ingress L3 Profile	Used entries
testL3-OneEntry	2
testL3-ZeroEntries	0
TOTAL	2

ACL CPU L3 Profile	Used entries
cpuL3	3
TOTAL	3

Interface	Used L2 Entries	Used L3 Entries
gigabit-ethernet-1/1/1	2	
gigabit-ethernet-1/1/2	2	1
gigabit-ethernet-1/1/3	2	1
TOTAL	6	2

To display an extensive information use **show acl-resources extensive** command. The description of the profiles will be the same as in **show acl-resources detail**, but the description of the interfaces will name all profiles that are consuming entries on that particular interface, instead of just the entry amount:

```
DmOS# show acl-resources extensive
```

ACL Ingres L2 Profile	Used entries
testL2	6
TOTAL	6

ACL Ingress L3 Profile	Used entries
testL3-OneEntry	2
testL3-ZeroEntries	0
TOTAL	2

ACL CPU L3 Profile	Used entries
cpuL3	3

```

-----
TOTAL                                                    3
=====
= gigabit-ethernet-1/1/1                                =
=====

ACL Ingress L2 Profile                                Used entries
-----
testL2                                                    2
-----
TOTAL                                                    2
=====
= gigabit-ethernet-1/1/2                                =
=====

ACL Ingress L2 Profile                                Used entries
-----
testL2                                                    2
-----
TOTAL                                                    2
=====

ACL Ingress L3 Profile                                Used entries
-----
testL3-OneEntry                                           1
-----
TOTAL                                                    1
=====
= gigabit-ethernet-1/1/3                                =
=====

ACL Ingress L2 Profile                                Used entries
-----
testL2                                                    2
-----
TOTAL                                                    2
=====

ACL Ingress L3 Profile                                Used entries
-----
testL3-OneEntry                                           1
testL3-ZeroEntries                                        0
-----
TOTAL                                                    1

```

When it's necessary to display only information about the interfaces, or about a specific interface, it's possible to use **show acl-resources interface** or **show acl-resources interface interface-name**. These commands can also be followed by **detail** and **extensive** marks:

```

DmOS# show acl-resources interface detail

Interface                                Used L2 Entries  Used L3 Entries
-----
gigabit-ethernet-1/1/1                    2
gigabit-ethernet-1/1/2                    2                1
gigabit-ethernet-1/1/3                    2                1
-----
TOTAL                                    6                2

DmOS# show acl-resources interface extensive
=====
= gigabit-ethernet-1/1/1                                =
=====

ACL Ingress L2 Profile                                Used entries
-----
testL2                                                    2
-----
TOTAL                                                    2
=====
= gigabit-ethernet-1/1/2                                =
=====

ACL Ingress L2 Profile                                Used entries
-----
testL2                                                    2
-----

```

```

TOTAL 2
ACL Ingress L3 Profile ----- Used entries
testL3-OneEntry ----- 1
TOTAL 1
=====
= gigabit-ethernet-1/1/3 =
=====

ACL Ingress L2 Profile ----- Used entries
testL2 ----- 2
TOTAL 2

ACL Ingress L3 Profile ----- Used entries
testL3-OneEntry ----- 1
testL3-ZeroEntries ----- 0
TOTAL 1

DmOS# show acl-resources interface gigabit-ethernet-1/1/1 detail
Interface ----- Used L2 Entries ----- Used L3 Entries -----
gigabit-ethernet-1/1/1 2

DmOS# show acl-resources interface gigabit-ethernet-1/1/1 extensive
=====
= gigabit-ethernet-1/1/1 =
=====

ACL Ingress L2 Profile ----- Used entries
testL2 ----- 2
TOTAL 2

```

Impacts and precautions

N/A

Hardware restrictions

The **Total Entries** value could vary according to the product.

CHAPTER 11: SECURITY

This chapter describes the commands related to management of security features in the DmOS CLI.

AAA

This topic describes the commands related to management of authentication, authorization and accounting such as commands to configure Radius or Tacacs+ external servers or to manage the local user database.

aaa authentication-next-method-on-fail

Description

Command to instruct AAA to use the next authentication method defined in the authentication order list, even when the current method returns a FAIL response. By default, AAA proceeds to the next authentication method only when there is an ERROR, which means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. A FAIL response means that the user has not met the criteria contained in the security server authentication database to be successfully authenticated. In order to force local user authentication in this situation, for example, authentication-next-method-on-fail must be enabled and local authentication must be present in the authentication order list.

Supported Platforms

This command is supported in all platforms.

Syntax

aaa authentication-next-method-on-fail

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
---------	--------------

5.0.0	This command was introduced.
-------	------------------------------

Usage Guidelines

Example: This example shows how to enable the flag.

```
DM4160# config
Entering configuration mode terminal
DM4610(config)# aaa authentication-next-method-on-fail
```

Impacts and precautions

For local authentication, the next method is always tried on failure. But it is not recommended to use local before other methods on the authentication order list.

Hardware restrictions

N/A

aaa authentication-order

Description

Command to set user authentication Order. The order must be set using brackets and separated by spaces.

Supported Platforms

This command is supported in all platforms.

Syntax

aaa authentication-order { local | radius | tacacs }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

local

Description:	Configure authentication order to authenticate user locally.
Value:	N/A.
Default Value:	N/A.

radius

Description:	Configure authentication order to authenticate user against a remote radius server.
Value:	N/A.
Default Value:	N/A.

tacacs

Description:	Configure authentication order to authenticate user against a remote tacacs server.
Value:	N/A.
Default Value:	N/A.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
2.4	Added note for local authentication when the user is not present.
1.4	This command was introduced.

Usage Guidelines

After configuring the remote servers, authentication order must be set to determine in which order users will be authenticated. Using brackets allows user to replace older configurations.

Example: This example shows how to set authentication order.

```
DM4160# config
Entering configuration mode terminal
DM4610(config)# aaa authentication-order [ local radius tacacs ]
```

Impacts and precautions

For local authentication when the user is not present the next authentication method will be attempted. For radius or tacacs the next method is used only if there is no connection to the server.

Hardware restrictions

N/A

aaa authentication-type

Description

Configures the authentication type for remote servers.

Supported Platforms

This command is supported in all platforms.

Syntax

aaa authentication-type tacacs { pap | ascii }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

tacacs

Description:	Configures authentication type for TACACS servers.
Value:	{ pap ascii }
Default Value:	pap

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
---------	--------------

4.2.0	This command was introduced.
-------	------------------------------

Usage Guidelines

To authenticate users using TACACS the correct authentication type must be selected. The selected authentication type will be applied to all TACACS servers.

Example: This example shows how to configure the authentication type.

```
DM4160# config
Entering configuration mode terminal
DM4610(config)# aaa authentication-type tacacs ascii
```

Impacts and precautions

N/A

Hardware restrictions

N/A

aaa server radius

Description

Configure an (AAA) authentication, authorization and accounting remote RADIUS server.

Supported Platforms

This command is supported in all platforms.

Syntax

```
aaa server radius server name host IPv4address shared-secret secret [ authentication ] [ accounting ] [ retries number of retries ] [ authentication-port port number ] [ accounting-port port number ] [ source { ipv4 address IPv4address | interface interface-name } ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

server name

Description: Configures a name for the RADIUS server.

Value: String with with maximum length of 64

Default Value: None

host *IPv4address*

Description: Configures an address for the server.

Value: a.b.c.d

Default Value: None

shared-secret *secret*

Description: Configures a secret that is shared with the server and used to validate the transaction.

Value: String with maximum length of 128

Default Value: N/A.

authentication

Description: Enables remote user authentication via authentication server, it will also enable authorization.

Value: N/A

Default Value: N/A

accounting

Description: Enables remote accounting via accounting server.

Value: N/A

Default Value: N/A

retries *number of retries*

Description: Configures server communication retries.

Value: 1-5

Default Value: 3

authentication-port *port number*

Description: Configures server authentication port to allow communication.

Value: 0-65535

Default Value: 1812

accounting-port *port number*

Description: Configures server accounting port to allow communication.

Value: 0-65535

Default Value: 1813

source ipv4 address *IPv4address*

Description: Specifies the source IPv4 address from which Radius server connection will be established.

Value: a.b.c.d

Default Value: None

source interface *interface-name*

Description: Specifies the interface whose IP address will be used for all outgoing RADIUS packets. Interface must have an IPv4 address configured and cannot be associated with a VRF.

Value: Interface name in format I3-<name> or loopback-<id>.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
1.4	This command was introduced.
5.0	Added support for source IPv4 address.

Usage Guidelines

Configure remote servers before remote authentication can be enabled.

Example: This example shows how to set a remote Radius server.

```
DM4160# config
Entering configuration mode terminal
DM4610(config)# aaa server radius rad01
DM4610(config-radius-rad01)# host 10.1.1.1
DM4610(config-radius-rad01)# shared-secret dmos-radius
DM4610(config-radius-rad01)# authentication
DM4610(config-radius-rad01)# accounting
```

Example: This example shows how to configure an IPv4 source address for a remote Radius server.


```
DM4160# config
Entering configuration mode terminal
DM4610(config)# aaa server radius rad01
DM4610(config-radius-rad01)# source ipv4 address 1.1.1.1
```

Impacts and precautions

If the IPv4 source address parameter is not a configured IPv4 address of any interface, the Radius requests will not be sent to the server.

Hardware restrictions

None

aaa server tacacs

Description

Configures a remote TACACS+ server.

Supported Platforms

This command is supported in all platforms.

Syntax

aaa server tacacs *server name* **host** *IPv4address* **shared-secret** *secret* [**authentication**] [**authorization**] [**accounting**] [**timeout** *timeout time*] [**authentication-port** *port number*] [**authentication-type** *type*] [**source** { **ipv4 address** *IPv4address* | **interface** *interface-name* }] [**vrf** *vrf-name*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

server name

Description:	Configures a name for the TACACS+ server.
Value:	String with with maximum length of 64
Default Value:	N/A

host *IPv4address*

Description:	Configures an address for the server.
Value:	a.b.c.d
Default Value:	N/A

shared-secret *secret*

Description:	Configures a secret that is shared with the server and used to validate the transaction.
Value:	String with maximum length of 128
Default Value:	N/A

authentication

Description: Enables remote user authentication.

Value: N/A

Default Value: N/A

authorization

Description: Enables remote user commands authorization.

Value: N/A

Default Value: N/A

accounting

Description: Enables remote user commands accounting.

Value: N/A

Default Value: N/A

timeout *timeout time*

Description: Configures server communication timeout.

Value: 0-255

Default Value: 5

authentication-port *port number*

Description: Configures server authentication port to allow communication.

Value: 0-65535

Default Value: tacacs: 49

authentication-type *type*

Description: The authentication encryption type requested from TACACS+ server.

Value: { pap | ascii }

Default Value: pap

source ipv4 address *IPv4address*

Description: Specifies the source IPv4 address from which TACACS+ server connection will be established.

Value: a.b.c.d

Default Value: None

source interface *interface-name*

Description: Specifies the interface whose IP address will be used for all outgoing TACACS+ packets. In the case a loopback interface is selected and it belongs to a VRF, it's needed to configure the VRF parameter too.

Value: Interface name in format I3-<name> or loopback-<id>.

Default Value: None

vrf *vrf-name*

Description: Specifies the VRF used for all outgoing TACACS+ packets. VRF mgmt is not supported yet.

Value: VRF name.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
1.4	This command was introduced.
4.0	Added support for authorization and up to 5 servers.

Release	Modification
4.6	Added support for accounting.
5.0	Added support for source interface.
6.0	Added support to interface loopback in VRF.

Usage Guidelines

The remote servers must be previously configured before enabling the remote authentication on the equipment.

The system supports up to 5 TACACS+ servers, that means 4 redundant servers. Once a server is reached for authorization, this server will be preferred for the command authorization until it is unreachable. If this server becomes unreachable the list of servers will be inspected to return the next available server for authorization.

When there is a TACACS+ server with authentication and without authorization configured, the authorization level will be performed by user group. This group is mapped from the user privilege level present in the TACACS+ server used for authentication.

Example: This example shows how to set a remote TACACS+ server for authentication, authorization and accounting services.

```
# config
Entering configuration mode terminal
(config)# aaa server tacacs tac01
(config-tacacs-tac01)# host 10.1.1.1
(config-tacacs-tac01)# shared-secret dmos-tacacs
(config-tacacs-tac01)# authentication
(config-tacacs-tac01)# authorization
(config-tacacs-tac01)# accounting
(config-tacacs-tac01)# commit
```

Example: This example shows how to use **insert** to add new server with the desired priority.

```
(config)# insert aaa server tacacs tac3 before tac2
(config)# aaa server tacacs tac3 host 3.3.3.3 shared-secret 3333
(config-tacacs-tac3)# commit
Commit complete.
(config-tacacs-tac3)#
(config)# show aaa server
aaa server tacacs tac1
  host 1.1.1.1
```

```

shared-secret $7$kkfWsrXallbrgAQDad3S7w==
!
aaa server tacacs tac3
host 3.3.3.3
shared-secret $7$oS7m7YUa2o6c+secJrARZhQ==
!
aaa server tacacs tac2
host 2.2.2.2
shared-secret $7$IVkBhwucZ66bhXM+00Vzzw==
!

```

Example: This example shows how to use **move** to change the server priority.

```

(config)# move aaa server tacacs tac1 last
(config)# commit
Commit complete.
(config)# show aaa server
aaa server tacacs tac3
host 3.3.3.3
shared-secret $7$oS7m7YUa2o6c+secJrARZhQ==
!
aaa server tacacs tac2
host 2.2.2.2
shared-secret $7$IVkBhwucZ66bhXM+00Vzzw==
!
aaa server tacacs tac1
host 1.1.1.1
shared-secret $7$kkfWsrXallbrgAQDad3S7w==
!

```

Example: These examples show how to configure TACACS server to use a specific VRF.

```

(config)# aaa server tacacs tacacs2 host 60.1.1.3 vrf green
(config)# commit

(config)# aaa server tacacs tacacs1 host 60.1.1.3 vrf green source interface loopback-1
(config)# commit

```

Impacts and precautions

It is not recommended the configuration of the same user on both local host and remote authentication server when the group permission is different. Otherwise, the user authentication will be done and its privilege level will follow the higher permission.

Currently, commands authorization and accounting via NETCONF are not supported. However, the authorization and accounting level will be performed by user group. This group is based on the user privilege level present in the TACACS+ server used for authentication. A privilege level of 15 is mapped to the *admin* group, otherwise the user is mapped to the *audit* group.

It's not possible to use multiple TACACs servers on different VRFs.

Hardware restrictions

N/A

aaa user

Description

The AAA user command is used to create local users to access the device.

Supported Platforms

This command is supported in all platforms.

Syntax

aaa user *username* [**change-password** **new-password** *new password* **old-password** *old password* **confirm-password** *confirm password*] **password** *password* [**group** {*admin|config|audit*}]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

username

Description:	Set a local user name.
Value:	String with maximum length of 64
Default Value:	None

new password

Description:	New user password.
Value:	String with unlimited length
Default Value:	None

old password

Description:	Old user password.
Value:	String with unlimited length
Default Value:	None

confirm password

Description: Same as the old user password.

Value: String with unlimited length

Default Value: None

password *password*

Description: Defines a user password. The argument can be in plaintext or MD5 digest hash.

Value: String with unlimited length

Default Value: None

group *group*

Description: Set a local privilege group for the new user.

Value: { admin | config | audit }

Default Value: audit

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
1.2	Added group parameter.

Usage Guidelines

Users with admin access can change any user password and every user can change it's own password.

Example: This example shows how to set a local user.

```
DM4610# config
Entering configuration mode terminal
DM4610(config)# aaa user audit password audit group audit
```

Login via serial has a 128 characters limitation to username and password.

Impacts and precautions

Maximum number of local users are 32.

Hardware restrictions

N/A

id

Description

Command to show authenticated user and groups as well as user privilege level

Supported Platforms

This command is supported in all platforms.

Syntax

id

Parameters

N/A

Output Terms

Output	Description
<code>user</code>	Display connected user
<code>gid</code>	Main group id that the connected user is member of
<code>groups</code>	Group names that the connected user is member of
<code>gids</code>	All group ids that the connected user is member of

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Example: This example shows the output of the command.

```
DM4160# id
user = admin(0), gid=0, groups=admin
```

Impacts and precautions

N/A

Hardware restrictions

N/A

who

Description

Command to show all authenticated users currently connected

Supported Platforms

This command is supported in all platforms.

Syntax

```
who
```

Parameters

N/A

Output Terms

Output	Description
Session	Session number referencing the authenticated user session.
User	User name of the authenticated user.
Context	Context in which the user is authenticated(eg.: cli)
From	Ip address from which the connection was established.
Proto	Connection protocol being used(eg.: console).
Date	System time that user has been logged.
Mode	Command mode that user is using (eg.: operational).

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Example: This example shows how to obtain logged users.

```
DM4160# who
Session User Context From Proto Date Mode
*12 admin cli 127.0.0.1 console 00:03:05 operational
```

Impacts and precautions

N/A

Hardware restrictions

N/A

PORT SECURITY

This topic describes the commands related to management of interface restrictions.

anti-ip-spoofing

Description

Anti-ip-spoofing is used for security reasons, it is possible to enable anti-ip-spoofing for a specific interface and add static IP configuration.

When anti-ip-spoofing is enabled for an interface just **granted** traffic will be accepted by device, otherwise it will be dropped.

Device considers granted traffic:

- ARP packets;
- ip-address received by DHCP connections through device;
- ip-address configured in allowed-ip list;
- PPP connections;
- TLS connections;

Currently if anti-ip-spoofing is enabled for (ten-)gigabit-ethernet interfaces, it will drop all IP traffic and will accept just following **granted** traffic:

- ARP packets;
- ip-address configured in allowed-ip list;

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

anti-ip-spoofing

interface *interface-name-chassis/slot/port or id*

allowed-ip ipv4 address *ip-address* **vlan** *vid* **mac** *mac_addr*

allowed-ip all | ipv4-all | ipv6-all

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Interface where configuration will be applied.
Enables anti-ip-spoofing for ethernet interfaces.
Anti-ip-spoofing is always enabled for service-ports.

Value: [ten-gigabit-ethernet | gigabit-ethernet | service-port]

Default Value: None.

allowed-ip

Description: Option to configure a static IP rule.

Value: None.

Default Value: None.

all

Description: Inform that all IP addresses in any VLAN will be permitted by device in the interface.

Value: None.

Default Value: None.

ipv4-all

Description: Inform that all IPv4 addresses in any VLAN will be permitted by device.

Value: None.

Default Value: None.

ipv6-all

Description: Inform that all IPv6 addresses in any VLAN will be permitted by device.

Value: None.

Default Value: None.

ipv4 address *ip-address*

Description: IPv4 address of the client that will be permitted by device.

Value: IPv4 address

Default Value: None.

vlan *vid*

Description: VLAN of packets that will be permitted by device.

Value: 1-4094

Default Value: None

mac *mac-address*

Description: Source MAC address of the client that will be permitted by device.

Value: XX:XX:XX:XX:XX:XX

Default Value: None

Default

None.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
1.6	Changed CLI layout for entire anti-ip-spoofing command. Added “allowed-ip all” option.
1.10	Added “allowed-ip ipv4-all” option. Added “allowed-ip ipv6-all” option.

Usage Guidelines

Use the **interface** option to enable anti-ip-spoofing for a specific interface.

Anti-ip-spoofing is always enabled for service-port interfaces, but these interfaces are accepted by anti-ip-spoofing command in order to configure allowed-ip rules.

Inside **interface** node there are the options: **allowed-ip ipv4 address**, **allowed-ip ipv4-all**, **allowed-ip ipv6-all** and **allowed-ip all**.

Using **allowed-ip ipv4 address** option the traffic with the source IPv4 address and VLAN can pass through the interface.

Using **allowed-ip ipv4-all** option the traffic from any ipv4 and VLAN can pass through the interface. Note that for service-ports just packets from service vlan configured in service-port command will be accepted.

Using **allowed-ip ipv6-all** option the traffic from any ipv6 and VLAN can pass through the interface. Note that for service-ports just packets from service vlan configured in service-port command will be accepted.

Using **allowed-ip all** option the traffic from any ip can pass through the interface (this command is just allowed for service-port interfaces).

See usage examples below:

To enable anti-ip-spoofing for an interface (i.e: gigabit-ethernet 1/1/1), the following command must be issued.

Note that anti-ip-spoofing is always enabled for service-ports.

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface gigabit-ethernet-1/1/1
(config-ip-spoofing-gigabit-ethernet-1/1/1)#commit
```

To disable anti-ip-spoofing, the following command must be issued:

Please note that all allowed-ip rules of this interface will be removed too.

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#no interface gigabit-ethernet-1/1/1
(config-ip-spoofing)#commit
```

To allow all IPv4 addresses in any VLAN on a gigabit interface, the following command must be issued:

Please note that all allowed-ip rules for IPv4 addresses on this interface will be removed too and that all IPv6 addresses will be blocked.

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface gigabit-ethernet-1/1/1
(config-ip-spoofing-gigabit-ethernet-1/1/1)#allowed-ip ipv4-all
(config-ip-spoofing-gigabit-ethernet-1/1/1)#commit
```

To allow the client with IPv4 address 10.0.0.1, using VLAN id 10 on the service-port 1, to have the traffic permitted, the following command must be issued:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-1
(config-ip-spoofing-service-port-1)#allowed-ip ipv4 address
10.0.0.1 vlan 10
(config-ip-spoofing-service-port-1)#commit
```

To remove an allowed-ip rule, the following command must be issued:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-1
(config-ip-spoofing-service-port-1)#no allowed-ip ipv4 address
10.0.0.1 vlan 10
(config-ip-spoofing-service-port-1)#commit
```

To allow the traffic from client with IP address 10.0.0.1 and MAC address F0:7D:00:00:00:01, using VLAN id 10 on the service-port 1, the following command must be issued:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing-service-port-1)#allowed-ip ipv4 address
10.0.0.1 vlan 10 mac F0:7D:00:00:00:01
(config-ip-spoofing-service-port-1)#commit
```

To allow the client with any IPv4 address on the service-port 2, to have the traffic permitted, the following command must be issued:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-2
(config-ip-spoofing-service-port-2)#allowed-ip ipv4-all
(config-ip-spoofing-service-port-2)#commit
```

To allow the traffic from client with any IPv6 address on the service-port 1, the following command must be issued:

```
(config)#
```

```
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-1
(config-ip-spoofing-service-port-2)#allowed-ip ipv6-all
(config-ip-spoofing-service-port-2)#commit
```

To allow the client with any IP address on the service-port 1, to have the traffic permitted, the following command must be issued:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-1
(config-ip-spoofing-service-port-2)#allowed-ip all
(config-ip-spoofing-service-port-2)#commit
```

Note that same effect is achieved by following commands:

```
(config)#
(config)#anti-ip-spoofing
(config-ip-spoofing)#interface service-port-1
(config-ip-spoofing-service-port-2)#allowed-ip ipv4-all
(config-ip-spoofing-service-port-2)#allowed-ip ipv6-all
(config-ip-spoofing-service-port-2)#commit
```

To check if the configuration was applied, issue the **show running-config** command:

```
#show running-config
anti-ip-spoofing
  interface service-port-1
    allowed-ip ipv4 10.0.0.1 vlan 10
  !
  interface service-port-2
    allowed-ip all
  !
!
```

Impacts and precautions

Clients that use static IP address configuration shall have an allowed-ip configuration, otherwise its traffic won't pass through the device.

An interface with anti-ip-spoofing enabled will drop any IP traffic, will just allow ARP packets and traffic with IP addresses configured by allowed-ip or received by DHCP connections.

TLS and PPP traffic will not be affected by anti-ip-spoofing configuration.

For (ten-)gigabit-ethernet interfaces with anti-ip-spoofing enabled, just ARP packets and traffic with IP addresses configured by allowed-ip will be accepted.

Anti-ip-spoofing should not be enabled for interfaces being used as **Uplink** interfaces, it was designed to be used in **access-like** interfaces.

The misuse of anti-ip-spoofing feature with **uplink-like** interfaces can stop all traffic on it.

Allowed-ip configuration will not work with service-ports without match and action configuration (VLAN translate).

Hardware restrictions

For DM46xx family, the maximum number of allowed IP addresses is 1024. However, this limit is shared with DHCP entries. It means that equipment will be limited to 1024 connections (Static plus DHCP assigned addresses).

show allowed-ip

Description

This command shows the list of allowed ip entries.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show allowed-ip [**mac** *mac-address* | **vlan** *vlan id* | **address** *ip-address* | **interface** *interface-name-chassis/slot/port* | **entry-type** *type* | **status** *entry-status*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mac *mac-address*

Description: MAC address used to filter the output.
Value: [<XX:XX:XX:XX:XX:XX> MAC Address | all]
Default Value: N/A

vlan *vlan-id*

Description: VLAN id used to filter the output.
Value: [<1-4094> VLAN ID | all]
Default Value: N/A

address *ip-address*

Description: IP address used to filter the output.
Value: [<A.B.C.D> IP Address | all | ipv4-all | ipv6-all]
Default Value: N/A

interface *interface-name-chassis/slot/port*

Description: Interface used to filter the output.
Value: [ten-gigabit-ethernet | gigabit-ethernet | service-port]
Default Value: N/A

entry-type *type*

Description: Type of entry to filter the output.
Value: [static | dhcp]
Default Value: N/A

status *entry-status*

Description: Entry status, indicate if entry is operational or not.
Value: [active | pending]
Default Value: N/A

Output Terms

Output	Description
MAC-Address	Display the MAC addresses associated with the allowed IP addresses.
IP-Address	Display the allowed IP addresses.
VLAN	Display the VLAN ids associated with the allowed IP entries.
Entry-Type	Display the Entry Types of the allowed IP entries.
Interface	Display the Interface on which the respective IP is allowed.
Status	Display the Status of the allowed IP entries.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Access level audit

History

Release	Modification
1.4	This command was introduced.
1.6	Added Status column. Allowed-ip table layout changed.
1.10	Added new values: ipv4-all and ipv6-all. Allowed-ip table layout changed.

Usage Guidelines

To simply show the list of all allowed IP entries the following command can be used:

```
#show allowed-ip
```

It is possible to filter the results by MAC address, IP address, VLAN id, interface, entry type and status.

Filter by MAC:

```
#show allowed-ip mac 44:55:33:22:11:00
```

Filter by IP:

```
#show allowed-ip address 10.0.0.1
```

Filter by Interface:

```
#show allowed-ip interface gigabit-ethernet-1/1/1
```

Filter by VLAN:


```
#show allowed-ip vlan 1100
```

Filter by Entry Type:

```
#show allowed-ip entry-type static
```

Filter by Status:

```
#show allowed-ip status active
```

Impacts and precautions

N/A

Hardware restrictions

N/A

CHAPTER 12: OAM

This chapter describes the CLI commands related to Operation, Administration and Management of the DmOS.

CONTINUITY CHECK AND FAULT MANAGEMENT

This topic describes the commands related to management of fault detection using CFM or Y.1731 such as commands to configure and inspect Maintenance End Points (MEPs), CCM rates or to execute on-demand Ethernet link trace.

cfm delay-measurement probe

Description

Configure CFM delay-measurement probes. Essentially, a probe is the periodic execution of sessions for a specified Maintenance Domain (MD), Maintenance Association (MA), local Maintenance Endpoint (MEP) and, remote MEP. In turn, a session holds all parameters that a user would choose when manually running a troubleshooting command. For each session, consolidated statistics of the last 10 executions are saved and rotated to discard the oldest results.

Supported Platforms

This command is supported in all platforms.

Syntax

oam cfm delay-measurement probe *id md id ma id mep id remote-mep id interval interval*

oam cfm delay-measurement probe *id session id [count value] [pcp value] [interval value] [size value]*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

probe *id*

Description: Unique probe identifier.

Value: 1 - 512

Default Value: N/A

interval *minutes*

Description: The interval between two probe executions, in minutes.

Value: 1 - 1440

Default Value: 1

md *id*

Description: Unique Maintenance Domain (MD) identifier that contains the local MEP to issue delay-measurement messages.

Value: String with MD identifier. Only an already created MD is accepted.

Default Value: N/A

ma *id*

Description: Unique Maintenance Association (MA) identifier that contains the local MEP to issue delay-measurement messages.

Value: String with MA identifier. Only an already created MA is accepted.

Default Value: N/A

mep *id*

Description: Local MEP ID. Only an existing local MEP is accepted.

Value: 1 - 8191

Default Value: N/A

remote-mep *id*

Description: Remote MEP ID. Only an existing remote MEP is accepted.

Value: 1 - 8191

Default Value: N/A

session *id*

Description: Unique session identifier. A probe contains up to 8 sessions, where each session has a different PCP (priority code point) value.

Value: 1 - 8

Default Value: N/A

count *value*

Description: Number of delay-measurement frames in the session.

Value: 1 - 1024

Default Value: 10

pcp *value*

Description: PCP (priority code point) value used in the 802.1Q VLAN tag.

Value: 0 - 7

Default Value: N/A

interval *value*

Description: Interval between each delay-measurement frame.

Value: { 1s | 10s | 1min | 10min }

Default Value: 1s

size *value*

Description: Set delay-measurement frame size; padding is added if necessary.

Value: 64 - 9000

Default Value: 64

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

5.10	This command was introduced.
------	------------------------------

Usage Guidelines

Considering the following scenario, with local MEP 11 and remote MEP 12:

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# interface gigabit-ethernet-1/1/2
(config-dot1q-interface-gigabit-ethernet-1/1/2)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 3
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# remote-meps 12
(cfm-ma-CFM_MA)# vlan-list 10,20,30
(cfm-ma-CFM_MA)# primary-vlan-id 20
(cfm-ma-CFM_MA)# mep 10
(cfm-mep-11)# interface gigabit-ethernet-1/1/2
(cfm-mep-11)# direction up
(cfm-mep-11)# primary-vlan-id 10
(cfm-mep-11)# commit
```

In this example, local MEP 11 will run two delay-measurement sessions to remote MEP 12 every 20 minutes. The first session sends 5 frames with 128 bytes every second to monitor PCP 3, which is typically used for voice applications:

```
(config)# oam cfm delay-measurement probe 1 md CFM_MD ma CFM_MA mep 11
remote-mep 12 interval 20
(cfm-dm-probe-1)# session 1 interval 1s count 5 size 128 pcp 3
```

A second session is used to monitor PCP 1, which usually has the lowest network priority, and will use a different interval and packet size:

```
(cfm-dm-probe-2)# session 2 interval 10s count 15 size 512 pcp 1
```

To see the consolidated statistics of session 1, run the following command:

```
# show oam cfm delay-measurement probe 1 session 1
```

SESSION	PCP	LAST AVG DELAY (us)	LAST AVG JITTER (us)	LAST LOSS RATIO %	LAST PCP MISMATCH RATIO %	ALL AVG DELAY (us)	ALL AVG JITTER (us)	ALL LOSS RATIO %	ALL PCP MISMATCH RATIO %
1	3	4493	784	0	0	4493	784	0	0

Impacts and precautions

N/A

Hardware restrictions

N/A

cfm ma

Description

Create a Maintenance Association (MA) and configure its parameters.

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam cfm md id ma id ccm-interval interval primary-vlan-id vlan-id vlan-list vlan-ids
{ remote-mepps mep-ids }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ccm-interval *interval*

Description:	Set the interval between CCM transmissions to be used by all MEPs in the MA.
Value:	{ 1s 10s 1min 10min }
Default Value:	N/A

primary-vlan-id *vlan-id*

Description: Set the MA primary VLAN ID.

Value: 1 - 4094

Default Value: N/A

vlan-list *vlan-ids*

Description: Configure VLAN IDs monitored by the MA. Ranges of VLANs or single VLAN are allowed and can be combined to specify the MA VLAN list.

Example: vlan-list 1-3,5,7-9

Value: 1 - 4094

Default Value: N/A

remote-meps *mep-ids*

Description: Configure the remote MEPs in the MA. Ranges of MEP IDs or single MEP ID are allowed and can be combined to specify the remote MEP list.

Example: remote-meps 1-3,5,7-9

Value: 1 - 8191

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To create a CFM Maintenance Association it is necessary to create a valid Maintenance Domain and configure the CCM interval time and a primary VLAN ID. The VLANs of the VLAN list must be created in the equipment. The example below shows the creation of an MA that monitors the VLANs 10, 20 and 30, with VLAN 20 as the primary VLAN ID.

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 1
(cfm-md-CFM_MD)# ma CFM_MA1
(cfm-ma-CFM_MA1)# ccm-interval 1s
(cfm-ma-CFM_MA1)# vlan-list 10,20,30
(cfm-ma-CFM_MA1)# primary-vlan-id 20
(cfm-ma-CFM_MA1)# remote-meps 10-15
(cfm-ma-CFM_MA1)# commit
Commit complete.
(cfm-ma-CFM_MA1)# end
#
```

One-line like command is also supported. The example below shows the creation of another MA.

```
# config
(config)# dot1q vlan 10
(config-vlan-10)# top
(config)# oam cfm md CFM_MD level 1 ma CFM_MA2 ccm-interval 10s
vlan-list 10 primary-vlan-id 10 remote-meps 2-10
(cfm-ma-CFM_MA2)# commit
Commit complete.
(cfm-ma-CFM_MA2)# end
#
```

Impacts and precautions

- The MA is part of an MD and a valid MD configuration is required for the configuration to be committed successfully.
- The VLANs in the VLAN list monitored by the MA need to be configured in the equipment for the configuration to be committed successfully.

Hardware restrictions

N/A

cfm ma ais

Description

Configure transmission and reception of Alarm Indication Signal (AIS) frames for a given Maintenance Association (MA).

When transmission is enabled, AIS frames are transmitted when a fault is detected, regardless of any alarm configuration and report.

When AIS alarm suppression is enabled, alarms are not reported if AIS frames are received.

Supported Platforms

This command is supported in all platforms.

Syntax

oam cfm md *id* ma *id* ais transmission level *target-level* [*interval* *packets-interval*] [*vlan-priority* *priority*] [*vlan-list* *vlan-ids*]

oam cfm md *id* ma *id* ais reception alarm-suppression

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ais transmission level *target-level*

Description: Destination MD level of the sent AIS packets. The target level must be greater than the MD level where the AIS is configured.

Value: 1 - 7

Default Value: N/A

ais transmission interval *packets-interval*

Description: Time interval between AIS packets sending.

Value: {1s | 1min}

Default Value: 1s

ais transmission vlan-priority *priority*

Description: PCP (802.1p priority) to be used on VLAN Tags for AIS packets.

Value: 0 - 7

Default Value: 7

ais transmission vlan-list *vlan-ids*

Description: List of inner VLANs (second VLAN TAGs) which the AIS must be sent with. A copy of the packet is sent with each inner VLAN. The outer VLAN is the MEP's primary-vlan. Leave it blank when an inner VLAN is unnecessary. VLAN ranges or single VLANs are allowed and can be combined.

Value: 1 - 4094

Default Value: N/A

ais reception alarm-suppression

Description: Enables the alarm suppression on AIS packet reception.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

To configure AIS transmission it is necessary to create a valid MA and configure all parameters of AIS transmission. AIS reception takes the alarm-suppression parameter only. Transmission and reception can be configured independently.

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 1
(cfm-md-CFM_MD)# ma CFM_MA1
(cfm-ma-CFM_MA1)# ccm-interval 1s
(cfm-ma-CFM_MA1)# vlan-list 10,20,30
(cfm-ma-CFM_MA1)# primary-vlan-id 20
(cfm-ma-CFM_MA1)#ais transmission
(cfm-ais-tx)# level 3
(cfm-ais-tx)# interval 1min
(cfm-ais-tx)# vlan-list 10
(cfm-ais-tx)# vlan-priority 1
(cfm-ais-rx)# ais reception
(cfm-ais-rx)# alarm-suppression
(cfm-ma-CFM_MA1)# remote-meps 10-15
(cfm-ma-CFM_MA1)# commit
Commit complete.
(cfm-ma-CFM_MA1)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

cfm md

Description

Enables Connectivity Fault Management (CFM) and create a Maintenance Domain (MD).

Supported Platforms

This command is supported in all platforms.

Syntax

oam cfm md *id level md-level*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

md *id*

Description:	Unique identifier to the MD.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

level *md-level*

Description:	Set the MD level.
Value:	0 - 7
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To create a CFM Maintenance Domain it is necessary to configure at least the MD level. The example below shows the creation of an MD.

```
# config
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD1
(cfm-md-CFM_MD1)# level 5
(cfm-md-CFM_MD1)# commit
Commit complete.
(cfm-md-CFM_MD1)# end
#
```

One-line like command is also supported. The example below shows the creation of another MD.

```
# config
(config)# oam cfm md CFM_MD2 level 6
(cfm-md-CFM_MD2)# commit
Commit complete.
(cfm-md-CFM_MD2)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

cfm mep

Description

Create a Maintenance End Point (MEP) and configure its parameters.

Supported Platforms

This command is supported in all platforms.

Syntax

oam cfm md *id* **ma** *id* **mep** *id* **interface** *interface-name* **direction** *direction* **primary-vlan-id** *vlan-id* **inner-vlan-id** *vlan-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA associated to the MEP.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

mep *id*

Description:	MEP Unique identifier inside the MA.
Value:	1 - 8191
Default Value:	N/A

interface *interface-name*

Description:	Set the interface to which the MEP is attached.
Value:	{ gigabit-ethernet-chassis/slot/port ten-gigabit-ethernet-chassis/slot/port twenty-five-g-ethernet-chassis/slot/port forty-gigabit-ethernet-chassis/slot/port hundred-gigabit-ethernet-chassis/slot/port lag-id }
Default Value:	N/A

direction *direction*

Description:	Set the direction in which the MEP faces on the interface.
Value:	{ up down }
Default Value:	N/A

primary-vlan-id *vlan-id*

Description:	Set the MEP primary VLAN ID.
Value:	1 - 4094
Default Value:	N/A

inner-vlan-id *vlan-id*

Description:	Specify the inner VLAN ID (second tag) for this MEP.
Value:	1 - 4094
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.
4.9	Added support for inner tag on MEP.
5.0	Added support for 25G interfaces.

Usage Guidelines

To create a CFM Maintenance End Point it is necessary to create a valid Maintenance Association and configure the MEP interface and direction. The interface must be a valid one. The primary VLAN ID specified must be part of the parent MA VLAN list and the MEP interface must be a member of this VLAN. The example below shows the creation of a MEP attached to the VLAN 10.

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# interface gigabit-ethernet-1/1/2
(config-dot1q-interface-gigabit-ethernet-1/1/2)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 3
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# vlan-list 10,20,30
(cfm-ma-CFM_MA)# primary-vlan-id 20
(cfm-ma-CFM_MA)# mep 1
(cfm-mep-1)# interface gigabit-ethernet-1/1/2
(cfm-mep-1)# direction up
(cfm-mep-1)# primary-vlan-id 10
(cfm-mep-1)# commit
Commit complete.
(cfm-mep-1)# end
#
```

One-line like command is also supported. The example below shows the creation of another MEP.

```
# config
(config)# dot1q vlan 1 interface gigabit-ethernet-1/1/10
(config-dot1q-interface-gigabit-ethernet-1/1/10)# top
(config)# oam cfm md CFM_MD level 3 ma CFM_MA ccm-interval 1s
vlan-list 1 primary-vlan-id 1 mep 2 interface gigabit-ethernet-1/1/10
direction down primary-vlan-id 1
(cfm-mep-2)# commit
Commit complete.
(cfm-mep-2)# end
#
```

Impacts and precautions

- The MEP is part of an MA and a valid MA configuration is required for the configuration to be committed successfully.
- Only pre-existing interfaces will be accepted when entering an interface name.
- Interfaces added as members of a Link Aggregation Group (LAG) cannot be attached in a MEP. The LAG itself should be configured instead.
- The primary VLAN ID must be present in the parent MA's VLAN list.
- The MEP interface must be a member of the MEP primary VLAN.
- MEPs configured with direction down do not respect VLAN Mapping rules.

Hardware restrictions

N/A

cfm mep continuity-check

Description

Configure the Continuity Check Messages (CCM) generation, fault detection and fault notification.

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam cfm md id ma id mep id continuity-check { cci-enabled | lowest-fault-priority-defect fault-type | [ fault-action action ] | fault-alarm-time time | fault-reset-time time }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA associated to the MEP.
Value:	String with a maximum of 43 characters. It only accepts alphanumeric characters and '_', '+' and '-'.
Default Value:	N/A

mep *id*

Description:	MEP Unique identifier inside the MA.
Value:	1 - 8191

Default Value: N/A

cci-enabled

Description: Enable the MEP's generation of CCMs.

Value: N/A

Default Value: N/A

lowest-fault-priority-defect *fault-type*

Description: Set the lowest priority defect that is allowed to generate a Fault Alarm.

Value: { remote-rdi | remote-mac-error | remote-invalid-ccm | invalid-ccm | cross-connect-ccm }

Default Value: N/A

fault-alarm-time *time*

Description: Set the time (in milliseconds) before a Fault Alarm is issued (100ms step).

Value: { 2500 - 10000 }

Default Value: 2500

fault-reset-time *time*

Description: Set the time (in milliseconds) before resetting a Fault Alarm (100ms step).

Value: { 2500 - 10000 }

Default Value: 10000

fault-action *action*

Description: Set the action when this MEP enters in fail state, as controlled by the Continuity Check lowest-fault-priority-defect configuration.

Value: { none | block-port | shutdown-port }

Default Value: none

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.
4.6	Added MEP fault action block-port.
4.8	Added MEP fault action shutdown-port.
4.9	Fault action controlled by lowest-fault-priority-defect only.

Usage Guidelines

To configure the Continuity Check Messages generation it is necessary to create a valid CFM Maintenance End Point. The example below shows the creation of a MEP and CCMs generation configuration.

```
# config
(config)# dot1q vlan 50
(config-vlan-50)# interface gigabit-ethernet-1/1/1
(config-dot1q-interface-gigabit-ethernet-1/1/1)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 0
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# vlan-list 50
(cfm-ma-CFM_MA)# primary-vlan-id 50
(cfm-ma-CFM_MA)# mep 1
(cfm-mep-1)# interface gigabit-ethernet-1/1/1
(cfm-mep-1)# direction up
(cfm-mep-1)# primary-vlan-id 50
(cfm-mep-1)# continuity-check
(cfm-mep-1-cci)# cci-enabled
(cfm-mep-1-cci)# lowest-fault-priority-defect invalid-ccm
(cfm-mep-1-cci)# fault-alarm-time 3000
(cfm-mep-1-cci)# fault-reset-time 9000
(cfm-mep-1-cci)# commit
Commit complete.
```

```
(cfm-mep-1-cci) # end
#
```

One-line like command is also supported. The example below shows the configuration in another MEP.

```
# config
(config) # dot1q vlan 50 interface gigabit-ethernet-1/1/1
(config-dot1q-interface-gigabit-ethernet-1/1/1) # top
(config) # oam cfm md CFM_MD level 0 ma CFM_MA ccm-interval 1s
vlan-list 50 primary-vlan-id 50 mep 2 interface gigabit-ethernet-1/1/4
direction down primary-vlan-id 50 continuity-check cci-enabled
(cfm-mep-2-cci) # commit
Commit complete.
(cfm-mep-2-cci) # end
#
```

Fault Alarm is priority based, so a given value will enable all the values below it:

remote-rdi - Enable fault alarm notification for all errors

remote-mac-error - Enable fault alarm notification for remote MEPs with Port Status or Interface Status failure and all errors below

remove-invalid-ccm - Enable fault alarm notification for remote MEPs without connectivity or remote MEP FSM receiving invalid CCMs and all errors below

invalid-ccm - Enable fault alarm notification for reception of invalid CCMs and cross-connection CCMs

cross-connect-ccm - Enable fault alarm notification only for reception of cross-connection CCMs

Impacts and precautions

- CCMs generation is part of MEP and a valid MEP configuration is required for the configuration to be committed successfully.
- Fault-Action Block-Port can be used only on MEP with direction Down.
- Fault-Action Shutdown-Port can be used only on MEP with direction Up.

Hardware restrictions

N/A

clear oam cfm statistics

Description

Clear statistics information related to CFM.

Supported Platforms

This command is supported in all platforms.

Syntax

clear oam cfm statistics [**md** *md-id*] [**ma** *ma-id*] [**mep** *mep-id*]

Parameters

md *md-id*

Description: This parameter selects the MD ID to the statistics be cleared. If omitted, all MD IDs will be selected.

Value: N/A

Default Value: N/A

ma *ma-id*

Description: This parameter selects the MA ID to the statistics be cleared. If omitted, all MA IDs will be selected.

Value: N/A

Default Value: N/A

mep *mep-id*

Description: This parameter selects the MEP ID to the statistics be cleared. If omitted, all MEP IDs will be selected.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0.0	This command was introduced.
-------	------------------------------

Usage Guidelines

```
# clear oam cfm statistics md my-md ma my-ma mep 1  
#
```

Impacts and precautions

None

Hardware restrictions

None

delay-measurement

Description

Trigger a delay-measurement session from a local MEP to a remote MEP in order to collect network statistics such as delay and jitter.

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam cfm delay-measurement md id ma id mep id remote-mep id [count value]  
[pcp value] [interval value] [size value]
```

Parameters

md *id*

Description: Unique Maintenance Domain (MD) identifier.
Value: String with MD identifier. Only an already created MD is accepted.
Default Value: N/A

ma *id*

Description: Unique Maintenance Association (MA) identifier.
Value: String with MA identifier. Only an already created MA is accepted.
Default Value: N/A

mep *id*

Description: Local MEP ID. Only an already created local MEP is accepted.
Value: 1 - 8191
Default Value: N/A

remote-mep *id*

Description: Remote MEP ID. Only an already created remote MEP is accepted.

Value: 1 - 8191

Default Value: N/A

count *value*

Description: Number of delay-measurement frames in the session.

Value: 1 - 1024

Default Value: 10

pcp *value*

Description: PCP (priority code point) value used in the 802.1Q VLAN tag.

Value: 0 - 7

Default Value: 0

interval *value*

Description: Interval between each delay-measurement frame.

Value: { 1s | 10s | 1min | 10min }

Default Value: 1s

size *value*

Description: Set delay-measurement frame size; padding is added if necessary.

Value: 64 - 9000

Default Value: 64

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.10	This command was introduced.

Usage Guidelines

In order to start a delay-measurement session, the CFM Maintenance Domain (MD), the Maintenance Association (MA) with at least one remote Maintenance Endpoint (MEP), and the local MEP must be previously configured.

The example below shows the creation of the entities, as mentioned earlier in the configuration:

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 1
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# vlan-list 10,20,30
(cfm-ma-CFM_MA)# primary-vlan-id 20
(cfm-ma-CFM_MA)# remote-meeps 10-15
(cfm-ma-CFM_MA)# mep 1
(cfm-mep-1)# interface gigabit-ethernet-1/1/2
(cfm-mep-1)# direction down
(cfm-mep-1)# primary-vlan-id 10
(cfm-mep-1)# commit
(cfm-ma-CFM_MA1)# commit
Commit complete.
(cfm-ma-CFM_MA1)# end
#
```

The remote MEP must also be known. Therefore, at least one valid CCM must be received from the remote MEP before starting a session.

According to this example, a possible delay-measurement command would be:

```
# oam cfm delay-measurement md CFM_MD ma CFM_MA mep 1
remote-mep 10 count 5 interval 1s size 500 pcps 7
```

The delay-measurement replies are shown interactively, and the session summary is provided in the end:

```
Reply from 00:04:df:2f:ad:18
Reply from 00:04:df:2f:ad:18
Reply from 00:04:df:2f:ad:18
Reply from 00:04:df:2f:ad:18
Reply from 00:04:df:2f:ad:18
```

Session summary:

Received 5 of 5 expected replies (0% packet loss, 0% PCP mismatch).

	Average	Minimum	Maximum
Delay (us):	4303	3559	5226
Jitter (us):	615	483	833

Impacts and precautions

- When a delay-measurement probe or manual session runs on a specific local MEP, parallel requests on the same MEP are not allowed.

Hardware restrictions

N/A

linktrace

Description

Trigger a linktrace.

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam cfm linktrace md id ma id mep id remote-mep id [ttl value]
```

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with MD identifier. Only an already created MD is accepted.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA.
Value:	String with MA identifier. Only an already created MA is accepted.
Default Value:	N/A

mep *id*

Description:	Local MEP unique identifier inside the MA. Only an already created Local MEP is accepted.
Value:	1 - 8191
Default Value:	N/A

remote-mep *id*

Description:	Remote MEP unique identifier inside the MA. Only an already created Remote MEP is accepted.
---------------------	---

Value: 1 - 8191

Default Value: N/A

ttl *value*

Description: Time To Live for the first linktrace packet.

Value: 2 - 255

Default Value: 64

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.9	This command was introduced.
-----	------------------------------

Usage Guidelines

In order to start a linktrace operation, the CFM Maintenance Domain (MD), the Maintenance Association (MA) with at least one remote Maintenance Endpoint (MEP) and the local MEP must be previously configured.

The example below shows the creation of the aforementioned elements in the configuration:

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# top
```



```
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 1
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# vlan-list 10,20,30
(cfm-ma-CFM_MA)# primary-vlan-id 20
(cfm-ma-CFM_MA)# remote-meps 10-15
(cfm-ma-CFM_MA)# mep 1
(cfm-mep-1)# interface gigabit-ethernet-1/1/2
(cfm-mep-1)# direction down
(cfm-mep-1)# primary-vlan-id 10
(cfm-mep-1)# commit
(cfm-ma-CFM_MA1)# commit
Commit complete.
(cfm-ma-CFM_MA1)# end
#
```

The remote MEP must also be known. Therefore, at least one valid CCM must be received from the remote MEP before starting a linktrace session.

According to the example, a possible linktrace command would be:

```
# oam cfm linktrace md CFM_MD ma CFM_MA mep 1 remote-mep 10 ttl 16
```

The linktrace result will be displayed interactively, but can also be seen with the command:

```
# show oam cfm linktrace
```

Impacts and precautions

- A linktrace is automatically started by a local MEP to a remote MEP when three consecutive Continuity Check Messages are missed from that remote MEP.
- When an automatic or manual linktrace transaction is running on a specific MEP, parallel linktrace requests on the same MEP are not allowed.

Hardware restrictions

N/A

loopback

Description

Trigger a loopback session.

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam cfm loopback md id ma id mep id remote-mep id [count value] [size value]
```

Parameters

md *id*

Description:	Unique identifier to the MD associated to the MA.
Value:	String with MD identifier. Only an already created MD is accepted.
Default Value:	N/A

ma *id*

Description:	Unique identifier to the MA.
Value:	String with MA identifier. Only an already created MA is accepted.
Default Value:	N/A

mep *id*

Description:	Local MEP unique identifier inside the MA. Only an already created Local MEP is accepted.
Value:	1 - 8191
Default Value:	N/A

remote-mep *id*

Description:	Remote MEP unique identifier inside the MA. Only an already created Remote MEP is accepted.
---------------------	---

Value: 1 - 8191

Default Value: N/A

count *value*

Description: Number of loopback messages to be sent.

Value: 1 - 1024

Default Value: 10

size *value*

Description: Size of loopback messages; padding is added if necessary to ensure the requested frame size.

Value: 64 - 16383

Default Value: 64

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.9

This command was introduced.

Usage Guidelines

In order to start a loopback operation, the CFM Maintenance Domain (MD), the Maintenance Association (MA) with at least one remote Maintenance Endpoint (MEP) and the local MEP must be previously configured.

The example below shows the creation of the aforementioned elements in the configuration:

```
# config
(config)# dot1q vlan 10,20,30
(config-vlan-10,20,30)# top
(config)# oam
(oam)# cfm
(cfm)# md CFM_MD
(cfm-md-CFM_MD)# level 1
(cfm-md-CFM_MD)# ma CFM_MA
(cfm-ma-CFM_MA)# ccm-interval 1s
(cfm-ma-CFM_MA)# vlan-list 10,20,30
(cfm-ma-CFM_MA)# primary-vlan-id 20
(cfm-ma-CFM_MA)# remote-meps 10-15
(cfm-ma-CFM_MA)# mep 1
(cfm-mep-1)# interface gigabit-ethernet-1/1/2
(cfm-mep-1)# direction down
(cfm-mep-1)# primary-vlan-id 10
(cfm-mep-1)# commit
(cfm-ma-CFM_MA1)# commit
Commit complete.
(cfm-ma-CFM_MA1)# end
#
```

The remote MEP must also be known. Therefore, at least one valid CCM must be received from the remote MEP before starting a loopback session.

According to the example, a possible loopback command would be:

```
# oam cfm loopback md CFM_MD ma CFM_MA mep 1 remote-mep 2 count 10
```

Loopback replies are shown as they are received, and a session summary is presented when it is terminated.

```
Loopback session started to 00:04:df:01:02:03
```

```
Reply from 00:04:df:01:02:03, transaction 1
Reply from 00:04:df:01:02:03, transaction 2
Reply from 00:04:df:01:02:03, transaction 3
Reply from 00:04:df:01:02:03, transaction 4
Reply from 00:04:df:01:02:03, transaction 5
Reply from 00:04:df:01:02:03, transaction 6
Reply from 00:04:df:01:02:03, transaction 7
Reply from 00:04:df:01:02:03, transaction 8
Reply from 00:04:df:01:02:03, transaction 9
Reply from 00:04:df:01:02:03, transaction 10
```

```
Session summary:
```

```
Expected 10 replies, received 10 with valid order and 0 out of order.
Replies with wrong payload: 0.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show oam cfm delay-measurement

Description

Display consolidated delay-measurement statistics for the specified probe and session. If no probe is specified, all probes are shown. If no session is specified for a given probe, all sessions probe sessions are shown. For each session, consolidated statistics of the last 10 executions are saved and rotated to discard the oldest results.

Supported Platforms

This command is supported in all platforms.

Syntax

show oam cfm delay-measurement [detail]

show oam cfm delay-measurement probe *id* [detail]

show oam cfm delay-measurement probe *id session id* [detail]

Parameters

probe *id*

Description: Unique probe identifier.

Value: 1 - 512

Default Value: N/A

session *id*

Description: Unique session identifier. A probe contains up to 8 sessions, where each session has a different PCP (priority code point) value.

Value: 1 - 8

Default Value: N/A

Output Terms

Output	Description
SESSION	Session identifier, unique for a given probe.
PCP	Priority code point value configured for the probe.
LAST AVG DELAY	Average delay for all frames of the most recent execution of this session.
LAST MIN DELAY	Minimum delay for all frames of the most recent execution of this session.
LAST MAX DELAY	Maximum delay for all frames of the most recent execution of this session.
LAST AVG JITTER	Average jitter for all frames of the most recent execution of this session.
LAST MIN JITTER	Minimum jitter for all frames of the most recent execution of this session.
LAST MAX JITTER	Maximum jitter for all frames of the most recent execution of this session.
LAST LOSS RATIO	Frame loss ratio (missing replies) for the most recent execution of this session.
LAST PCP MISMATCH RATIO	Ratio of frames received with PCP value that is not equal to the transmitted value for the most recent execution of this session..
ALL AVG DELAY	Average delay for all frames for all execution of this session.
ALL MIN DELAY	Minimum delay for all frames for all execution of this session.
ALL MAX DELAY	Maximum delay for all frames for all execution of this session.

Output	Description
ALL AVG JITTER	Average jitter for all frames for all execution of this session.
ALL MIN JITTER	Minimum jitter for all frames for all execution of this session.
ALL MAX JITTER	Maximum jitter for all frames for all execution of this session.
ALL LOSS RATIO	Frame loss ratio (missing replies) for all execution of this session.
ALL PCP MISMATCH RATIO	Ratio of frames received with PCP value that is not equal to the transmitted value for all execution of this session.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.1	This command was introduced.

Usage Guidelines

Detailed show:

```
DM4050# show oam cfm delay-measurement probe 1 session 1 detail
```


SESSION	PCP	LAST AVG DELAY (us)	LAST MIN DELAY (us)	LAST MAX DELAY (us)	LAST AVG JITTER (us)	LAST MIN JITTER (us)	LAST MAX JITTER (us)	LAST LOSS RATIO %	LAST PCP MISMATCH RATIO %	ALL AVG DELAY (us)	ALL MIN DELAY (us)	ALL MAX DELAY (us)	ALL AVG JITTER (us)
1	1	4892	3176	7063	940	524	1144	0	0	4892	3176	7063	940

Simplified show:

```
DM4050# show oam cfm delay-measurement probe 1 session 2
```

SESSION	PCP	LAST AVG DELAY (us)	LAST AVG JITTER (us)	LAST LOSS RATIO %	LAST PCP MISMATCH RATIO %	ALL AVG DELAY (us)	ALL AVG JITTER (us)	ALL LOSS RATIO %	ALL PCP MISMATCH RATIO %
2	2	4635	330	0	0	4635	330	0	0

Impacts and precautions

None

Hardware restrictions

None

show oam cfm local

Description

Display information about CFM Local status and configuration.

Supported Platforms

This command is supported in all platforms.

Syntax

show oam cfm local [**brief**] [**detail**] [**statistics**]

Parameters

brief

Description:	This parameter displays a summary information about the status, including MD name, MA name, MEP ID, MAC Address, TX RDI, Defects, Highest Defect, TX Interface Status, TX Port Status.
Value:	N/A
Default Value:	N/A

detail

Description:	This parameter displays all that the brief parameter displays plus some current configurations. These include Level, Primary VLAN ID, VLAN List, CCM Interval, Remote MEP IDs, Interface, Direction, Fault Alarm Time and Fault Reset Time. When no parameter is given the show command displays the same content of detail parameter.
Value:	N/A
Default Value:	N/A

statistics

Description:	This parameter displays the statistics related to local the MEPs, including the number of received CCMs with sequence errors,
---------------------	---

the current sequence number of transmitted CCMs and the total number of transmitted CCMs.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
MD	The Maintenance Domain name.
MA	The Maintenance Association name.
MEP	The Maintenance End Point ID.
MAC Address	The MAC Address of local MEP.
TX RDI	The Remote Defect Indication in Continuity Check Messages being transmitted by this MEP.
Defects	Show all defects detected by state machines in this local MEP.
Highest Priority Defect	Show the highest priority defect presented in this configuration.
TX Interface Status TLV	The link status of the interface where the local MEP is configured. This status can be Up or Down.
Block State:	Blocking state that CFM applies to the interface on which the Down MEP is attached. When fault-action is block-port, this status can be Blocked or Forwarding. Status N/A is presented if fault-action is not configured.

Output	Description
Shutdown State:	Shutdown state that CFM applies to the interface on which the UP MEP is attached. When fault-action is shutdown-port, this status can be Up or Down. Status N/A is presented if fault-action is not configured.
TX Port Status TLV	The link status of the port where the local MEP is configured. Currently this status only shows "Not present" and will be implemented in the future.
Level	Level of the Maintenance Domain on which this MEP is configured.
Primary VLAN ID	The primary VLAN ID, used in Continuity Check Messages transmitted by this local MEP.
Inner VLAN ID	The inner VLAN ID (second tag) used in Continuity Check Messages transmitted by this local MEP.
VLAN List	List of VLANs from the Maintenance Association on which this MEP is configured.
CCM Interval	Transmission interval for Continuity Check Messages, inherited from the configuration of the Maintenance Association on which this MEP is configured.
Remote MEP IDs	The list of Remote MEPs, inherited from the configuration of the Maintenance Association on which this MEP is configured.
Interface	The interface on which the MEP is configured.
Direction	The MEP direction, either Up or Down
Fault Alarm Time	Configuration of Fault Alarm Time.
Fault Reset Time	Configuration of Fault Reset Time.

Output	Description
<code>RX Seq Error Count</code>	Number of received Continuity Check Messages with sequence number errors.
<code>TX Curr Seq Num</code>	Current sequence number for Continuity Check Messages transmitted by this MEP.
<code>TX CCM Total</code>	Total transmitted Continuity Check Messages.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.0	This command was introduced.
4.6	Added <i>Block State</i> information.
4.8	Added <i>Shutdown State</i> information.

Usage Guidelines

Given the equipment has the following CFM configuration: md Domain level 5 ma Association primary-vlan-id 1 vlan-list 1 ccm-interval 1s remote-meps 2 mep 1 interface gigabit-ethernet-1/1/9 direction down primary-vlan-id 1 continuity-check cci-enabled lowest-fault-priority-defect remote-mac-error fault-action block-port. Let's see the **brief** information:

```
# show oam cfm local brief | notab
oam cfm local
  md Domain
  ma Association
  mep 1
  mac-address 00:04:df:40:9c:1b
  tx-rdi False
  defects -
    highest-priority-defect -
  tx-interface-status-tlv Up
  block-state Forwarding
  tx-port-status-tlv "Not Present"
#
```

Now let's see the **detail** information:

```
# show oam cfm local detail | notab
oam cfm local
  md Domain
  ma Association
  mep 1
  mac-address 00:04:df:40:9c:1b
  tx-rdi False
  defects -
    highest-priority-defect -
  tx-interface-status-tlv Up
  block-state Forwarding
  tx-port-status-tlv "Not Present"
  level 5
  primary-vlan-id 1
  vlan-list 1
  ccm-interval 1s
  remote-mep-ids 2
  interface gigabit-ethernet-1/1/9
  direction Down
  fault-alarm-time 2500ms
  fault-reset-time 10000ms
#
```

Impacts and precautions

None

Hardware restrictions

None

show oam cfm remote

Description

Display information about CFM Remote status and configuration.

Supported Platforms

This command is supported in all platforms.

Syntax

show oam cfm remote [**brief**] [**detail**] [**statistics**]

Parameters

brief

Description: This parameter displays a summary information about the status, including MD name, MA name, Local MEP ID, Remote MEP ID, MAC Address, RX RDI, State, RX Interface Status, RX Port Status, Last State Change and Sender ID.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays all that the **brief** parameter displays. When no parameter is given the show command displays the same content of **detail** parameter.

Value: N/A

Default Value: N/A

statistics

Description: This parameter displays the statistics related to the MEPs, including the sequence number of the Continuity Check Message that was last received from this remote MEP.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
MD	The Maintenance Domain name.
MA	The Maintenance Association name.
Local MEP	The Local Maintenance End Point ID.
Remote MEP	The Remote Maintenance End Point ID.
MAC Address	The MAC Address of Remote MEP.
RX RDI	The Remote Defect Indication.
State	The operational state of the Remote MEP. 'Failed' means that a local MEP is missing Continuity Check Messages from this remote MEP. 'OK' means that valid Continuity Check Messages from this remote MEP are being received with the expected periodicity.
RX Interface Status TLV	The link status of the interface where the remote MEP is configured. This status can be Up or Down
RX Port Status TLV	The link status of the port where the remote MEP is configured. This status can be Up or Blocked.
Last State Change	The time past since last state change occurred. If current remote MEP state is 'OK', this time since the MEP recovered from a failure. If the current remote MEP state is 'Failed', this is the time since the failure occurred.
Sender ID	The sender ID from the last CCM received.
RX Last Seq Num	Last received Continuity Check Messages sequence number.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.0.0	This command was introduced.
-------	------------------------------

Usage Guidelines

Given the equipment has the following CFM configuration: md Domain level 5 ma Association primary-vlan-id 1 vlan-list 1 ccm-interval 1s remote-meps 2 mep 1 interface gigabit-ethernet-1/1/9 direction down primary-vlan-id 1 continuity-check cci-enabled lowest-fault-priority-defect remote-mac-error. Let's see the **brief** information:

```
# show oam cfm remote brief | notab
oam cfm remote
md Domain
ma Association
local-mep 1
remote-mep 2
mac-address 00:04:df:61:25:49
rx-rdi False
state Ok
rx-interface-status-tlv Up
rx-port-status-tlv "Not Present"
last-state-change "1min 41s ago"
rx-sender-id ""
#
```

Now let's see the **detail** information:

```
# show oam cfm remote detail | notab
oam cfm remote
md Domain
ma Association
local-mep 1
remote-mep 2
```

```
mac-address 00:04:df:61:25:49
rx-rdi False
state Ok
rx-interface-status-tlv Up
rx-port-status-tlv "Not Present"
last-state-change "1min 52s ago"
rx-sender-id ""
#
```

Impacts and precautions

None

Hardware restrictions

None

ACTIVATION TEST

This topic describes the commands related to management of activation test features such as commands to configure RFC2544 generator or traffic loop with MAC swap support.

traffic-loop

Description

Create traffic loopback to test and verify the transmit and receive ports.

Supported Platforms

This command is supported in all platforms.

Syntax

traffic-loop *id* **interface** *interface-name* **destination-mac-address** *mac-address* **source-mac-address** *mac-address* **vlan** *vlan-id*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

traffic-loop *id*

Description: Traffic loopback test identifier.

Value: 1 - 8

Default Value: N/A

interface *interface-name*

Description: Interface to configure loopback mode on.

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: N/A

destination-mac-address *mac-address*

Description: Destination MAC address of the generated traffic.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

source-mac-address *mac-address*

Description: Source MAC address from data generator device.

Value: xx:xx:xx:xx:xx:xx

Default Value: N/A

vlan *vlan-id*

Description: ID of VLAN used on this traffic test session.

Value: 1 - 4094

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.2	This command was introduced.
-----	------------------------------

Release	Modification
5.0	Added support for 25G interfaces.
5.10	Added support to DM4270, DM4380 and DM4770 platforms.

Usage Guidelines

Example:

This example show how to create a traffic loopback test.

```
#config
Entering configuration mode terminal
(config)# traffic-loop 1
(traffic-loop-1)# interface gigabit-ethernet-1/1/1
(traffic-loop-1)# destination-mac-address a3:84:b3:8a:2e:59
(traffic-loop-1)# source-mac-address 21:7d:ed:70:B1:5f
(traffic-loop-1)# vlan 100
(traffic-loop-1)# top
(config)# commit
Commit complete.
(config)#
```

Impacts and precautions

- Only pre-existing interfaces will be accepted when entering an interface name.
- Link aggregation groups (LAG) cannot be used on for interface parameter.
- Interfaces added as a member of a link aggregation group (LAG) can be used.
- Traffic Loopback may cause loss of access to inband management! Therefore it is recommended to use **commit confirmed** for safety.

Hardware restrictions

N/A

EFM

This topic describes the commands related to the management of transport layer functions between network elements such as commands to monitor the link status or detect remote failures.

efm

Description

Ethernet in the First Mile configuration according to the specification described in IEEE 802.3ah-2004.

Supported Platforms

This command is supported in all platforms.

Syntax

oam efm interface *interface-name* **mode** *working-mode*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Ethernet interface where EFM is being enabled.
Value: *interface-type-chassis/slot/port*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.
Default Value: N/A

mode *working-mode*

Description: Set the EFM working mode on the interface to be configured.
Value: *active | passive*
Default Value: active

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

The EFM can be enabled on Ethernet interfaces to monitor link operation and improve fault isolation on a network.

```
# config
(config)# oam efm interface gigabit-ethernet-1/1/1
(config-oam-efm-interface-gigabit-ethernet-1/1/1)# mode passive
(config-oam-efm-interface-gigabit-ethernet-1/1/1)# commit
Commit complete.
(config-oam-efm-interface-gigabit-ethernet-1/1/1)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show oam efm

Description

Display information about EFM status and configuration. This show only presents ports that are configured for EFM.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show oam efm interface [ port ]
```

Parameters

port

Description: The Interface with EFM whose status is desired to show.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
INTERFACE	The Interface that is configured for EFM.
MODE	EFM working mode configured on port.
BLOCKED	The block status on port.
LOCAL DISCOVERY STATUS	The local status of the EFM discovery process.

Output	Description
LOCAL LINK FAULT	The event indicating if a loss of signal (LoS) error has occurred on local physical link.
LOCAL CRITICAL EVENT	The event indicating if an unspecified critical event has occurred on local physical link.
REMOTE DISCOVERY STATUS	The remote status of the EFM discovery process.
REMOTE LINK FAULT	The event indicating if a loss of signal (LoS) error has occurred on remote physical link.
REMOTE CRITICAL EVENT	The event indicating if an unspecified critical event has occurred on remote physical link.
REMOTE DYING GASP	The timestamp of the last time an unrecoverable remote fault has occurred.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

5.0	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has the following ports configured for EFM.

```
# show running-config oam efm
efm
interface ten-gigabit-ethernet-1/1/1
  mode active
!
!
```

A show will present:

```
# show oam efm
```

INTERFACE	MODE	BLOCKED	LOCAL DISCOVERY STATUS	LOCAL LINK FAULT	LOCAL CRITICAL EVENT	REMOTE DISCOVERY STATUS	REMOTE LINK FAULT	REMOTE CRITICAL EVENT	REMOTE DYING GASP
gigabit-ethernet-1/1/1	active	no	stable	no	no	stable	no	no	-

```
#
```

Impacts and precautions

None

Hardware restrictions

None

LLDP

This topic describes the commands related to management of link layer discovery protocol such as commands to configure optional TLVs or to inspect neighbor's information.

Ildp

Description

Link Layer Discovery Protocol configuration according to the specification described in IEEE 802.1AB (2009).

Supported Platforms

This command is supported in all platforms.

Syntax

Ildp interface *interface-name* [**admin-status** *status* | **notification** | **tlvs-tx** *tlv*]

Ildp message-fast-tx *seconds*

Ildp message-tx-hold-multiplier *tvl-multiplier*

Ildp message-tx-interval *seconds*

Ildp notification-interval *seconds*

Ildp reinit-delay *seconds*

Ildp tx-credit-max *frames*

Ildp tx-fast-init *transmissions*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface *interface-name*

Description: Selects the interface to be configured.

Value: *interface-type-chassis/slot/port*
 Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, twenty-five-g-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: None

admin-status *status*

Description: Sets the LLDP administrative status for the interface.

Value: *disabled | rx-only | tx-and-rx | tx-only*

Default Value: tx-and-rx (transmit and receive LLDP frames)

notification

Description: Enables generation of SNMP notifications for events associated with this interface.

Value: N/A

Default Value: N/A

tlvs-tx *tlv*

Description: Selects which optional TLVs are transmitted to neighbors.

Value: *port-description | system-capabilities | system-description | system-name*

Default Value: None

message-fast-tx *seconds*

Description: Sets the time interval in seconds between transmissions during fast transmission periods.

Value: 1-3600

Default Value: 1

message-tx-hold-multiplier *tvl-multiplier*

Description: Sets the TTL value that is carried in transmitted LLDP frames. It is used as a multiplier for message-tx-interval.

Value: 2-10

Default Value: 4

message-tx-interval *seconds*

Description: Sets the time interval in seconds between transmissions during normal transmission periods.

Value: 5-32768

Default Value: 30

notification-interval *seconds*

Description: Sets the time interval in seconds between transmissions of SNMP notifications during normal transmission periods.

Value: 5-3600

Default Value: 30

reinit-delay *seconds*

Description: Sets the amount of delay in seconds from when admin-status of an interface becomes 'disabled' until re-initialization is attempted.

Value: 1-10

Default Value: 2

tx-credit-max *frames*

Description: Sets the maximum number of consecutive LLDP frames that can be transmitted in a second.

Value: 1-100

Default Value: 5

tx-fast-init *transmissions*

Description: Sets the number of LLDP frames that are transmitted during a fast transmission period.

Value: 1-8

Default Value: 4

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.6	This command was introduced.
5.10	Added support for 25G interfaces.

Usage Guidelines

Example:

This example shows how to configure LLDP with port-description and system-name TLVs transmission disabled.

```
# config
Entering configuration mode terminal
(config)# lldp
(lldp)# message-fast-tx 100
(lldp)# message-tx-hold-multiplier 5
(lldp)# message-tx-interval 20
(lldp)# notification-interval 10
(lldp)# reinit-delay 5
(lldp)# tx-credit-max 50
(lldp)# tx-fast-init 5
(lldp)# interface gigabit-ethernet-1/1/1
(lldp-gigabit-ethernet-1/1/1)# admin-status tx-only
(lldp-gigabit-ethernet-1/1/1)# notification
(lldp-gigabit-ethernet-1/1/1)# no tlvs-tx port-description
(lldp-gigabit-ethernet-1/1/1)# no tlvs-tx system-name
(lldp-gigabit-ethernet-1/1/1)# top
(config)# commit
Commit complete.
(config)#
```

Impacts and precautions

All optional TLVs are transmitted to neighbors by default. To disable the transmission of a specific TLV use the **no tlvs-tx** command.

Hardware restrictions

This command is not available for the management interface.

show lldp local

Description

Displays information about LLDP Local status and configuration.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show lldp local [ interface interface-name ] [ detail ] [ statistics ]
```

Parameters

interface *interface-name*

Description: Selects the interface to display local LLDP information.

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: N/A

detail

Description: This parameter displays detailed local LLDP information.

Value: N/A

Default Value: N/A

statistics

Description: Displays the statistics related to LLDP agent, including current number of frames transmitted, received or dropped by interface, current number of inserts and deletions in the LLDP table as well as number of neighbors aged out and more.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
CHASSIS ID SUBTYPE	The value that indicates the basis for the chassis ID entity that is listed in the chassis ID field. For the local system this value is <i>mac-address</i> .
CHASSIS ID	The specific identifier for the chassis in this system. For the local system it is represented by the system MAC.
SYSTEM NAME	The local system's assigned name.
SYSTEM DESCRIPTION	The description of this network entity. Includes the full name and version identification of the local system's hardware type, software operating system and networking software.
SYSTEM CAPABILITIES SUPPORTED	The primary functions supported by the local system.
SYSTEM CAPABILITIES ENABLED	The primary functions enabled on the local system.
INTERFACE NAME	The local interface.
PORT ID SUBTYPE	The value that indicates the basis for the identifier that is listed in the port ID field. For the local system this value is <i>interface-name</i> .
PORT ID	The specific identifier for the local interface.
PORT DESCRIPTION	The description of the local interface.
REMOTE TABLE INSERTS	Total number of neighbors inserted in the LLDP remote table.

Output	Description
REMOTE TABLE DELETES	Total number of neighbors deleted in the LLDP remote table.
REMOTE TABLE DROPS	Total number of neighbors dropped in the LLDP remote table.
REMOTE TABLE AGEOUTS	Total number of neighbors aged out in the LLDP remote table.
TX FRAMES	Current number of LLDP frames transmitted on a given interface.
RX FRAMES	Current number of LLDP frames received on a given interface.
FRAME DROPS	Current number of LLDP frames dropped on a given interface.
FRAMES WITH ERROR	Current number of LLDP frames with error received on a given interface.
PDU LENGTH ERRORS	The number of LLDPDU length errors recorded on a given interface.
UNKNOWN TLVS COUNT	Current number of unknown/unrecognized TLVs received on a given interface.
DISCARDED TLVS COUNT	Current number of discarded TLVs on a given interface.
NEIGHBORS AGEOUTS	Current number of neighbors aged out on a given interface.
Default	
N/A	

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has 2 interfaces the command could result in the following output:

```
# show lldp local
lldp local chassis-id-subtype mac-address
lldp local chassis-id 00:04:DF:60:D0:18
lldp local system-name ""
lldp local system-description "Local System Description"
lldp local system-capabilities-supported bridge,router
lldp local system-capabilities-enabled bridge
PORT ID
INTERFACE NAME SUBTYPE ...
-----
gigabit-ethernet-1/1/1 interface-name ...
gigabit-ethernet-1/1/2 interface-name ...
PORT ID PORT DESCRIPTION
-----
gigabit-ethernet-1/1/1 Gigabit Ethernet Port 1
gigabit-ethernet-1/1/2 Gigabit Ethernet Port 2
```

The output of **statistics** command could look like this:

```
# show lldp statistics
lldp remote-table-inserts 50
lldp remote-table-deletes 12
lldp remote-table-drops 40
lldp remote-table-ageouts 12
TX RX FRAME ...
FRAMES FRAMES DROPS ...
-----
gigabit-ethernet-1/1/1 140 500 0 ...
gigabit-ethernet-1/1/2 150 1240 40 ...
FRAMES PDU UNKNOWN DISCARDED
WITH LENGTH TLVS TLVS NEIGHBOR
ERROR ERRORS COUNT COUNT AGEOUTS
-----
10 0 20 3 2
15 0 32 5 10
```

Impacts and precautions

None

Hardware restrictions

None

show lldp neighbors

Description

Displays information about LLDP neighbors status.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show lldp neighbors [ interface-name ] [ brief ] [ detail ] [ management ] [ unknown-tlvs ]
```

Parameters

interface-name

Description: Selects the local interface to display neighbor LLDP information.

Value: *interface-type-chassis/slot/port*
Examples of *interface-type*: **gigabit-ethernet, ten-gigabit-ethernet, forty-gigabit-ethernet, hundred-gigabit-ethernet.**

Default Value: N/A

brief

Description: This parameter displays a summary information from neighbors, including ID, chassis ID subtype, chassis ID, system name and port Description.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays all that the **brief** parameter displays plus system capabilities supported, system capabilities enabled, port ID subtype and port ID from neighbors. When no parameter is given the show command displays the same content of **brief** parameter.

Value: N/A

Default Value: N/A

management

Description: This parameter displays the management information from neighbors, including neighbor ID, management address subtype, management address, interface ID subtype and interface ID.

Value: N/A

Default Value: N/A

unknown-tlvs

Description: This parameter displays the unknown TLVs received from neighbors.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
LOCAL INTERFACE	The local interface associated with this neighbor.
NEIGHBOR ID	The neighbor's identification for the system.
CHASSIS ID SUBTYPE	The value that indicates the basis for the chassis ID entity that is listed in the chassis ID field. Possible values are <i>chassis-component</i> , <i>interface-alias</i> , <i>port-component</i> , <i>mac-address</i> , <i>network-address</i> , <i>interface-name</i> and <i>local</i> .
CHASSIS ID	The specific identifier for the neighbor's chassis.
SYSTEM NAME	The neighbor's system name.
SYSTEM DESCRIPTION	The neighbor's description. Includes the full name and version identification of the system's hardware type, software operating system and networking software.

Output	Description
SYSTEM CAPABILITIES SUPPORTED	The primary functions supported by the neighbor.
SYSTEM CAPABILITIES ENABLED	The functions enabled on the neighbor.
PORT ID SUBTYPE	The value that indicates the basis for the identifier that is listed in the port ID field. Possible values are <i>interface-alias</i> , <i>port-component</i> , <i>mac-address</i> , <i>network-address</i> , <i>interface-name</i> , <i>agent-circuit-id</i> and <i>local</i> .
PORT ID	The specific identifier for the neighbor's interface.
PORT DESCRIPTION	The description of the neighbor's interface.
ADDRESS SUBTYPE	The type of the management address listed in the address field.
ADDRESS	The management address of the neighbor.
INTERFACE ID SUBTYPE	The value that indicates the numbering method used for defining the interface ID field. Possible values are <i>unknown</i> , <i>if-index</i> and <i>system-port-number</i> .
INTERFACE ID	The assigned number that identifies the interface associated with the management address.
TLV TYPE	The type of the unknown TLV received.
TLV INFO	The value of the unknown TLV received.
Default	
N/A	

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has 2 interfaces with a neighbor attached at each one of them, the command could result in the following output:

```
# show lldp neighbors
LOCAL INTERFACE      NEIGHBOR ID      CHASSIS ID      CHASSIS ...
                        ID      SUBTYPE      ID
-----
gigabit-ethernet-1/1/1  1      chassis-component  4      ...
gigabit-ethernet-1/1/2  2      chassis-component  4      ...

SYSTEM NAME  PORT DESCRIPTION
-----
DmSwitch     Ethernet Port 12
DmSwitch     Ethernet Port 15
```

The output of **management** command could look like this:

```
# show lldp neighbors management
LOCAL INTERFACE      NEIGHBOR ID      ADDRESS      ADDRESS ...
                        ID      SUBTYPE      ADDRESS
-----
gigabit-ethernet-1/1/1  1      ipv4      40.0.0.4      ...
gigabit-ethernet-1/1/2  2      ipv4      30.0.0.4      ...

INTERFACE      INTERFACE ID
SUBTYPE      SUBTYPE
-----
system-port-number  12
system-port-number  15
```

The output of **detail** command could look like this:

```
# show lldp neighbors detail
LOCAL INTERFACE      NEIGHBOR ID      CHASSIS ID      CHASSIS ...
                        ID      SUBTYPE      ID
-----
gigabit-ethernet-1/1/1  1      chassis-component  4      ...
gigabit-ethernet-1/1/2  2      chassis-component  4      ...
```


SYSTEM NAME	SYSTEM DESCRIPTION	SYSTEM CAPABILITIES SUPPORTED	SYSTEM CAPABILITIES ENABLED	...
DmSwitch	Switch Description	bridge	bridge	...
DmSwitch	Switch Description	bridge	bridge	...

PORT ID SUBTYPE	PORT ID	PORT DESCRIPTION
interface-name	gigabit-ethernet-1/1/12	Ethernet Port 12
interface-name	gigabit-ethernet-1/1/15	Ethernet Port 15

Impacts and precautions

None

Hardware restrictions

None

TWAMP

This topic describes the commands related to management of Active Measurement Protocol such as commands to configure and inspect OWAMP, TWAMP Generator or TWAMP Reflector.

show oam twamp reflector connection

Description

Shows the list of current and deactivated TWAMP-control connections.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector connection [brief | detail]

Parameters

brief

Description: This parameter displays a summary information about all current and previous TWAMP-Control connections.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays a detailed information about all current and previous TWAMP-Test connections.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Client address	Display the TWAMP Control-Client IP address for this connection.
Client port	Display the TCP port used by the TWAMP Control-Client to initiate this connection.
Server address	Display the IP address from the current device used by the TWAMP Server on this connection.
Server port	Display the TCP port used by the TWAMP Server to initiate this connection.
State Connection state	Display state of the TWAMP-Control connection. States may be: <i>unknown, connecting, established, active</i> or <i>finished</i> .
Connection identifier	Display the TWAMP-Control connection identifier.
VRF name	Display the name of VRF instance assigned to TWAMP reflector.
Mode	Display the operational mode of TWAMP reflector (not configurable).
Inactive connection timeout	Display the timeout to close the connection if no packet is received.
Test Session Number	Display the timeout to close the connection if no packet is received.
Default	
N/A	

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.4	This command was introduced.

Usage Guidelines

This example below demonstrates two TWAMP-Control sessions. The first session is deactivated, and the second is running at the moment of the show.

Example:

```
# show oam twamp reflector connection brief
Client-address Client-port Server-address Server-port State
-----
192.168.0.30    58500      192.168.0.25    862      finished
192.168.0.26    58548      192.168.0.25    862      active
```

The description for each TWAMP-Control session state is shown below:

- *connecting*: the TWAMP-Control session parameters are being negotiated by the Server and Control-Client.
- *established*: TWAMP-Control session established but no tests are running.
- *active*: TWAMP-Control session is active and a related TWAMP-Test session is running.
- *finished*: TWAMP-Control session is closed.
- *unknown*: unknown state. Either an error occurred or it was not possible to determine the current TWAMP-Control session state

Impacts and precautions

- Former TWAMP-Control sessions will appear in this show with state *closed*.

Hardware restrictions

N/A

show oam twamp reflector test-session

Description

Shows the list of current and deactivated TWAMP-Test sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector test-session [brief | detail]

Parameters

brief

Description: This parameter displays a summary information about all current and previous TWAMP-Test sessions.

Value: N/A

Default Value: N/A

detail

Description: This parameter displays a detailed information about all current and previous TWAMP-Test sessions.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Sender address	Display the TWAMP Control-Client IP address for this session.

Output	Description
Sender port	Display the UDP port used by the TWAMP Control-Client to send TWAMP test packets.
Reflector address	Display the IP address from the current device used by the TWAMP Session-Reflector on this TWAMP-Test session.
Reflector port	Display the UDP port used by the TWAMP Session-Reflector to reflect TWAMP test packets.
State Test session state	Display state of the TWAMP-Test session. States may be: <i>unknown</i> , <i>inactive</i> , <i>active</i> .
Connection ID	Display the TWAMP connection identifier.
Session ID	Display the TWAMP Session identifier in hexadecimal format.
VRF name	Display the name of VRF instance assigned to TWAMP reflector.
Mode	Display the operational mode of TWAMP reflector (not configurable).
DSCP	Display the Differentiated Services Code Point (DSCP) transmitted in this TWAMP-Test session.
Payload length	Payload length of received test packets.
Created time	Display the TWAMP-Test session creation time.
Last start time	Display the TWAMP-Test session start time.
Last stop time	Display the TWAMP-Test session stop time.
Test RX packets	Display the total of received packets.

Output	Description
Test RX packets error	Display the total of received packets with error.
Test TX packets	Display the total of transmitted packets.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.4	Brief command was introduced.
4.6	Detail command was introduced.

Usage Guidelines

This example below demonstrates two TWAMP-Test sessions. The first TWAMP-Test session is deactivated, and the second is running at the moment of the show.

Example:


```
# show oam twamp reflector test-session brief
Sender-address  Sender-port  Reflector-address  Reflector-port  State
-----
192.168.0.30    9785           192.168.0.25      9785           finished
192.168.0.26    9328           192.168.0.25      9328           active
```

```
# show oam twamp reflector test-session detail
Test-session-state : finished
Connection-ID      : 1
Session-ID         : 0x1e1e1e02e18809228f6e503f9c958a74
Sender-address     : 192.168.0.30
Sender-port        : 9785
Reflector-address  : 192.168.0.25
Reflector-port     : 9785
VRF name           : global
Mode               : unauthenticated
DSCP               : 0 (CS0)
Payload-length     : 50
Created-time       : 2019-11-26 20:27:14
Last-start-time    : 2019-11-26 20:27:16
Last-stop-time     : 2019-11-26 20:27:29
Test-RX-packets    : 50
Test-RX-packets-error: 0
Test-TX-packets    : 50

Test-session-state : active
Connection-ID      : 2
Session-ID         : 0x1e1e1e02e18809374bb7b6bbfd86610
Sender-address     : 192.168.0.26
Sender-port        : 9328
Reflector-address  : 192.168.0.25
Reflector-port     : 9328
VRF name           : global
Mode               : unauthenticated
DSCP               : 0 (CS0)
Payload-length     : 50
Created-time       : 2019-11-26 20:28:33
Last-start-time    : 2019-11-26 20:28:35
Last-stop-time     : never
Test-RX-packets    : 18
Test-RX-packets-error: 0
Test-TX-packets    : 18
```

Impacts and precautions

- Closed TWAMP-Test sessions will appear in these shows with state *finished*.

Hardware restrictions

N/A

show oam twamp sender connection

Description

Shows the list of current and deactivated TWAMP-Control connections.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector connection *connection-id* [**brief** | **test-session** | **test-session-statistics**]

Parameters

connection-id

Description: Specify Configure the TWAMP Control-Client connection ID.

Value: 1 - 65535

Default Value: N/A

brief

Description: This parameter displays information about TWAMP-Control client configuration.

Value: N/A

Default Value: N/A

test-session

Description: This parameter displays information about every TWAMP-Test session configuration.

Value: N/A

Default Value: N/A

test-session-statistics

Description:	This parameter displays information about every TWAMP-Test session statistics.
Value:	N/A
Default Value:	N/A

Output Terms

Output	Description
Connection ID	Display the TWAMP connection identifier.
Administrative Status	Display the TWAMP connection administrative status configured.
Client IP	Display the TWAMP Control-Client IP address for this connection.
Client port	Display the TCP port used by the TWAMP Control-Client to initiate this connection.
Server IP	Display the IP address from the current device used by the TWAMP Server on this connection.
Server port	Display the TCP port used by the TWAMP Server to initiate this connection.
VRF name	Display the name of VRF instance assigned to TWAMP connection.
Mode	Display the operational mode of TWAMP connection (not configurable).
Number of packets	Display the number of packets sent on TWAMP-Test sessions.
Packets interval	Display the packet interval on TWAMP-Test sessions.
Test Interval	Display the test interval on TWAMP-Test sessions.

Output	Description
Number of Test-Sessions	Display the number of TWAMP-Test sessions configured on TWAMP-Control connection.
Connection State	Display state of the TWAMP-Control connection.
Last-connection-start-time	Display date and time of last TWAMP-Control connection started.
Last-connection-stop-time	Display date and time of last TWAMP-Control connection finished.
Test-session-ID	Display the TWAMP-Test session identifier configured.
Session-ID	Display the TWAMP-Test session identifier generated the server.
State	Display state of the TWAMP-Test session.
Sender IP	Display the TWAMP Control-Client address.
Sender Port	Display the UDP port negotiated by the TWAMP Control-Client to run this TWAMP-Test session.
Reflector IP	Display the TWAMP Session-Reflector address.
Reflector Port	Display the UDP port negotiated by the TWAMP Session-Reflector to run this TWAMP-Test session.
DSCP	Display the DSCP configured for this TWAMP-Test session.
Packet Size	Display the packet size configured for this TWAMP-Test session.
Min Port	Display the UDP minimum port configured for this TWAMP-Test session.

Output	Description
Max Port	Display the UDP maximum port configured for this TWAMP-Test session.
Minimum Delay	Display the minimum delay value identified during the test.
Maximum Delay	Display the maximum delay value identified during the test.
Average Delay	Display the average delay value identified during the test.
Minimum Jitter	Display the minimum jitter value identified during the test.
Maximum Jitter	Display the maximum jitter value identified during the test.
Average Jitter	Display the average jitter value identified during the test.
Loss Ratio	Display the percentage of packets lost during the test.
Packets Sent	Display the number of packets sent during the test.
Packets Received	Display the number of packets received during the test.
Packets Error	Display the number of packets with errors received during test.
Packets Reordered	Display the number of packets reordered during test.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

4.8	These commands were introduced.
-----	---------------------------------

6.4	The connection ID range was modified from [1..255] to [1..65535].
-----	---

Usage Guidelines

This example below demonstrates the *show oam twamp sender connection brief*.

Example:

```
# show oam twamp sender connection 1 brief
Connection ID           : 1
Administrative Status   : enabled
Client IP               : 192.168.0.26
Client Port             : 53073
Server IP               : 192.168.0.25
Server Port             : 862
VRF name                : global
Mode                   : unauthenticated
Number of packets       : 50
Packets interval        : 200 ms
Test Interval           : 30 s
Number of Test-Sessions : 1
-----
#
```

This example below demonstrates the *show oam twamp sender connection test-session*.

Example:

```
# show oam twamp sender connection 1 test-session
Connection ID           : 1
Connection State        : last run successful
Last-connection-start-time : 2019-12-3 20:07:52
Last-connection-stop-time  : 2019-12-3 20:08:06
Test-session-ID         : 1
```

```

Session-ID       : 0xc0a80019e1913f1821d323fdb76f7c6
State            : last run successful
Sender IP        : 192.168.0.26
Sender Port      : 30119
Reflector IP     : 192.168.0.25
Reflector Port   : 30119
VRF name         : global
DSCP             : 0 (CS0)
Packet Size      : 64
Min Port         : 1024
Max Port         : 655351
-----

```

#

This example below demonstrates the *show oam twamp sender connection test-session-statistics*.

Example:

```

# show oam twamp sender connection 1 test-session
Connection ID      : 1
Last-connection-start-time : 2019-12-3 20:07:52
Last-connection-stop-time  : 2019-12-3 20:08:06
Test-session-ID    : 1
Session-ID         : 0xc0a80019e1913f1821d323fdb76f7c6
State              : last run successful
Minimum Delay      : 1.70 ms
Maximum Delay      : 4.36 ms
Average Delay      : 2.07 ms
Minimum Jitter     : 0.03 ms
Maximum Jitter     : 0.19 ms
Average Jitter     : 0.05 ms
Loss Ratio         : 0.000%
Packets Sent       : 50
Packets Received   : 50
Packets Error      : 0
Packets Reordered  : 0
-----

```

#

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp reflector

Description

Enable TWAMP Session-Reflector on the device.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to enable the TWAMP Session-Reflector on this device.

```
(config)# oam twamp reflector
(twamp-reflector)# commit
```

Impacts and precautions

The TWAMP Session-Reflector will respond to any reachable IP address configured in the device. This includes the management interface, any L3 logical interface or loopback interface given they are reachable by the TWAMP controller. To restrict which IP addresses should be allowed to start a test session, use the command *twamp reflector client-address*.

Hardware restrictions

N/A

twamp reflector administrative-status

Description

Configures the desired administrative status of the TWAMP Session-Reflector.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector administrative-status *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

administrative-status *status*

Description:	Set to <i>up</i> to (re)activate or <i>down</i> to deactivate the TWAMP Session-Reflector.
Value:	up down.
Default Value:	up.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.4	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a TWAMP Session-Reflector.

```
(config)# oam twamp reflector
(twamp-reflector)# administrative-status down
(twamp-reflector)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp reflector client-address

Description

Configures a list of IP addresses allowed to start a TWAMP-Test session with this reflector. This list works as a whitelist ACL.

If there is no IP address configured, any IP address will be allowed to start a TWAMP-Test session with this reflector with no restriction.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector { *ipv4* | *ipv6* } **client-address** { *a.b.c.d* | *x:x:x:x::x* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

client-address { *a.b.c.d* | *x:x:x:x::x* }

Description:	IP address allowed to start a TWAMP-Test session.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to allow an IP address to start a TWAMP-Test session with this reflector.

```
(config)# oam twamp reflector
(twamp-reflector)# ipv4 client-address 192.168.1.1
(config-client-address-192.168.1.1)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp reflector client-network

Description

Configures a list of IP networks allowed to start a TWAMP-Test session with this reflector. This command is similar to *twamp reflector client-address* but allows any IP inside the configured network to start a test session. This list works as a whitelist ACL.

If there is no IP address or IP network configured, any IP address will be allowed to start a TWAMP-Test session with this reflector with no restriction.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector { *ipv4* | *ipv6* } **client-network** { *a.b.c.d/x* | *x:x:x:x::x/x* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

client-network { *a.b.c.d/x* | *x:x:x:x::x/x* }

Description: Network which IPs are allowed to start a TWAMP-Test session.

Value: a.b.c.d/x or x:x:x:x::x/x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to allow any IP on a network to start a TWAMP-Test session with this Session-Reflector.

```
(config)# oam twamp reflector
(twamp-reflector)# ipv4 client-network 192.168.1.0/24
(config-client-network-192.168.1.0/24)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp reflector port

Description

Configures which TCP port will listen for connections on this TWAMP Session-Reflector. Note that the TWAMP Session-Reflector must be disabled to allow the change of the port number.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector port *port-number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

port *port-number*

Description:	Set the TCP port number that will be listening for new TWAMP-Control connections.
Value:	862 1024-65535
Default Value:	862

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.6	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to change the TWAMP Session-Reflector listening TCP port.

```
(config)# oam twamp reflector
(twamp-reflector)# port 50000
(twamp-reflector)# commit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp reflector vrf

Description

Assign a VRF instance to TWAMP reflector.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp reflector vrf *vrf-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vrf *vrf-name*

Description:	Assign a VRF instance to TWAMP reflector.
Value:	Name of an existent VRF.
Default Value:	global

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to assign the VRF to TWAMP reflector on this device.

```
(config)# oam twamp reflector
(twamp-reflector)# vrf red
(twamp-reflector)# commit
Commit complete.
(twamp-reflector)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender administrative-status

Description

Configure the TWAMP Control-Client global administrative-status on the device.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender administrative-status *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

administrative-status *status*

Description: Activate (up) or deactivate (down) the TWAMP Control-Client global administrative status.

Value: up | down.

Default Value: up

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the global administrative status of TWAMP Control-Client on this device.

```
(config)# oam twamp sender administrative-status down
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection

Description

Configure the TWAMP Control-Client connection on the device.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* [**ipv4** | **ipv6**] [**source-address** | **target-address**] *ipv4 address* | *ipv6 address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP Control-Client connection ID.

Value: 1 - 255

Default Value: N/A

[**ipv4** | **ipv6**] **source-address** *ipv4 address* | *ipv6 address*

Description: Configure the TWAMP Control-Client source address.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

[**ipv4** | **ipv6**] **target-address** *ipv4 address* | *ipv6 address*

Description: Configure the TWAMP Control-Client target address.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
5.0	The connection range was modified from [0..255] to [1..255].
6.4	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the TWAMP Control-Client connection on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)#
(config-connection-1)# ipv4 source-address 192.168.0.26
(config-source-address-192.168.0.26)# exit
(config-connection-1)# ipv4 target-address 192.168.0.25
(config-target-address-192.168.0.25)# exit
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

The number of TWAMP Control-Client connection is limited to 10 connections. The number of TWAMP-Test sessions is limited to 8 per connection or 10 TWAMP-Test sessions globally in the device.

Hardware restrictions

N/A

twamp sender connection

Description

Configure the TWAMP Control-Client connection administrative-status on the device.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **administrative-status** *status*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP Control-Client connection ID.

Value: 1 - 65535

Default Value: N/A

administrative-status *status*

Description: Activate (up) or deactivate (down) the TWAMP Control-Client connection.

Value: up | down.

Default Value: up

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the administrative status of TWAMP Control-Client connection on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# administrative-status down
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection number-of-packets

Description

Configure the number of packets sent on every TWAMP-Test session.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **number-of-packets** *number*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP Control-Client connection ID.

Value: 1 - 65535

Default Value: N/A

number-of-packets *number*

Description: Configure the number of packets sent on every test-session.

Value: 1 - 65535

Default Value: 50

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.4	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the number of packets used on every TWAMP-Test session on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# number-of-packets 100
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection server-port

Description

Configure the server port number for TCP connection.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **server-port** *TCP port*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description:	Configure the TWAMP Control-Client connection ID.
Value:	1 - 65535
Default Value:	N/A

server-port

Description:	Configure the server port number for TCP connection.
Value:	1024 - 65535
Default Value:	862

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.4	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the server port of the TWAMP Control-Client connection on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# server-port 1024
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection test-session

Description

Configure the TWAMP-Test sessions in the device.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-session** *test-session ID* [**ipv4** | **ipv6**] [**source-address** | **target-address**] *ipv4 address* | *ipv6 address*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP sender connection ID.

Value: 1 - 65535

Default Value: N/A

test-session

Description: Configure the TWAMP-Test session.

Value: 1 - 255

Default Value: N/A

[**ipv4** | **ipv6**] **source-address** *ipv4 address* | *ipv6 address*

Description: Configure the TWAMP-Test session source address.

Value: a.b.c.d or x:x:x:x::x.

Default Value: N/A

[**ipv4** | **ipv6**] **target-address** *ipv4 address* | *ipv6 address*

Description:	Configure the TWAMP-Test session target address.
Value:	a.b.c.d or x:x:x:x::x.
Default Value:	N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
5.0	The test-session range was modified from [0..255] to [1..255].
6.4	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the TWAMP-Test sessions on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-session 1
(config-test-session-1)# ipv4 source-address 192.168.0.26
(config-source-address-192.168.0.26)# exit
(config-test-session-1)# ipv4 target-address 192.168.0.25
(config-target-address-192.168.0.25)# exit
```



```
(config-test-session-1)# commit
Commit complete.
(config-test-session-1)#
```

Impacts and precautions

The number of TWAMP sender connection is limited to 10 connections. The number of TWAMP-Test sessions is limited to 8 per connection or 10 TWAMP-Test sessions globally in the device.

Hardware restrictions

N/A

twamp sender connection test-session dscp

Description

Configure the DSCP used in TWAMP-Test sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-session** *test-session ID* **dscp** *dscp value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP sender connection ID.

Value: 1 - 65535

Default Value: N/A

test-session *test-session ID*

Description: Configure the TWAMP-Test session.

Value: 1 - 255

Default Value: N/A

dscp *dscp value*

Description: Configure the DSCP used in TWAMP-Test sessions.

Value: 0 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34
| 36 | 38 | 40 | 46 | 48 | 56

Default Value: 0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.4	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the DSCP used in TWAMP-Test session on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-session 1
(config-test-session-1)# dscp 56
(config-test-session-1)# commit
Commit complete.
(config-test-session-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection test-session max-port

Description

Configure the UDP maximum port number used in TWAMP-Test sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-session** *test-session ID* **max-port** *UDP port*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP sender connection ID.

Value: 1 - 65535

Default Value: N/A

test-session *test-session ID*

Description: Configure the TWAMP-Test session.

Value: 1 - 255

Default Value: N/A

max-port *UDP port*

Description: Configure the UDP maximum port number.

Value: 1024 - 65535

Default Value: 65535

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the UDP maximum port of a TWAMP-Test session on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-session 1
(config-test-session-1)# max-port 6500
(config-test-session-1)# commit
Commit complete.
(config-test-session-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection test-session min-port

Description

Configure the UDP minimum port number used in TWAMP-Test sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-session** *test-session ID* **min-port** *UDP port*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP sender connection ID.

Value: 1 - 65535

Default Value: N/A

test-session *test-session ID*

Description: Configure the TWAMP-Test session.

Value: 1 - 255

Default Value: N/A

min-port *UDP port*

Description: Configure the UDP minimum port number.

Value: 1024 - 65535

Default Value: 1024

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the UDP minimum port of a TWAMP-Test session on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-session 1
(config-test-session-1)# min-port 2048
(config-test-session-1)# commit
Commit complete.
(config-test-session-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection test-session packet-size

Description

Configure the size of packets sent in TWAMP-Test sessions.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-session** *test-session ID* **packet-size** *size*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description: Configure the TWAMP sender connection ID.

Value: 1 - 65535

Default Value: N/A

test-session *test-session ID*

Description: Configure the TWAMP-Test session.

Value: 1 - 255

Default Value: N/A

packet-size *size*

Description: Configure the size of packets sent in TWAMP-Test sessions.

Value: 64 - 65535

Default Value: 64

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the packet size used in a TWAMP-Test session on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-session 1
(config-test-session-1)# packet-size 128
(config-test-session-1)# commit
Commit complete.
(config-test-session-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection vrf

Description

Assign a VRF instance to TWAMP Control-Client connection.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **vrf** *vrf-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description:	Configure the TWAMP Control-Client connection ID.
Value:	1 - 65535
Default Value:	N/A

vrf *vrf-name*

Description:	Assign a VRF instance to TWAMP Control-Client connection.
Value:	Name of an existent VRF.
Default Value:	global

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.0	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

The VRF must be previously created.

Example:

This example shows how to assign the VRF to TWAMP Control-Client connection.

```
(config)# oam twamp sender connection 1
(config-connection-1)# vrf red
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

twamp sender connection vrf

Description

Configure the test interval in seconds.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

oam twamp sender connection *connection-id* **test-interval** *interval*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

connection-id

Description:	Configure the TWAMP Control-Client connection ID.
Value:	1 - 65535
Default Value:	N/A

test-interval *interval*

Description:	Configure the test interval in seconds.
Value:	0 - 65535
Default Value:	300

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
6.2	The connection ID range was modified from [1..255] to [1..65535].

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the TWAMP Control-Client connection on this device.

```
(config)# oam twamp sender connection 1
(config-connection-1)# test-interval 60
(config-connection-1)# commit
Commit complete.
(config-connection-1)#
```

Impacts and precautions

All TWAMP-Test sessions of a connection will start after test-interval counting. Before the first round of tests the state of all TWAMP-Test sessions will show – indicating that tests don't run yet.

Hardware restrictions

N/A

SFLOW

This topic describes the commands related to the configuration of sFlow Protocol.

sflow agent ipv4

Description

Configures the IP address of sFlow agent

Supported Platforms

This command is supported in all platforms.

Syntax

oam sflow agent ipv4 *ip*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

agent ipv4 *ip*

Description: Specifies the agent IPv4 identifier.

Value: a.b.c.d

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.8	This command was introduced.
-----	------------------------------

Usage Guidelines

This command can be executed directly via CLI.

The IP address of sFlow agent is not mandatory and if it is not configured, the IP from management interface will be used. In case outband management IP is not available, the address 0.0.0.0 is used.

Example:

This example shows how to configure the IP address (identifier) of sFlow agent.

```
(config)# oam
(oam)# sflow agent ipv4 192.168.0.26
(sflow)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

sflow collector

Description

Configures a sFlow collector

Supported Platforms

This command is supported in all platforms.

Syntax

```
oam sflow collector name ipv4 address [ enabled | disabled ] [ max-datagram-size size ] [ port value ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

name

Description:	Specifies a name for the collector.
Value:	String (1-32 characters)
Default Value:	N/A

ipv4 *address*

Description:	Specifies collector IPv4 address.
Value:	a.b.c.d
Default Value:	N/A

enabled

Description:	Enables the collector (this is set by default)
Value:	n/a
Default Value:	N/A

disabled

Description:	Disables the collector.
---------------------	-------------------------

Value: n/a
Default Value: N/A

max-datagram-size *size*

Description: Specifies the maximum datagram size of sFlow packets
Value: 200-9116
Default Value: 1400

port *value*

Description: Specifies the sFlow collector listening UDP port number.
Value: 1-65535
Default Value: 6343

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a sFlow collector.

```
(config)# oam
(oam)# sflow collector collector_1
(config-sflow-collector-collector_1)# ipv4 10.1.1.1
(config-sflow-collector-collector_1)# commit
Commit complete.
(config-sflow-collector-collector_1)#
```

Example:

This example shows how to configure a sFlow collector UDP port and maximum datagram size.

```
(config)# oam
(oam)# sflow collector collector_1
(config-sflow-collector-collector_1)# port 32768
(config-sflow-collector-collector_1)# max-datagram-size 4500
(config-sflow-collector-collector_1)# commit
Commit complete.
(config-sflow-collector-collector_1)#
```

Impacts and precautions

The collector IP address must be reachable through mgmt or L3 interface.

The maximum datagram size must take into account the maximum header size configured at the interfaces, otherwise samples may be dropped. Also, if those values are close enough to each other, it may happen to have sFlow datagrams with 0 (zero) samples sent to collector.

Hardware restrictions

N/A

sflow interface

Description

Configures the interface to be monitored by sFlow.

Supported Platforms

This command is supported in all platforms.

Syntax

oam sflow interface *interface* [**counter-sampling-collector** *collector-name* | **counter-sampling-interval** *interval* | **flow-sampling-collector** *collector-name* | **flow-sampling-rate** *rate* | **max-header-size** *size*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

interface

Description: Specifies the interface to be monitored.

Value: String

Default Value: N/A

flow-sampling-rate *rate*

Description: Specifies the interface sampling rate in the format 1/*rate*. Flow sampling average of 1 out of N packets transmitted or received on the port.

Value: 4096-16777215 for gigabit-ethernet
4096-16777215 for ten-gigabit-ethernet
4096-16777215 for twenty-five-g-ethernet
20480-16777215 for forty-gigabit-ethernet
51200-16777215 for hundred-gigabit-ethernet

Default Value: 8192 for gigabit-ethernet
 20480 for ten-gigabit-ethernet
 51200 for twenty-five-g-ethernet
 81920 for forty-gigabit-ethernet
 204800 for hundred-gigabit-ethernet

max-header-size *size*

Description: Specifies the sFlow maximum header size in bytes.

Value: 64-512

Default Value: 128

flow-sampling-collector *collector-name*

Description: Specifies the collector to send flow samples.

Value: String

Default Value: N/A

counter-sampling-collector *collector-name*

Description: Specifies the collector to send counter samples.

Value: String

Default Value: N/A

counter-sampling-interval *interval*

Description: Specifies the time interval in seconds to send a new counter sampling to counter collector.

Value: 2-3600

Default Value: 20

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.8	This command was introduced.
5.10	Added support for 25G interfaces.

Usage Guidelines

This command can be executed directly via CLI.
Only Ethernet interfaces are supported. Link Aggregation and L3 interfaces are not supported.

Example:

This example shows how to configure an interface to be monitored by sFlow.

```
(config)# oam
(oam)# sflow
(sflow)# collector collector_1 ipv4 10.1.1.1
(sflow-collector-collector_1)# interface gigabit-ethernet-1/1/1
(sflow-gigabit-ethernet-1/1/1)# flow-sampling-collector collector_1
(sflow-gigabit-ethernet-1/1/1)# commit
Commit complete.
(sflow-gigabit-ethernet-1/1/1)#
```

Example:

This example shows how to configure a sampling rate in a monitored interface.

```
(config)# oam
(oam)# sflow
(sflow-collector-collector_1)# interface gigabit-ethernet-1/1/1
(sflow-gigabit-ethernet-1/1/1)# flow-sampling-rate 8192
(sflow-gigabit-ethernet-1/1/1)# commit
Commit complete.
(sflow-gigabit-ethernet-1/1/1)#
```

Example:

This example shows how to configure the maximum header size in a monitored interface.

```
(config)# oam
(oam)# sflow
(sflow-collector-collector_1)# interface gigabit-ethernet-1/1/1
(sflow-gigabit-ethernet-1/1/1)# max-header-size 256
(sflow-gigabit-ethernet-1/1/1)# commit
Commit complete.
(sflow-gigabit-ethernet-1/1/1)#
```

You can use ranges and wildcards to edit more than one interface at once. Note that range operations do not add new interfaces, they only act on already added interfaces.

```
(config)# oam
(oam)# sflow
(sflow)# collector collector_1 ipv4 10.1.1.1
(sflow-collector-collector_1)# interface gigabit-ethernet-1/1/1
(sflow-gigabit-ethernet-1/1/1)# interface gigabit-ethernet-1/1/3
(sflow-gigabit-ethernet-1/1/3)# interface ten-gigabit-ethernet-1/1/1
(sflow-ten-gigabit-ethernet-1/1/1)# exit
(sflow)# interface gigabit-ethernet-1/1/1-3
(sflow-gigabit-ethernet-1/1/1-3)# flow-sampling-rate 5000
(sflow-gigabit-ethernet-1/1/1-3)# interface ten-gigabit-ethernet-1/1/*
(sflow-ten-gigabit-ethernet-1/1/*)# flow-sampling-rate 40000
(sflow-gigabit-ethernet-1/1/1)# commit
Commit complete.
(sflow-gigabit-ethernet-1/1/1)# top
(config)# show oam sflow
oam
sflow
  interface gigabit-ethernet-1/1/1
    flow-sampling-rate 5000
  !
  interface gigabit-ethernet-1/1/2
    flow-sampling-rate 5000
  !
  interface gigabit-ethernet-1/1/3
    flow-sampling-rate 5000
  !
  interface ten-gigabit-ethernet-1/1/1
    flow-sampling-rate 40000
  !
  !
  !
```

Example:

This example shows how to configure an interface to send counter samples to a counter collector.

```
(config)# oam
(oam)# sflow
(sflow)# collector collector_1 ipv4 10.1.1.1
(sflow-collector-collector_1)# interface gigabit-ethernet-1/1/1
(sflow-gigabit-ethernet-1/1/1)# counter-sampling-collector collector_1
(sflow-gigabit-ethernet-1/1/1)# counter-sampling-interval 10
(sflow-gigabit-ethernet-1/1/1)# commit
Commit complete.
(sflow-gigabit-ethernet-1/1/1)#
```

Impacts and precautions

Once an interface and collector are configured in sFlow, it starts sampling on that interface with default sampling rate. In order to disable the sampling, the user must remove the interface or collector from sFlow. Some sample packets can be dropped if the maximum datagram size does not take into account the maximum header size.

For egress flow sampling, only unicast packets are sent to sflow collector. Multicast, broadcast and unknown unicast packets are not supported in the egress direction.

Hardware restrictions

N/A

REMOTE DEVICES MANAGEMENT

This topic describes the commands related to Remote Devices Management (RDM) such as commands to allow remote control by a master device.

remote-devices

Description

Remote Devices Management (RDM) configuration.

Supported Platforms

This command is supported only in the following platforms: DM4370, DM4360.

Syntax

remote-devices mode *operational-mode* **interface** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

mode *operational-mode*

Description: Set the RDM operational mode on the equipment.

Value: *slave*

Default Value: slave

interface *interface-name*

Description: Ethernet interface where RDM is being enabled.

Value: *interface-type-chassis/slot/port*
Examples of interface-type: gigabit-ethernet, ten-gigabit-ethernet.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.2	This command was introduced.

Usage Guidelines

RDM can be enabled on Ethernet interfaces to allow the remote control by a master device. EFM protocol must be enabled on the interface to allow the configuration.

```
# config
(config)# oam efm interface gigabit-ethernet-1/1/1
(config-oam-efm-interface-gigabit-ethernet-1/1/1)# mode passive
(config-oam-efm-interface-gigabit-ethernet-1/1/1)# top
(config)# remote-devices interface gigabit-ethernet-1/1/1
(rdm-gigabit-ethernet-1/1/1)# commit
Commit complete.
(rdm-gigabit-ethernet-1/1/1)# end
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show remote-devices

Description

Display information about RDM status and configuration. This show only presents ports that are configured for RDM.

Supported Platforms

This command is supported in all platforms.

Syntax

show remote-interface interface [*port*]

Parameters

port

Description: The Interface with RDM whose status is desired to show.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
MODE	RDM operational mode configured on equipment.
RECEIVED VLAN ID	VLAN ID configuration received from remote equipment.
RECEIVED IP ADDRESS	IP address configuration received from remote equipment.
RECEIVED DEFAULT GATEWAY	Default Gateway address configuration received from remote equipment.

Output	Description
INTERFACE NAME	The Interface that is configured for RDM.
STATE	The current state of the RDM protocol on port.
OUI	Organization Unique Identifier received from remote equipment.
OID	The SNMP Object Identifier from remote equipment.
VENDOR NUMBER	Vendor specific information from remote equipment.
MAC ADDRESS	MAC Address in hexadecimal presentation from remote equipment.
SERIAL NUMBER	Serial Number from remote equipment.
REMOTE INTERFACE	The remote interface with the communication established.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

5.2	This command was introduced.
-----	------------------------------

Usage Guidelines

Given the equipment has established the communication with another equipment through RDM protocol and the following port configured for RDM.

```
# show running-config remote-devices
remote-devices
interface gigabit-ethernet-1/1/1
!
!
#
```

A show will present:

```
# show remote-devices
remote-devices
mode slave
received vlan-id 100
received ip-address 63.161.169.137/16
received default-gateway 63.161.169.1

INTERFACE NAME          STATE      OUI         OID          ...
-----
gigabit-ethernet-1/1/1  ready     00:04:df    1.3.6.1.4.1.3709.1.2.91 ...
gigabit-ethernet-1/1/2  detected  00:04:df    1.3.6.1.4.1.3709.1.2.91 ...

VENDOR      SERIAL      REMOTE
NUMBER      NUMBER      INTERFACE
-----
1           00:04:df:10:11:12  1731295    eth 1/20
1           00:04:df:10:11:12  8721983    eth 1/23

#
```

Impacts and precautions

None

Hardware restrictions

None

CHAPTER 13: SYNCHRONIZATION

This chapter describes the CLI commands related to time synchronization signals at DmOS.

NTP

This topic describes the commands related to management of Network Time Protocol such as commands to configure an external NTP Server or to inspect the system clock.

clock

Description

Configure settings related to the local clock.

Supported Platforms

This command is supported in all platforms.

Syntax

clock timezone *timezone name* *timezone offset*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

timezone name

- | | |
|-----------------------|---|
| Description: | Set a friendly name for the timezone. Any value will be accepted. |
| Value: | Length 2-30 |
| Default Value: | None. |

timezone offset

- | | |
|---------------------|---|
| Description: | Define an offset from UTC for the <code>show system clock</code> command. |
|---------------------|---|

Value: From -12 to 14.

Default Value: 0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

`clock timezone` is used to describe the current device location and its offset from UTC (a value of 0 defines that the device should output times in UTC); `show system clock` displays the current system clock, using the offset information provided by `clock timezone`.

Usage example:

```
DM4610# config
DM4610(config)# clock timezone Brazil -3
DM4610(config)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

set system clock

Description

Set the hardware clock (RTC).

Supported Platforms

This command is supported in all platforms.

Syntax

set system clock *date time*

Parameters

date

Description: Set the clock date.

Value: YYYYMMDD

Default Value: None.

time

Description: Set the clock time, in “hh:mm:ss” format. The clock must be set in a 24-hour format.

Value: hh:mm:ss

Default Value: None.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.8	The command syntax was modified from “set clock” to “set system clock”.

Usage Guidelines

Usage example:

```
DM4610# set system clock 20150815 13:30:00
Clock is set.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show sntp

Description

Displays the current status of sntp servers.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show sntp { brief }
```

Parameters

brief

Description: Shows summarized information about sntp servers.

Value: N/A.

Default Value: N/A.

Output Terms

Output	Description
Tally Codes (TC)	The server clock selection process status.
Server IP	The remote server IP to request NTP information.
Stratum	The stratum level of remote server.
When	Time in seconds of last message replied.
Poll	Time selected to send next synchronization message.

Output	Description
Delay	Round-trip delay to the server (in milliseconds).
Offset	Relative time of the server clock to the local clock (in milliseconds).
Reach	Server reachability status.
Auth	The server authentication status.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
3.0	This command was introduced.

Usage Guidelines

Usage example:

```
# show sntp brief
Tally Codes (TC):
 *: syspeer, .: distance exceeded, o: PPS derived, +: candidate, #: selected,
 -: outlier, x: falseticker, blank: unreachable
```

TC	Server IP	Stratum	When(*)	Poll(*)	Delay(ms)	Offset(ms)	Reach	Auth
*	1.1.1.1	2	2	32	17.891	-1.252	yes	none
+	1.1.1.2	3	22	32	0.287	0.777	yes	ok
	1.1.1.3	16	-	1024	0.000	0.000	no	bad

*Field in seconds if not specified, otherwise 'h' for hours and 'm' for minutes.

Note that if SNTP authentication fail the server will be shown as unreachable like Server IP 1.1.1.3 on table above.

Impacts and precautions

N/A

Hardware restrictions

N/A

show system clock

Description

Displays the current date and time.

Supported Platforms

This command is supported in all platforms.

Syntax

show system clock

Parameters

N/A

Output Terms

Output	Description
Current date and time	Displays the Current date and time in “YYYY-MM-DD HH:MM:SS UTC[offset] [Timezone-name]” format

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.8	<p>The command syntax was modified from “show clock” to “show system clock”.</p> <p>Date and time display format for “show system clock” command was changed from “[day of the week] [month] [day] HH:MM:SS (timezone name/UTC[offset])” to “YYYY-MM-DD HH:MM:SS UTC[offset] [Timezone-name]”.</p>

Usage Guidelines

Usage example:

```
DM4610# show system clock
1980-05-17 00:30:15 UTC+3 Brazil
```

Impacts and precautions

N/A

Hardware restrictions

N/A

sntp

Description

Configure the settings related to the local clock.

Supported Platforms

This command is supported in all platforms.

Syntax

sntp { **authenticate** | **authentication-key** *key ID* **md5** *MD5 key* | **client** | **min-poll** *poll-interval* | **max-poll** *poll-interval* | [**source** { **ipv4 address** *a.b.c.d* | **ipv6 address** *X:X:X:X::X* | **interface** *interface-name* }] | **server** *IP address* [**key** *key ID*] | **vrf** *vrf-name* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

authenticate

Description: Enables NTP authentication feature.

Value: None

Default Value: Disabled

client

Description: Enables SNTP client functionality.

Value: None

Default Value: Disabled

min-poll *poll-interval*

Description: Sets the minimum polling interval in power of two seconds.

Value: 3-17 (2^3 to 2^{17})

Default Value: 6 ($2^6 = 64$ seconds)

max-poll *poll-interval*

Description: Sets the maximum polling interval in power of two seconds.

Value: 3-17 (2^3 to 2^{17})

Default Value: 10 ($2^{10} = 1024$ seconds)

source ipv4 address *a.b.c.d*

Description: Specifies the source IPv4 address from which NTP server connection will be established.

Value: a.b.c.d

Default Value: None

source ipv6 address *X:X:X:X::X*

Description: Specifies the source IPv6 address from which NTP server connection will be established.

Value: X:X:X:X::X

Default Value: None

source interface *interface-name*

Description: Specifies the interface whose IP address will be used for outgoing SNTP packets.

Value: Interface name in format I3-<name> or loopback-<id>.

Default Value: None

vrf *vrf-name*

Description: Specifies the name of VRF in which the NTP server connection will be established.

Value: VRF name.

Default Value: None

server *IP address*

Description: Sets the IP address of a NTP server the SNTP Client is allowed to synchronize with. Max number of servers is six.

Value: a.b.c.d or X:X:X:X::X

Default Value: None

key *key ID*

Description: Associate the server with the given key identifier.

Value: 1-4294967295.

Default Value: None

authentication-key *key ID*

Description: Specify the authentication key identifier.

Value: 1-4294967295.

Default Value: None

md5 *MD5 key*

Description: Specify the key for NTP authenticated connections.

Value: String value up to 20 characters.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.2	SNTP client was introduced.
3.0	Replaced parameter “poll-interval” by “min-poll” and “max-poll”. Added IPv6 and source support.
5.2	Source interface can be selected by name.

Release	Modification
---------	--------------

7.0	Source interface loopback and VRF can be selected by name.
-----	--

Usage Guidelines

Since the parameters **min-poll** and **max-poll** are defined using an exponent in power of two, in accordance to RFC 5905, the following table exemplifies the exponent converted value in different time units for a better comprehension of its impact in the configuration.

Both the **source ip address** and **source interface** fields specify the source of NTP packets, and therefore cannot be configured together.

To use the **source interface** command, the I3 interface must be configured with an IP Address.

Exponent to Time Conversion Table:

Exponent	Time
3	8s
4	16s
5	32s
6	1m04s
7	2m08s
8	4m16s
9	8m32s
10	17m04s
11	34m08s
12	1h08m16s
13	2h16m32s
14	4h33m04s
15	9h06m08s
16	18h12m16s
17	36h24m32s

Example:

Enable ntp to server 172.22.110.101 with a polling interval between 32 (2^5) and 256 (2^8) seconds:

```
# config
(config)# sntp client
(config)# sntp authenticate
(config)# sntp authentication-key 1 md5 "?![:]21476a8*x"
(config)# sntp min-poll 5
(config)# sntp max-poll 8
(config)# sntp server 172.22.110.101 key 1
(config)# commit
Commit complete.
```

Enable ntp to server 2001:DB8::1 with a polling interval between 8 (2^3) and 16 (2^4)

seconds:

```
# config
(config)# sntp client
(config)# sntp authenticate
(config)# sntp authentication-key 1 md5 "?![:]21476a8*x"
(config)# sntp min-poll 3
(config)# sntp max-poll 4
(config)# sntp server 2001:DB8::1 key 1
(config)# commit
Commit complete.
```

Enable ntp to server 172.22.110.101 and source IPv4 must be 127.22.110.1:

```
# config
(config)# sntp client
(config)# sntp server 172.22.110.101
(config)# sntp source ipv4 address 127.22.110.1
(config)# commit
Commit complete.
```

Enable ntp to server 2001:DB8::100 and source IPv6 must be 2001:DB8::1:

```
# config
(config)# sntp client
(config)# sntp server 2001:DB8::100
(config)# sntp source ipv6 address 2001:DB8::1
(config)# commit
Commit complete.
```

Enable ntp to server 172.22.110.101 and source interface l3

```
# config
(config)# interface l3 l3
(config-l3-l3)# ipv4 address 172.22.110.10/24
(config-l3-l3)# top
(config)# sntp client
(config)# sntp server 172.22.110.101
(config)# sntp source interface l3-l3
(config)# commit
Commit complete.
```

Enable ntp to server 172.22.110.101 and source interface loopback

```
# config
(config)# interface loopback-0
(config-loopback-0)# ipv4 address 172.22.110.10/24
(config-loopback-0)# top
(config)# sntp client
(config)# sntp server 172.22.110.101
(config)# sntp source interface loopback-0
(config)# commit
Commit complete.
```

Enable ntp to server 172.22.110.101 and vrf green

```
# config
(config)# vrf green
(config-vrf-green)# top
(config)# sntp client
(config)# sntp server 172.22.110.101
(config)# sntp vrf green
(config)# commit
Commit complete.
```

Impacts and precautions

When **source interface** is used, the NTP transaction is in unsymmetric mode, i.e. the source and destination ports of NTP packets are different. This is described in RFC 958, inside 5. Protocol Operation, 5.1. Protocol Modes.

The **sntp source** and **sntp vrf** configuration is applied to all server destinations, not being configurable per server.

Hardware restrictions

N/A

CHAPTER 14: GPON

This chapter describes the commands related to management of GPON interfaces and remote ONUs.

OLT

This topic describes the global commands related to GPON OLT, service-port and service-vlan.

aes-key-exchange

Description

Sets the AES Key Exchange interval.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

aes-key-exchange { *interval* }

Parameters

aes-key-exchange *interval*

Description: The time interval for the AES Key Exchange procedure.

Value: Number from 30 to 26000.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

To set an aes-key-interval it is necessary to enter in the given gpon card menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# gpon 1/1
(config-gpon-1/1)# aes-key-exchange 30
```

Impacts and precautions

None

Hardware restrictions

N/A

clear interface statistics gpon

Description

This command clears the statistics for a GPON interface, ONU Ethernet or ONU GEM port.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
clear interface statistics gpon { id | onu onu-id | ethernet ethernet-port | gem gem-id }
```

Parameters

id

Description: GPON interface ID to clear statistics.

Value: Text: chassis/slot/port format

Default Value: None

onu-id

Description: ONU ID to clear statistics.

Value: Number: 0 to 127.

Default Value: None

ethernet-port

Description: ONU Ethernet port to clear statistics.

Value: Number: 1 to 4.

Default Value: None

gem-port

Description: ONU GEM port to clear statistics.

Value: Number: 1 to 16.

Default Value: None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
1.8	Removed no longer valid ONU ethernet and GEM port statistics parameters.
1.8.2	Added ONU ethernet port statistics parameters.
5.12.0	Added ONU GEM port statistics parameters.

Usage Guidelines

To clear interface statistics gpon it is necessary to enter in config menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# clear interface statistics gpon 1/1/1
```

Impacts and precautions

All statistics counters for the selected GPON interface, ONU Ethernet or ONU GEM port will be erased.

Hardware restrictions

N/A

interface gpon

Description

The interface gpon command is responsible for configuring a gpon interface.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

interface gpon *chassis/slot/port*

interface gpon *chassis/slot/port* [**upstream-fec** | **downstream-fec** | **shutdown** | **description** { *string* }*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

upstream-fec

Description: Enables forwarding of error correction for upstream flow. Changing the value of this field will prompt the user with a confirmation on the CLI. This confirmation is intended to make the user aware of the data traffic stop that will happen once this config is changed due to ponlink reset.

Value: None.

Default Value: Enable.

downstream-fec

Description: Enables forwarding of error correction for downstream flow. Changing the value of this field will prompt the user with a confirmation on the CLI. This confirmation is intended to make the user aware of the

data traffic stop that will happen once this config is changed due to ponlink reset.

Value: None.

Default Value: Enable.

reach min-distance *min-distance*

Description: Configures the minimum logical distance from OLT to ONU (in km).

The difference between maximum and minimum distance must be at least 20 km and cannot exceed 40 km.

Value: 0-40

Default Value: 0

reach max-distance *max-distance*

Description: Configures the maximum logical distance from OLT to ONU (in km).

The difference between maximum and minimum distance must be at least 20 km and cannot exceed 40 km.

Value: 0-60

Default Value: 40

shutdown

Description: Disables the GPON interface.

Value: None.

Default Value: Shutdown.

description

Description: Set the interface description or alias. Valid characters are A-Z, a-z, 0-9 and - _ / + * @

Value: The interface description.

Default Value: N/A

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
2.0	Port reach configuration option was added.

Usage Guidelines

To set interface gpon parameters is necessary to enter in the interface gpon menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)#
```

To set description

```
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# description "test interface name"
Or
(config-gpon-1/1/1)# description test_interface_name
```

To change the gpon interface logical reach to the range of 20 to 60 km:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# reach min-distance 20 max-distance 60
```

Impacts and precautions

On shutdown, the GPON interface will be disabled affecting ongoing data traffic. The user must enter 'interface gpon <id>' mode to issue other interface commands.

IMPORTANT: Upon changing upstream-fec and/or downstream-fec configuration on pon-link the data traffic of all ONUs attached to the ponlink will be temporarily stopped. This happens because the ponlink must be reset for the fec configurations to be applied.

When configuring PON link reach max-distance, take special care to give a room of 5km considering the farthest ONU. For example, if the farthest ONU is at 20km, set reach max-distance to 25km.

Hardware restrictions

N/A

load default-gpon-profiles

Description

Loads the default GPON profiles, which allow a quick configuration of GPON features.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

load default-gpon-profiles

load default-gpon-profiles-bridge

load default-gpon-profiles-router

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.8.2	This command was introduced.
4.0.0	Remove ONU-profile from default profiles list. Remove service-profile from default profiles list. Command load-default-gpon-profiles added.

Usage Guidelines

The commands create all default GPON profiles that are required to add ONUs to the configuration database. That is, the user have to neither create the profiles nor select them on the ONU. There are different sets of profiles for different applications.

There are three different sets of GPON profiles that can be loaded.

- 1) load default-gpon-profiles-bridge: suitable for bridge ONUs.
- 2) load default-gpon-profiles-router: suitable for router ONUs.
- 3) load default-gpon-profiles: suitable for bridge or router ONUs. Contains a line-profile that supports bridge (ethernet-uni) or router (veip). The OLT will skip any of the flow mappings (see line profile) if the ONU does not support it.

As the command **load factory-config**, only the candidate configuration is modified, therefore the user must commit the modifications in order to apply the configuration.

Example: Creating profiles for bridge.

```
# config
Entering configuration mode terminal
(config)# show configuration this
% No configuration changes found.
(config)# load default-gpon-profiles-?
Possible completions:
  default-gpon-profiles-bridge  Load the default GPON profiles for bridge ONUs
  default-gpon-profiles-router  Load the default GPON profiles for router ONUs
(config)# load default-gpon-profiles-bridge
Loading.
Done.
(config)# show configuration this
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
  traffic type-4 max-bw 1106944
!
profile gpon line-profile DEFAULT-LINE
  upstream-fec
  tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
  gem 1
    tcont 1 priority 1
    map any-ethernet
      ethernet any vlan any cos any
  !
!
gem 2
  tcont 1 priority 0
```

```

map any-iphost
  iphost vlan any cos any
!
!
!
(config)# commit
Commit complete.
(config)#

```

Example: Creating an ONU without explicitly selecting its profiles.

```

# config
Entering configuration mode terminal
(config)# interface gpon 1/1/3
(config-gpon-1/1/3)# onu 7
(config-gpon-onu-7)# show configuration this
interface gpon 1/1/3
  onu 7
    line-profile DEFAULT-LINE
  !
!
!
(config-gpon-onu-7)# serial-number DTCM12345678
(config-gpon-onu-7)# show configuration this
interface gpon 1/1/3
  onu 7
    serial-number DTCM12345678
    line-profile DEFAULT-LINE
  !
!
!
(config-gpon-onu-7)# commit
Commit complete.
(config-gpon-onu-7)#

```

Example: Editing profiles before the commit, to make them suitable for a different application.

```

# config
Entering configuration mode terminal
(config)# load default-gpon-profiles-router
Loading.
Done.
(config)# show configuration this
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
  traffic type-4 max-bw 1106944
!
profile gpon line-profile DEFAULT-LINE
  upstream-fec
  tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
  gem 1
    tcont 1 priority 1
    map any-veip
    veip 1 vlan any cos any
  !
!
gem 2
  tcont 1 priority 0
  map any-iphost
  iphost vlan any cos any
!
!
!
!

```

Edit the Bandwidth Profiles with a different traffic type and bandwidth:

```

(config)# profile gpon bandwidth-profile DEFAULT-BANDWIDTH
(config-bandwidth-profile-DEFAULT-BANDWIDTH)# traffic type-1 fixed-bw 5120

```

Edit the Line Profile with a different mapping, specifying a VLAN:

```
(config-bandwidth-profile-DEFAULT-BANDWIDTH)# top
(config)# profile gpon line-profile DEFAULT-LINE
(config-line-profile-DEFAULT-LINE)# gem 1
(config-line-prof-gem-1)# no map any-veip
(config-line-prof-gem-1)# map veip-300
(config-line-prof-gem-map-veip-300)# veip 1 vlan 300 cos any
```

Check the edited profiles:

```
(config-line-prof-gem-map-veip-300)# top
(config)# show configuration this
profile gpon bandwidth-profile DEFAULT-BANDWIDTH
  traffic type-1 fixed-bw 5120
!
profile gpon line-profile DEFAULT-LINE
  upstream-fec
  tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
  gem 1
    tcont 1 priority 1
    map veip-300
    veip 1 vlan 300 cos any
  !
!
gem 2
  tcont 1 priority 0
  map any-iphost
  iphost vlan any cos any
!
!
(config)# commit
Commit complete.
(config)#
```

Impacts and precautions

It is advised to use only one of the commands at a time, as running more than one will merge the configurations, potentially creating non-functional configurations.

Hardware restrictions

N/A

onu-auto-provisioning

Description

Configure all parameters to be applied to an ONU when added automatically to database. This configuration is present in the gpon-card prompt.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

onu-auto-provisioning service-port *sp-id* **gem** *gem port* **match vlan** **vlan-id** { *user-vlan* | **any** } **action** { **vlan** { **add vlan-id** *vid* | **replace vlan-id** *vid* } } [**inner-vlan** **replace vlan-id** *vid*]

onu-auto-provisioning ipv4 vlan **vlan-id** *vlan-val* { **cos** *cos-val* }

onu-auto-provisioning line-profile *line-profile-name*

onu-auto-provisioning rg-profile *rg-profile-name*

onu-auto-provisioning service-profile *svc-profile-name*

onu-auto-provisioning snmp-profile *snmp-profile-name*

onu-auto-provisioning ethernet *ethernet-uni-id* { **native vlan** **vlan-id** *vlan-val* { **cos** *cos-val* } }

onu-auto-provisioning veip *veip-id* { **native vlan** **vlan-id** *vlan-val* { **cos** *cos-val* } }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

enable

Description: Enable or disable ONU auto provisioning function.

Value: None

Default Value: None

ipv4 dhcp

Description: Configures the ONU IP Host interface to use DHCP.

Value: None

Default Value: None

ipv4 vlan vlan-id *vlan-val*

Description: Configures the VLAN ID to be configured in the ONU IP Host interface.

Value: 1-4094

Default Value: None

ipv4 vlan vlan-id *vlan-val* **cos** *cos-val*

Description: Configures the VLAN ID and CoS to be configured in the ONU IP Host interface.

Value: 0-7

Default Value: None

line-profile *line-profile-name*

Description: Reference to line-profile that will be applied to the auto provisioned ONU.

Value: Text with up to 48 characters.

Default Value: "DEFAULT-LINE".

rg-profile *rg-profile-name*

Description: Reference to rg-profile that will be applied to the auto provisioned ONU.

Value: Text with up to 48 characters.

Default Value: None.

service-profile *service-profile-name*

Description: Reference to a service-profile that will be applied to the auto provisioned ONU.

Value: Text with up to 48 characters.

Default Value: None.

snmp-profile *snmp-profile-name*

Description: Reference to snmp-profile that will be applied to the auto provisioned ONU.

Value: Text with up to 48 characters.

Default Value: None.

sp-id

Description: Service Port number.

Value: 1-16

Default Value: None.

gem *gem port*

Description: The name of the GEM Port where the service-port must apply.

Value: 1-16

Default Value: None

match vlan **vlan-id** { *user-vlan* | **any** }

Description: The value of the user VLAN where the service-port must apply.

Value: { *user-vlan* | **any** }

Default Value: None

action vlan { **add vlan-id** *vid* | **replace vlan-id** *vid* }

Description: Adds, replaces or allow a transparent flow for the matched VLAN on network side. **add vlan-id** *vid*: Adds the *vid* VLAN to the packets matched by the user-VLAN; **replace vlan-id** *vid*: Replaces the *vid* VLAN in the packets matched by the user-VLAN;

Value: 1-4094

Default Value: None

action inner-vlan **replace vlan-id** *vid*

Description: Replaces the inner-VLAN for the matched VLAN on network side. **replace vlan-id** *vid*: Replaces the *vid* VLAN in the packets matched by the user-VLAN;

Value: 1-4094

Default Value: None

ethernet *ethernet-uni-id*

Description: Specify an ethernet UNI that must be created by the ONU auto provisioning function. Required in order to monitor SNMP OIDs for the ethernet UNI.

Value: 1-4

Default Value: None

native vlan *vlan-id*

Description: Configures the VLAN ID to be added for the untagged traffic in the ONU ethernet UNI.

Value: 1-4094

Default Value: None

native vlan *vlan-id* **cos** *cos-val*

Description: Configures the VLAN ID and CoS for the untagged traffic in the ONU ethernet UNI.

Value: 0-7

Default Value: 0

veip *veip-id*

Description: Specify a VEIP that must be created by the ONU auto provisioning function.

Value: 1

Default Value: None

native vlan *vlan-id*

Description: Configures the VLAN ID to be added for the untagged traffic in the ONU VEIP.

Value: 1-4094

Default Value: None

native vlan *vlan-id* **cos** *cos-val*

Description: Configures the VLAN ID and CoS to be added for the untagged traffic in the ONU VEIP.

Value: 0-7

Default Value: 0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The following configuration will enable auto provisioning feature and make auto provisioned ONUs with one traffic flow.

Example:

```
DM4610# configure terminal
Entering configuration mode terminal
DM4610(config)# gpon 1/1
DM4610(config-gpon-1/1)# onu-auto-provisioning
DM4610(config-onu-auto-provisioning)# line-profile MY_LINE
DM4610(config-onu-auto-provisioning)# service-port 1 gem 1 match vlan vlan-id 10
action vlan replace vlan-id 10
DM4610(config-onu-auto-provisioning)# ethernet 1 native vlan vlan-id 10
```

Auto provisioned ONUs with RG Profile configuration and IP Host.

Example:

```
DM4610# configure terminal
Entering configuration mode terminal
DM4610(config)# gpon 1/1
DM4610(config-gpon-1/1)# onu-auto-provisioning
DM4610(config-onu-auto-provisioning)# line-profile MY_LINE_VEIP_GEM1_IPHOST_GEM2
DM4610(config-onu-auto-provisioning)# rg-profile RG_WAN_PPPOE_VID_10
DM4610(config-onu-auto-provisioning)# ipv4 vlan vlan-id 20
DM4610(config-onu-auto-provisioning)# service-port 1 gem 1 match vlan vlan-id 10
```

```

action vlan replace vlan-id 10
DM4610(config-onu-auto-provisioning)# service-port 2 gem 2 match vlan vlan-id 20
action vlan replace vlan-id 20
DM4610(config-onu-auto-provisioning)# veip 1

```

Disable ONU auto provisioning but keep the base configuration.

Example:

```

DM4610# configure terminal
Entering configuration mode terminal
DM4610(config)# gpon 1/1
DM4610(config-gpon-1/1)# onu-auto-provisioning
DM4610(config-onu-auto-provisioning)# no enable

```

Disable ONU auto provisioning but remove the base configuration.

Example:

```

DM4610# configure terminal
Entering configuration mode terminal
DM4610(config)# gpon 1/1
DM4610(config-gpon-1/1)# no onu-auto-provisioning

```

Impacts and precautions

When auto provisioning is enabled, ONUs are added automatically to database upon an ONU discovery.

It is possible that the database configuration may be rejected due to some database validation, such as maximum number of ONUs in the PON link was reached, PON link bandwidth exceeded etc.

In those cases, an alarm per GPON interface is raised. The reject cause will be present in the user logs.

Once solved the problem, the alarm will be cleared and new ONUs can be added automatically again.

If upstream FEC is enabled on the line profile used for auto provisioning, it must also be enabled on all PON links.

When using auto provisioning it is recommended to use T-CONT traffic type 4, which has no assured or fixed bandwidths. Using any other type, and depending on the values configured, the PON link may run out of bandwidth and new ONUs will not be correctly provisioned.

IMPORTANT NOTE 1: Avoid entering in configuration prompt by using “config exclusive”. Using this mode may cause undesired behavior once auto provisioning feature does

commits into the database. Mode “config exclusive” is recommended when ONU configuration must be changed manually by the operator, preventing auto provisioning feature to add ONUs concurrently.

IMPORTANT NOTE 2: Even when using default configuration mode, upon commit, the following message may be displayed: “Aborted: the configuration database is locked by session 59 dummy tcp (system from 127.0.0.1). . .”. This means that there was a commit concurrency with the auto provisioning feature. Try to run commit again.

Hardware restrictions

N/A

profile gpon line-profile

Description

Defines the line characteristics of an ONU or of a group of ONUs, such as:

- T-CONT and GEM port linkage (GEM port priority included);
- T-CONT and Bandwidth Profile linkage;
- GEM port Ethernet/iphost/veip mapping (using VLAN and CoS);

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
profile gpon line-profile profile-name [ gem gem-id | tcont tcont-id | upstream-fec ]
```

```
profile gpon line-profile profile-name gem gem-id [ map map-name { ethernet | iphost | veip } | tcont tcont-id { priority priority-value | gem-traffic-profile profile-name } ]
```

```
profile gpon line-profile profile-name gem gem-id map map-name [ ethernet { vlan { vlan-id | any } cos { cos-val | any } } ]
```

```
profile gpon line-profile profile-name gem gem-id map map-name [ iphost { vlan { vlan-id | any } cos { cos-val | any } } ]
```

```
profile gpon line-profile profile-name gem gem-id map map-name [ veip veip-id { vlan { vlan-id | any } cos { cos-val | any } } ]
```

```
profile gpon line-profile profile-name tcont tcont-id [ bandwidth-profile bandwidth-profile-name ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

line-profile *profile-name*

Description:	Indicates the line-profile name.
Value:	Text with up to 48 characters.
Default Value:	None.

tcont *tcont-id*

Description:	Indicates the ID of the T-CONT.
Value:	1-6.
Default Value:	None.

bandwidth-profile *bandwidth-profile-name*

Description:	Indicates the name of a bandwidth-profile to be mapped to the T-CONT.
Value:	Text with up to 48 characters.
Default Value:	"DEFAULT-BANDWIDTH".

priority *priority-value*

Description:	Configures a priority for the T-CONT.
Value:	0-7.
Default Value:	0.

gem-traffic-profile *profile-name*

Description:	Indicates the name of a GEM traffic profile to be associated with the GEM port.
Value:	Text with up to 48 characters.
Default Value:	None.

upstream-fec

Description:	Enables forwarding of error correction for upstream flow.
Value:	None.
Default Value:	None.

gem *gem-id*

Description:	Indicates the ID to identify the GEM port list.
Value:	1-16.
Default Value:	None.

map *map-name***Description:** Indicates the name for the UNI port mapping.**Value:** Text with up to 48 characters.**Default Value:** None.**ethernet** { *eth-val* | **any** }**Description:** Ethernet ports to be mapped to a GEM port. To use all Ethernet ports, set any. The syntax for a range is 1-3, to use the ports 1 to 3 or 1,2,4 to use the ports 1, 2 and 4.**Value:** { 1-4 | any }**Default Value:** None.**iphost****Description:** Indicates iphost type of mapping to a GEM port.**Value:** None.**Default Value:** None.**veip** { *veip-id* }**Description:** VEIP port to be mapped to a GEM port.**Value:** VEIP values:

1.

Default Value: None.**vlan** { *vlan-id* | **any** }**Description:** VLAN ID to be mapped to a GEM port. To use all VLAN IDs, set any. Use value any in conjunction with service-port match any for untagged traffic.**Value:** { 1-4094 | any }**Default Value:** None.**cos** { *cos-val* | **any** }**Description:** CoS values that will be taken into account by the GEM port. To use all CoS values, set any. The syntax for a range is 0-3, to use the CoS values 0 to 3, or 1,2,4 to use the CoS 1, 2 and 4.**Value:** { 0-7 | any }

Default Value: None.

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.4	The the maximum GEM ID value was changed from 40 to 16.
1.8	The VEIP configuration command was added.
1.8.2	Default profiles were added.

Usage Guidelines

Create a Bandwidth Profile before binding to a T-CONT by using command **profile gpon bandwidth-profile** *bandwidth-profile-name* and configure a traffic type. See bandwidth-profile page.

Bind a Bandwidth Profile to a T-CONT before mapping GEM ports.

To set interface line profile is necessary to enter in the line profile menu.

Example:


```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon line-profile lineProfName
(config-line-profile-lineProfName)#
```

The mapping of Ethernet ports to a GEM port is done through line profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon line-profile lineProfName
(config-line-profile-lineProfName)#tcont 1 bandwidth-profile bw1
(config-line-profile-lineProfName)#gem 1
(config-line-prof-gem-1)#gem 1
(config-line-prof-gem-1)# tcont 1 priority 0
(config-line-prof-gem-1)# map map1
(config-line-prof-gem-map-map1)# ethernet 1 vlan 400 cos 0
```

Ethernet ports mapping accepts range.

Example:

```
(config-line-prof-gem-1)# map map1
(config-line-prof-gem-map-map1)# ethernet 1-2,4 vlan 400 cos 0
```

The mapping of IPHOST port to a GEM port is done through line profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon line-profile lineProfName
(config-line-profile-lineProfName)#tcont 1 bandwidth-profile bw1
(config-line-profile-lineProfName)#gem 1
(config-line-prof-gem-1)#gem 1
(config-line-prof-gem-1)# tcont 1 priority 0
(config-line-prof-gem-1)# map map1
(config-line-prof-gem-map-map1)# iphost vlan 400 cos 0
```

The mapping of VEIP port to a GEM port is done through line profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon line-profile lineProfName
(config-line-profile-lineProfName)#tcont 1 bandwidth-profile bw1
(config-line-profile-lineProfName)#gem 1
(config-line-prof-gem-1)#gem 1
(config-line-prof-gem-1)# tcont 1 priority 0
(config-line-prof-gem-1)# map map1
(config-line-prof-gem-map-map1)# veip 1 vlan 500 cos 0
```

Some third-party ONUs may not support native VLAN configuration on Ethernet UNI. To use untagged traffic set line-profile match VLAN to any and use service-port match any with action add, this will work as a native VLAN on the service-port.

Impacts and precautions

The sum of the rates of the bandwidth-profiles of the line-profile must not exceed the ponlink capacity (1.25 Gbps).

For DM4610 platform, line profile cannot have more than 3 TCONTs with bandwidth traffic type 2 to 5 and 3 TCONTs with bandwidth traffic type 1.

For DM4610-HW2/DM4615 platforms, line profile cannot have more than 4 TCONTs with bandwidth traffic type 2 to 5 and 3 TCONTs with bandwidth traffic type 1.

Configuring one **gem map** with *vlan any* and another **gem map**, with the same ports, with a specific vlan will result in undefined behavior because it is not guaranteed which mapping will match first.

Example of an invalid profile:

```
profile gpon line-profile invalid
  upstream-fec
  tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
  gem 1
    tcont 1 priority 0
    map service-1
      ethernet any vlan 100 cos any
  gem 2
    tcont 1 priority 0
    map service-2
      ethernet any vlan any cos any
```

It is also not valid to use **vlan any** on more than one **gem map** for the same group of ports.

Example of an invalid profile:

```
profile gpon line-profile invalid
  upstream-fec
  tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
  gem 1
    tcont 1 priority 0
    map service-1
      ethernet any vlan any cos any
  gem 2
    tcont 1 priority 0
    map service-2
      ethernet any vlan any cos any
```

When using an ONU with more than one Ethernet interface, the group of ports in a **gem map** should not have an intersection with another **gem map**, though it can be the same.

Example of an invalid profile:

```
profile gpon line-profile invalid
  upstream-fec
```

```
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
  tcont 1 priority 0
  map ethernet1
    ethernet 1-2 vlan 100 cos any
gem 2
  tcont 1 priority 0
  map ethernet2
    ethernet 2-4 vlan 200 cos any
```

Example of a valid profile:

```
profile gpon line-profile invalid
upstream-fec
tcont 1 bandwidth-profile DEFAULT-BANDWIDTH
gem 1
  tcont 1 priority 0
  map ethernet1
    ethernet 1-2 vlan 100 cos any
gem 2
  tcont 1 priority 0
  map ethernet2
    ethernet 1-2 vlan 200 cos any
```

It is recommended to use only one **gem map** for each GEM port because some ONUs may not support configuring more than one mapping for each GEM. With the exception of having a **gem map** for Ethernet and one for VEIP on the same GEM port, because the ONU will effectively only use one of them.

Hardware restrictions

None

rg-one-shot-prov

Description

Configures RG Profile One-shot Provisioning.

When enabled, OLT sends RG profile to ONUs only once, so any further user configuration on ONUs is not overwritten by the OLT.

When disabled, RG profile configuration is always sent to the associated ONUs, whenever they go online to the OLT.

In this case, local changes in the ONU configuration (i.e. through its WEB interface) can be lost.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

rg-one-shot-prov

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

4.9	This command was introduced.
-----	------------------------------

Usage Guidelines

To enable rg-one-shot-prov it is necessary to enter in the given gpon card menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# gpon 1/1
(config-gpon-1/1)# rg-one-shot-prov
```

To force the reprovisioning of an ONU, see command rg-reprovision.

Impacts and precautions

RG Profile will not be issued automatically in the following situations:

- 1) Enabling or disabling rg-one-shot-prov flag.
- 2) RG Profile switch to another RG Profile in an ONU.
- 3) Any change in rg-profile-override-settings in an ONU.
- 4) When the user makes a factory-reset locally at the ONU.

To re-provision RG Profile to ONU, the command rg-reprovision, available on the onu configuration tree, must be used.

Hardware restrictions

N/A

service vlan block

Description

Command used to configure service flood blocking on preexisting VLAN type n:1.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

service vlan { *vlan-id* } [**block** *traffic-type*]*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: ID of VLAN to be configured.

Value: 1 - 4094

Default Value: None

block *traffic-type*

Description: Block downstream flood traffic on configured VLAN. This configuration is only applied on VLAN type n:1. The value *broadcast* blocks broadcast traffic. The value *multicast* blocks unknown multicast traffic. The value *unicast* blocks unknown unicast traffic.

Value: {broadcast | multicast | unicast}

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.6	This command was introduced.
-----	------------------------------

Usage Guidelines

VLAN must be created and configured to type n:1 to configure a service block for it. The commit of a configuration with a service block on a non existing VLAN will result in an error message and the configuration won't be applied.

Changing service type to other than n:1 will erase any previous service block configuration.

Default behaviour of VLANs is not to block any traffic.

Impacts and precautions

This command only applies on VLANs type n:1.

Only with pre-existing VLANs the configuration commit will be successful.

Hardware restrictions

N/A

service vlan type

Description

Command used to configure service type on preexisting VLAN.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

service vlan { *vlan-id* } [**type** *service-type*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: ID of VLAN to be configured.

Value: 1 - 4094

Default Value: None

type *service-type*

Description: Service type configured on VLAN.

Value: {n:1 | 1:1 | tls}

Default Value: n:1

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.2	This command was introduced.
-----	------------------------------

Usage Guidelines

VLAN must be created to configure a service for it. The commit of a configuration with a service type on a non existing VLAN will result in an error message and the configuration won't be applied.

Impacts and precautions

Some packets might be lost when this configuration is applied due to changes on VLAN behavior.

Only with pre-existing VLANs the configuration commit will be successful.

Hardware restrictions

N/A

service-port

Description

Individualizes the data flow for each user, allowing the passthrough of this traffic and even do VLAN translation on it. It is used to connect the network side and the user device side.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

service-port *rule-id*

service-port new

gpon *ponlink* **onu** *onu-id* **gem** *gem* **port** [**match vlan** **vlan-id** { *user-vlan* | **any** } **action** { **vlan** { **add vlan-id** *vid* | **replace vlan-id** *vid* } } [**inner-vlan** **replace vlan-id** *vid*]] [**description** *description-text*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

service-port *rule-id*

Description: Enters the service-port configuration. ID of the rule to create. Must be unique for all service-ports. The “rule-id” can be used in a range format to show the active configuration of some service ports.

Value: 1-16777215

Default Value: None.

service-port new

Description: Enters the service-port configuration. ID is automatically selected (lowest free ID).

Value: None.

Default Value: None.

gpon *ponlink*

Description: Value of the ponlink where the service-port must apply.

Value: chassi/slot/port

Default Value: None.

onu *onu-id*

Description: The ID of the ONU where the service-port must apply.

Value: 0-127

Default Value: None

gem *gem port*

Description: The name of the GEM Port where the service-port must apply.

Value: 1-16

Default Value: None

match vlan *vlan-id { user-vlan | any }*

Description: The value of the user VLAN where the service-port must apply.

Value: { *user-vlan* | **any** }

Default Value: None

action vlan { **add vlan-id** *vid* | **replace vlan-id** *vid* }

Description: Adds, replaces or allow a transparent flow for the matched VLAN on network side. **add vlan-id** *vid*: Adds the *vid* VLAN to the packets matched by the user-VLAN, if using match **any** this will work as a native VLAN; **replace vlan-id** *vid*: Replaces the *vid* VLAN in the packets matched by the user-VLAN;

Value: 1-4094

Default Value: None

action inner-vlan **replace vlan-id** *vid*

Description: Replaces the inner-VLAN for the matched VLAN on network side. **replace vlan-id** *vid*: Replaces the *vid* VLAN in the packets matched by the user-VLAN;

Value: 1-4094

Default Value: None

description *description-text*

Description: A textual description of the service-port.

Value: Text up to 128 characters. Valid characters are A-Z, a-z, 0-9, space and . - _ / + * @.

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.4	The “rule-name” parameter of the service-port command was changed to “rule-id”. The “line-profile” parameter was removed from the service-port command. The the maximum GEM ID value was changed from 40 to 16.
5.6	The “service-port new” command was added to automatically allocate the “rule-id”. The “description” command was added. Line breaks was inserted between gpon, match, action and description commands.

Release	Modification
5.8	The line breaks between commands below service-port when shown running configuration was removed.

Usage Guidelines

To set a service-port it is necessary to enter in the config menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# service-port 1 gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 10
action vlan replace vlan-id 100
```

Some third-party ONUs may not support native VLAN on Ethernet UNI, a possible workaround is to use **match vlan vlan-id any** with **action vlan add**, thus doing the native VLAN on the service-port. Note that it is also necessary to use vlan any on the line-profile for the ONU used on this service-port for untagged traffic to work.

To use a service-port as an access port for a MPLS tunnel, VLAN translate must not be configured.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# service-port 1 gpon 1/1/1 onu 1 gem 1
```

Service-port parameters can be entered in a line after service-port command. Use “new” to select the first free index automatically.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# service-port 1
(config-service-port-1)# gpon 1/1/1 onu 1 gem 1 match vlan vlan-id 10 action vlan replace vlan-id 100 de
(config)# service-port new
(config-service-port-2)# gpon 1/1/1 onu 2 gem 1 match vlan vlan-id 10 action vlan replace vlan-id 100 de
```

Impacts and precautions

No flow is allowed through OLT without a service-port rule.

Up to 4096 service-ports can be configured.

A gem port that is associated to a service-port used for MPLS services should not be used in other service-ports.

Service-ports without match and action configuration must be used only for MPLS services.

Hardware restrictions

None

show interface gpon

Description

Displays GPON interface information. Regarding the discovered ONUs show operation, an ONU is only displayed if it discovered in the GPON port but not provisioned. Once an ONU is provisioned, it is no longer displayed.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show interface gpon [*chassis/slot/port*] [**brief** | **statistics** | **detail** | **discovered-onus**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

chassis/slot/port

Description: The ponlink to display information.

Value: Text: chassis/slot/port format.

Default Value: N/A

brief

Description: Display brief information of the GPON interface.

Value: brief: Fixed text 'brief'.

Default Value: N/A

statistics

Description: Display statistics information of the GPON interface.

Value: statistics: Fixed text 'statistics'.

Default Value: N/A

detail**Description:** Display detailed information of the GPON interface.**Value:** detail: Fixed text 'detail'.**Default Value:** N/A**discovered-onus****Description:** Display discovered ONUs.**Value:** N/A**Default Value:** N/A**Output Terms**

Output	Description
Physical interface	Name and status of the GPON interface.
Link-level type	Type of the Link-level.
Logical reach	Show the interface differential logical reach (in kilometers).
Downstream FEC	Downstream FEC status.
Upstream FEC	Upstream FEC status.
Transceiver type	Type of the transceiver.
Allocated upstream bandwidth	Header for the types of bandwidth allocated.
Fixed + Assured	Allocated bandwidth of both Fixed and Assured types added.
Fixed	Allocated bandwidth of Fixed type.
Assured	Allocated bandwidth of Assured type.

Output	Description
Max	Allocated bandwidth of Maximum type.
Overhead	Allocated bandwidth for inband management of all ONUs on the GPON interface.
ONUs	Number of ONUs configured on the GPON interface.
Available upstream bandwidth	Header for the types of available upstream bandwidth.
CBR BW	Available fixed bandwidth (traffic type-1 and type-5) in the ponlink.
Total BW	Available total bandwidth (assured+fixed; traffic type-1, type-2, type-3 and type-5) in the ponlink.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.

Release	Modification
---------	--------------

2.4	Added more information to usage guidelines and output parameters.
-----	---

4.2.0	Added support for range of IDs in show options.
-------	---

Usage Guidelines

Show gpon 1/1/1 information

```
# show interface gpon 1/1/4
Physical interface      : gpon 1/1/4, Enabled, Physical link is Up
Link-level type        : GPON
Logical reach          : 0-40 km
Downstream FEC         : Enabled
Upstream FEC           : Enabled
Transceiver type       : neophotonics-b
Allocated upstream bandwidth
    Fixed + Assured    : 0          kbit/s
    Fixed              : 0          kbit/s
    Assured            : 0          kbit/s
    Max                : 0          kbit/s
    Overhead           : 0          kbit/s (0 ONUs)
Available upstream bandwidth
    CBR   BW           : 439449    kbit/s
    Total BW           : 1098624   kbit/s
```

Show all gpon interfaces information

```
# show interface gpon
Physical interface      : gpon 1/1/1, Disabled, Physical link is Down
Link-level type        : GPON
Logical reach          : 0-40 km
Downstream FEC         : Enabled
Upstream FEC           : Enabled
Transceiver type       : none
Allocated upstream bandwidth
    Fixed + Assured    : 0          kbit/s
    Fixed              : 0          kbit/s
    Assured            : 0          kbit/s
    Max                : 1106944    kbit/s
    Overhead           : 33         kbit/s (1 ONUs)
Available upstream bandwidth
    CBR   BW           : 0          kbit/s
    Total BW           : 0          kbit/s

Physical interface      : gpon 1/1/2, Disabled, Physical link is Down
Link-level type        : GPON
Logical reach          : 0-40 km
Downstream FEC         : Enabled
Upstream FEC           : Enabled
Transceiver type       : none
Allocated upstream bandwidth
    Fixed + Assured    : 0          kbit/s
    Fixed              : 0          kbit/s
    Assured            : 0          kbit/s
    Max                : 0          kbit/s
    Overhead           : 0          kbit/s (0 ONUs)
Available upstream bandwidth
    CBR   BW           : 0          kbit/s
    Total BW           : 0          kbit/s

Physical interface      : gpon 1/1/3, Disabled, Physical link is Down
```

```

Link-level type      : GPON
Logical reach       : 0-40 km
Downstream FEC      : Enabled
Upstream FEC        : Enabled
Transceiver type    : none
Allocated upstream bandwidth
    Fixed + Assured  : 0          kbit/s
    Fixed            : 0          kbit/s
    Assured          : 0          kbit/s
    Max              : 0          kbit/s
    Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
    CBR BW          : 0          kbit/s
    Total BW        : 0          kbit/s

Physical interface   : gpon 1/1/4, Disabled, Physical link is Down
Link-level type      : GPON
Logical reach       : 0-40 km
Downstream FEC      : Enabled
Upstream FEC        : Enabled
Transceiver type    : none
Allocated upstream bandwidth
    Fixed + Assured  : 0          kbit/s
    Fixed            : 0          kbit/s
    Assured          : 0          kbit/s
    Max              : 0          kbit/s
    Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
    CBR BW          : 0          kbit/s
    Total BW        : 0          kbit/s

```

Show all gpon interfaces information

```

# show interface gpon *

Physical interface   : gpon 1/1/1, Disabled, Physical link is Down
Link-level type      : GPON
Logical reach       : 0-40 km
Downstream FEC      : Enabled
Upstream FEC        : Enabled
Transceiver type    : none
Allocated upstream bandwidth
    Fixed + Assured  : 0          kbit/s
    Fixed            : 0          kbit/s
    Assured          : 0          kbit/s
    Max              : 1106944    kbit/s
    Overhead         : 33         kbit/s (1 ONUs)
Available upstream bandwidth
    CBR BW          : 0          kbit/s
    Total BW        : 0          kbit/s

Physical interface   : gpon 1/1/2, Disabled, Physical link is Down
Link-level type      : GPON
Logical reach       : 0-40 km
Downstream FEC      : Enabled
Upstream FEC        : Enabled
Transceiver type    : none
Allocated upstream bandwidth
    Fixed + Assured  : 0          kbit/s
    Fixed            : 0          kbit/s
    Assured          : 0          kbit/s
    Max              : 0          kbit/s
    Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
    CBR BW          : 0          kbit/s
    Total BW        : 0          kbit/s

Physical interface   : gpon 1/1/3, Disabled, Physical link is Down
Link-level type      : GPON
Logical reach       : 0-40 km
Downstream FEC      : Enabled
Upstream FEC        : Enabled
Transceiver type    : none
Allocated upstream bandwidth
    Fixed + Assured  : 0          kbit/s
    Fixed            : 0          kbit/s
    Assured          : 0          kbit/s
    Max              : 0          kbit/s

```

```

Overhead          : 0          kbit/s (0 ONUs)
Available upstream bandwidth
  CBR   BW         : 0          kbit/s
  Total BW         : 0          kbit/s

Physical interface : gpon 1/1/4, Disabled, Physical link is Down
Link-level type   : GPON
Logical reach     : 0-40 km
Downstream FEC    : Enabled
Upstream FEC      : Enabled
Transceiver type  : none
Allocated upstream bandwidth
  Fixed + Assured  : 0          kbit/s
  Fixed            : 0          kbit/s
  Assured          : 0          kbit/s
  Max              : 0          kbit/s
  Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
  CBR   BW         : 0          kbit/s
  Total BW         : 0          kbit/s

```

Show a range of gpon interfaces information

```

# show interface gpon 1/1/3-4

Physical interface : gpon 1/1/3, Disabled, Physical link is Down
Link-level type   : GPON
Logical reach     : 0-40 km
Downstream FEC    : Enabled
Upstream FEC      : Enabled
Transceiver type  : none
Allocated upstream bandwidth
  Fixed + Assured  : 0          kbit/s
  Fixed            : 0          kbit/s
  Assured          : 0          kbit/s
  Max              : 0          kbit/s
  Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
  CBR   BW         : 0          kbit/s
  Total BW         : 0          kbit/s

Physical interface : gpon 1/1/4, Disabled, Physical link is Down
Link-level type   : GPON
Logical reach     : 0-40 km
Downstream FEC    : Enabled
Upstream FEC      : Enabled
Transceiver type  : none
Allocated upstream bandwidth
  Fixed + Assured  : 0          kbit/s
  Fixed            : 0          kbit/s
  Assured          : 0          kbit/s
  Max              : 0          kbit/s
  Overhead         : 0          kbit/s (0 ONUs)
Available upstream bandwidth
  CBR   BW         : 0          kbit/s
  Total BW         : 0          kbit/s

```

Show all gpon interfaces information (brief option)

```

# show interface gpon brief

```

Interface	DS FEC	US FEC	Admin	Link	Transceiver type
1/1/1	Enabled	Enabled	Disabled	Down	none
1/1/2	Enabled	Enabled	Disabled	Down	none
1/1/3	Enabled	Enabled	Disabled	Down	none
1/1/4	Enabled	Enabled	Disabled	Down	none

Show all gpon interfaces information (brief option)

```

# show interface gpon * brief

```

Interface	DS FEC	US FEC	Admin	Link	Transceiver type
1/1/1	Enabled	Enabled	Disabled	Down	none
1/1/2	Enabled	Enabled	Disabled	Down	none
1/1/3	Enabled	Enabled	Disabled	Down	none
1/1/4	Enabled	Enabled	Enabled	Up	neophotonics-b

Show all gpon interfaces in a given chassis/slot information (brief option)

```
# show interface gpon 1/1/* brief
```

Interface	DS FEC	US FEC	Admin	Link	Transceiver type
1/1/1	Enabled	Enabled	Disabled	Down	none
1/1/2	Enabled	Enabled	Disabled	Down	none
1/1/3	Enabled	Enabled	Disabled	Down	none
1/1/4	Enabled	Enabled	Enabled	Up	neophotonics-b

Show a range of gpon interfaces information (brief option)

```
# show interface gpon 1/1/2-3 brief
```

Interface	DS FEC	US FEC	Admin	Link	Transceiver type
1/1/2	Enabled	Enabled	Disabled	Down	none
1/1/3	Enabled	Enabled	Disabled	Down	none

Show a list of gpon interfaces information (brief option)

```
# show interface gpon 1/1/1,3 brief
```

Interface	DS FEC	US FEC	Admin	Link	Transceiver type
1/1/1	Enabled	Enabled	Disabled	Down	none
1/1/3	Enabled	Enabled	Disabled	Down	none

Show discovered ONUs in all gpon interfaces

```
# show interface gpon discovered-onus
```

Chassis / Slot / Port	Serial Number
1/1/1	DACM00000351
1/1/3	DACM00000352

Show discovered ONUs in all gpon interfaces

```
# show interface gpon * discovered-onus
```

Chassis / Slot / Port	Serial Number
1/1/1	DACM00000351
1/1/3	DACM00000352

Show discovered ONUs in all gpon interfaces in a given chassis/slot

```
# show interface gpon 1/1/* discovered-onus
```

Chassis / Slot / Port	Serial Number
1/1/1	DACM00000351
1/1/3	DACM00000352

Show discovered ONUs in a range of gpon interfaces

```
# show interface gpon 1/1/1-3 discovered-onus
```

```
Chassis / Slot / Port  Serial Number
-----
1/1/1                DACM00000351
1/1/3                DACM00000352
```

Show statistics of all gpon interfaces using table mode

```
# show interface gpon * | tab | select statistics
```

CHASSIS ID/SLOT ID/PORT ID	IN OCTETS	IN UNICAST PKTS	IN BROADCAST PKTS	IN MULTICAST PKTS	IN DISCARDS	IN ERRORS	IN UNKNOWN PROTOS	OUT OCTETS	OUT UNICAST PKTS	OUT BROADCAST PKTS	OUT MULTICAST PKTS
1/1/1	0	0	0	0	0	0	0	0	0	0	0
1/1/2	0	0	0	0	0	0	0	0	0	0	0
1/1/3	0	0	0	0	0	0	0	0	0	0	0
1/1/4	0	0	0	0	0	0	0	0	0	0	0

Impacts and precautions

It is not supported to use commas in the key wildcard in gpon interface discovered-onus

show option (

```
show interface gpon 1/1/2,3,4 discovered-onus
).
```

Hardware restrictions

N/A

ONU PROFILES

This topic describes the ONU profiles commands related to ONU traffic configuration, such as line and service profiles.

profile gpon bandwidth-profile

Description

The bandwidth-profile is used to enter in bandwidth-profile mode and manage the dynamic allocation of bandwidth for upstream flow. In this mode is possible to choose the traffic type between type-1 to type-5.

The no profile gpon bandwidth-profile command is used to delete a specific bandwidth profile.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon bandwidth-profile *profile-name* **traffic** { **type-1 fixed-bw** *fixed-bandwidth* | **type-2 assured-bw** *assured-bandwidth* | **type-3 assured-bw** *assured-bandwidth* **max-bw** *max-bandwidth* | **type-4 max-bw** *max-bandwidth* | **type-5 fixed-bw** *fixed-bandwidth* **assured-bw** *assured-bandwidth* **max-bw** *max-bandwidth* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

bandwidth-profile *profile-name*

Description: Name of the profile to create. Must be unique for all bandwidth-profiles. Can have up to 48 characters.

Value: Text: up to 48 characters.

Default Value: None

traffic type-1

Description:	Fixed bandwidth. Type-1 defines a fix bandwidth that will be fully allocated to a T-CONT. Although the user is not using the bandwidth it will not be shared with another user. Used for constant traffic with high relevance for jitter and delay parameters. VoIP for instance.
Value:	See fixed-bw parameter values.
Default Value:	None

traffic type-2

Description:	Assured bandwidth. Type-2 defines an assured bandwidth that will be allocated at the moment an ONU requires the bandwidth. The bandwidth that is not in use by the user will be shared with another ONU.
Value:	See assured-bw parameter values.
Default Value:	None

traffic type-3

Description:	Assured + maximum bandwidth. Type-3 bandwidth defines an assured bandwidth (can be shared when not in use) and an additional maximum limit (not assured) that the bandwidth can reach. Used for variable rates services for guaranteeing an average rate. This type is mainly used for VoIP services.
Value:	See assured-bw and max-bw parameters values.
Default Value:	None

traffic type-4

Description:	Max bandwidth. Type-4 defines a maximum bandwidth (not assured) that can be reached in the T-CONT. Used for variable traffic services that does not take in count jitter or delay like Internet and low priority services.
Value:	See max-bw parameter values.
Default Value:	None

traffic type-5

Description:	Fixed + assured + max bandwidth. Type-5 defines the user will have a guaranteed bandwidth, an assured bandwidth that can
---------------------	--

be occupied when necessary and a maximum bandwidth that the user can reach.

Value: See fixed-bw, assured-bw and max-bw paremeters values.

Default Value: None

fixed-bw *fixed-bandwidth*

Description: Fixed bandwidth defines a bandwidth that cannot be shared when allocated.

Value: type-1:
Number from 512 to 442752 kbit/s in steps of 64.

type-5:
Number from 128 to 442752 kbit/s in steps of 64.

type-5 for DM4610HW2:
Number from 256 to 442752 kbit/s in steps of 64.

Default Value: None

assured-bw *assured-bandwidth*

Description: Assured bandwidth defines a bandwidth that can be shared between users.

Value: Number from 256 to 1106816 kbit/s in steps of 64.

Default Value: None

max-bw *max-bandwidth*

Description: Max bandwidth defines the bandwidth the user can reach.

Value: type-3:
Number from 384 to 1106816 kbit/s in steps of 64.

type-4:
Number from 128 to 1106944 kbit/s in steps of 64.

type-4 for DM4610HW2:
Number from 256 to 1106944 kbit/s in steps of 64.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

When using traffic type-3, maximum bandwidth must be greater than or equal to assured bandwidth + 128 kbit/s.

When using traffic type-5, assured bandwidth must be greater than or equal to fixed bandwidth + 128 kbit/s and max bandwidth must be greater or equal to fixed + assured + 128 kbit/s.

When using DM4610HW2 and traffic type-3, maximum bandwidth must be greater than or equal to assured bandwidth + 256 kbit/s.

When using DM4610HW2 and traffic type-5, assured bandwidth must be greater than or equal to fixed bandwidth + 256 kbit/s and max bandwidth must be greater or equal to fixed + assured + 256 kbit/s.

To set a bandwidth profile it is necessary to enter in bandwidth profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon bandwidth-profile bwProfName
(config-bandwidth-profile-bwProfName)# traffic type-1 fixed-bw 512
```

Impacts and precautions

The profile cannot be modified after it is committed.

Hardware restrictions

N/A

profile gpon gem-traffic-profile

Description

Defines rate-limiting parameters to be associated with a GEM port, such as committed information rate (CIR), excess information rate (EIR) and upstream GEM priority.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon gem-traffic-profile *profile-name* { **cir** *rate* | **eir** *rate* | **upstream-gem-priority** *priority-value* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

gem-traffic-profile *profile-name*

Description: Name of the GEM traffic profile.

Value: String (1-48 characters).

Default Value: None

cir *rate*

Description: Committed information rate (CIR) in steps of 64 kbit/s.

Value: 64-2499968

Default Value: None

eir *rate*

Description: Excess information rate (EIR) in steps of 64 kbit/s.

Value: 0-2499904

Default Value: None

upstream-gem-priority *priority-value*

Description:	Upstream GEM port priority.
Value:	0-7
Default Value:	0

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.6	This command was introduced.
-----	------------------------------

Usage Guidelines

In order to configure a GEM traffic profile, it is necessary to enter the gem-traffic-profile menu.

Both CIR and EIR parameters must be specified, and their sum cannot exceed 2499968 kbit/s.

The total rate, also known as PIR (Peak Information Rate), is the sum of CIR and EIR.

The profile cannot be modified after it is committed.

The profile cannot be deleted if it is referenced by a line profile.

In order for the profile to be effective, it must be referenced by a line profile.

The rate-limiting configuration specified by the profile is applied in both upstream and downstream directions.

Example:

```
# config terminal
Entering configuration mode terminal
(config)# profile gpon gem-traffic-profile gemTrProfName
(config-gem-traffic-profile-gemTrProfName)# cir 10240
(config-gem-traffic-profile-gemTrProfName)# eir 5120
(config-gem-traffic-profile-gemTrProfName)# upstream-gem-priority 2
```

Impacts and precautions

Some ONU models may not support GEM traffic profile. Check the ONU datasheet for reference.

Hardware restrictions

N/A

profile gpon media-profile

Description

The media-profile command is used to configure media parameters for VoIP services, allowing the user to set a priority ordered codec list, where is set the codec type, packet-period and silence-suppression for each entry on the list. Media-profile command is also used to enable/disable out-of-band DTMF, configure the target of the jitter buffer, and the maximum depth of the jitter buffer.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
profile gpon media-profile { media-profile-name [ codec-order order-index { type codec-type | packet-period packet-period-value | silence-suppression } | jitter { target { dynamic-buffer | buffer target-buffer-value } | maximum { onu-internal-buffer | buffer maximum-buffer-value } } | oob-dtmf | pstn-protocol-variant country-code-value] }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

media-profile *media-profile-name*

Description: Indicates the media profile name.

Value: String: up to 48 characters.

Default Value: None.

codec-order *order-index*

Description: Indicates the codec selection order which will be configured. The list can be filled in any order.

Value: 1-4

Default Value: None.

type *codec-type***Description:** Select the codec type defined by IETF RFC 3551.**Value:** cn | dvi4-8000 | dvi4-11025 | dvi4-16000 | dvi4-22050 | gsm | g722 | g723 | g728 | g729 | lpc | l16-2-channel | l16-1-channel | mpa | pcma | pcmu | qcelp.**Default Value:** pcma.**packet-period** *packet-period-value***Description:** Select the packet period interval in milliseconds.**Value:** 10-30 milliseconds.**Default Value:** 10 milliseconds.**silence-suppression****Description:** Enable or disable silence suppression for the codec entry.**Value:** None.**Default Value:** Disable.**jitter target dynamic-buffer****Description:** Set the target value of the jitter buffer as dynamic.**Value:** N/A**Default Value:** None.**jitter target buffer** *target-buffer-value***Description:** Select the target value of the jitter buffer in milliseconds.**Value:** 1-65535 milliseconds.**Default Value:** 135 milliseconds.**jitter maximum onu-internal-buffer****Description:** Configure the ONU to use its internal default value for the maximum jitter buffer.**Value:** N/A**Default Value:** None.**jitter maximum buffer** *maximum-buffer-value***Description:** Select the maximum depth of the jitter buffer in milliseconds.**Value:** 1-65535 milliseconds.

Default Value: 135 milliseconds.

oob-dtmf

Description: Enable or disable out-of-band DTMF. When enabled, DTMF signals are carried out-of-band. When disabled, DTMF signals are carried in the PCM stream.

Value: None.

Default Value: Disable.

pstn-protocol-variant *country-code-value*

Description: Configure PSTN protocol variant (Country Codes). This parameter controls which variant of POTS signalling is used.

Value: AGO | ARE | ARG | AUS | AUT | BEL | BOL | BRA | CHE | CHL | CHN | COL | CYP | CZH | DEU | DNK | ECU | EGY | ESP | FIN | FRA | GBR | GHA | HKG | HUN | IND | IRL | ITA | JPN | KOR | MAR | MEX | NLD | NOR | NZL | PER | POL | PRY | ROU | SVK | SVN | SWE | TUN | TWN | URY | USA | VEN | ZAF.

Default Value: None.

Default

None.

Command Mode

Configuration mode

Required Privileges

Config

History

Release

Modification

Release	Modification
1.12	This command was introduced.

Usage Guidelines

To set the media profile it is necessary to enter in the media-profile menu.

Example:

```
# config
Entering configuration mode terminal
(config)# profile gpon media-profile mediaName
(config-media-profile-mediaName)# pstn-protocol-variant BRA
(config-media-profile-mediaName)# jitter target dynamic-buffer
(config-media-profile-mediaName)# jitter maximum buffer 30000
(config-media-profile-mediaName)# codec-order 1
(config-codec-order-1)# type pcma
(config-codec-order-1)# codec-order 2
(config-codec-order-2)# type g723
(config-codec-order-2)# codec-order 3
(config-codec-order-3)# type g729
(config-codec-order-3)# codec-order 4
(config-codec-order-4)# type pcmu
(config-codec-order-4)# packet-period 20
```

Impacts and precautions

First check the ONU capabilities before configuring the codec list, because some ONU models do not support all the codecs listed. There must be 4 codecs configured in a Media Profile.

When there is no pstn-protocol-variant configured, the ONU must use its internal default.

Hardware restrictions

None.

profile gpon onu-profile

Description

Defines the amount of each type of port of an ONU or a group of ONUs.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon onu-profile *profile-name* { **ethernet** { *eth-ports* | **adaptive** } | **pots** { *pots-ports* | **adaptive** } | **veip** *veip-ports* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

onu-profile *profile-name*

Description: Name of the ONU profile.

Value: String (1-48 characters; accepts alphanumeric characters, '+', '-', and '_').

Default Value: None

ethernet { *eth-ports* | **adaptive** }

Description: Number of Ethernet ports or adaptive mode (auto discovery).

Value: 1-4 or adaptive

Default Value: None

pots { *pots-ports* | **adaptive** }

Description: Number of POTS (Voice) ports or adaptive mode (auto discovery).

Value: 1-4 or adaptive

Default Value: None

veip *veip-ports*

Description:	Number of Virtual Ethernet Interface Points (for router/residential gateway ONUs).
Value:	1
Default Value:	None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.8	Configuration of number of VEIPs was added.

Usage Guidelines

To configure an ONU profile, it is necessary to enter the onu-profile menu.
It is not possible to create an ONU profile with no Ethernet, POTS or VEIP value.
The profile cannot be modified after it is committed.
The profile cannot be deleted if it is referenced by a service-profile.

Example (configuring an ONU profile with 4 Ethernet ports and 2 POTS ports):

```
# config
Entering configuration mode terminal
```

```
(config)# profile gpon onu-profile onuProfName
(config-onu-profile-onuProfName)# ethernet 4
(config-onu-profile-onuProfName)# pots 2
```

Example (configuring an ONU profile with a VEIP interface):

```
# config
Entering configuration mode terminal
(config)# profile gpon onu-profile onuProfName2
(config-onu-profile-onuProfName2)# veip 1
```

Impacts and precautions

N/A

Hardware restrictions

N/A

profile gpon rg-profile

Description

The rg-profile (residential gateway) is used to enter in rg-profile mode and manage the ONU DM984-42x WAN, LAN and WLAN configuration through the OLT. DM985-100 ONU also supports the rg-profile configuration, but some parameters may not be fully supported. Check DM985-100 release notes for reference. The `no profile gpon rg-profile` command is used to delete a specific RG profile.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon rg-profile *profile-name*

wan-pppoe-connection *connection-name* [**auth-type** { **auto** | **chap** | **mschap** | **pap** } | **firewall** | **fullcone-nat** | **multicast-proxy** { **igmp** } | **multicast-source** { **igmp** } | **nat** | **username** *username* | **password** *password* | **vlan-mux** **vlan** *vlan-id* **cos** *cos* **tpid** *tpid*]

wan-ip-connection *connection-name* [**firewall** | **fullcone-nat** | **multicast-proxy** { **igmp** } | **multicast-source** { **igmp** } | **nat** | **vlan-mux** **vlan** *vlan-id* **cos** *cos* **tpid** *tpid* | **ipv4** { **dhcp** | **static default-gateway** *def-gw-addr* }]

wan-bridge-connection *connection-name* [**multicast-source** { **igmp** } | **vlan-mux** **vlan** *vlan-id* **cos** *cos* **tpid** *tpid*]

wlan *wlan-name* [**network-auth** { **open** | **wpa2-psk** | **wpa2/wpa-psk** } | **ssid** { **auto** { **onu-serial-number** { **prefix** *prefix* | **suffix** *sufix* } } | **custom** *ssid* } | **wpa-encryption** { **aes** | **tkip+aes** } | **wpa-passphrase** *wpa-passphrase*]

wan-pppoe-connection *connection-name* [**itf-grouping** [**dhcp-server** | **dhcp-server-address-pool** **start-address** *starting-ip-address* **end-address** *ending-ip-address* | **igmp-snooping** | **ipv4** **address** *ip-addr* **netmask** *addr-netmask* | **ports** { **eth1** | **eth2** | **eth3** | **eth4** | **wl0** | **wl0-vap1** }] [**vlan** *vlan-id* **cos** *cos*]]]

wan-ip-connection *connection-name* [**itf-grouping** [**dhcp-server** | **dhcp-server-address-pool** **start-address** *starting-ip-address* **end-address** *ending-ip-address* | **igmp-**

snooping | **ipv4 address** *ip-addr* **netmask** *addr-netmask* | **ports** { **eth1** | **eth2** | **eth3** | **eth4** | **wl0** | **wl0-vap1** } [**vlan** *vlan-id* **cos** *cos*]]]

wan-bridge-connection *connection-name* [**itf-grouping** [**igmp-snooping** | **ipv4 address** *ip-addr* **netmask** *addr-netmask* | **ports** { **eth1** | **eth2** | **eth3** | **eth4** | **wl0** | **wl0-vap1** } [**vlan** *vlan-id* **cos** *cos*]]]

wan-pppoe-connection *connection-name* [**ip-filtering** *priority* *filtering-type* **action** *act* **match** [**destination-ip-address** *dest-addr* | **source-ip-address** *src-addr* | **protocol** *proto* | **source-port** { *port* | *port-proto* | **range** **start** *start-port* **stop** *stop-port* } | **destination-port** { *port* | *port-proto* | **range** **start** *start-port* **stop** *stop-port* }]]

wan-ip-connection *connection-name* [**ip-filtering** *priority* *filtering-type* **action** *act* **match** [**destination-ip-address** *dest-addr* | **source-ip-address** *src-addr* | **protocol** *proto* | **source-port** { *port* | *port-proto* | **range** **start** *start-port* **stop** *stop-port* } | **destination-port** { *port* | *port-proto* | **range** **start** *start-port* **stop** *stop-port* }]]

user-mgmt [**priv-lvl-support** | **priv-lvl-user**] **password** { **auto** { **onu-serial-number** { **prefix** *prefix* | **suffix** *sufix* } } | **custom** *password* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

rg-profile *profile-name*

Description: Name of the profile to create. Must be unique within all RG profiles. Can have up to 48 characters.

Value: Text: up to 48 characters.

Default Value: None

wan-pppoe-connection *connection-name*

Description: WAN PPPoE connection configuration. Each connection represents a WAN connection in the ONU.

Value: Text: up to 48 characters.

Default Value: None

auth-type { **auto** | **chap** | **mschap** | **pap** }

Description: PPPoE authentication type.

Value: auto, chap, mschap or pap.

Default Value: auto

firewall

Description: Enables firewall for the PPPoE WAN interface.

Value: None.

Default Value: no firewall

fullcone-nat

Description: Enables fullcone NAT for the PPPoE WAN interface.

Value: None.

Default Value: no fullcone-nat

multicast-proxy { igmp }

Description: Enables IGMP multicast proxy for the PPPoE WAN interface. IGMP multicast source must be enabled too.

Value: None.

Default Value: no multicast-proxy igmp

multicast-source { igmp }

Description: Enables IGMP multicast source for the PPPoE WAN interface.

Value: None.

Default Value: no multicast-source igmp

nat

Description: Enables NAT for the PPPoE WAN interface.

Value: None.

Default Value: nat

password *password*

Description: PPPoE connection password.

Value: Text: up to 32 characters.

Default Value: None.

username *username*

Description: PPPoE connection username.

Value: Text: up to 64 characters.

Default Value: None.

service-name *service-name*

Description: PPPoE connection service name.

Value: Text with up to 32 characters.

Default Value: None.

vlan-mux vlan *vlan-id*

Description: VLAN ID to be used for the WAN PPPoE interface.

Value: 1-4094.

Default Value: None.

vlan-mux cos *cos*

Description: CoS to be used for the WAN PPPoE interface.

Value: 0-7.

Default Value: 0.

vlan-mux tpid *tpid*

Description: TPID to be used for the WAN PPPoE interface.

Value: 0x88a8, 0x8100 or 0x9100.

Default Value: 0x8100.

wlan *wlan-name*

Description: WLAN interface. It can be a physical interface (wl0) or virtual access points (wl0-vpax).

Value: wl0 (refers to the physical wlan interface), wl0-vap1 (Virtual access point 1), wl0-vap2 (Virtual access point 2), wl0-vap3 (Virtual access point 3).

Default Value: None

network-auth { **open** | **wpa2-psk** | **wpa2/wpa-psk** }

Description: Wireless LAN network authentication method.

Value: open, wpa2-psk or wpa2/wpa-psk.

Default Value: wpa2/wpa-psk

ssid auto onu-serial-number

Description: Enables automatic fill of WLAN interface SSID, which in this case will be equal to the associated ONU serial number.

Value: None.

Default Value: None.

ssid auto onu-serial-number prefix* *prefix*

Description: A textual prefix to be added (prepended) to the auto-generated SSID.

Value: Text: up to 20 characters.

Default Value: None.

ssid auto onu-serial-number suffix* *suffix*

Description: A textual suffix to be added (appended) to the auto-generated SSID.

Value: Text: up to 20 characters.

Default Value: None.

ssid custom *ssid*

Description: Set WLAN interface SSID.

Value: Text: up to 32 characters.

Default Value: None.

wpa-passphrase *wpa-passphrase*

Description: WPA passphrase.

Value: Text: up to 63 characters.

Default Value: None.

wpa-encryption aes tkip+aes

Description: WPA encryption mode.

Value: aes or tkip+aes.

Default Value: tkip+aes.

ipv4 dhcp

Description: Configures DHCP mode for the IP connection.

Value: a.b.c.d

Default Value: None

ipv4 static default-gateway *def-gw-addr*

Description: Configures a default gateway address for related IP connection (static address mode).

Value: a.b.c.d

Default Value: None

itf-grouping dhcp-server

Description: Enables the DHCP server on LAN side.

Value: None.

Default Value: dhcp-server

dhcp-server-address-pool start-address *starting-ip-address*

Description: Starting IP address for the DHCP pool on LAN side. If no value is specified and the DHCP server is enabled, the default generated by the ONU will be used.

Value: a.b.c.d

Default Value: None.

dhcp-server-address-pool end-address *ending-ip-address*

Description: Ending IP address for the DHCP pool on LAN side. If no value is specified and the DHCP server is enabled, the default generated by the ONU will be used.

Value: a.b.c.d

Default Value: None.

itf-grouping igmp-snooping

Description: Enables IGMP snooping on the LAN side.

Value: None.

Default Value: igmp-snooping

ipv4 address *ip-addr*

Description: IP address set for this interface grouping. If no value is configured, the default generated by the ONU will be used.

Value: a.b.c.d

Default Value: None.

ipv4 netmask *addr-netmask*

Description: Netmask set for this interface grouping. If no value is configured, the default generated by the ONU will be used.

Value: a.b.c.d

Default Value: None.

ports { **eth1** | **eth2** | **eth3** | **eth4** | **wl0** | **wl0-vap1** }

Description: Sets the ports that will be members of this interface grouping.

Value: eth1, eth2, eth3, eth4, wl0, wl0-vap1

Default Value: None.

vlan *vlan-id*

Description: Add a VLAN to this port.

Value: 1-4094.

Default Value: None.

cos *cos*

Description: Add cos to port.

Value: 0-7.

Default Value: 0.

ip-filtering *priority*

Description: Create an IP filtering rule with the given priority. The highest priority is 0.

Value: 0-7.

Default Value: None

filtering-type

Description: IP filtering type.

Value: incoming.

Default Value: None

action *act*

Description: IP filtering action.

Value: permit.

Default Value: None

match destination-ip-address *dest-addr*

Description: Filter by destination IP address and prefix length.

Value: IPv4 address and prefix length.

Default Value: None

match source-ip-address *src-addr*

Description: Filter by source IP address and prefix length.

Value: IPv4 address and prefix length.

Default Value: None

match protocol *proto*

Description: Filter by IP protocol.

Value: icmp, tcp, udp, tcp/udp.

Default Value: None

match source-port *port*

Description: Filter TCP/UDP source port. It is necessary to also select protocol TCP or UDP.

Value: 1-65535.

Default Value: None

match source-port *port-protocol*

Description: Filter TCP/UDP source port of given protocol.

Value: dns, http, https, snmp, snmptrap, ssh, telnet, whois.

Default Value: None

match source-port range start *start-port*

Description: Starting TCP/UDP port for range filter.

Value: 1-65535.

Default Value: None

match source-port range stop *stop-port*

Description: Stopping TCP/UDP port for range filter.

Value: 1-65535.

Default Value: None

match destination-port *port*

Description: Filter TCP/UDP destination port. It is necessary to also select protocol TCP or UDP.

Value: 1-65535.

Default Value: None

match destination-port *port-proto*

Description: Filter TCP/UDP destination port of given protocol.

Value: dns, http, https, snmp, snmptrap, ssh, telnet, whois.

Default Value: None

match destination-port range start *start-port*

Description: Starting TCP/UDP port for range filter.

Value: 1-65535.

Default Value: None

match destination-port range stop *stop-port*

Description: Stopping TCP/UDP port for range filter.

Value: 1-65535.

Default Value: None

user-mgmt [priv-lvl-support | priv-lvl-user] password auto onu-serial-number

Description: Enables automatic fill of the ONU user (level support or user) WEB login credential, which in this case will be equal to the associated ONU serial number.

Value: None.

Default Value: None.

user-mgmt [priv-lvl-support | priv-lvl-user] password auto onu-serial-number prefix* *prefix*

Description: A textual prefix to be added (prepended) to the auto-generated ONU user (level support or user) WEB login credential.

Value: Text: up to 4 characters.

Default Value: None.

user-mgmt [priv-lvl-support | priv-lvl-user] password auto onu-serial-number suffix* *suffix*

Description: A textual suffix to be added (appended) to the auto-generated ONU user (level support or user) WEB login credential.

Value: Text: up to 4 characters.

Default Value: None.

user-mgmt [priv-lvl-support | priv-lvl-user] password custom *password*

Description: Set ONU user (level support or user) WEB login credential.

Value: Text: up to 16 characters.

Default Value: None.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
3.0	This command was introduced.
5.2	Command user-mgmt added.

Usage Guidelines

When associated with an ONU, the OLT will apply all configuration present in the RG profile to specified DM984-42x/DM985-100 ONU, erasing any other WAN configuration, and

their dependencies, made through its WEB interface.

Some parameters can be specified per ONU basis, overriding the values in the RG profile. See the 'onu' command for reference.

To use an IP filtering rule it is necessary to enable the firewall on the WAN.

To set RG profile it is necessary to enter in rg-profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon rg-profile MY_PLAN
(config-rg-profile-MY_PLAN)# wan-pppoe-connection pppoe_1
(config-wan-pppoe-connection-pppoe_1)# vlan-mux vlan 100
(config-wan-pppoe-connection-pppoe_1)# nat
(config-wan-pppoe-connection-pppoe_1)# ip-filtering 0 incoming action permit
(config-ip-filtering-0)# match protocol tcp/udp destination-port range start 2000 stop 3000
(config-ip-filtering-0)# itf-grouping
(config-itf-grouping)# ipv4-address 192.168.0.1 netmask 255.255.255.0
(config-itf-grouping)# dhcp-server-address-pool start-address 192.168.0.2 end-address 192.168.0.254
(config-itf-grouping)# ports eth1
(config-itf-grouping)# ports eth2
(config-itf-grouping)# ports eth3
(config-itf-grouping)# ports eth4
(config-itf-grouping)# ports wl0
(config-itf-grouping)# ports wl0-vap1
(config-itf-grouping)# exit
(config-wan-pppoe-connection-pppoe_1)# exit
(config-rg-profile-MY_PLAN)# wlan wl0-vap1
(config-wlan-wl0-vap1)# ssid custom test
(config-wlan-wl0-vap1)# wpa-encryption tkip+aes
(config-wlan-wl0-vap1)# wpa-passphrase teste123
```

Impacts and precautions

Editing this profile will cause all associated ONUs to be reconfigured causing traffic loss.

If the IP connection is configured for static IP address mode, the static IP address must be configured in the related ONU override settings.

The ONU has a default interface grouping which will always aggregate all ports and WANs that are not included in other groupings. IP address for this default grouping is 192.168.0.1 and DHCP server is enabled. As new interface groupings are created, the ONU will automatically assign IPs 192.168.2.1, 192.168.3.1 and so on, if no custom value is configured. When configuring the custom IP address of an interface grouping to an IP 192.168.X.X, it is necessary to be aware of possible conflicts with the default grouping, or with other groupings which don't have a custom IP configured.

The names of WLAN ports on interface grouping are a little bit different from the ONU

DM984-42X web interface. The WLAN port wl0 is referred to wlan0 and the wl0-vap1 port is referred to wl0_Guest1. The port wl0-vap1 only can be present on a interface grouping if the WLAN interface wl0-vap1 is configured on rg-profile.

Hardware restrictions

N/A

profile gpon service-profile

Description

The service-profile command is used to create an ONU service profile. This profile configures ONU capability and the parameters related to services. These parameters include the user's ONU and VLAN.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon service-profile *profile-name* { **onu-profile** *profile-name* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

service-profile *profile-name*

Description: Indicates the service-profile name.

Value: Text.

Default Value: None

onu-profile *profile-name*

Description: Indicates the onu-profile name tied to service-profile.

Value: Text.

Default Value: None.

Default

N/A. There is no default profile.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.8.2	Default profiles were added.
4.0.0	Binding an ONU-profile is not mandatory.

Usage Guidelines

The onu-profile to be tied to service-profile must be configured. To set a service profile is necessary to enter in the service-profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon service-profile servProfName
(config-service-profile-servProfName)#
```

Impacts and precautions

The profile cannot be modified if it is already committed to configuration.

Hardware restrictions

N/A

profile gpon sip-agent-profile

Description

The sip-agent-profile command is used to enter in SIP Agent profile mode and set the SIP server configuration, such as registrar address, proxy server address and outbound proxy server address.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon sip-agent-profile { *sip-agent-profile-name* [**registrar** *registrar-address* | **proxy-server** *proxy-server-address* | **outbound-proxy** *outbound-proxy-address*] }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

sip-agent-profile *expires-timeout*

Description: This attribute specifies the SIP registration expiration time in seconds. The ONU will resend registration messages before the expiration time.

Value: 20-604800

Default Value: 3600

sip-agent-profile *sip-agent-profile-name*

Description: Indicates the SIP Agent profile name.

Value: String: up to 48 characters.

Default Value: None.

registrar *registrar-address*

Description: Indicates the SIP registrar IPv4 address.

Value: String: IPv4 address.

Default Value: None.

proxy-server *proxy-server-address*

Description: Indicates the SIP proxy server IPv4 address.

Value: String: IPv4 address.

Default Value: None.

outbound-proxy *outbound-proxy-address*

Description: Indicates the SIP outbound proxy IPv4 address.

Value: String: IPv4 address.

Default Value: None.

Default

None.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.

Usage Guidelines

To set the sip-agent profile it is necessary to enter in the sip-agent-profile menu.

Example:

```
# config
Entering configuration mode terminal
(config)# profile gpon sip-agent-profile sipAgentName
(config-sip-agent-profile-sipAgentName)#
```

Impacts and precautions

No field validation is performed at registrar, proxy-server and outbound-proxy parameters.

The user must inform a valid IPv4 address format for each of these fields.

Hardware restrictions

None.

profile gpon snmp-profile

Description

Defines which OIDs will be available for SNMP monitoring of GPON objects.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon snmp-profile *profile-name* [**if-alias** | **if-name** | **if-type** | **if-descr** | **if-admin-status** | **if-oper-status** | **if-onu-power-tx** | **if-onu-power-rx** | **if-onu-sysuptime** | **statistics-in-octets** | **statistics-in-ucast-pkts** | **statistics-in-multicast-pkts** | **statistics-in-broadcast-pkts** | **statistics-in-discards** | **statistics-in-errors** | **statistics-in-unknown-protos** | **statistics-out-octets** | **statistics-out-ucast-pkts** | **statistics-out-multicast-pkts** | **statistics-out-broadcast-pkts** | **statistics-out-discards** | **statistics-out-errors** | **statistics-in-bw-usage** | **statistics-out-bw-usage**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

snmp-profile *profile-name*

Description:	Name of the SNMP profile.
Value:	String (1-48 characters; accepts alphanumeric characters, '+', '-' and '_').
Default Value:	None

if-alias

Description:	Enable monitoring of interface textual description.
Value:	None
Default Value:	Disabled

if-name

Description: Enable monitoring of interface name.

Value: None

Default Value: Disabled

if-type

Description: Enable monitoring of global IANA interface type.

Value: None

Default Value: Enabled

if-descr

Description: Enable monitoring of interface description.

Value: None

Default Value: Enabled

if-admin-status

Description: Enable monitoring of interface administrative state.

Value: None

Default Value: Disabled

if-oper-status

Description: Enable monitoring of interface operational state.

Value: None

Default Value: Enabled

if-onu-power-tx

Description: Enable monitoring of ONU Tx optical power.

Value: None

Default Value: Disabled

if-onu-power-rx

Description: Enable monitoring of ONU Rx optical power.

Value: None

Default Value: Enabled

if-onu-sysuptime

Description: Enable monitoring of ONU system uptime.

Value: None

Default Value: Disabled

statistics-in-octets

Description: Enable monitoring of ethernet UNI input octets.

Value: None

Default Value: Disabled

statistics-in-ucast-pkts

Description: Enable monitoring of ethernet UNI input unicast packets.

Value: None

Default Value: Disabled

statistics-in-multicast-pkts

Description: Enable monitoring of ethernet UNI input multicast packets.

Value: None

Default Value: Disabled

statistics-in-broadcast-pkts

Description: Enable monitoring of ethernet UNI input broadcast packets.

Value: None

Default Value: Disabled

statistics-in-discards

Description: Enable monitoring of ethernet UNI input discarded packets.

Value: None

Default Value: Disabled

statistics-in-errors

Description: Enable monitoring of ethernet UNI input packets with errors.

Value: None

Default Value: Disabled

statistics-in-unknown-protos

Description: Enable monitoring of ethernet UNI input packets with unknown protocol.

Value: None

Default Value: Disabled

statistics-out-octets

Description: Enable monitoring of ethernet UNI output octets.

Value: None

Default Value: Disabled

statistics-out-ucast-pkts

Description: Enable monitoring of ethernet UNI output unicast packets.

Value: None

Default Value: Disabled

statistics-out-multicast-pkts

Description: Enable monitoring of ethernet UNI output multicast packets.

Value: None

Default Value: Disabled

statistics-out-broadcast-pkts

Description: Enable monitoring of ethernet UNI output broadcast packets.

Value: None

Default Value: Disabled

statistics-out-discards

Description: Enable monitoring of ethernet UNI output discarded packets.

Value: None

Default Value: Disabled

statistics-out-errors

Description: Enable monitoring of ethernet UNI output packets with errors.

Value: None

Default Value: Disabled

statistics-in-bw-usage

Description: Enable monitoring of ethernet UNI input bandwidth usage.

Value: None

Default Value: Enabled

statistics-out-bw-usage

Description: Enable monitoring of ethernet UNI output bandwidth usage.

Value: None

Default Value: Enabled

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
----------------	---------------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

To configure a GPON SNMP profile, it is necessary to enter the snmp-profile menu.

The profile cannot be deleted if it is referenced by an ONU.

Example (configuring an SNMP profile to monitor the administrative status of GPON interfaces):

```
# config
Entering configuration mode terminal
(config)# profile gpon snmp-profile snmpProfName
(config-snmp-profile-snmpProfName)# if-admin-status
```

Example (configuring an SNMP profile to monitor the bandwidth usage of GPON

interfaces):

```
# config
Entering configuration mode terminal
(config)# profile gpon snmp-profile snmpProfName
(config-snmp-profile-snmpProfName)# statistics-in-bw-usage
(config-snmp-profile-snmpProfName)# statistics-out-bw-usage
```

Impacts and precautions

Some OIDs (such as if-type/if-descr) are enabled by default and cannot be removed from the profile.

Hardware restrictions

N/A

profile gpon tr069-ac profile

Description

The tr069-ac profile command is used to configure parameters for access to TR069 ACS (Auto Configuration Server). This allows the ONU to be managed and upgraded by a TR069 ACS. The no profile gpon tr069-ac profile command is used to delete a specific TR069 ACS profile.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

profile gpon tr069-ac profile *profile-name*

url *url*

username *username*

password *password*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

tr069-ac profile *profile-name*

Description: Name of the profile to create. Must be unique within all TR069 profiles. Can have up to 48 characters.

Value: Text: up to 48 characters.

Default Value: None

url *url*

Description: ACS network address URL.

Value: Text: up to 128 characters. URL cannot contain white spaces or the following characters: " < > ^ ' { | }.

Default Value: None

username *username*

Description: ACS username credential.

Value: Text: up to 25 characters.

Default Value: None

password *password*

Description: ACS password credential

Value: Text: up to 25 characters.

Default Value: None

Default

N/A

Command Mode

Configuration mode

History

Release	Modification
---------	--------------

5.0	This command was introduced.
-----	------------------------------

Usage Guidelines

When associated with an ONU, the OLT will apply all configuration present in the TR069 ACS profile to specified ONU.

To set TR069 ACS profile it is necessary to enter in tr069-ac profile menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# profile gpon tr069-ac profile MY_PROF
(config-rg-profile-MY_PROF)# url http://myacs.com:7547
```

```
(config-rg-profile-MY_PROF)# username admin  
(config-rg-profile-MY_PROF)# password admin
```

Impacts and precautions

Editing this profile will cause all associated ONUs to be reconfigured causing traffic loss.

Configuring an url is mandatory.

Hardware restrictions

N/A

vlan-mapping

Description

The VLAN-mapping command is part of the service-profile structure and is used to add VLAN IDs and CoS values to packets.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
profile gpon service-profile service-profile-id vlan-mapping name symmetric { ethernet ethernet-ports | veip veip-idx } match vlan vlan-id { vlan-val | any } cos { cos-val | any } action vlan { add | replace } vlan-id { vlan-val | copy-vlan } cos { cos-val | copy-vlan }
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

name

Description:	Name of the VLAN-mapping.
Value:	Text: up to 48 characters.
Default Value:	None

symmetric

Description:	Symmetric VLAN-mapping specifies that the operation performed in the downstream direction is the inverse of the VLAN tagging operation that is performed in the upstream direction.
Value:	None
Default Value:	None

ethernet *ethernet-ports*

Description:	Ethernet ports to be affected.
---------------------	--------------------------------

Value: Number: from 1 to 4. Range: two values from 1 to 4 separated by hifen. List of ranges/values: a combination of the above separated by commas. Examples: ethernet 1 ethernet 1,3 ethernet 1-4 ethernet 1-2,4 ethernet 1-2,3-4

Default Value: None

veip *veip-idx*

Description: VEIP to be affected.

Value: Number: 1.

Default Value: None

match

Description: Parameters after **match** and before **action** describe the type of flow that the rule applies to.

Value: None

Default Value: None

vlan *vlan-id* { *vlan-val* | **any** }

Description: VLAN ID to be matched, or **any** in case all VLAN IDs apply.

Value: None in case of 'any'. *vlan-val*: Number from 0 to 4094.

Default Value: None.

cos { *cos-val* | **any** }

Description: CoS value to be matched, or **any** in case all CoS values apply.

Value: None in case of 'any'. *cos-val*: Number from 0 to 7.

Default Value: None.

action

Description: Parameters after **action** describe the action to be taken upon the flow that the rule applies to.

Value: None.

Default Value: None.

vlan { **add** | **replace** }

Description: Add a new VLAN tag or replace an existing one.

Value: None.

Default Value: None.

vlan-id { *vlan-val* | **copy-vlan** }

Description: New VLAN ID for the VLAN tag, or **copy-vlan** in case the original VLAN ID should be kept.

Value: None in case of 'copy-vlan'. *vlan-val*: Number from 0 to 4094.

Default Value: None.

cos { *cos-val* | **copy-vlan** }

Description: New CoS value for the VLAN tag, or **copy-vlan** in case the original CoS value should be kept.

Value: None in case of 'copy-vlan'. *cos-val*: Number from 0 to 7.

Default Value: None.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
5.8	This command supports creating VLAN mapping rules for VEIP.

Usage Guidelines

For the ethernet field, valid configuration could be:

A single port:

```
(config-service-profile-servProfName)# vlan-mapping vlanMapName
symmetric ethernet 2 ...
```

Multiple ports separated by commas:

```
(config-service-profile-servProfName)# vlan-mapping vlanMapName
symmetric ethernet 1,3,4 ...
```

A range of ports:

```
(config-service-profile-servProfName)# vlan-mapping vlanMapName
symmetric ethernet 1-3 ...
```

A mix of the above:

```
(config-service-profile-servProfName)# vlan-mapping vlanMapName
symmetric ethernet 1-3,4 ...
```

The command requires all fields configured to be applied.

To set a VLAN-mapping is necessary to enter in the interface service-profile menu.

```
(config)# profile gpon service-profile servProfName
(config-service-profile-servProfName)# vlan-mapping vlanMapName
symmetric ethernet 1 match vlan vlan-id 10 cos any action vlan replace vlan-id 100 cos copy-vlan
```

To actually apply the VLAN mapping rules, the service-profile must be selected on the ONU and the interface must be created.

```
(config)# interface gpon 1/1/1 onu 0
(config-gpon-onu-0)# service-profile servProfName
(config-gpon-onu-0)# ethernet 1
```

Impacts and precautions

- VLAN mapping rules will only be applied to ONUs that configured the service-profile containing the rules.
- A VLAN mapping rule will only be applied if the target interface (Ethernet UNI, VEIP) is present in the ONU configuration.

Hardware restrictions

N/A

ONU

This topic describes the commands related to ONU such as commands to authenticate an ONU and configure its UNIs.

interface gpon onu

Description

Adds, modifies, removes, activates or deactivates an ONU as well as assigns profiles and configures Ethernet/POTS/VEIP UNI.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

interface gpon *<chassis/slot/port>* **onu** *onu-id*

interface gpon *<chassis/slot/port>* **onu** *onu-id* [**name** *onu-name* | **serial-number** *serial-number* [**password** *password*] | **password** *password* [**serial-number** *serial-number*] | **service-profile** *service-profile-name* [**line-profile** *line-profile-name*] | **line-profile** *line-profile-name* [**service-profile** *service-profile-name*] | **ethernet** *ethernet-port* | **ipv4** { **dhcp** **vlan** { **cos** *cos-val* | **vlan-id** *vlan-val* } | **static** { **address** *ip-addr* | **default-gateway** *def-gw-addr* } | **vlan** { **vlan-id** *vlan-val* | **cos** *cos-val* } } | **rg-profile** *rg-profile-name* | **rg-profile-override-settings** | **tr069-ac** **profile** *tr069-ac-profile-name* | **auto-provisioned** { *true* | *false* }]

interface gpon *<chassis/slot/port>* **onu** *onu-id* **ethernet** *ethernet-port* [**speed** { **10** | **100** | **1000** } [**duplex** { **full** | **half** }] | **duplex** { **full** | **half** } [**speed** { **10** | **100** | **1000** }] | **native** **vlan** { **cos** *cos-val* | **vlan-id** *vlan-val* } * | **native** **downstream-mode** { **filter-on-vid-only** | **inverse-of-upstream** } | **negotiation** | **shutdown** | **mac-limit** *mac-limit-value* | **description** { *string* } *]

interface gpon *<chassis/slot/port>* **onu** *onu-id* **pots** *pots-port* [**sip-user-agent** **display-name** *display-name* **username** *user-name* **password** *password* **user-part-aor** *user-part-aor* [**sip-agent-profile** *sip-agent-profile-name*] | **media-profile** *media-profile-name* **sip-agent-profile** *sip-agent-profile-name* [**sip-user-agent** **display-name**

```
display-name username user-name password password user-part-aor user-part-aor
]]
```

```
interface gpon <chassis/slot/port> onu onu-id veip veip-port [ native vlan { vlan-id vlan-val | cos cos-val } ]
```

```
interface gpon <chassis/slot/port> onu onu-id rg-profile-override-settings wan-pppoe-connection pppoe-connection-name [ username username | password password ]*
```

```
interface gpon <chassis/slot/port> onu onu-id rg-profile-override-settings wan-ip-connection ip-connection-name static { address ip-addr | default-gateway def-gw-addr }
```

```
interface gpon <chassis/slot/port> onu onu-id rg-profile-override-settings wan-wlan wlan-name [ wpa-passphrase wpa-passphrase | ssid ssid ]
```

```
interface gpon <chassis/slot/port> onu onu-id rg-profile-override-settings user-mgmt [ priv-lvl-support | priv-lvl-user ] password password
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

onu *onu-id*

Description: Configures the ONU ID

Value: 0-127

Default Value: None

name *onu-name*

Description: Configures the ONU name. The name is optional.

Value: Text with up to 48 characters.

Default Value: None

serial-number *onu-name*

Description: Text beginning with 4 ASCII characters, case sensitive, followed by 8 HEX characters, case insensitive.

Value: ONU's serial number.

Default Value: None

password *password*

- Description:** ONU's password. The ONU's password must be unique inside the ponlink it is located.
However, this condition must only be met if the GPON Card ONU Authentication Method is set to password only. The password is case sensitive.
- Value:** Text beginning with 0x followed by up to 20 HEX characters, or up to 10 alphanumerical characters.
- Default Value:** None

service-profile *service-profile-name*

- Description:** Reference to service-profile to be bound.
- Value:** Text with up to 48 characters.
- Default Value:** None.

line-profile *line-profile-name*

- Description:** Reference to line-profile to be bound.
- Value:** Text with up to 48 characters.
- Default Value:** "DEFAULT-LINE".

rg-profile *rg-profile-name*

- Description:** Reference to rg-profile to be bound.
- Value:** Text with up to 48 characters.
- Default Value:** None.

rg-profile-override-settings

- Description:** Enter in RG profile override settings mode.
- Value:** N/A.
- Default Value:** N/A.

wan-pppoe-connection *pppoe-connection-name*

- Description:** Reference to WAN PPPoE connection inside the related rg-profile.
- Value:** Text with up to 48 characters.
- Default Value:** None.

username *username*

Description: Override PPPoE username of the WAN PPPoE connection inside the related rg-profile.

Value: Text with up to 64 characters.

Default Value: None.

password *password*

Description: Override PPPoE password of the WAN PPPoE connection inside the related rg-profile.

Value: Text with up to 32 characters.

Default Value: None.

wan-ip-connection *ip-connection-name*

Description: Reference to WAN IPoE connection inside the related rg-profile.

Value: Text with up to 48 characters.

Default Value: None.

wan-ip-connection *ip-connection-name* **ipv4 static address** *ip-addr*

Description: Configures an IP address for related IP connection in RG Profile. The subnet mask prefix must be passed.

Value: a.b.c.d/x

Default Value: None

wan-ip-connection *ip-connection-name* **ipv4 static default-gateway** *def-gw-addr*

Description: Configures a default gateway address for related IP connection in RG Profile.

Value: a.b.c.d

Default Value: None

wlan *wlan-name*

Description: Reference to WLAN interface inside the related rg-profile.

Value: One of the WLAN interface name from the rg-profile.

Default Value: None.

wpa-passphrase *wpa-passphrase*

Description: Override WPA passphrase of the WLAN interface inside the related rg-profile.

Value: Text with up to 64 characters.

Default Value: None.

ssid *ssid*

Description: Override SSID name of the WLAN interface inside the related rg-profile.

Value: Text with up to 32 characters.

Default Value: None.

auto-provisioned { *true* | *false* }

Description: Indicates that ONU was configured by auto provisioned (true) or not (false).
If ONU configuration is changed after ONU was auto provisioned, it is recommended to set auto-provisioned to false.

Value: True (auto provisioned) or false (not auto provisioned).

Default Value: False.

user-mgmt [**priv-lvl-support** | **priv-lvl-user**] **password** *password*

Description: RG profile override of ONU user (level support or user) WEB login credential configuration.

Value: Text: up to 16 characters.

Default Value: None.

ethernet *ethernet-port*

Description: Configures the user network interface.
An entry of the ethernet port must be created in order to monitor SNMP OIDs for the Ethernet UNI.

Value: 1-4

Default Value: None

speed { **10** | **100** | **1000** }

Description: Configures the user network interface speed to 10 Mbit/s, 100 Mbit/s or 1 Gbit/s.

Value: { 10 | 100 | 1000 }

Default Value: None

duplex { **full** | **half** }

Description: Configures the user network interface flow to half-duplex or full-duplex.

Value: { full | half }

Default Value: None

native vlan *vlan-id*

Description: Configures a VLAN ID to be added to incoming Ethernet untagged traffic.

Value: 1-4094

Default Value: None

native vlan cos *cos-val*

Description: Configures a class-of-service value for the VLAN configured.

Value: 0-7

Default Value: 0

native downstream-mode

Description: Configures the tagging action to be applied for downstream native VLAN tagged packets.

When filter-on-vid-only value is used, the operation performed in the downstream direction is the inverse of that performed in the upstream direction but only VID match is applied, that is, the VLAN tag of downstream packets matching the same VLAN ID, regardless of their CoS, configured in the native vlan settings will be stripped.

When inverse-of-upstream value is used, the operation performed in the downstream direction is the inverse of that performed in the upstream direction, that is, the VLAN tag of downstream packets matching the same VLAN ID and CoS configured in the native vlan settings will be stripped.

Value: { filter-on-vid-only | inverse-of-upstream }

Default Value: filter-on-vid-only

negotiation

Description: Configures the user network interface to auto-negotiation mode.

Value: None

Default Value: Negotiation

shutdown

Description: Disables the user network interface.

Value: None

Default Value: no shutdown

snmp all

Description: Enables SNMP monitoring for the ONU. This command enables the ONU to report all available OIDs, including Ethernet UNI counters.

Value: None

Default Value: Disabled (no snmp all)

snmp profile *snmp-profile-name*

Description: Reference to snmp-profile to be bound. Enables SNMP monitoring for the ONU.

This command enables the ONU to report the OIDs selected in the specified SNMP profile, including Ethernet UNI counters.

Value: Text with up to 48 characters.

Default Value: Disabled (no snmp profile)

snmp real-time

Description: Enables real-time SNMP monitoring for the ONU Ethernet UNI counters.

When this parameter is disabled, Ethernet UNI counters are collected and updated in a 15-minute window.

When enabled, these counters are collected continuously, being updated with a higher frequency.

This frequency is inversely proportional to the number of ONUs configured and the number of ONUs with real-time update enabled.

Value: None

Default Value: Disabled (no snmp real-time)

mac-limit *mac-limit-value*

Description: Configure MAC address learning limit.

When this parameter is disabled (no mac-limit), there is no limitation on how many MAC addresses could be learned. In this case, the limitation will be given by the ONU MAC address table size.

Value: 1-255

Default Value: None (unlimited MAC address learning).

description

Description: Set the interface description or alias. Valid characters are A-Z, a-z, 0-9 and - _ / + * @

Value: The interface description.

Default Value: N/A

ipv4 dhcp vlan vlan-id *vlan-val*

Description: Configures a VLAN ID for ONUs IP address.

Value: 1-4094

Default Value: None

ipv4 dhcp vlan cos *cos-val*

Description: Configures a class-of-service value for the VLAN configured in ipv4 VLAN parameter.

Value: 0-7

Default Value: None

ipv4 static address *ip-addr*

Description: Configures an IP address for the ONU. The subnet mask prefix must be passed.

Value: a.b.c.d/x

Default Value: None

ipv4 static default-gateway *def-gw-addr*

Description: Configures a default gateway address for the ONU.

Value: a.b.c.d

Default Value: None

ipv4 vlan vlan-id *vlan-val*

Description: Configures an outer VLAN for the ONU.

Value: 1-4094

Default Value: None

ipv4 vlan cos *cos-val*

Description: Configure an outer CoS for the ONU.

Value: 0-7

Default Value: None

pots *pots-port*

Description: Configures the POTS interface.

Value: 1-4

Default Value: None

display-name *display-name*

Description: Indicates the display-name of the SIP user.

Value: Text with up to 48 characters.

Default Value: None

username *user-name*

Description: Indicates the user name for the SIP user authentication.

Value: Text with up to 32 characters.

Default Value: None

password *password*

Description: Indicates the password for the SIP user authentication.

Value: Text with up to 32 characters.

Default Value: None

user-part-aor *user-part-aor*

Description: Defines the user identity by unique AOR (address of record).

Value: Text with up to 256 characters.

Default Value: None

media-profile *media-profile-name*

Description: Reference to the media profile.

Value: Text with up to 48 characters.

Default Value: None

sip-agent-profile *sip-agent-profile-name*

Description: Reference to the SIP agent profile.

Value: Text with up to 48 characters.

Default Value: None

veip *veip-port*

Description: Configures the ONU Virtual Ethernet Interface Point (VEIP).

Value: 1.

Default Value: None

native vlan *vlan-id*

Description: Configures a VLAN ID to be added to incoming VEIP untagged traffic.

Value: 1-4094

Default Value: None

native vlan cos *cos-val*

Description: Configures a class-of-service value for the VLAN configured.

Value: 0-7

Default Value: 0

tr069-accs-profile *tr069-accs-profile-name*

Description: Reference to tr069-accs-profile to be bound.

Value: Text with up to 48 characters.

Default Value: None.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
1.6	The POTS configuration command was added.
1.8	Ethernet UNI Mac address learning limit command was added. The VEIP configuration command was added.
1.8.2	Default profiles were added.
1.12	Media profile was added.
2.0	Command 'snmp all' option was added.
2.4	Command 'snmp profile' and 'snmp real-time' options were added.
3.0	Commands 'rg-profile' and 'rg-profile-override-settings' were added.
4.0.0	Binding a service-profile is not mandatory. Added auto-provisioned command.
5.0	Command 'tr069-acis-profile' was added.
5.2	Command user-mgmt added.

Usage Guidelines

To set interface gpon onu parameters is necessary to enter in the interface gpon onu menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# ethernet 1
(config-ethernet-1)# description test_interface_name
```

To configure service profile:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# service-profile serviceName
```

To configure media profile:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# pots 1
(config-pots-1)# media-profile mediaName
```

To enable SNMP monitoring for the ONU:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# snmp all
```

To configure a RG profile and override only the PPPoE password:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# rg-profile MY_RG_PROFILE
(config-gpon-onu-1)# rg-profile-override-settings
(config-gpon-onu-1-rg-...)# wan-pppoe-connection pppoe_1 password MY_PASSWORD
```

To configure a RG profile and static IP address for the WAN interface:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# rg-profile MY_RG_PROFILE
(config-gpon-onu-1)# rg-profile-override-settings
(config-...-rg-...)# wan-ip-connection ipoe_1 ipv4 static address 10.2.3.4/24
```

To configure a RG profile and override SSID and wpa-passphrase for the WLAN interface:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# rg-profile MY_RG_PROFILE
(config-gpon-onu-1)# rg-profile-override-settings
(config-gpon-onu-1-rg-...)# wlan w10 wpa-passphrase MY_PASSWORD ssid MY_SSID
```

To configure a TR069 ACS profile:


```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# tr069-acis-profile MY_TR069_PROFILE
```

Some third-party ONUs may not support the use of a native VLAN on the Ethernet UNI. As a workaround the service-port may be configured to work as a native VLAN (match “any” plus action “add” operation).

Impacts and precautions

Configuring a serial-number and/or password must match with gpon authentication method command defined configuration.

Binding a line-profile is mandatory.

An outer-VLAN must be set when configuring ipv4.

Binding a valid SIP agent profile is mandatory when configuring ONU POTS interfaces.

Even if SNMP (all or profile) configured, Ethernet UNI SNMP counters are published each 15 minutes.

If Ethernet UNI SNMP counters needs to be updated more frequently, turn on real-time update.

When real-time SNMP update is enabled, Ethernet UNI SNMP counters are published continuously, being updated with a higher frequency. This frequency is inversely proportional to the number of ONUs configured and the number of ONUs with real-time update enabled.

Up to 32 ONUs can have real-time SNMP monitoring turned on globally.

It is recommended that the polling interval by the external monitoring tool should be 5 minutes or higher.

In order to monitor SNMP OIDs for a given Ethernet UNI, an entry must be created with the **ethernet** *ethernet-port* command.

RG profile will only work for DM984-42x and DM985-100 ONU models.

When overriding RG profile settings, only the selected parameters will be overridden while others will come from the associated RG profile.

If the RG profile contains IP connections with static IP address mode, the static IP address for each connection must be configured in the override settings.

When using a TR069 ACS profile, ensure that the ONU has an IP path already configured for this service.

Hardware restrictions

None

onu-auth-method

Description

Defines the method that will be used to authenticate an ONU. This configuration is applied to the gpon-card as a whole, affecting all its ONUs.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

onu-auth-method { serial-number | password | serial-number-and-password }

Parameters

serial-number

Description: Sets the authentication method to serial number only.

Value: None

Default Value: None

password

Description: Sets the authentication method to password only.

Value: None

Default Value: None

serial-number-and-password

Description: Sets the authentication method to serial number and password.

Value: None

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To set an onu-auth-method it is necessary to enter in the given gpon card menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# gpon 1/1
(config-gpon-1/1)# onu-auth-method password
```

Impacts and precautions

None

Hardware restrictions

N/A

onu-enable

Description

This command re-enables an inactive ONU.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

onu-enable { *all* | *serial-number* }

Parameters

onu-enable *all*

Description: Enable all ONUs.

Value: None

Default Value: None

onu-enable *serial-number*

Description: Only the ONU with the given serial number will be enabled.

Value: Four letters followed by eight hexadecimal values (0-f).

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To apply an onu-enable it is necessary to enter in the given gpon interface menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu-enable all
```

Impacts and precautions

Depending on the reason why the ONU was disabled, it may not become enabled when this command is issued. This command merely attempts to enable an ONU.

Hardware restrictions

N/A

onu-force-status-update

Description

This command forces an ONU to update its status.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

onu-force-status-update { **onu** *onu-id* }

Parameters

onu *onu-id*

Description: Selects an ONU.

Value: A registered ONU ID. See command 'onu' for range information.

Default Value: None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
---------	--------------

2.4	This command was introduced.
-----	------------------------------

Usage Guidelines

In scenarios with hundreds of ONUs, status polling can take a long time to update a given ONU status. This command can be used to force a particular ONU to update its status.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu-force-status-update onu 1
```

In the example above, execute “show interface onu 1/1/1 onu 1” to check the updated status.

Impacts and precautions

It is expected that the ONU status might be updated a few seconds after the command is executed.

Hardware restrictions

N/A

onu-reset

Description

This command resets an ONU.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
onu-reset { onu onu-id }
```

Parameters

onu *onu-id*

Description: Resets a specific ONU.

Value: A registered ONU ID. See command 'onu' for range information.

Default Value: None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

To apply an onu-reset it is necessary to enter in the given gpon interface menu.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu-reset onu 1
```

Impacts and precautions

The referred ONU will be reset, affecting ongoing data traffic. Only works on configured and connected ONUs.

Hardware restrictions

N/A

request firmware onu cancel

Description

Cancels ONU firmware upgrade.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
request onu cancel interface gpon { chassis/slot/port } { onu onu-id | all }
```

Parameters

interface gpon *chassis/slot/port*

Description: Specifies the gpon interface in chassis/slot/port.

Value: chassis/slot/port

Default Value: None

onu *onu-id*

Description: Defines the ONU to be used in the operation.

Value: 0-127

Default Value: None

Default

None

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
2.0	Removed 'remote' from the command syntax.

Usage Guidelines

Use the **cancel** command to cancel the firmware installation in one or in all ONUs in a given gpon interface. **Example:**

```
# configure terminal
Entering configuration mode terminal
(config)# request firmware onu cancel interface gpon 1/1/1 onu 1
```

Impacts and precautions

None

Hardware restrictions

None

request firmware onu install

Description

Installs the firmware image to an ONU. For `in-band-upgrade` option, only DM984-42x ONU model is currently supported.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
request firmware onu install { filename } interface gpon { chassis/slot/port } {  
onu onu-id | all }
```

```
request firmware onu install { filename } in-band-upgrade { model onu-model  
} { ip-address ipv4-address } [ { username onu-username } ] [ { password onu-  
password } ]
```

Parameters

filename

Description:	Defines the name of the firmware image file to be used in a remote ONU update.
Value:	Text with no character limit
Default Value:	None

interface gpon *chassis/slot/port*

Description:	Specifies the gpon interface in chassis/slot/port.
Value:	chassis/slot/port
Default Value:	None

onu *onu-id*

Description:	Defines the ONU to be used in the operation.
Value:	0-127

Default Value: None

in-band-upgrade

Description: Selects the in-band mode for upgrade of ONU firmware.

Value: None

Default Value: N/A

model *onu-model*

Description: Identifies the model of the ONU that will be upgraded.

Value: dm984-42x

Default Value: None

ip-address *ipv4-address*

Description: ONU's IP Host address.

Value: a.b.c.d

Default Value: None

username *onu-username*

Description: ONU's management user. The username is case sensitive.

Value: Word with up to 32 characters

Default Value: None

password *onu-password*

Description: ONU's management password. The password is case sensitive.

Value: Word with up to 32 characters

Default Value: None

Default

None

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Config

History

Release	Modification
1.4	This command was introduced.
2.0	Removed <code>remote</code> from the command syntax.
2.4	Added text in <i>Impacts and precautions</i> .
4.9	The <code>in-band-upgrade</code> operation mode was introduced. Also moved some text from <i>Impacts and precautions</i> to <code>request firmware onu add section</code> .

Usage Guidelines

Use `install filename interface` command to install the firmware at some ONU connected to a GPON interface. For this option, use the `cancel` command to stop the operation.

Example:

```
# request firmware onu install fwName interface gpon 1/1/1 onu 1
```

Use `install filename in-band-upgrade` command to install the firmware at some ONU known by its IPv4 address. The `cancel` command does not apply here because the operation blocks until finished, when the result of operation is printed. If the upgrade fails, the message informs about the reason.

Examples:

Succeeded operation:

```
# request firmware onu install fwName in-band-upgrade model dm984-42x
ip-address 192.168.10.10 username anon password rightpass
in-band-upgrade succeeded for 192.168.10.10
```

Failed operation:

```
# request firmware onu install fwName in-band-upgrade model dm984-42x
ip-address 192.168.10.10 username anon password wrongpass
in-band-upgrade FAILED for 192.168.10.10 (not authorized)
```

Impacts and precautions

The ONU will reboot to activate the new firmware image.

When upgrading using the `interface` operation mode, it is the operator responsibility to check if the selected ONU (or ONUs) is (are) compatible with the selected ONU firmware file. The OLT will not check this compatibility, even though most of ONU models have the capability of performing this function. In these cases, ONU firmware transfer will fail and the ONU will remain in the previous state.

When upgrading using the `in-band-upgrade` operation mode, the addressed ONU's model will be read and compared with the selected model in the command. In case of mismatch, the command will be refused.

Only one firmware file can be used at a time globally in the equipment. That is, if the operator is upgrading a given ONU model, another upgrade with a different firmware file cannot happen while the all other transfers finish. In other words, once started one or more ONU firmware file transfers, the operator needs to wait for all of them to complete in order to start a new one with a different ONU firmware file.

Hardware restrictions

None

rg-reprovision

Description

This command re-provision an ONU associated with an rg-profile.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

rg-reprovision

Parameters

N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
4.9.0	This command was introduced.

Usage Guidelines

To apply an rg-reprovision it is necessary to enter in the given onu config.

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu 1
(config-gpon-onu-1)# rg-reprovision
```

To use the command on multiple ONUs, ranges can be used. **Example:**

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1
(config-gpon-1/1/1)# onu *
(config-gpon-onu-*)# rg-reprovision
```

Example:

```
# configure terminal
Entering configuration mode terminal
(config)# interface gpon 1/1/1-8
(config-gpon-1/1/1-8)# onu *
(config-gpon-onu-*)# rg-reprovision
```

Impacts and precautions

This command will reprovision the ONU and configurations made via the ONU web interface might be erased.

Hardware restrictions

N/A

show firmware

Description

General information about ONU firmware.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show firmware onu

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

onu

Description:	General information on ONU firmware.
Value:	N/A
Default Value:	N/A

Output Terms

Output	Description
Name	Field to show the firmware name.
MD5	Field to show the Message-Digest algorithm 5 (MD5).
Size	Field to show the firmware size in bytes.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.4	Removed the “show firmware gpon onu interface” command. Modified “show firmware info” command.

Usage Guidelines

```
# show firmware onu
Available_Firmwares_for_ONU
  Name : 0906-02.R4.2.30.027.man
  MD5  : 9e42ded778438cb1b1d4ad9f56846c70
  Size : 7098372
----
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show interface gpon onu

Description

Displays ONU information.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show interface gpon *chassis/slot/port* **onu** *onu-id* [**version** | **optical-info** | **brief** | **rsi**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

chassis/slot/port

Description: The GPON port on which the ONU is located.

Value: Text: chassis/slot/port format.

Default Value: N/A

onu *onu-id*

Description: The ONU referred.

Value: onu-id: Number from 0 to 127.

Default Value: N/A

version

Description: Display firmware version of the ONU.

Value: N/A

Default Value: N/A

optical-info

Description: Display informations of the ONU's optical interface.

Value: N/A

Default Value: N/A

brief

Description: Display brief information of the ONU.

Value: N/A

Default Value: N/A

rssl

Description: Display the RSSI (received signal strength indication) for a specific ONU. The value represents the power level received at the OLT for the selected ONU. Only one ONU can be selected each time.

The value read from the CLI may be different from the actual value read by a power meter. The value can also be affected by the amount of traffic transmitted by ONU.

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Last updated	Shows the timestamp of the last time the selected ONU has its status published to the database.
ID	ID of the ONU.
Serial Number	Serial number of the ONU.
Password	ONU password.
Uptime	The uptime reported by the ONU.

Output	Description
Last Seen Online	The time since ONU was online.
Vendor ID	Vendor ID part of the ONU.
Equipment ID	Equipment ID of the ONU.
Name	User defined name of the ONU.
Operational state	State of operation of the ONU.
Primary status	Primary status of the ONU.
Distance	Approximate ONU logical distance (in kilometers) from the OLT.
IPv4 mode	ONU IP-Host mode: static or DHCP.
IPv4 Address	ONU IP-Host IPv4 Address.
IPv4 default gateway	ONU IP-Host IPv4 default gateway.
IPv4 VLAN	ONU IP-Host VLAN.
IPv4 CoS	ONU IP-Host CoS.
Line Profile	Line Profile assigned to the ONU.
Service Profile	Service Profile assigned to the ONU.
RG Profile	RG Profile assigned to the ONU.

Output	Description
RG One Shot Provision	Indicates the time that RG Profile was provisioned at ONU.
TR069 ACS Profile	TR069 ACS Profile assigned to the ONU.
SNMP	Shows if the ONU has snmp enabled and the SNMP profile when applicable.
Allocated bandwidth	Type and amount of bandwidth allocated for the ONU.
Upstream-FEC	Upstream-FEC state.
Anti Rogue ONU isolate	Anti Rogue ONU isolate state.
Version	ONU firmware version.
Active FW	Firmware version of the ONU active image.
Standby FW	Firmware version of the ONU standby image.
Software Download State	ONU firmware upgrade state.
Rx Optical Power -dBm-	Rx power level in dBms.
Tx Optical Power -dBm-	Tx power level in dBms.
RSSI -dBm-	Power level received at the OLT for a specific ONU.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.10	Added configured password.
2.4	Added more information to usage guidelines and output parameters.
4.2.0	Added support for range of IDs in show options.
6.2.0	Added support to RSSI (Received signal strength indication) measurement for ONUs.

Usage Guidelines

```
# show interface gpon 1/1/8 onu 1
Last updated       : 2017-11-22 15:00:27 UTC+0
ID                 : 1
Serial Number      : DACM00000353
Password           :
Uptime             : 22:34
Last Seen Online   : N/A
Vendor ID          : DACM
Equipment ID       : DM984-100B
Name               :
Operational state   : Up
Primary status      : Active
Distance           : 0 [km]
```

```

IPv4 mode           : Not configured
IPv4 address        :
IPv4 default gateway :
IPv4 VLAN           :
IPv4 CoS            :
Line Profile         : DEFAULT-LINE
Service Profile      :
RG Profile           :
RG One Shot Provision : Not provisioned
TR069 ACS Profile    :
SNMP                : Disabled
Allocated bandwidth  : 0 fixed, 0 assured+fixed [kbit/s]
Upstream-FEC         : Enabled
Anti Rogue ONU isolate : Disabled
Version             :
Active FW            : v1.3.2 valid, committed
Standby FW           : v1.3.1 valid, not committed
Software Download State : None
Rx Optical Power [dBm] : -8.16
Tx Optical Power [dBm] : -0.08

```

Show all ONUs in all gpon interfaces

```

# show interface gpon onu
-----
Itf      ONU ID  Serial Number  Oper State  Software Download State  Name
-----
1/1/1    1          CIGG12345671  Up          Complete                ONU1
1/1/1    2          CIGG12345672  Up          Complete                ONU2
1/1/3    1          CIGG12345673  Up          Complete                ONU3
1/1/4    1          CIGG12345674  Up          Complete                ONU4
1/1/4    5          CIGG12345675  Up          Complete                ONU5

```

Show all ONUs in all gpon interfaces

```

# show interface gpon * onu
-----
Itf      ONU ID  Serial Number  Oper State  Software Download State  Name
-----
1/1/1    1          CIGG12345671  Up          Complete                ONU1
1/1/1    2          CIGG12345672  Up          Complete                ONU2
1/1/3    1          CIGG12345673  Up          Complete                ONU3
1/1/4    1          CIGG12345674  Up          Complete                ONU4
1/1/4    5          CIGG12345675  Up          Complete                ONU5

```

Show all ONUs in all gpon interfaces in a given chassis/slot

```

# show interface gpon 1/1/* onu
-----
Itf      ONU ID  Serial Number  Oper State  Software Download State  Name
-----
1/1/1    1          CIGG12345671  Up          Complete                ONU1
1/1/1    2          CIGG12345672  Up          Complete                ONU2
1/1/3    1          CIGG12345673  Up          Complete                ONU3
1/1/4    1          CIGG12345674  Up          Complete                ONU4
1/1/4    5          CIGG12345675  Up          Complete                ONU5

```

Show all ONUs in range of gpon interfaces/slot

```

# show interface gpon 1/1/1-4 onu
-----
Itf      ONU ID  Serial Number  Oper State  Software Download State  Name
-----
1/1/1    1          CIGG12345671  Up          Complete                ONU1
1/1/1    2          CIGG12345672  Up          Complete                ONU2
1/1/3    1          CIGG12345673  Up          Complete                ONU3

```

Show all ONUs in a list of gpon interfaces/slot

```

# show interface gpon 1/1/2,4 onu

```

Itf	ONU ID	Serial Number	Oper State	Software Download State	Name
1/1/2	1	CIGG12345671	Up	Complete	ONU1
1/1/2	2	CIGG12345672	Up	Complete	ONU2
1/1/4	1	CIGG12345673	Up	Complete	ONU3

Show all ONUs in a given gpon interface/slot

```
# show interface gpon 1/1/1 onu
```

Itf	ONU ID	Serial Number	Oper State	Software Download State	Name
1/1/1	1	CIGG12345671	Up	Complete	ONU1
1/1/1	9	CIGG12345672	Up	Complete	ONU9
1/1/1	22	CIGG12345673	Up	Complete	ONU22

Show a range of ONUs in a given gpon interface/slot

```
# show interface gpon 1/1/1-10 onu *
```

Itf	ONU ID	Serial Number	Oper State	Software Download State	Name
1/1/1	1	CIGG12345671	Up	Complete	ONU1
1/1/1	9	CIGG12345672	Up	Complete	ONU9

Impacts and precautions

It is not supported to use a key pattern in both ONU and gpon interface IDs (

```
show interface gpon * onu *
```

).

It is not supported to use ONU ID key pattern together with brief/optical-info/version options (

```
show interface gpon 1/1/1 onu * brief
```

).

In some scenarios, the ONU logical distance cannot be retrieved correctly and it will be shown as N/A. This behavior can happen specially when the configured PON link maximum distance is close to the ONU logical distance, for example, when the ONU is at 20km distant and PON link maximum distance is configured to 21km.

Hardware restrictions

N/A

show interface gpon onu Ethernet

Description

Displays information about the user's Ethernet ports of the ONU.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show interface gpon *chassis/slot/port* **onu** [*onu-id*] **ethernet** [*ethernet-port* [**brief** | **detail** | **statistics**]]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

chassis/slot/port

Description: The GPON port on which the ONU is located.

Value: Text: chassis/slot/port format.

Default Value: N/A

onu-id

Description: The ONU to which the Ethernet port belongs to.

Value: onu-id: Number from 0 to 127.

Default Value: N/A

ethernet-port

Description: Number of the ONU's Ethernet port.

Value: Number from 1 to 4 depending on the ONU profile of the ONU.

Default Value: N/A

brief

Description: Display brief information of the ONU's Ethernet interfaces.

Value: brief: Fixed text 'brief'.

Default Value: N/A

statistics

Description: Display statistics information of the ONU's Ethernet interfaces.

Value: statistics: Fixed text 'statistics'.

Default Value: N/A

detail

Description: Display detailed information of the ONU's Ethernet interfaces.

Value: detail: Fixed text 'detail'.

Default Value: N/A

Output Terms

Output	Description
Physical interface	Name and status of the GPON interface.
Link-level type	Type of the Link-level.
Speed	Speed of the Ethernet UNI.
Duplex	Duplex configuration.
Negotiation	Negotiation status (enabled/disabled).
Status Negotiation	Negotiated Speed and Duplex.
Native-vlan	Native VLAN of the Ethernet UNI.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.8	Removed no longer valid 'detail' and 'statistics' parameters.
1.8.2	Added 'detail' and 'statistics' parameters.
4.2.0	Added support for range of IDs in show options.

Usage Guidelines

```
# show interface gpon 1/1/8 onu 1 ethernet 1
Physical interface : ethernet 1, Enabled, Physical link is up
GPON Information : gpon-1/1/1, ONU 1
Link-level type : Ethernet
Speed/Duplex : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS : -
MAC limit : Unlimited
```

Show all ethernet UNIs in a given ONU

```
# show interface gpon 1/1/1 onu 1 ethernet *
Physical interface : ethernet 1, Enabled, Physical link is up
GPON Information : gpon-1/1/1, ONU 1
Link-level type : Ethernet
Speed/Duplex : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
```

```

Native VLAN/CoS : -
MAC limit       : Unlimited
Physical interface : ethernet 2, Enabled, Physical link is up
GPON Information : gpon-1/1/1, ONU 1
Link-level type  : Ethernet
Speed/Duplex     : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS : -
MAC limit       : Unlimited

```

Show all ethernet UNIs in a given ONU

```

# show interface gpon 1/1/1 onu 1 ethernet
Physical interface : ethernet 1, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited
Physical interface : ethernet 2, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited

```

Show a range ethernet UNIs in a given ONU

```

# show interface gpon 1/1/1 onu 1 ethernet 1-2
Physical interface : ethernet 1, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited
Physical interface : ethernet 2, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited

```

Show all ethernet UNIs in all ONUs in a given gpon interface

```

# show interface gpon 1/1/1 onu * ethernet *
Physical interface : ethernet 1, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited
Physical interface : ethernet 2, Enabled, Physical link is up
GPON Information   : gpon-1/1/1, ONU 1
Link-level type    : Ethernet
Speed/Duplex       : Auto
Status Negotiation: 1 Gbit/s Full-Duplex
Native VLAN/CoS    : -
MAC limit          : Unlimited
Physical interface : ethernet 1, Enabled, Physical link is down
GPON Information   : gpon-1/1/1, ONU 10

```

```
Link-level type   : Ethernet
Speed/Duplex     : Auto
Status Negotiation:
Native VLAN/CoS  : -
MAC limit        : Unlimited
```

When using detail option, it will override other show options passed. For example, if the operator runs “show interface gpon 1/1/1 onu 1 ethernet 1 brief detail”, “show interface gpon 1/1/1 onu 1 ethernet 1 statistics detail” or “show interface gpon 1/1/1 onu 1 ethernet 1 brief detail statistics” only detail option will be shown.

The same way, statistics option will override the default “show interface gpon 1/1/1 onu 1 ethernet 1” or it will have precedence over brief option in “show interface gpon 1/1/1 onu 1 ethernet 1 brief statistics” outputs as well.

Impacts and precautions

It is not supported to use a key pattern in gpon interface IDs (`show interface gpon * onu * ethernet`).

Hardware restrictions

N/A

show interface gpon onu gem

Description

Displays ONU GPON Encapsulation Method information.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

```
show interface gpon chassis/slot/port onu [ onu-id ] gem [ gem-id ] [ brief | statistics ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

chassis/slot/port

Description: The GPON port on which the ONU is located.

Value: Text: chassis/slot/port format.

Default Value: N/A

onu-id

Description: The ONU where the GEM is located.

Value: onu-id: Number from 0 to 127 (maximum of 64 elements).

Default Value: N/A

gem-id

Description: The ID of the GEM for information display.

Value: gem-id: Number from 1 to 16.

Default Value: N/A

brief

Description: Display brief information of the GEM.

Value: brief: Fixed text 'brief'.

Default Value: N/A

statistics

Description: Display statistics information of the ONU's GEM port.

Value: statistics: Fixed text 'statistics'.

Default Value: N/A

Output Terms

Output	Description
<code>GEM ID</code>	ID of the GEM.
<code>Operation status is</code>	Operational status.
<code>GEM Port-ID</code>	ID of the GEM Port.
<code>Alloc-ID</code>	Alloc ID of the GEM.
<code>T-CONT</code>	T-CONT ID related to the GEM.
<code>Encryption</code>	Encryption state (enabled/disabled).

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.4	The the maximum GEM ID value was changed from 40 to 16.
1.8	Removed no longer valid 'statistics' parameter.
4.2.0	Added support for range of IDs in show options.
5.12.0	Added 'statistics' parameter.

Usage Guidelines

Show a GEM in an ONUs

```
# show interface gpon 1/1/1 onu 13 gem 1

GEM ID                : 1
GPON Information       : gpon-1/1/1, ONU 10
Operational status is : up
GEM Port-ID           : 352
Alloc-ID              : 256
T-CONT                : 1
Encryption             : disabled
```

Show all GEMs in all ONUs in a given gpon interface

```
# show interface gpon 1/1/1 onu * gem *

GEM ID                : 1
GPON Information       : gpon-1/1/1, ONU 1
Operational status is : up
GEM Port-ID           : 305
Alloc-ID              : 256
T-CONT                : 1
Encryption             : disabled

GEM ID                : 1
GPON Information       : gpon-1/1/1, ONU 10
Operational status is : up
GEM Port-ID           : 450
Alloc-ID              : 257
T-CONT                : 1
Encryption             : disabled
```

Show all GEMs in a given ONU

```
# show interface gpon 1/1/1 onu 10 gem *

GEM ID          : 1
GPON Information : gpon-1/1/1, ONU 10
Operational status : down
GEM Port-ID     : 449
Alloc-ID        : 0
T-CONT          : 1
Encryption      : disabled

GEM ID          : 2
GPON Information : gpon-1/1/1, ONU 10
Operational status : down
GEM Port-ID     : 450
Alloc-ID        : 0
T-CONT          : 1
Encryption      : disabled
```

Show all GEMs in a given ONU

```
# show interface gpon 1/1/1 onu 10 gem

GEM ID          : 1
GPON Information : gpon-1/1/1, ONU 10
Operational status : down
GEM Port-ID     : 449
Alloc-ID        : 256
T-CONT          : 1
Encryption      : unknown

GEM ID          : 2
GPON Information : gpon-1/1/1, ONU 10
Operational status : down
GEM Port-ID     : 450
Alloc-ID        : 256
T-CONT          : 1
Encryption      : disabled
```

Show GEM statistics

```
# show interface gpon 1/1/1 onu 10 gem

GEM ID          : 1
GPON Information : gpon-1/1/1, ONU 10
Operational status : down
GEM Port-ID     : 449
Alloc-ID        : 256
T-CONT          : 1
Encryption      : unknown
Traffic statistics :
  Input packets   : 750
  Output packets  : 1100
  Input octets    : 150000
  Output octets   : 220000
```

Impacts and precautions

It is not supported to use a key pattern in gpon interface IDs. For example:

```
show interface gpon * onu * gem
```

Hardware restrictions

N/A

CHAPTER 15: SERVICES

This chapter describes the CLI commands related to DmOS available services.

MANAGEMENT

This topic describes the commands related to use of management clients such as commands to open a telnet or SSH connection to a remote device.

assistant-task

Description

Configures tasks to be executed at a scheduled time.

Supported Platforms

This command is supported in all platforms.

Syntax

assistant-task *task-name* **action cli-file** *file-name* [**enabled|disabled**]

assistant-task *task-name* **schedule** {**recursive|once**} [**day** *day*] [**hour** *hour*] [**minute** *minute*] [**month** *month*] [**weekday** *weekday*] [**second** *second*]

assistant-task *task-name* **run-now**

assistant-task *task-name* **action watch cli-cmd** *cli-cmd* **match** *match* **cli-file** *file-name* **regex** *regex* [**disable-after-match**]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

task-name

Description: Name of assistant task.

Value: Text (1-100 characters)

Default Value: N/A

action

Description: Action to be executed by the assistant-task.

Value: N/A

Default Value: N/A

cli-file *file-name*

Description: File containing CLI commands. Special characters are not allowed in the file or in the file name. Must be an ASCII file.

Value: File name

Default Value: N/A

enabled

Description: Enables the assistant-task. This parameter takes effect only for scheduled actions.

Value: N/A

Default Value: N/A

disabled

Description: Disables the assistant-task. This parameter takes effect only for scheduled actions.

Value: N/A

Default Value: N/A

schedule recursive

Description: Indicates this task is to be executed recursively at a configured time.

Value: N/A

Default Value: N/A

schedule once

Description: Indicates this task is to be executed once at a configured time.

Value: N/A

Default Value: N/A

day *day*

Description: Day of month when the task is to be executed. If omitted, task will be executed every day. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any day or 1-31 range.

Value: 1-31

Default Value: N/A

hour *hour*

Description: Hour when the task is to be executed. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any hour or 0-23 range.

Value: 0-23

Default Value: 0

minute *minute*

Description: Minute when the task is to be executed. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any minute or 0-59 range.

Value: 0-59

Default Value: 0

month *month*

Description: Month when the task is to be executed. If omitted, task will be executed every month. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any month or 1-12 range.

Value: 1-12

Default Value: N/A

weekday *weekday*

Description: Weekday when the task is to be executed. If omitted, task will be executed every day. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any weekday or 0-6 range.

Value: 0-7 (where 0 and 7 correspond to Sunday)

Default Value: N/A

second *second*

Description: Second when the task is to be executed. If omitted, task will be executed every second 0. If task is recursive, it may contain ranges. Field value can be asterisk (*), which always stands for “first-last”, that is, any second or 0-59 range.

Value: 0-59

Default Value: 0

run-now

Description: Executes a committed task immediately ignoring the scheduled configuration and the enabled/disabled parameter.

Value: N/A

Default Value: N/A

watch

Description: Actions to be executed based on a watch/match pattern.

Value: N/A

Default Value: N/A

cli-cmd *cli-cmd*

Description: CLI command in quotes to be executed according to schedule. Special characters are not allowed in the file or in the file name. Must be an ASCII file.

Value: CLI command

Default Value: N/A

match *match*

Description: Match and its related actions to be executed when a regex pattern is found.

Value: Match name

Default Value: N/A

regex *regex*

Description: Regular expression pattern in quotes for match configuration.

Value: Regex pattern

Default Value: N/A

disable-after-match

Description: Disables the assistant-task after a regex match.

Value: N/A

Default Value: N/A

Default

N/A

Command Mode

Configuration mode

Required Privileges

Admin

History

Release	Modification
---------	--------------

4.9	This command was introduced.
-----	------------------------------

5.0	Watch command addition
-----	------------------------

Usage Guidelines

This command is used to configure frequent tasks to be scheduled by the user.

Example:

First of all you must create a CLI command file and transfer it to the equipment. Alternatively, it is possible to edit or create a new file using the 'file edit <filename>' command. Remember that the 'config' command must be included in the file to enter the configure mode.

When saving files, use the 'save overwrite' option to avoid being asked about existing files. The example below shows a file that can be used to save a configuration backup and send it to a tftp server.

```
# file show backup.cli
show running-config | save overwrite backup.cfg
copy file backup.cfg tftp://10.1.1.1
#
```

Assistant task runs in non-interactive mode, so there is no need to include the confirmation response in the command file. Older DmOS versions, such as 4.10.2, required the confirmation response to be included. This will not work anymore. Operators need to remove all confirmation responses from existing cli command files, using file edit command, otherwise the assistant task may return a failure during its execution.

Configure a task to be run once today at midnight (no time/date specified):

```
# config
Entering configuration mode terminal
(config)# assistant-task backup
(config-assistant-task-backup)# action cli-file backup.cli
(config-assistant-task-backup)# schedule once
(config)# commit
Commit complete.
```

Configure a task to be run once Sunday at midnight:

```
# config
Entering configuration mode terminal
(config)# assistant-task backup
(config-assistant-task-backup)# action cli-file backup.cli
(config-assistant-task-backup)# schedule once weekday 0
(config)# commit
Commit complete.
```

Configure a task to be run from Monday to Friday, except Thursday, at 8am and 6pm. It is possible to provide a combination of range and list:

```
# config
Entering configuration mode terminal
(config)# assistant-task backup
(config-assistant-task-backup)# action cli-file backup.cli
(config-assistant-task-backup)# schedule recursive hour 8,18
(config-assistant-task-backup)# schedule recursive weekday 1-3,5
(config)# commit
Commit complete.
```

Configure a task to be run at the first day of the month at 9am:

```
# config
Entering configuration mode terminal
(config)# assistant-task backup
(config-assistant-task-backup)# action cli-file backup.cli
(config-assistant-task-backup)# schedule recursive hour 9 day 1
```

```
(config)# commit
Commit complete.
```

Run a configured task immediately to test if it is running correctly. The *run-now* command will work even if the task is disabled. After executing this command, use the *show assistant-task* command to see the command result.

```
# config
Entering configuration mode terminal
(config)# assistant-task backup
(config-assistant-task-backup)# action cli-file backup.cli
(config-assistant-task-backup)# schedule recursive day 1
(config-assistant-task-backup)# commit
Commit complete.
(config-assistant-task-backup)# run-now
(config-assistant-task-backup)# top; exit
# show assistant-task backup last-success output
Last successful execution - Thu Aug 29 09:23:35 -03 2019
<
Transfer complete.
>
```

It is possible to inspect currently running tasks by using the *show* command. Running tasks can also be interrupted by disabling them:

```
# show assistant-task
TASK
NAME      LAST START                LAST FAILURE    LAST SUCCESS    STATUS
-----
backup    Tue Aug 20 23:00:00 -03 2019 -          -              running
# config
(config)# assistant-task backup
(config-assistant-task-backup)# disabled
(config-assistant-task-backup)# commit
(config-assistant-task-backup)# top ; exit
# show assistant-task
TASK
NAME      LAST START                LAST FAILURE    LAST SUCCESS    STATUS
-----
backup    Tue Aug 20 23:00:00 -03 2019 -          -              disabled
```

Configure a task to be run every second (no time/date specified) checking a link health and when a problem occurs changes the link interface.

```
# file show connectTo1.cli
config
no dot1q vlan 500
dot1q vlan 500
no interface 1/1/10
interface 1/1/9
commit
top
exit
#
# file show connectTo2.cli
config
no dot1q vlan 500
dot1q vlan 500
no interface 1/1/9
interface 1/1/10
commit
```

```

top
exit
#
# config
Entering configuration mode terminal
(config)# assistant-task vlanSwitch
(config-assistant-task-vlanSwitch)# schedule recursive minute * hour * second 0-59
(config-assistant-task-vlanSwitch)# action watch cli-cmd "ping 10.1.1.2 | include
\"100% packet l\" | count ; show running-config dot1q vlan 500 |
include ethernet ;"
(config-assistant-task-vlanSwitch)# action watch match M0
(config-assistant-task-match-M0)# cli-file connectTo1.cli
(config-assistant-task-match-M0)# regex ".*Count: 1 lines.*1/1/10"
(config-assistant-task-match-M0)# exit
(config-assistant-task-vlanSwitch)# action watch match M1
(config-assistant-task-match-M1)# cli-file connectTo2.cli
(config-assistant-task-match-M1)# regex ".*Count: 1 lines.*1/1/9"
(config-assistant-task-match-M1)# exit
(config-assistant-task-vlanSwitch)# commit
Commit complete.

```

Schedule example to run an assistant task at 00:00 on the first day of every month:

```

(config)# assistant-task example
(config-assistant-task-example)# schedule recursive minute 0 hour 0 day 1 month *

```

Schedule example to run an assistant task at 01:00 every day:

```

(config)# assistant-task example
(config-assistant-task-example)# schedule recursive minute 0 hour 1 day * month *

```

Schedule example to run an assistant task at minute 30 of every hour:

```

(config)# assistant-task example
(config-assistant-task-example)# schedule recursive minute 30 hour * day * month *

```

Schedule example to run an assistant task at 03:00 every Sunday:

```

(config)# assistant-task example
(config-assistant-task-example)# schedule recursive minute 0 hour 3 weekday 0 month *

```

Impacts and precautions

Commands executed by the assistant-task feature are executed by special users called *batch_<task_name>*. This user may appear in logs depending on the commands present in the CLI file.

Tasks configured to run only once will be automatically disabled after executed. It is possible to reschedule it to run at a later date by enabling it again.

ATTENTION: When saving files in the CLI script, be careful not to let them grow indefinitely to avoid using all available memory. Use copy-file to transfer it to another machine

and remove them.

ATTENTION: Do not use “| repeat” or other commands that do not return, otherwise the assistant task will not be able to log its output and the task will run indefinitely, until it is disabled.

Hardware restrictions

N/A

logout

Description

Terminates a specific session or all CLI and NETCONF sessions of a specific user. If no session or user is specified, the current session is terminated. If the terminated session held the **configure exclusive** lock, it will be released.

Supported Platforms

This command is supported in all platforms.

Syntax

logout [**session** *session-id* | **user** *user-name*]

Parameters

session *session-id*

Description: Terminates a specific session.

Value: Integer value representing the session ID, which can be obtained by using command “who” or by pressing <TAB>.

Default Value: N/A

user *user-name*

Description: Terminates all CLI and NETCONF sessions of a specific user.

Value: String representing the user name.

Default Value: N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.

Usage Guidelines

Before using this command, use command “who” to check the existing sessions. The session marked with a “*” is the current one.

Example:

This example shows how to logout a specific session.

```
# who
Session User Context From Proto Date Mode
*22 admin cli 127.0.0.1 console 17:10:47 operational
21 config cli 192.168.0.26 telnet 17:10:37 operational
19 config cli 192.168.0.26 ssh 17:10:03 operational
18 audit cli 192.168.0.26 ssh 17:09:38 operational
# logout session 21
# who
Session User Context From Proto Date Mode
*22 admin cli 127.0.0.1 console 17:10:47 operational
19 config cli 192.168.0.26 ssh 17:10:03 operational
18 audit cli 192.168.0.26 ssh 17:09:38 operational
#
```

This example shows how to logout all sessions of a specific user.

```
# who
Session User Context From Proto Date Mode
24 config cli 192.168.0.26 telnet 17:14:27 operational
23 audit cli 192.168.0.26 ssh 17:14:20 operational
*22 admin cli 127.0.0.1 console 17:10:47 operational
19 config cli 192.168.0.26 ssh 17:10:03 operational
# logout user config
# who
Session User Context From Proto Date Mode
23 audit cli 192.168.0.26 ssh 17:14:20 operational
*22 admin cli 127.0.0.1 console 17:10:47 operational
#
```

The logged out user will receive a message informing what happened:

```
login: config
Password:
Welcome to the DmOS CLI
config connected from 192.168.0.26 using telnet on
#
Message from admin@ at 2017-03-27 17:12:13...
Your session has been terminated by admin
# Connection closed by foreign host.
```


Impacts and precautions

All uncommitted changes in the terminated sessions will be lost.

Hardware restrictions

N/A

show assistant-task

Description

Used to list assistant-task results.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show assistant-task [task-name [[last-start|last-failure|last-success|task-status]  
[output]]
```

Parameters

task-name

Description: Name of assistant task.
Value: Text (1 to 100 characters)
Default Value: N/A

last-start

Description: Shows the timestamp of the last execution start.
Value: N/A
Default Value: N/A

last-failure

Description: Shows the timestamp of the last unsuccessful execution.
Value: N/A
Default Value: N/A

last-success

Description: Shows the timestamp of the last successful execution.
Value: N/A
Default Value: N/A

task-status**Description:** Shows the current task status.**Value:** idle | running | disabled**Default Value:** N/A**output****Description:** Shows the task output between "< >"(may be empty depending on the executed task).**Value:** N/A**Default Value:** N/A**Output Terms**

Output	Description
Task Name	Name of assistant task.
Last Start	Start time of the last execution.
Last Failure	Time of the last unsuccessful execution.
Last Success	Time of the last successful execution.
Task status	Current status of the task.
Task output	Examples of this command are displayed in the Usage Guidelines field

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
4.9	This command was introduced.

Usage Guidelines

The examples below show how to use the command show assistant-task.

Example:

Listing all configured tasks:

```
# show assistant-task
TASK
NAME      LAST START                LAST FAILURE                LAST SUCCESS  STATUS
-----
task_1    Fri Aug 20 08:46:00 -03 2019  Tue Aug 20 10:00:15 -03 2019  -             idle
task_2    Fri Aug 21 06:11:00 -03 2019  -                          -             running
```

It is possible to see a specific task, by providing the task name:

```
# show assistant-task task_1
TASK
NAME      LAST START                LAST FAILURE                LAST SUCCESS  STATUS
-----
task_1    Fri Aug 20 08:46:00 -03 2019  Tue Aug 20 10:00:15 -03 2019  -             idle
```

To see the actual output of executed task:

```
DM4170# show assistant-task task_1 last-failure output
Last failed execution - Tue Aug 20 10:00:15 -03 2019
<
The file backup.cli does not exist
>
```

The same is valid for successful output:

```
DM4170# show assistant-task task_2 last-success output
% No entries found.
```

To see the actual status of the task:

```
DM4170# show assistant-task task_1 task-status
Task status - idle
```

Impacts and precautions

N/A

Hardware restrictions

N/A

show ssh-server

Description

Show the public key from Secure shell (SSH) server

Supported Platforms

This command is supported in all platforms.

Syntax

show ssh-server { public-key }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

public-key

Description: Show the public key of internal ssh-server.

Value: No value.

Default Value: No default value.

Output Terms

Output	Description
Status	Internal public key from server

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.4	Added option of the management the keys of equipment. Will be have possible show the public keys and delete keys of equipment. The options include the all keys or by type keys.

Usage Guidelines

To show ssh public keys

```
# show ssh-server public-key
Key information
Type:
Size:
Date Generated:
Data:
```

Impacts and precautions

N/A

Hardware restrictions

N/A

ssh

Description

"SSH" is an utility whose purpose is to allow the user to connect to a remote network host or device through a secure encrypted connection, after the connection has been established it is possible to execute commands on the remote destination host or device.

Supported Platforms

This command is supported in all platforms.

Syntax

```
ssh [ username@ ] ipv4-address [ port port-number ] [ vrf vrf-name ]
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

username@

Description:	User name to login.
Value:	N/A
Default Value:	User logged in the system.

ipv4-address

Description:	Destination IPv4 address to connect.
Value:	N/A
Default Value:	No default value.

port *port-number*

Description:	Destination port.
Value:	1-65535
Default Value:	22

vrf *vrf-name*

Description:	Specifies the VRF used for all outgoing SSH packets.
Value:	VRF name
Default Value:	None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.0	This command was introduced.
7.0	Added VRF support.

Usage Guidelines

The following example shows how to use the ssh command with all options:

```
hostname# ssh thomaz@10.0.120.80 port 23 vrf green
```

The following example shows how to use the ssh command without server port, it will use the default value (22):

```
hostname# ssh thomaz@10.0.120.80
```

The following example uses only ip address, it will use the logged user and the default port:

```
hostname# ssh 10.0.120.80
```

Impacts and precautions

VRFs global and mgmt are not supported.

Hardware restrictions

N/A

ssh-server

Description

SSH server configurations.

Supported Platforms

This command is supported in all platforms.

Syntax

```
ssh-server { legacy-support | max-connections max-connections-number | port port-number }*
```

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

legacy-support

Description:	Support for ssh clients running openssh versions older than 7.0.
Value:	N/A
Default Value:	N/A

max-connections *max-connections-number*

Description:	Defines the maximum number of SSH connections via CLI for each address family. NETCONF access connections are handled separately.
Value:	1-16
Default Value:	8

port *port-number*

Description:	Defines the SSH server port number via CLI.
Value:	22 1024-65535
Default Value:	22

Default

N/A.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.8.2	Added support for ssh clients running openssh versions older than 7.0.
1.12	Parameter max-connections was added.
2.4	Parameter port was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure ssh-server legacy-support.

```
(config)# ssh-server legacy-support
(config)# commit
The following warnings were generated:
'ssh-server': Enabling legacy ssh key exchange algorithms will bring security vulnerabilities.
Proceed? [yes,no] yes
Commit complete.
```

This example shows how to configure no ssh-server legacy-support.

```
(config)# no ssh-server legacy-support
(config)# commit
Commit complete.
```

To limit number of SSH connections

Example:

This example shows how to configure ssh-server max-connections.

```
(config)# ssh-server max-connections 2
(config)# commit
Commit complete.
```

This example shows how to return the number of ssh max-connection to the default value.

```
(config)# no ssh-server max-connections
(config)# commit
Commit complete.
```

To configure the port number of SSH

Example:

This example shows how to configure ssh-server port number.

```
(config)# ssh-server port 2048
(config)# commit
The following warnings were generated:
'ssh-server port': New SSH connections must use the configured port.
Proceed? [yes,no] yes
Commit complete.
```

This example shows how to return the port number of ssh to the default value.

```
(config)# no ssh-server port
(config)# commit
The following warnings were generated:
'ssh-server port': New SSH connections must use the configured port.
Proceed? [yes,no] yes
Commit complete.
```

Impacts and precautions

When *legacy-support* is enabled, a deprecated key exchange algorithm will be used. This can bring security vulnerabilities.

Hardware restrictions

None.

ssh-server

Description

Secure shell (SSH) server, for secure access from remote hosts.

Supported Platforms

This command is supported in all platforms.

Syntax

ssh-server generate-key { type | size }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

type

Description: Specifies the type of key to create.

Value: {all | dsa | rsa | ecdsa | ed25519}

Default Value: None.

size

Description: Specifies the size of key to create. The option only present in keys of the type rsa.

Value: 1024-2048

Default Value: None.

Output Terms

Output	Description
Status	'Generated keys' if success. Error message otherwise

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.4	Added option of the management the keys of equipment. Will be have possible show the public keys and delete keys of equipment. The options include the all keys or by type keys.
4.0	Added support for ECDSA and ED25519 keys.

Usage Guidelines

To generated new keys, all types

```
# ssh-server generate-key all
Really want to do this? [yes,no] yes
Generated keys
#
```

To generated keys dsa type

```
# ssh-server generate-key dsa
Really want to do this? [yes,no] yes
Generated keys
#
```

To generated keys ecdsa type

```
# ssh-server generate-key ecdsa
Really want to do this? [yes,no] yes
Generated keys
#
```

To generated keys ed25519 type

```
# ssh-server generate-key ed25519
Really want to do this? [yes,no] yes
Generated keys
#
```

To generated keys rsa type

```
# ssh-server generate-key rsa size 1024
Really want to do this? [yes,no] yes
Generated keys
#
```

Impacts and precautions

N/A

Hardware restrictions

N/A

telnet

Description

“TELNET” is a network protocol which uses TCP to establish a connection with the destination host. Through TELNET it is possible to run programs, transmit data and execute many other remote administration tasks such as changing various settings on a device.

Supported Platforms

This command is supported in all platforms.

Syntax

telnet *host* [**port** *port-number*]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

host

Description: Specifies the destination IPv4 address.

Value: None.

Default Value: None.

port *port-number*

Description: (Optional) Specifies the destination port number.

Value: Range: 1-65535

Default Value: 23

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

1.0	This command was introduced.
-----	------------------------------

Usage Guidelines

The following example shows how to use the telnet command with all options:

```
hostname# telnet 10.0.120.88 port 56
```

The following example shows how to use the telnet command without server port, it will use the default value (23):

```
hostname# telnet 10.0.120.88
```

Impacts and precautions

N/A

Hardware restrictions

N/A

telnet-server

Description

Configures internal telnet server for external access.

Supported Platforms

This command is supported in all platforms.

Syntax

telnet-server { **enabled** | **disabled** | **max-connections** *max-connections-number* | **port** *port-number* }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

enabled

Description: Enables the telnet server.

Value: N/A

Default Value: N/A

disabled

Description: Disables the telnet server.

Value: N/A

Default Value: N/A

max-connections *max-connections-number*

Description: Defines the maximum number of Telnet connections via CLI for each address family.

Value: 1-16

Default Value: 8

port *port-number*

Description:	Defines the Telnet server port number via CLI.
Value:	23 1024-65535
Default Value:	23

Default

Disabled.

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.
1.12	Parameter max-connections was added.
5.12	Parameter port was added.

Usage Guidelines

Enable example:

```
# config
(config)# telnet-server enabled
(config)# commit
Commit complete.
```

Disable example:

```
# config
(config)# telnet-server disabled
(config)# commit
Commit complete.
```

To limit number of Telnet connections

```
(config)# telnet-server max-connections 2
(config)# commit
Commit complete.
```

This example shows how to return the number of telnet max-connection to the default value.

```
(config)# no telnet-server max-connections
(config)# commit
Commit complete.
```

This example shows how to configure telnet-server port number.

```
DM4400(config)# telnet-server port 2048
DM4400(config)# commit
Commit complete.
```

This example shows how to return the port number of telnet to the default value.

```
DM4400(config)# no telnet-server port
DM4400(config)# Commit
Commit complete.
```

Impacts and precautions

None.

Hardware restrictions

None.

who

Description

Lists the current user sessions.

Supported Platforms

This command is supported in all platforms.

Syntax

who

Parameters

N/A

Output Terms

Output	Description
Session	Session identification
User	Connected user
Context	User session context: cli, netconf or snmp
From	Connection source IP address
Proto	Protocol used for connection: ssh, tcp (telnet) or console
Date	Date/time of user connection (date is only shown if different from current date)

Output	Description
Mode	Current user mode: operational, config-exclusive, config-terminal or config-shared

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
4.6	Telnet connections are now indicated by protocol 'tcp'.

Usage Guidelines

Example:

```
(config)# do who
Session User Context From Proto Date Mode
27 admin cli 192.168.0.10 tcp 20:41:25 config-exclusive
26 admin netconf 192.168.0.26 ssh 20:55:29 operational
*25 admin cli 127.0.0.1 console 20:41:23 config-terminal
```

Impacts and precautions

N/A

Hardware restrictions

N/A

SYSTEM

This topic describes the commands related to the device management such as commands of reboot and stacking.

card-model

Description

Switch the card-model to select 24XS+3CX or 24XS+4QX interface set.

Supported Platforms

This command is supported only in the following platforms: DM4270.

Syntax

card-model [**card-model** {*card_model*}]

Parameters

card-model *card_model*

Description: Identifies the model of the card that will be used by DmOS.

Value: 24XS+3CX or 24XS+4QX

Default Value: None

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
4.7	This command was introduced.
4.9	Addition of the 24XS+2QX+1CX option.
5.12	Replaces card model 24XS+2CX with 24XS+3CX. Removes the support to choose the model 24XS+2QX+1CX.

Usage Guidelines

The DM4270 has a flexible interface set composed of 24 10 Gbps Ethernet interfaces and four interfaces that can be used in two physical configurations:

- three 100 Gbps interfaces;
- four 40 Gbps interfaces.

This design results in the two supported card-models: 24XS+3CX and 24XS+4QX.

The “card-model” command selects which interface set will be used and takes effect after the factory configuration is automatically loaded and the device is rebooted.

An example of the command usage is shown below.

```
DM4270# card-model 24XS+4QX
Warning: The system will automatically reboot and load the factory configuration.
Proceed with this action? [yes,NO] yes
Loading.
Done.
Switching to runlevel: 6
Broadcast message from root@DM4270 (pts/0) (Thu Jan 10 17:04:37 2019):
The system is going down for reboot NOW!
Commit complete.
```

Impacts and precautions

This command will cause the factory-config to be loaded and will reboot the device immediately. Be aware that this operation will cause loss of remote management access.

Hardware restrictions

N/A

clear log

Description

This command allows you to delete all logs persisted in equipment.

Supported Platforms

This command is supported in all platforms.

Syntax

clear log

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release**Modification**

1.0 This command was introduced.

Usage Guidelines

N/A

Impacts and precautions

N/A

Hardware restrictions

N/A

log

Description

This command focuses all logs system settings.

Supported Platforms

This command is supported in all platforms.

Syntax

log { **severity** { **alert** | **critical** | **emergency** | **error** | **informational** | **notice** | **warning** } | **syslog** *ip-address* [**vrf** *vrf-name*] [**port** *port*] [**source** { **ipv4** **address** *ip-address* | **interface** *interface-name* }] }

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

severity { **alert** | **critical** | **emergency** | **error** | **informational** | **notice** | **warning** }

Description: This parameter allows you to set the minimum log level to be persisted.

Value: N/A

Default Value: informational

syslog *ip-address*

Description: This parameter allows the registration of IP(v4/v6) hosts to receive the logs generated by the equipment. It can add up to six hosts.

Value: a.b.c.d or X:X:X:X::X.

Default Value: None

vrf *vrf-name*

Description: (Optional) Specifies the name of VRF which the syslog server can be reached.

Value: String.

Default Value: None.

port *port*

Description: (Optional) Specifies the port that syslog server is listening for UDP syslog messages.

Value: 514, 1025-65534

Default Value: 514

source ipv4 address *ip-address*

Description: (Optional) Specify the source ip address where syslog messages should be send through.

Value: a.b.c.d.

Default Value: None

source interface *interface-name*

Description: (Optional) Specify the source interface where syslog messages should be send through.

Value: Interface name in format I3-<name> or loopback-<id>.

Default Value: None

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.0	This command was introduced.
5.2	Added vrf option to syslog configuration.
5.12	Added option to configure UDP port for syslog server.
6.0	Added option to configure source ipv4 address and interface for syslog server.

Usage Guidelines

Enable syslog to server 172.22.110.101, associate to vrf green, configure a UDP port and source ip-address 172.22.110.10

```
# config
(config)# vrf green
(config-vrf-green)# top
(config)# dot1q vlan 100
(config-vlan-100)# top
(config)# interface l3 l3
(config-l3-l3)# lower-layer-if vlan 100
(config-l3-l3)# ipv4 address 172.22.110.10/24
(config-l3-l3)# vrf green
(config-l3-l3)# top
(config)# log syslog 172.22.110.101 vrf green port 5000 source ipv4 address 172.22.110.10
(config-syslog-172.22.110.101)# commit
Commit complete.
```

Impacts and precautions

N/A

Hardware restrictions

N/A

reboot

Description

Restarts the system.

Supported Platforms

This command is supported in all platforms.

Syntax

reboot

Parameters

N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.2	This command was introduced.

Release	Modification
---------	--------------

1.10	The chassis and slot parameters were removed.
------	---

Usage Guidelines

This command is to be used when the user wants to restart the entire system. For restarting the system in cases when the system can not be restarted using this command, see the **reboot-forced** command.

This command is safe because it only restarts the system after terminating its activities that includes storing the remaining data and unmounting the partitions.

Impacts and precautions

None

Hardware restrictions

None

reboot-forced

Description

Restarts the system using forced mode.

Supported Platforms

This command is supported in all platforms.

Syntax

reboot-forced

Parameters

N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
1.2	This command was introduced.

Release	Modification
---------	--------------

1.10	The chassis and slot parameters were removed.
------	---

Usage Guidelines

This command is to be used when the user wants to restart the system despite any software hang problem that may happen, which would prevent the system of being restarted using the reboot command.

Impacts and precautions

It may cause permanent loss of configuration or other data, because a critical operation can be interrupted. It can happen if the equipment was restarted during a configuration commit or firmware activation, for example. Use only if the **reboot** command fails.

Hardware restrictions

None

show inventory

Description

This command displays the system inventory information, including the part number, hardware version, serial number and other relevant information.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show inventory [chassis {chassis_id} [brief | factory-codes | macs | transceivers |  
slot {slot_id} [brief | factory-codes | macs | transceivers | port [port_type] [port_id]  
[mac | transceiver]]]]
```

Parameters

chassis *chassis_id*

Description: Chassis Identifier. If the value of this parameter is '*' or ' ', a list of all present chassis will be shown. Currently only one chassis_id is supported.

Value: 1

Default Value: None

brief

Description: Shows brief inventory information about the chassis or a specific card.

Value: N/A

Default Value: N/A

factory-codes

Description: Shows factory information about the chassis or a specific card.

Value: N/A

Default Value: N/A

macs

Description: Shows the MAC addresses of all ports of the chassis or a specific card.

Value: N/A

Default Value: N/A

transceivers

Description: Shows inventory information about all transceivers present on chassis or a specific card.

Value: N/A

Default Value: N/A

slot *slot_id*

Description: Identifies a card present on chassis. If the value of this parameter is '*' or ' ', a list of all present cards will be shown. This will be dependent on the product being managed. The values below are for Dm4610.

Value: 1, PSU1, PSU2 or FAN

Default Value: None

port *port_type*

Description: Identifies the desired type of port present on the card. If the value of this parameter is '*' or ' ', a list of all ports of the card will be shown. This will be dependent on the product being managed. The values below are for Dm4610.

Value: gigabit-ethernet, gpon or ten-gigabit-ethernet

Default Value: None

port_type *port_id*

Description: Identifies a port of a specific type. If the value of this parameter is '*' or ' ', a list of all ports of the card with the desired type will be shown. This parameter values are dependent on the card present at the card. The value below is for Dm4610 cards.

Value: 1-12

Default Value: None

Output Terms

Output	Description
Chassis/Slot	Chassis and slot identification
Product model	Hardware model of the product/card
Part number	Product part number
Serial number	Product serial number
Product revision	Product revision
PCB revision	Printed Circuit Board revision
Hardware version	Hardware version
Operat. temp.	Range of operating temperature
System MAC address	Product MAC Address in hexadecimal presentation
Factory code	Equipment factory information
Interface	Physical interface type and location in the format Chassis/Slot/Port
MAC address	Interface MAC Address in hexadecimal presentation, if applicable
Port type	Port type of the interface, which may be Electrical or Transceiver
Transceiver information	Presence and inventory information of the transceiver
Presence	Informs if the transceiver is present

Output	Description
Vendor name	Name of the vendor that provides this Transceiver
Serial number	Transceiver serial number
Part number	Transceiver part number
Type	Transceiver type, e.g., SFP, QSFP.
Media	Transceiver media, e.g., Optical, Electrical.
Connector	Transceiver connector
Laser wavelength	Transceiver wavelength
Fiber Type	Transceiver supported fiber type, e.g., Single Mode, Multimode.
Ethernet standards	Transceiver supported ethernet standards
Digital Diagnostics thresholds	Transceiver digital diagnostics thresholds

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.2	Added support for displaying transceiver inventory information
5.10	Added fiber type information for transceivers

Usage Guidelines

The user can display information about chassis, slots, ports and transceivers. Please see below examples of usage for each type of inventory information in display.

This example shows how to display the chassis inventory

```
DM4610# show inventory chassis 1
Chassis          : 1
Product model    : DM4610

Chassis/Slot     : 1/1
Product model    : 8GPON+8GX+4GT+2XS
...
```

This example shows how to display a slot's inventory

```
DM4610# show inventory chassis 1 slot PSU1
Chassis/Slot     : 1/PSU1
Product model    : PSU 120 AC
Part number      : 800.5079.03
Serial number    : 3047214
Product revision : 3
...
```

This example shows how to display a transceiver's inventory

```
DM4610# show inventory chassis 1 slot 1 port gigabit-ethernet 1 transceiver
Interface gigabit-ethernet 1/1/1
Port type        : Transceiver
Transceiver information
Presence         : Yes
Vendor name      : APAC Opto
...
```

Impacts and precautions

If any value is identified as Not Available, it will be considered as having no meaning in that particular chassis/slot/interface. If any value is identified as Unknown, it means that the value is valid for that particular chassis/slot/interface, but it wasn't possible to obtain that information.

Hardware restrictions

N/A

show log

Description

Display all logs persisted in equipment.

Supported Platforms

This command is supported in all platforms.

Syntax

show log [**component** {components}* | **severity** {severities}* | **tail** {number_of_logs}]

Parameters

component {components}*

Description: If this filter is used, only messages generated by the specified components are displayed. A component is an identifier for the functionality which the log message refers to. More than one component can be filtered at the same time.

Value: {components}*

Default Value: N/A

severity {severities}*

Description: If this filter is used, only messages generated with the specified severities will be displayed. More than one severity can be filtered at the same time.

Value: alert, critical, emergency, error, informational, notice, warning

Default Value: N/A

tail {number_of_logs}

Description: Show only the last logs.

Value: 1-65535.

Default Value: 10

Output Terms

Output	Description
Date	Date of log entry in the format: YYYY-MM-DD.
Time	Time of log entry in the format: hh:mm:ss.ddd (3 digits for the decimal fraction of a second).
Slot	Chassis/slot where the log message was generated.
Severity	Severity level of the log message.
Component	An identifier for the functionality which the log message refers to. Each log Component comprises a set of Message Codes.
MessageCode	An identifier (mnemonic) for the log message.
ProcessName	The name of the operational system process that generated the log message. It may not be unique.
PID	The ID of the operational system process that generated the log message. It is unique inside the corresponding slot. It may not be unique across a multi-CPU system.
Text	The log message itself, which may contain fixed and variable parts, describing an event.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.8	New format for logs output. Added MessageCode, ProcessName and PID fields.
1.12	Added the parameter 'tail' that allows to show only the last logs.

Usage Guidelines

Log entries are displayed in the following general format:

```
Date Time : Slot : <Severity> %Component-MessageCode : ProcessName[PID] : Text
```

This example shows how to display all equipment logs:

```
DM4610# show log
Show Contents of All Known UserLog Files

*** Active Log File ***
2015-07-23 00:01:33.919 : 1/1 : <Info> %SYS_CONFIG-HOSTNAME_CHANGED :
sys_configd[2025] : The hostname of equipment has been changed to: 'DM4610'
2015-07-23 00:02:13.106 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
Card inserted in slot 1/1 (model: 8GPON+8GX+4GT+2XS, serial number: 3048274)
2015-07-23 00:02:15.907 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
Card inserted in slot 1/PSU1 (model: Not supported, serial number: 3047195)
2015-07-23 00:02:15.914 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
Card inserted in slot 1/FAN (model: DM4610 FAN, serial number: Not available)
2015-07-23 00:02:16.209 : 1/1 : <Notice> %TCV-TCV_INSERTED :
tcvd[2047] : Transceiver inserted at interface gigabit-ethernet-1/1/1.
2015-07-23 00:02:16.253 : 1/1 : <Notice> %TCV-TCV_INSERTED :
tcvd[2047] : Transceiver inserted at interface gigabit-ethernet-1/1/8.

** End of log ** (6 records)
```

This example shows how to display logs generated by specific components:

```
DM4610# show log component aaa card_manager
Show Contents of All Known UserLog Files

*** Active Log File ***
2015-07-23 00:02:13.106 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
Card inserted in slot 1/1 (model: 8GPON+8GX+4GT+2XS, serial number: 3048274)
2015-07-23 00:02:15.907 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
```

```
Card inserted in slot 1/PSU1 (model: Not supported, serial number: 3047195)
2015-07-23 00:02:15.914 : 1/1 : <Notice> %CARDMGR-CARD_INSERTED : card-mgr[2032] :
Card inserted in slot 1/FAN (model: DM4610 FAN, serial number: Not available)
2015-07-23 00:05:36.545 : 1/1 : <Info> %AAA-GROUP_ASSIGN : authenticationd[2060] :
User [admin]: Was assigned to groups: admin.

** End of log ** (5 records)
```

This example shows how to display logs from specific severities:

```
DM4610# show log severity informational warning
Show Contents of All Known UserLog Files

*** Active Log File ***
2015-07-23 00:02:12.238 : 1/1 : <Info> %CARDAPP-INITIAL_SYSTEM_SETUP_STARTED :
card-app[2153] : The system initial configuration has been started
2015-07-23 00:02:15.343 : 1/1 : <Info> %HWMONITOR-FAN_DETECTED : hal_devices
[2179] : New FAN device detected. FAN ID 1/FAN/1
2015-07-23 00:02:16.253 : 1/1 : <Info> %CARDAPP-INITIAL_SYSTEM_SETUP_FINISHED :
card-app[2153] : The system initialization is complete
2015-07-23 00:02:21.009 : 1/1 : <Warn> %TCV-UNSUPPORTED_TCV_INSERTED : tcvd[2210] :
Unsupported transceiver detected in interface gigabit-ethernet-1/1/1. Ethernet
Standard 1000BASE-T read from transceiver.
2015-07-23 00:02:23.217 : 1/1 : <Warn> %ETHL1-ETHL1_STATUS_DOWN : eth11portmgr
[2266] : Interface gigabit-ethernet-1/1/4 changed state to down (Admin state: up)

** End of log ** (5 records)
```

Impacts and precautions

The use of **show log** or another verbose command under serial interface may cause the session to become unresponsive to user intervention (until the command finishes its execution). Consider this before executing the respective command.

Hardware restrictions

N/A

show platform

Description

This command is used to show information about the system cards, like firmware version and status.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show platform [chassis {chassis_id} [detail | slot {slot_id} [detail]]]
```

Parameters

chassis *chassis_id*

Description: Chassis identifier. If the value of this parameter is '*' a list of all present chassis will be shown. Currently only one *chassis_id* is supported.

Value: 1

Default Value: None

detail

Description: Shows detailed system information about a chassis or a specific card.

Value: N/A

Default Value: N/A

slot *slot_id*

Description: Identifies a card present on chassis. If the value of this parameter is '*' a list of all present cards will be shown. This parameter will be dependent on the product being managed. The possible values for Dm4610 are displayed below.

Value: 1, PSU1, PSU2 or FAN

Default Value: None

Output Terms

Output	Description
<code>Chassis/Slot</code>	Chassis and slot identification
<code>Product model</code>	Hardware model of the chassis or slot
<code>Role</code>	Role of each card: Master, Standby, Active or Passive
<code>Status</code>	Status of each card: Ready, Initializing, Blocked, or Failed
<code>Firmware version</code>	Firmware version of the card, if available

Default

N/A. There is no default profile.

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
1.2	The command was changed and the detail option was introduced.

Usage Guidelines

The user can display status, role and firmware version information about all chassis and cards present at the system. Some of the information for it can be found at other commands, like show inventory and show firmware, so this is the place to summarize it and display it in a concise form.

An example of the command is displayed below.

```
DM4610# show platform
Chassis/Slot_ Product_model_ Role_ Status_ Firmware_version_
1_ DM4610_ -_ -_ Not available
1/1_ 8GPON+8GX+4GT+2XS_ Master_ Ready_ 1.4.0-116-1-ga3bd61b
1/FAN_ DM4610 FAN_ Passive_ Ready_ Not available
1/PSU2_ PSU 120 AC_ Passive_ Ready_ Not available
```

Impacts and precautions

If any value is identified as Not Available, it will be considered as having no meaning in that particular chassis/slot. Example of this is the field “Firmware version” in the command displayed at the Usage guidelines.

Hardware restrictions

N/A

show system reboot

Description

Shows the reason of the last system reboot.

Supported Platforms

This command is supported in all platforms.

Syntax

show system reboot

Parameters

N/A

Output Terms

Output	Description
Last reboot cause	Shows the last reboot reason.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
---------	--------------

5.0	This command was introduced.
-----	------------------------------

Usage Guidelines

This command should be used when the user wants to identify the reason of the last (most recent) system reboot.

Possible reboot causes:

- Reboot requested by user;
- Firmware activation requested by user;
- Over Temperature Protection (OTP) mode recovery;
- Power input failure;
- System failure (crash);
- Unknown reason.

This information remains available until the next reboot, and then it gets overwritten. This status is logged in user logs, and is available through SNMP.

Impacts and precautions

None

Hardware restrictions

None

DHCP

This topic describes the commands related to management of DHCP Server and Relay such as commands to configure DHCP Pools and timers or to inspect the devices connected to local server.

dhcp l2-relay

Description

Configure settings related to the DHCP Relay L2.

DHCP L2 Relay is responsible for the insertion of DHCP information option 82 field as specified in Section 3.9.1/TR-101 and 5.7/TR-156.

This function only works for packets switched among GPON service-ports and uplink ethernet ports. Packets switched among ethernet ports are forwarded transparently.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

dhcp l2-relay [**vlan** *vlan-id*] [**circuit-id format** *format*] [**filter-by** {**ip** | **mac**}]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

vlan *vlan-id*

Description: Enable DHCP Relay L2 on VLAN. Max number of VLANs is 234. The options to configure are: a single VLAN, list or range of VLANs and both combinations, range and list.

Value: 1-4094

Default Value: None

circuit-id format *format*

- Description:** Configure a format template for DHCP Relay L2 Option 82 Circuit-ID.
- The format template can be composed by literal text and the combination of available fields separated by, at least, one delimiter.
- Available fields are described below, and are case insensitive.
- Mandatory fields:** <gemPort>
<oltSlot> <panelPort> <onuld> **OR** <onuSerial>
- Optional fields:** <hostname> <onuSlot> <svlan>
- Delimiters:** space . / :
- Value:** Text up to 136 characters. Valid characters are A-Z, a-z, 0-9, space and . / @ :
The circuit-id generated by this template must not exceed 63 bytes.
- Default Value:** <hostname> eth <oltSlot>/<panelPort>/<onuld>/<onuSlot>/<gemPort>:<svlan>

filter-by {ip | mac}

- Description:** Configure a data traffic filter rule. The filter by IP option (default mode) allows the data traffic with anti-ip-spoofing functionality. On the filter by MAC mode, the traffic is allowed via MAC address.
- Value:** List of supported filters: **ip** and **mac**.
- Default Value:** ip.

Output Terms

Output	Description
<hostname>	Hostname for this equipment.
<oltSlot>	Equipment line card slot. Fixed value 1 for equipment that doesn't support line card.
<panelPort>	Equipment ponlink numeric id as seen physically in panel.

Output	Description
<onuId>	Numeric ONU ID (0-127) configured within a PON.
<onuSerial>	ONU Serial value (e.g. DACM12345678).
<svlan>	Uplink Service VLAN.
<gemPort>	ONU numeric config-level GEM ID (1-40).
<onuSlot>	Fixed value 0.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
1.6	This command was introduced.
5.6	Command was modified from 'dhcp relay' to 'dhcp l2-relay'.
6.4	Support to custom Circuit-ID format.
7.0	Support to traffic filter by MAC.

Usage Guidelines

Usage example of configuring a VLAN of ID 15:

```
# config
(config)# dhcp l2-relay vlan 15
(config)# commit
Commit complete.
```

Usage example of configuring a VLAN range from ID 1 to 10:

```
# config
(config)# dhcp l2-relay vlan 1-10
(config)# commit
Commit complete.
```

Usage example of configuring a list containing the VLAN IDs 1, 10 and 15:

```
# config
(config)# dhcp relay vlan 1,10,15
(config)# commit
Commit complete.
```

Usage example of configuring circuit-id format with a fixed string, onuSerial and gemPort:

```
# config
(config)# dhcp l2-relay circuit-id format <onuSerial> fixed string <gemPort>
(config)# commit
Commit complete.
```

Usage example of configuring a VLAN of ID 20 with filter by MAC:

```
# config
(config)# dhcp l2-relay vlan 20 filter-by mac
(config)# commit
Commit complete.
```

Impacts and precautions

For backward compability purposes, 'dhcp relay vlan' command is mapped to 'dhcp l2-relay vlan'.

Avoid setting dhcp l2-relay to a VLAN configured as 'service vlan type tls', since it will disable DHCP traffic inspection.

When DHCP relay is turned on for a given VLAN, it monitors for DHCP packets of all service-ports running over this VLAN.

After the DHCP session is properly established, a filter is installed at HW level to allow traffic on the respective service-port for the particular assigned IPv4 address.

If there is no renew within the assigned lease time, the filter is removed, blocking all user traffic for the particular service-port.

DHCP relay supports only DHCPv4. DHCPv6 packets are forwarded transparently without information option insertion.

Server DHCP packets (such as DHCPACK) received on service-ports are silent discarded.

Downstream DHCP packets that not match circuit-id syntax are discarded.

Circuit-id format <hostname> field is used to determine whether a downstream dhcp packet must be processed or forwarded to other ethernet interfaces. When this field is not configured, the packet will be processed if circuit-id information format matches.

DHCP L2 relay inserts information option 82 with suboption 1 and suboption 2, with the following content as defined in R-127/TR-156:

1) Suboption 1 - Default Agent Circuit ID:

<hostname> eth <oltSlot>/<oltPort>/<onuld>/0/<gemPort>:<svlan>

Example for VLAN 333, gem 2, onu 55, PON link 1/1/3:

DM4610 eth 1/3/55/0/2:333

2) Suboption 2 - Remote Circuit ID:

Contains the ONU name configured under the ONU configuration path.

Hardware restrictions

N/A

dhcp relay

Description

Configure settings related to the DHCP Relay Agent function.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

dhcp relay *instance-name*

dhcp relay *instance-name* **server ipv4** *a.b.c.d*

dhcp relay *instance-name* **interface** *interface-name*

dhcp relay *instance-name* **information** [**check** | **option** | **trust-all** | **policy** { *keep* | *drop* | *replace* }]

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

instance-name

Description: Specifies the name of the DHCP Relay instance.

Value: String with up to 64 characters.

Default Value: N/A

server ipv4 *a.b.c.d*

Description: Specifies a list of DHCP servers that will be used by the DHCP relay agent to forward DHCP client messages. Up to 16 DHCP server IPv4 addresses can be specified.

Value: IPv4 address in a.b.c.d format.

Default Value: N/A

interface *interface-name*

Description: Specifies a list of L3 interfaces to be part of the DHCP relay agent instance pool.

Adding a L3 interface to the DHCP agent instance means that all DHCP client packets arriving in the related VLAN will be relayed to the configured DHCP servers.

Value: It must be a valid L3 interface name with "l3-" prefix.

Default Value: N/A

information check

Description: If enabled, DHCP Relay will check for a valid option 82 coming from DHCP server packets and drop them in case they don't contain an option 82.

This configuration is valid only for drop and replace information policies and when information option is enabled. When information policy is set to keep mode, check configuration is ignored, that is, no verification is performed.

Value: N/A

Default Value: Enabled.

information option

Description: When enabled, instructs the DHCP Relay agent to add DHCP option 82 to DHCP client packets. DHCP relay agent will strip off option 82 from packets arriving from the DHCP server before sending them back to the user side.

Option 82 circuit-ID is filled with the physical interface short name from which the DHCP client packet arrived plus the VLAN information.

That is, circuit-ID will have the format <itf-name>:<vlan-id>, for example "1ge-1/1/1:4012", "10ge-1/1/1:4012", "40ge-1/1/1:4012", "100ge-1/1/1:4012".

Option 82 remote-ID is always equal to the in-band management MAC/hardware address of the switch.

Value: N/A

Default Value: Disabled.

information trust-all

Description: Instructs the DHCP relay agent to trust DHCP client packets containing information option 82 but without GIADDR set.

By default, if the gateway address (GIADDR) is set to all zeros in the DHCP packet and the relay agent information option is already present in the packet, the DHCP relay agent will discard the packet. In other words, when the configuration is disabled (default), DHCP relay discards messages carrying option 82.

Use the command to override this behavior and accept the packets.

This configuration is independent from the information policy (keep/drop/replace).

When trust-all is enabled, the relay agent will replace or set the GIADDR field to its own IP address when GIADDR is not present or when it is set to all zeros.

Value: N/A

Default Value: Disabled.

information policy

Description: Configures the information option 82 strategy for the DHCP relay agent instance.

Policy behavior:

- keep:

Packet has no option 82 field: append option 82

Packet includes an option 82 field: keep incoming option 82 untouched

- replace:

Packet has no option 82 field: append option 82

Packet includes an option 82 field: replace incoming option 82, rewriting circuit/remote IDs

- drop:

Packet has no option 82 field: append option 82

Packet includes an option 82 field: drop packet

Value: drop | keep | replace

Default Value: replace

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.2	DHCP Relay command added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a DHCP Relay for VLAN 200 relaying client requests to VLAN 300 with DHCP option 82 turned on.

```
(config)# dot1q vlan 200
(config-vlan-200)# interface gigabit-ethernet-1/1/1-24
(config-dot1q-interface-gigabit-ethernet-1/1/1-24)# top
(config)# dot1q vlan 300
(config-vlan-300)# interface ten-gigabit-ethernet-1/1/1-2
(config-dot1q-interface-ten-gigabit-ethernet-1/1/1-2)# top
(config)# interface l3 itf-vlan200
(config-l3-itf-vlan200)# ipv4 address 192.168.1.25/24
(config-l3-itf-vlan200)# lower-layer-if vlan 200
(config-l3-itf-vlan200)# top
(config)# interface l3 itf-vlan300
(config-l3-itf-vlan300)# ipv4 address 10.1.1.25/24
(config-l3-itf-vlan300)# lower-layer-if vlan 300
(config-l3-itf-vlan300)# top
(config)# dhcp relay test
(dhcp-relay-test)# server ipv4 10.1.1.100
(config-ipv4-10.1.1.100)# exit
(dhcp-relay-test)# information option
(dhcp-relay-test)# interface l3-itf-vlan200
(config-interface-l3-itf-vlan200)# exit
```

Following the settings above, this configuration shows how to configure a switch to relay DHCP client messages with VLAN 200 coming from an OLT with DHCP option 82 relay agent turned on.

```
(config)# dhcp relay test
(dhcp-relay-test)# information policy keep
(dhcp-relay-test)# information trust-all
```

Impacts and precautions

The maximum number of DHCP relay instances will be limited to the maximum L3 interfaces allowed.

In scenarios with a very high load of DHCP messages, the system can experience an increase of CPU usage for a period of time until DHCP sessions are established.

It is not possible to set a specific source IP or source interface to be used to send relayed packets to the DHCP server. DmOS will set the source IP address of the interface from which the target network is reachable.

Information option is filled with the physical interface name, regardless this interface is a part of a link aggregation or not.

For platforms that have service vlan configuration (such as OLTs), DHCP relay cannot be turned on for a TLS service vlan.

Hardware restrictions

N/A

dhcp relay if-option

Description

Configure interface specific settings related to the DHCP Relay Agent function.

Supported Platforms

This command is not supported in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

dhcp relay *instance-name* **if-option** *interface-name*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

if-option *interface-name*

- | | |
|-----------------------|---|
| Description: | Enter in per-interface information configuration. Configuration made for any specific interface will override the DHCP relay instance information settings for the given interface. Other interfaces without if-option specific settings will follow the DHCP relay instance information configuration. |
| Value: | It must be a valid ethernet interface name, such as gigabit-ethernet-X/Y/Z or ten-gigabit-ethernet-X/Y/Z. |
| Default Value: | N/A |

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.2	DHCP Relay if-option command added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure a DHCP Relay for VLAN 200 relaying client requests to VLAN 300 with DHCP option 82 turned on. For gigabit-ethernet-1/1/1, interface is configured as trusted and with keep information policy. This configuration can be used to relay DHCP client messages coming from an OLT with DHCP option 82 relay agent turned on which is connected to gigabit-ethernet-1/1/1.

```
(config)# dot1q vlan 200
(config-vlan-200)# interface gigabit-ethernet-1/1/1-24
(config-dot1q-interface-gigabit-ethernet-1/1/1-24)# top
(config)# dot1q vlan 300
(config-vlan-300)# interface ten-gigabit-ethernet-1/1/1-2
(config-dot1q-interface-ten-gigabit-ethernet-1/1/1-2)# top
(config)# interface l3 itf-vlan200
(config-l3-itf-vlan200)# ipv4 address 192.168.1.25/24
(config-l3-itf-vlan200)# lower-layer-if vlan 200
(config-l3-itf-vlan200)# top
(config)# interface l3 itf-vlan300
(config-l3-itf-vlan300)# ipv4 address 10.1.1.25/24
(config-l3-itf-vlan300)# lower-layer-if vlan 300
(config-l3-itf-vlan300)# top
(config)# dhcp relay test
(dhcp-relay-test)# server ipv4 10.1.1.100
(config-ipv4-10.1.1.100)# exit
(dhcp-relay-test)# information option
(dhcp-relay-test)# interface l3-itf-vlan200
(config-interface-l3-itf-vlan200)# exit
(config-relay-test)# if-option gigabit-ethernet-1/1/1
(config-if-option-gigabit-ethernet-1/1/1)# information option
(config-if-option-gigabit-ethernet-1/1/1)# information policy keep
(config-if-option-gigabit-ethernet-1/1/1)# information trust-all
(config-if-option-gigabit-ethernet-1/1/1)# exit
```

Impacts and precautions

N/A

Hardware restrictions

N/A

PPP

This topic describes the commands related to management of PPP services such as commands to configure PPPoE or PPP CHAP.

intermediate-agent *Chassi/Slot/Port*

Description

Configuration of PPPoE Intermediate Agent.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

intermediate-agent *Chassi/Slot/Port*

intermediate-agent *Chassi/Slot/Port* **sub-option circuit-id**

intermediate-agent *Chassi/Slot/Port* **sub-option remote-id**

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

Chassi/Slot/Port

Description: Indicates the *Chassi/Slot/Port* configured.

Value: 1/1/1

Default Value: None

Output Terms

Output	Description
--------	-------------

None	None.
------	-------

Default

N/A. There is no default profile.

Command Mode

Configuration mode

Required Privileges

Access level config

History

Release	Modification
---------	--------------

1.4	This command was introduced.
-----	------------------------------

Usage Guidelines

None

Impacts and precautions

None

Hardware restrictions

None

pppoe

Description

This module contains definitions for the PPPoE(Point-to-Point Protocol over Ethernet)

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

pppoe

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

None

Description:	None
Value:	None
Default Value:	None

Output Terms

Output	Description
None	None.

Default

N/A. There is no default profile.

Command Mode

Configuration mode

Required Privileges

Access level config

History

Release	Modification
---------	--------------

1.4	This command was introduced.
-----	------------------------------

Usage Guidelines

None

Impacts and precautions

None

Hardware restrictions

None

show pppoe intermediate-agent sessions interface gpon *Chassi/Slot/Port*

Description

Show information about active PPPoE sessions.

Supported Platforms

This command is supported only in the following platforms: DM4610, DM4611, DM4612, DM4615.

Syntax

show pppoe intermediate-agent sessions interface gpon *Chassi/Slot/Port*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

Chassi/Slot/Port

Description: Indicates the *Chassi/Slot/Port* configured.

Value: 1/1/1

Default Value: None

Output Terms

Output	Description
---------------	--------------------

<code>interface, ONU ID, session id, remote mac</code>	Interfaces.
--	-------------

Default

N/A. There is no default profile.

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Access level audit

History

Release	Modification
---------	--------------

1.4	This command was introduced.
-----	------------------------------

Usage Guidelines

None

Impacts and precautions

None

Hardware restrictions

None

CHAPTER 16: HARDWARE

This chapter describes the CLI commands related to Hardware management of the DmOS.

ENVIRONMENT

This topic describes the commands related to management of environment conditions such as commands to inspect device's temperature or to configure thermal alarms.

show environment

Description

Displays real-time information about the device environment.

Supported Platforms

This command is supported in all platforms.

Syntax

show environment [**chassis** *chassis_id* [**slot** *slot_id*]] [**power**]

Parameters

chassis_id

Description: Chassis key identifier. If the value of this parameter is '*' or ' ', a list of all present chassis will be showed.

Value: 1

Default Value: None

slot_id

Description: Identifies a card present on a chassis (e.g: FAN, 1, etc.). If the value of this parameter is '*' or ' ', a list of all present cards will be showed.

Value: 1 or FAN

Default Value: None

Output Terms

Output	Description
Chassis/Slot/Id	Indicates the physical location of the sensor inside the equipment.
Sensor	Brief description of which device the sensor is measuring.
Temp.	Current temperature measured by the sensor.
Alarm Thresholds	Temperature limits of a specific sensor indicating its normal range of operation.
Hyster.	Hysteresis applied to the temperature limits (it indicates the temperature that the Status change from LOW or HIGH to NORMAL).
Temperature Status	Indicates the current status of the measured temperature (NORMAL for adequate operation, LOW or HIGH for out of normal range of operation and ERROR when reading the sensor fail).
Chassis/Slot/Fan-ID	Indicates the physical location of the fan inside the equipment.
Speed	Current speed measured by the fan's tachometer.
Fan Status	Indicates the current status of the measured fan (NORMAL for adequate operation, LOW when its speed is lower than expected for adequate operation, ERROR when is not possible to read the tachometer's value and FAIL when the fan status reports a failure).
PSU Status	Indicates the current status of the PSUs (OK for adequate operation, POWER INPUT FAILURE when there is no external power, FUSE FAILURE when the Fuse is blown, and ERROR when is not possible to read the PSU status)

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.2	This command was introduced.
1.8	Fan information was introduced.
2.4	Removed fan alarm for HIGH speed.
4.8	Removed fan control information.

Usage Guidelines

This command is available when there are sensors or fans at hardware. Use slot parameter to filter the output or let unspecified slots to see all cards info.

Example:

```
DM4610# show environment
```

```
Temperature Sensors:
-----
Chassis/      | Sensor              | Temp | Alarm  | Hyster | Status
Slot/Id       |                     |      | Thresholds |        |
-----
1/1/SENSOR1   | Card                | 49.5 | 0.0 ~ 55.0 | 5.0    | NORMAL
1/1/SENSOR2   | Switch Fabric       | 54.0 | 0.0 ~ 75.0 | 5.0    | NORMAL
1/1/SENSOR3   | GPON PHY/SFP        | 59.0 | 0.0 ~ 75.0 | 5.0    | NORMAL
1/1/SENSOR4   | CPU                 | 55.0 | 0.0 ~ 75.0 | 5.0    | NORMAL
1/1/SENSOR5   | CPU Core            | 65.3 | 0.0 ~ 110.0 | 5.0    | NORMAL
1/1/SENSOR2   | Switch Fabric Core  | 54.0 | 0.0 ~ 75.0 | 5.0    | NORMAL
1/PSU1/SENSOR1 | PSU1                | 50.5 | 0.0 ~ 85.0 | 5.0    | NORMAL
1/PSU2/SENSOR1 | PSU2                | 47.5 | 0.0 ~ 85.0 | 5.0    | NORMAL
-----

Fan Information:
-----
```

Chassis/Slot/Fan-ID	Speed (RPM)	Status
1/FAN/1	2500.0	NORMAL
1/FAN/2	2419.0	NORMAL
1/FAN/3	2343.0	NORMAL

Power Information:

Chassis/PSU-ID	Status
1/PSU1	POWER INPUT FAILURE
1/PSU2	OK

Impacts and precautions

Keep the fans module clear for the proper air flow.

Keep the air filter of the fans module clean.

Hardware restrictions

The sensors list depends on the equipment model.

show interface transceivers

Description

Shows the status, digital diagnostics and basic information of all present transceivers.

Supported Platforms

This command is supported in all platforms.

Syntax

```
show interface [ transceivers [ interface_type [ interface_id | status | digital-diagnostics  
[ current-thresholds | rx-power-thresholds | temperature-thresholds | tx-power-  
thresholds | voltage-thresholds ]]]]
```

Parameters

interface_type

Description: Interface type identifier such as 'gpon', 'gigabit-ethernet', 'ten-gigabit-ethernet', etc. If the value of this parameter is unspecified or is the character '*', a list of all present transceivers will be showed.

Value: gpon, gigabit-ethernet, ten-gigabit-ethernet or twenty-five-gigabit-ethernet or forty-gigabit-ethernet or hundred-gigabit-ethernet.

Default Value: N/A

interface_id

Description: Interface key identifier, chassis/slot/port. The interface_id equal to 1/2/3 is an example of chassis 1, slot 2 and port 3. If the value of this parameter is '*' or ' ', a list of all present transceivers will be showed.

Value: chassis/slot/port

Default Value: N/A

digital-diagnostics

Description: Show only the digital-diagnostics of all present transceivers

Value: N/A

Default Value: N/A

status

Description: Show only the status of all present transceivers

Value: N/A

Default Value: N/A

Output Terms

Output	Description
Transceiver ID	Identification of the transceiver
Temperature	Temperature of the transceiver
Voltage 3.3V	Voltage being supplied to transceiver
Current	Current being drawn by the transceiver
Tx-Power	Power of the transmitted signal
Rx-Power	Power of the received signal
Rx-LOS	Loss of signal on reception
Alarm Thresholds	Range in which data values can vary before alarm
Warning Thresholds	Range in which data values can vary before warning

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
1.0	This command was introduced.
4.5.2	Support to digital-diagnostics of forty-gigabit-ethernet transceivers.
4.6	Support to digital-diagnostics of hundred-ethernet transceivers.
5.0	Support to digital-diagnostics of twenty-five-ethernet transceivers.
5.10	Added information about transceiver supported fiber type.
6.2	Removed transceiver tx-fault status information.

Usage Guidelines

Examples:

Show the status of all gigabit-ethernet transceivers

```
DM4610# show interface transceivers gigabit-ethernet status
```

Transceiver ID	Rx-LOS
gigabit-ethernet 1/1/2	No
gigabit-ethernet 1/1/3	Yes
gigabit-ethernet 1/1/4	Yes
gigabit-ethernet 1/1/5	Yes
gigabit-ethernet 1/1/6	Yes
gigabit-ethernet 1/1/7	No

Show the digital diagnostics of all gpon transceivers

DM4610# show interface transceivers gpon digital-diagnostics

Transceiver ID	Temperature	Voltage 3.3V	Current	Tx-Power	Rx-Power
gpon 1/1/2	41.64 C	3.27 V	0.0 mA	-39.99 dBm	8.15 dBm
gpon 1/1/8	36.24 C	3.29 V	0.0 mA	8.16 dBm	3.92 dBm

Show the status and the digital diagnostics of all forty-gigabit-ethernet transceivers

DM4170# show interface transceivers forty-gigabit-ethernet

Transceiver ID	Rx-LOS
forty-gigabit-ethernet 1/1/1:1	No
forty-gigabit-ethernet 1/1/1:2	No
forty-gigabit-ethernet 1/1/1:3	No
forty-gigabit-ethernet 1/1/1:4	No
forty-gigabit-ethernet 1/1/2:1	No
forty-gigabit-ethernet 1/1/2:2	No
forty-gigabit-ethernet 1/1/2:3	No
forty-gigabit-ethernet 1/1/2:4	No

Transceiver ID	Temperature	Voltage 3.3V	Current	Tx-Power	Rx-Power
forty-gigabit-ethernet 1/1/1	36.05 C	3.26 V	N/A	N/A	N/A
forty-gigabit-ethernet 1/1/1:1	N/A	N/A	24.02 mA	-2.18 dBm	-1.27 dBm
forty-gigabit-ethernet 1/1/1:2	N/A	N/A	25.03 mA	-1.61 dBm	-0.92 dBm
forty-gigabit-ethernet 1/1/1:3	N/A	N/A	25.03 mA	-2.22 dBm	-0.91 dBm
forty-gigabit-ethernet 1/1/1:4	N/A	N/A	26.04 mA	-1.33 dBm	-0.6 dBm
forty-gigabit-ethernet 1/1/2	32.4 C	3.26 V	N/A	N/A	N/A
forty-gigabit-ethernet 1/1/2:1	N/A	N/A	23.94 mA	-1.57 dBm	-1.46 dBm
forty-gigabit-ethernet 1/1/2:2	N/A	N/A	24.02 mA	-1.52 dBm	-1.29 dBm
forty-gigabit-ethernet 1/1/2:3	N/A	N/A	25.7 mA	-1.87 dBm	-1.29 dBm
forty-gigabit-ethernet 1/1/2:4	N/A	N/A	26.71 mA	-1.69 dBm	-0.82 dBm

Show the voltage digital diagnostics of all gigabit ethernet transceivers

DM4610# show interface transceivers gigabit-ethernet digital-diagnostics voltage-thresholds

Transceiver ID	Voltage 3.3V	Alarm Thresholds	Warning Thresholds
gigabit-ethernet 1/1/2	3.29 V	2.8 V ~ 3.8 V	2.97 V ~ 3.6 V
gigabit-ethernet 1/1/3	3.29 V	2.8 V ~ 3.8 V	2.97 V ~ 3.6 V
gigabit-ethernet 1/1/4	3.3 V	2.8 V ~ 3.8 V	2.97 V ~ 3.6 V
gigabit-ethernet 1/1/6	3.24 V	3.0 V ~ 3.6 V	3.0 V ~ 3.6 V
gigabit-ethernet 1/1/7	3.29 V	2.8 V ~ 3.8 V	2.97 V ~ 3.6 V

Show a specific transceiver

DM4610# show interface transceivers gigabit-ethernet 1/1/2

Information of transceiver gigabit-ethernet 1/1/2

Vendor Information

Vendor Name: APAC Opto
 Serial Number: 9813050024
 Part Number: LS38-E3C-TC-N-DD
 Type: SFP
 Media: OPTICAL
 Connector: LC
 Laser Wavelength: 1310 nm
 Fiber Type: Single-Mode

Status

Rx-LOS: No

Information of transceiver gigabit-ethernet 1/1/2

Digital Diagnostics

Temperature [C]: 41.71 [-15.0 ~ 85.0]

```
Voltage 3.3V [V]: 3.29 [ 2.8 ~ 3.8]
Current [mA]: 9.72 [ 0.09 ~ 79.96]
Tx-Power [dBm]: -6.23 [ -11.0 ~ -0.99]
Rx-Power [dBm]: -6.86 [ -22.0 ~ -1.99]
```

Impacts and precautions

N/A

Hardware restrictions

According to transceiver inserted, these shows could be available or not.

RESOURCES

This topic describes the commands related to management of hardware resources.

forwarding-resources

Description

Forwarding resources configuration changes the switch forwarding table allocation profile, allowing to choose between L2 or L3 priority operation modes.

Supported Platforms

This command is supported only in the following platforms: DM4270, DM4380, DM4770.

Syntax

forwarding-resources {**profile** *profile-name*}

Parameters

profile *profile-name*

Description:	The default profile balances L2 and L3 capacities for general use. The extended-ip profile reduces L2 capacity to increase maximum L3 routes entries. The extended-mac profile reduces L3 capacity to increase maximum L2 addresses entries.
Value:	{default extended-ip extended-mac}
Default Value:	default

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Admin

History

Release	Modification
5.4.0	This command was introduced.

Usage Guidelines

Example:

This example shows how to update the forwarding table allocation profile to extended-ip.

```
# forwarding-resources profile extended-ip
This change will take effect on next reboot.
# reboot
Are you sure? [no,yes] yes
```

Impacts and precautions

Changing the forwarding table allocation profile requires a reboot for the new profile to take effect.

Hardware restrictions

The presence of this command is conditioned by hardware support. Not all profiles may be available for all models. The maximum capacity of each entry type for each profile is also hardware dependent.

show forwarding-resources

Description

Displays information about forwarding table profiles status.

Supported Platforms

This command is supported only in the following platforms: DM4270, DM4380, DM4770.

Syntax

show forwarding-resources

Parameters

N/A

Output Terms

Output	Description
Profile Name	Displays the profile name.
MAC	Displays the maximum L2 addresses of the profile.
IPv4	Displays the maximum IPv4 routes of the profile.
IPv6/64	Displays the maximum IPv6/64 routes of the profile.
IPv6/128	Displays the maximum IPv6/128 routes of the profile.
Running	Indicates if the profile is active and running.
Startup	Indicates if the profile is marked to be active on next reboot.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.4.0	This command was introduced.

Usage Guidelines

This example shows the command output when the default profile is active and the extended-mac is marked for the next reboot.

```
# show forwarding-resources
Profile Name  MAC      IPv4      IPv6/64   IPv6/128  Running  Startup
-----
default      128000   128000   32000     4000      true     false
extended-ip   32000   168000   42000     10000     false    false
extended-mac  288000   16000    4000      1000      false    true
```

Impacts and precautions

N/A

Hardware restrictions

The presence of this command is conditioned by hardware support. Not all profiles may be available for all models. The maximum capacity of each entry type for each profile is also hardware dependent.

CHAPTER 17: CPU PROTECTION

CPU DOS PROTECTION

This topic describes the commands related to CPU Denial of Service (DoS) Protection.

clear cpu-dos-protect counters

Description

Clear all CPU queue counters.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

clear cpu-dos-protect counters

Parameters

N/A

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
---------	--------------

6.0	This command was introduced.
-----	------------------------------

7.0	The queue ACL-BASED for ACL redirect action was added.
-----	--

Usage Guidelines

Given the equipment has statistic counters on the queues ARP, TTL-1, IN_BAND-MGMT, OSPF and BFD:

```
# show cpu-dos-protect
```

QUEUE	PROTOCOL	MAX PPS	RX OCTETS	DISCARDED OCTETS	RX PKTS	DISCARDED PKTS
2	ARP	100	3168	0	47	0
6	LLDP	900	0	0	0	0
7	LBD	900	0	0	0	0
8	TTL-1 (L3)	50	1904	0	28	0
9	IN_BAND-MGMT	900	25334	0	319	0
16	DHCP	900	0	0	0	0
17	PPPoE	900	0	0	0	0
18	IGMP	100	0	0	0	0
19	TUNNELING	900	0	0	0	0
21	CFM	900	0	0	0	0
24	OSPF	400	18118	0	177	0
25	MPLS-LDP	400	0	0	0	0
27	BGP	250	0	0	0	0
28	VRRP-IPv4	900	0	0	0	0
29	VRRP-IPv6	900	0	0	0	0
30	BFD	900	38258	0	517	0
32	STP	900	0	0	0	0
33	ERPS	900	0	0	0	0
34	EAPS	900	0	0	0	0
35	SLOW-PROTOCOLS	900	0	0	0	0
36	ACL-BASED	900	0	0	0	0

Let's clear all CPU queue counters:

```
# clear cpu-dos-protect counters
```

```
# show counters
```

QUEUE	PROTOCOL	MAX PPS	RX OCTETS	DISCARDED OCTETS	RX PKTS	DISCARDED PKTS
2	ARP	100	0	0	0	0
6	LLDP	900	0	0	0	0
7	LBD	900	0	0	0	0
8	TTL-1 (L3)	50	0	0	0	0
9	IN_BAND-MGMT	900	0	0	0	0
16	DHCP	900	0	0	0	0
17	PPPoE	900	0	0	0	0
18	IGMP	100	0	0	0	0
19	TUNNELING	900	0	0	0	0
21	CFM	900	0	0	0	0
24	OSPF	400	0	0	0	0
25	MPLS-LDP	400	0	0	0	0
27	BGP	250	0	0	0	0
28	VRRP-IPv4	900	0	0	0	0
29	VRRP-IPv6	900	0	0	0	0
30	BFD	900	0	0	0	0
32	STP	900	0	0	0	0

33	ERPS	900	0	0	0	0
34	EAPS	900	0	0	0	0
35	SLOW-PROTOCOLS	900	0	0	0	0
36	ACL-BASED	900	0	0	0	0

Impacts and precautions

None

Hardware restrictions

None

cpu-dos-protect global

Description

Update the maximum number of packets per second that the CPU should accept. Exceeding traffic will be discarded.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

cpu-dos-protect global *max-pps*

Parameters

max-pps

Description: Maximum packets per second.

Value: 900 - 5000

Default Value: The default value depends on the hardware platform. See the hardware restrictions below.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.10	This command was introduced.
5.12	This command was enabled for DM4360, DM4370, DM4610, and DM4615.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the global rate limit.

```
# cpu-dos-protect global max-pps 1500
(cpu-dos-protect)# commit
Commit complete.
(cpu-dos-protect)#
```

Impacts and precautions

Please select the maximum number of packets per second wisely, according to the active features and protocols. Using a value that is too low might cause the application to malfunction due to missing packets. In turn, picking an excessively high value might cause CPU overload during attacks or network loops, for instance.

Hardware restrictions

The default value for DM4770 is 3000 packets per second. For other platforms, the default value is 900 packets per second.

cpu-dos-protect protocols

Description

Update the maximum number of packets per second per protocol that the CPU should accept. Exceeding traffic will be discarded.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

cpu-dos-protect protocols *protocol_name* **max-pps** *max-pps-value*

Use the **no** form to revert this command. For further information about the **no** form, read the chapter [Using the "No" Form of a Command](#).

Parameters

protocol_name

Description: Protocol name.

Value: List of supported protocols: arp, bfd, bgp, cfm, dhcp, eaps, erps, igmp, in-band-mgmt, lbd, lldp, mpls-ldp, ospf, pppoe, slow-protocols, stp, ttl-1, tunneling, vrrp-ipv4, vrrp-ipv6, acl-based.

Default Value: N/A

max-pps *max-pps-value*

Description: Maximum packets per second.

Value: 1 - 5000

Default Value: The default value depends on the hardware platform.

Default

N/A

Command Mode

Configuration mode

Required Privileges

Config

History

Release	Modification
5.12	This command was introduced.
7.0	The queue ACL-BASED for ACL redirect action was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

This example shows how to configure the protocol maximum rate limit for ARP protocol.

```
# cpu-dos-protect protocols <protocol_name> max-pps 1500
# cpu-dos-protect protocols arp max-pps 1500
(cpu-dos-protect)# commit
Commit complete.
(cpu-dos-protect)#
```

Impacts and precautions

Please select the maximum number of packets per second wisely, according to the active features and protocols. Using a value that is too low might cause the application to malfunction due to missing packets. In turn, picking an excessively high value might cause CPU overload during attacks or network loops, for instance.

Hardware restrictions

None

show cpu-dos-protect

Description

Display configured cpu rate limit and statistics.

Supported Platforms

This command is not supported in the following platforms: DM4050, DM4250.

Syntax

```
show cpu-dos-protect
```

Parameters

N/A

Output Terms

Output	Description
Queue	Hardware CPU queue attached to the protocol.
Protocol	Protocol name.
Max-pps	Configured maximum number of packets per second accepted by the CPU for a given protocol.
RX Octets	Number of octets received by the CPU for a given protocol.
Discarded Octets	Number of octets discarded by the CPU due to traffic exceeding max-pps configured value.
RX Pkts	Number of packets received by the CPU for a given protocol.

Output	Description
Discarded Pkts	Number of packets discarded by the CPU due to traffic exceeding max-pps configured value.

Default

N/A

Command Mode

Operational mode. It is possible to execute this command also in the Configuration mode by using the **do** keyword before the command.

Required Privileges

Audit

History

Release	Modification
5.12	This command was introduced.
7.0	The queue ACL-BASED for ACL redirect action was added.

Usage Guidelines

This command can be executed directly via CLI.

Example:

```
# show cpu-dos-protect
```

QUEUE	PROTOCOL	MAX PPS	RX OCTETS	DISCARDED OCTETS	RX PKTS	DISCARDED PKTS
2	ARP	100	3168	0	47	0
6	LLDP	900	0	0	0	0
7	LBD	900	0	0	0	0

8	TTL-1 (L3)	50	1904	0	28	0
9	IN_BAND-MGMT	900	25334	0	319	0
16	DHCP	900	0	0	0	0
17	PPPoE	900	0	0	0	0
18	IGMP	100	0	0	0	0
19	TUNNELING	900	0	0	0	0
21	CFM	900	0	0	0	0
24	OSPF	400	18118	0	177	0
25	MPLS-LDP	400	0	0	0	0
27	BGP	250	0	0	0	0
28	VRRP-IPv4	900	0	0	0	0
29	VRRP-IPv6	900	0	0	0	0
30	BFD	900	38258	0	517	0
32	STP	900	0	0	0	0
33	ERPS	900	0	0	0	0
34	EAPS	900	0	0	0	0
35	SLOW-PROTOCOLS	900	0	0	0	0
36	ACL-BASED	900	0	0	0	0

Impacts and precautions

None

Hardware restrictions

None

Command Index

A

aaa authentication-next-method-on-fail	1288
aaa authentication-order	1290
aaa authentication-type	1293
aaa server radius	1295
aaa server tacacs	1299
aaa user	1305
access-list acl-profile	1263
access-list interface	1266
access-list protection	1269
access-list-entry	1272
aes-key-exchange	1482
anti-ip-spoofing	1312
assistant-task	1623

B

backup-link	432
banner login	41

C

card-model	1658
cfm delay-measurement probe	1323
cfm ma	1328
cfm ma ais	1332
cfm md	1336
cfm mep	1338
cfm mep continuity-check	1342
clear	45
clear bgp neighbor	488
clear bgp soft	491
clear core-dump	129
clear counters	131
clear cpu-dos-protect counters	1717
clear interface statistics gpon	1484
clear ip host-table	436
clear lacp	360

clear log	1661
clear mac-address-table	316
clear mpls l2vpn counters vpls	917
clear mpls l2vpn counters vpws	919
clear mpls l2vpn mac-address vpls	921
clear multicast igmp snooping statistics	1166
clear oam cfm statistics	1346
clear ospf	678
clear ospfv3	783
clear statistics	135
clock	1466
commit	47 50
commit abort	53
commit check	55
commit confirmed	57
compare file	61
config	64
copy core-dump	137
copy file	141
copy mibs	146
copy pcap	149
counters	152
cpu-dos-protect global	1720
cpu-dos-protect protocols	1722

D

debug	22
delay-measurement	1348
dhcp l2-relay	1685
dhcp relay	1690
dhcp relay if-option	1695
display-defaults	25
dot1q vlan	334
dot1q vlan interface	336
dwdm interface	243

E

eaps	397
------------	-----

efm	1375
erps ring	386

F

file	67
forwarding-resources	1713

H

hold-time	430
hostname	70

I

id	1308
interface forty-gigabit-ethernet	246
interface gigabit-ethernet	250
interface gpon	1487
interface gpon onu	1574
interface hundred-gigabit-ethernet	254
interface l3	290
interface l3 vrf	297
interface loopback	310
interface loopback vrf	314
interface mgmt	36
interface ten-gigabit-ethernet	258
interface tunnel-te	1084
interface tunnel-te administrative-status	1086
interface tunnel-te description	1088
interface tunnel-te destination	1090
interface tunnel-te name	1092
interface tunnel-te path-option	1094 1096
interface tunnel-te path-option dynamic attribute-set	1099
interface tunnel-te path-option explicit name	1102
interface twenty-five-g-ethernet	262
interface utilization	156
intermediate-agent ChassiSlotPort	1698
ip arp aging-time	439

L

layer2-control-protocol interface protocols action action-type	406
layer2-control-protocol tunnel-mac	410
layer2-control-protocol tunnel-priority	412
layer2-control-protocol vlan protocols action action-type	414
license	238
link-aggregation	362
link-flap	423
linktrace	1352
lldp	1380
load default-gpon-profiles	1491
load factory-config	73
load merge	75
load override	78
log	1663
logout	1632
loopback	1355
loopback-detection	417

M

mac-address-table aging-time	319
mac-address-table interface learning	321
mac-address-table interface limit	324
mac-address-table vlan limit	327
monitor session	160
mpls l2vpn logging pw-status	923
mpls l2vpn vpls-group	925
mpls l2vpn vpls-group vpn	927
mpls l2vpn vpls-group vpn administrative-status	929
mpls l2vpn vpls-group vpn bridge-domain	932
mpls l2vpn vpls-group vpn bridge-domain access-interface	934
mpls l2vpn vpls-group vpn bridge-domain access-interface administrative-status	937
mpls l2vpn vpls-group vpn bridge-domain access-interface encapsulation dot1q	940
mpls l2vpn vpls-group vpn bridge-domain access-interface encapsulation untagged	943
mpls l2vpn vpls-group vpn bridge-domain administrative-status	946
mpls l2vpn vpls-group vpn bridge-domain bridge-mtu	949
mpls l2vpn vpls-group vpn bridge-domain dot1q	952
mpls l2vpn vpls-group vpn bridge-domain mac-limit	955

mpls l2vpn vpls-group vpn bridge-domain qinq	958
mpls l2vpn vpls-group vpn bridge-domain transparent-lan-service	961
mpls l2vpn vpls-group vpn description	964
mpls l2vpn vpls-group vpn vfi	967
mpls l2vpn vpls-group vpn vfi administrative-status	969
mpls l2vpn vpls-group vpn vfi neighbor	972
mpls l2vpn vpls-group vpn vfi neighbor administrative-status	975
mpls l2vpn vpls-group vpn vfi neighbor pw-id	978
mpls l2vpn vpls-group vpn vfi neighbor pw-load-balance	981
mpls l2vpn vpls-group vpn vfi neighbor pw-load-balance flow-label	984
mpls l2vpn vpls-group vpn vfi neighbor pw-mtu	987
mpls l2vpn vpls-group vpn vfi neighbor split-horizon	990
mpls l2vpn vpls-group vpn vfi neighbor tunnel-interface	993
mpls l2vpn vpls-group vpn vfi pw-type	996
mpls l2vpn vpws-group	999
mpls l2vpn vpws-group vpn	1001
mpls l2vpn vpws-group vpn access-interface	1003
mpls l2vpn vpws-group vpn access-interface administrative-status	1006
mpls l2vpn vpws-group vpn access-interface dot1q	1009
mpls l2vpn vpws-group vpn access-interface encapsulation dot1q	1012
mpls l2vpn vpws-group vpn access-interface encapsulation untagged	1015
mpls l2vpn vpws-group vpn access-interface mtu	1018
mpls l2vpn vpws-group vpn administrative-status	1021
mpls l2vpn vpws-group vpn backup-neighbor	1024
mpls l2vpn vpws-group vpn description	1027
mpls l2vpn vpws-group vpn neighbor	1029
mpls l2vpn vpws-group vpn neighbor administrative-status	1032
mpls l2vpn vpws-group vpn neighbor pw-id	1035
mpls l2vpn vpws-group vpn neighbor pw-load-balance	1038
mpls l2vpn vpws-group vpn neighbor pw-load-balance flow-label	1041
mpls l2vpn vpws-group vpn neighbor pw-mtu	1044
mpls l2vpn vpws-group vpn neighbor pw-type	1047
mpls l2vpn vpws-group vpn neighbor tunnel-interface	1050
mpls l2vpn vpws-group vpn qinq	1053
mpls ldp lsr-id	1135
mpls ldp lsr-id interface	1137
mpls ldp lsr-id interface hello-holdtime	1139
mpls ldp lsr-id interface keep-alive-holdtime	1142
mpls ldp lsr-id neighbor targeted	1145

mpls ldp lsr-id neighbor targeted hello-holdtime	1147
mpls ldp lsr-id neighbor targeted keep-alive-holdtime	1150
mpls ldp lsr-id neighbor targeted password	1153
mpls rsvp	1105
mpls rsvp interface	1107
mpls traffic-eng	1109
mpls traffic-eng attribute-set	1111
mpls traffic-eng attribute-set path-option	1113
mpls traffic-eng attribute-set path-option affinity-flags exclude-any	1116
mpls traffic-eng attribute-set path-option affinity-flags include-all	1119
mpls traffic-eng attribute-set path-option affinity-flags include-any	1122
mpls traffic-eng explicit-path	1125
mpls traffic-eng explicit-path hop	1127
mpls traffic-eng interface	1130
mpls traffic-eng interface affinity-flags	1132
multicast igmp snooping	1169
multicast igmp snooping administrative-status	1171
multicast igmp snooping bridge-domain	1174
multicast igmp snooping interface	1176
multicast igmp snooping interface administrative-status	1179
multicast igmp snooping interface group-limit	1182
multicast igmp snooping interface ignore	1185
multicast igmp snooping interface immediate-leave	1188
multicast igmp snooping interface last-member-query	1191
multicast igmp snooping interface maximum response time	1194
multicast igmp snooping interface mrouter	1197
multicast igmp snooping interface query interval	1200
multicast igmp snooping interface robustness-variable	1203
multicast igmp snooping interface version	1206

O

onu-auth-method	1588
onu-auto-provisioning	1495
onu-enable	1590
onu-force-status-update	1592
onu-reset	1594

P

ping.....	163
ping6.....	168
pppoe.....	1700
prefix-list.....	441
profile gpon bandwidth-profile.....	1528
profile gpon gem-traffic-profile.....	1533
profile gpon line-profile.....	1502
profile gpon media-profile.....	1536
profile gpon onu-profile.....	1540
profile gpon rg-profile.....	1543
profile gpon service-profile.....	1555
profile gpon sip-agent-profile.....	1557
profile gpon snmp-profile.....	1560
profile gpon tr069-acis-profile.....	1566

Q

qos interface scheduler-profile.....	1249
qos policer hierarchical.....	1229
qos policer instance.....	1232
qos policer profile.....	1237
qos scheduler-profile.....	1252

R

rate-limit.....	1256
reboot.....	1666
reboot-forced.....	1668
remote-devices.....	1461
request firmware onu add.....	125
request firmware onu cancel.....	1596
request firmware onu install.....	1598
request firmware onu remove.....	127
resolved.....	81
rg-one-shot-prov.....	1509
rg-reprovision.....	1602
rollback configuration.....	84
rollback selective.....	88
router bgp.....	494

router bgp address-family	496	499
router bgp administrative-status		502
router bgp as-size		504
router bgp bgp cluster-id		506
router bgp bgp default-local-preference		508
router bgp neighbor		510
router bgp neighbor address-family		512
router bgp neighbor address-family prefix-list		515
router bgp neighbor address-family vpn		518
router bgp neighbor administrative-status		521
router bgp neighbor description		524
router bgp neighbor ebgp-multihop		527
router bgp neighbor next-hop-self		530
router bgp neighbor password		533
router bgp neighbor remote-as		536
router bgp neighbor route-policy		539
router bgp neighbor route-reflector		542
router bgp neighbor timers hold-time		545
router bgp neighbor timers keepalive		548
router bgp neighbor update-source-address		551
router bgp network address-family ipv4		554
router bgp network address-family ipv6		557
router bgp prefix-list		560
router bgp redistribute		565
router bgp redistribute administrative-status		568
router bgp redistribute match-address address-family ipv4		571
router bgp redistribute match-address address-family ipv6		574
router bgp route-map		577
router bgp route-map match-community		583
router bgp route-map set-community		586
router bgp route-map set-community-action		589
router bgp route-policy		592
router bgp router-id		595
router bgp vrf		597
router bgp vrf address-family		599
router bgp vrf address-family ipv4 ipv6 unicast redistribute		608
router bgp vrf address-family ipv4 ipv6 unicast redistribute administrative-status		612
router bgp vrf address-family network		602
router bgp vrf address-family redistribute match-address		605

router bgp vrf neighbor	615
router bgp vrf neighbor address-family	618
router bgp vrf neighbor address-family allow-as-in	621
router bgp vrf neighbor address-family as-override	624
router bgp vrf neighbor address-family prefix-list	627
router bgp vrf neighbor administrative-status	630
router bgp vrf neighbor next-hop-self	633
router bgp vrf neighbor password	636
router bgp vrf neighbor remote-as	639
router bgp vrf neighbor update-source-address	642
router bgp vrf router-id	645
router ospf	681
router ospf administrative-status	684
router ospf area	686
router ospf area administrative-status	688
router ospf area interface	691
router ospf area interface administrative-status	694
router ospf area interface authentication	697
router ospf area interface authentication-key	700
router ospf area interface bfd session-type	703
router ospf area interface cost	706
router ospf area interface dead-interval	709
router ospf area interface hello-interval	712
router ospf area interface mtu-ignore	715
router ospf area interface network-type	718
router ospf area interface passive	721
router ospf area interface router-priority	724
router ospf area nssa	727
router ospf area range	730
router ospf area stub	733
router ospf export-prefix-list	736
router ospf import-prefix-list	738
router ospf maximum paths	741
router ospf mpls-te router-id	743
router ospf redistribute	745
router ospf router-id	748
router ospf timers lsa-arrival	750
router ospf timers throttle lsa-originate	753
router ospf timers throttle spf	756

router ospfv3	785
router ospfv3 administrative-status	787
router ospfv3 area	789
router ospfv3 area administrative-status	791
router ospfv3 area interface	793
router ospfv3 area interface administrative-status	795
router ospfv3 area interface cost	798
router ospfv3 area interface dead-interval	801
router ospfv3 area interface hello-interval	804
router ospfv3 area interface mtu-ignore	807
router ospfv3 area interface network-type	810
router ospfv3 area interface passive	813
router ospfv3 area range	816
router ospfv3 maximum paths	819
router ospfv3 redistribute	821
router ospfv3 router-id	824
router ospfv3 timers lsa-arrival	826
router ospfv3 timers throttle lsa-originate	828
router ospfv3 timers throttle spf	831
router pbr	881
router static address-family ipv4	445
router static address-family ipv6	449
router vrrp	849
router vrrp interface	851
router vrrp interface address-family	853
router vrrp interface address-family vr-id	855
router vrrp interface address-family vr-id address	857
router vrrp interface address-family vr-id administrative-status	860
router vrrp interface address-family vr-id advertisement-interval	863
router vrrp interface address-family vr-id authentication	866
router vrrp interface address-family vr-id preempt	869
router vrrp interface address-family vr-id priority	872
router vrrp interface address-family vr-id track	875
router vrrp interface address-family vr-id version	878

S

save	92
screen-resize	27

service vlan block.....	1511
service vlan type.....	1513
service-port.....	1515
session.....	29
set system clock.....	1469
sflow agent ipv4.....	1451
sflow collector.....	1453
sflow interface.....	1456
show.....	96
show acl-resources.....	1282
show alarm.....	172
show allowed-ip.....	1319
show assistant-task.....	1635
show banner login.....	99
show bfd session.....	485
show configuration.....	101
show configuration commit changes.....	105
show configuration commit list.....	110
show configuration rollback changes.....	113
show configuration running.....	117
show core-dump.....	174
show counters.....	176
show cpu-dos-protect.....	1725
show dwdm channels.....	266
show eaps.....	402
show environment.....	1704
show erps.....	393
show firmware.....	1604
show forwarding-resources.....	1715
show interface description.....	268
show interface forty-gigabit-ethernet.....	271
show interface gigabit-ethernet.....	274
show interface gpon.....	1520
show interface gpon onu.....	1606
show interface gpon onu Ethernet.....	1613
show interface gpon onu gem.....	1618
show interface hundred-gigabit-ethernet.....	277
show interface link.....	280
show interface statistics.....	179

show interface ten-gigabit-ethernet	284
show interface transceivers	1708
show interface twenty-five-g-ethernet	287
show inventory	1670
show ip bgp	648
show ip bgp community	653
show ip bgp neighbor	656
show ip bgp prefixes	666
show ip bgp vpnv4 labels	671
show ip bgp vpnv6 labels	675
show ip fib	453
show ip host-table	457
show ip interface	300
show ip ospf	759
show ip ospf database	763
show ip ospf interface	770
show ip ospf neighbor	779
show ip rib	461
show ip route	465
show ipv6 fib	469
show ipv6 host-table	473
show ipv6 interface	304
show ipv6 ospf	834
show ipv6 ospf database	837
show ipv6 ospf neighbor	846
show ipv6 rib	477
show ipv6 route	481
show license	241
show link-aggregation	368
show link-flap	426
show lldp local	1385
show lldp neighbors	1390
show log	1676
show loopback detection	420
show mac-address-table	330
show mpls forwarding-table	899
show mpls l2vpn counters	1056
show mpls l2vpn hardware	1060
show mpls l2vpn vpls-group	1066

show mpls l2vpn vpws-group	1073
show mpls l3vpn	1080
show mpls ldp database	1156
show mpls ldp neighbor	1159
show mpls ldp parameters	1163
show mpls traffic-eng tunnel-te brief	905
show mpls traffic-eng tunnel-te id name	912
show multicast igmp snooping	1209
show multicast igmp snooping groups	1213
show multicast igmp snooping mrouter	1218
show multicast igmp snooping port	1221
show multicast igmp snooping statistics	1226
show oam cfm delay-measurement	1359
show oam cfm local	1363
show oam cfm remote	1368
show oam efm	1377
show oam twamp reflector connection	1395
show oam twamp reflector test-session	1399
show oam twamp sender connection	1403
show platform	1680
show pppoe intermediate-agent sessions interface gpon ChassiSlotPort	1702
show qos policer	1242
show qos policer resources	1246
show remote-devices	1463
show router pbr	886
show router vrrp	307
show running-config	120
show snmp	1471
show spanning-tree	373
show ssh-server	1639
show system clock	1474
show system cpu	183
show system memory	187
show system reboot	1683
show system uptime	190
show tech-support	192
show vlan	339
snmp agent	210
snmp community	216

snmp notify	219
snmp system	221
snmp target	223
snmp traps	228
snmp usm	231
snmp vacm	234
sntp	1476
spanning-tree	377
spanning-tree mst	383
ssh	1641
ssh-server.....	1644 1647
switchport acceptable-frame-types	342
switchport interface storm-control	1259
switchport native-vlan	344
switchport pcsp	347
switchport qinq	350
switchport tpid	353

T

tcpdump	196
telnet	1650
telnet-server	1652
top	123
traceroute	204
traceroute6	207
traffic-loop	1372
twamp reflector	1409
twamp reflector administrative-status	1411
twamp reflector client-address	1413
twamp reflector client-network	1415
twamp reflector port	1417
twamp reflector vrf	1419
twamp sender administrative-status	1421
twamp sender connection.....	1423 1426
twamp sender connection number-of-packets	1428
twamp sender connection server-port	1430
twamp sender connection test-session	1432
twamp sender connection test-session dscp	1435

twamp sender connection test-session max-port	1438
twamp sender connection test-session min-port.....	1441
twamp sender connection test-session packet-size.....	1444
twamp sender connection vrf.....	1447 1449

U

user	32
------------	----

V

vlan-mapping	355 1569
vrf.....	889
vrf address-family ipv4 unicast.....	892
vrf rd	894
vrf route-target.....	896

W

who	1310 1655
-----------	-----------